GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Introduction

Nigel Parker, Calum Burnett,
Jason Rix and Benjamin Scrace
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

Regulators and enforcement authorities across the globe are continuing their focus on the activities of corporations and their employees. Investigations are frequently cross-border and involve accessing information held in multiple jurisdictions. Successfully managing the risks arising from these investigations requires expertise across a number of areas. Data privacy and protection considerations present growing challenges to clients in their planning and conduct of internal and government investigations as individuals and regulators become increasingly alert to how data is collected and used, more data is generated and stored electronically, and regulators and enforcement authorities make expansive requests for that information, often without regard for national boundaries.

Every jurisdiction has its own laws and regulations concerning the collection and review of data and what information may be transferred out of the country. In the EU, the data privacy landscape changed with the introduction of the General Data Protection Regulation (GDPR) in 2018. More recently, the California Consumer Privacy Act came into effect in 2020. Data privacy issues may therefore arise under multiple applicable laws on an investigation, and at different phases during its course.

Where an investigation requires the extraction of significant amounts of information from multiple jurisdictions by corporations and/or third parties (eg, forensic accounts or consultants), it is likely that a large proportion of that information will include personal data (also known as personally identifiable information) of a client's employees and clients (or individuals connected with those clients, such as their employees). The corporation may wish to transfer that data between countries for the purposes of conducting review and analysis, or in order to meet requests or demands from authorities, or voluntarily to provide information to them to be cooperative. Any such actions require careful analysis. The conflict of laws presented by requests or demands for documents and other information by overseas authorities, in particular, is a significant problem for corporations. Data privacy laws, bank confidentiality and "blocking statutes" in some jurisdictions, such as France, often put corporations in a position where they are having to weigh competing risks that arise from conflicting legal or regulatory requirements.

There are, however, steps that can be taken to reduce those risks in a given situation. For example, in order to limit data privacy or confidentiality issues, it may be possible to negotiate the scope of the request, pre-review the information disclosed, redact documents or take other steps to mitigate the risk. Each request should be considered on a case-by-case basis to determine whether, and to what extent, a company is able to comply, and to determine whether any particular steps can be taken lawfully to undertake the disclosure and transfer of the personal data.

Data privacy should therefore be a key consideration for clients when planning, structuring and carrying out an investigation. The data privacy, protection and litigation teams at Allen & Overy have produced these guides to assist with identifying some of the issues that will need to be considered from a data protection perspective when managing complex domestic or cross-border investigations. However, it should be noted that other laws, regulations, contractual requirements or voluntary codes may also restrict the disclosure of certain types of data. Further information on the restrictions and requirements affecting transfers of data from one jurisdiction to another can also be found on aosphere's Rulefinder Cross Border Data Transfer (www.aosphere.com/aos/cbdt).

Nigel Parker

Allen & Overy LLP

Nigel specialises in data protection and privacy, commercial contracts and intellectual property law. He works across a wide variety of business sectors, including financial services, technology, media and life sciences.

Nigel regularly advises on multi-jurisdictional data protection matters. He advises companies across various sectors on strategic issues relating to personal data management and new technologies such as privacy impact assessment and privacy by design, international data transfers (including BCRs) as well as crisis management (eg data breaches) and data protection authority investigations.

Nigel is recognised in *Chambers* and *The Legal 500*, and was named one of the "Top 40 under 40" data lawyers by Global Data Review. *The Legal 500* cites Nigel as an expert in the field of data protection, privacy and cybersecurity, describing him as "a technical expert while also being extremely strategic and forward thinking" (*The Legal 500*, 2020). He is the contributing editor of the ICLG cross-border guide on cybersecurity and an editor of A&O's Digital Hub blog.

Calum Burnett

Allen & Overy LLP

Calum Burnett is head of the UK Litigation & Investigations Group. He is experienced in acting for financial institutions, corporations and individuals in domestic and international criminal and regulatory investigations and in conducting internal investigations. He also advises financial institutions on litigation and risk management issues. Calum has previously spent time on secondment with the fraud division of the Crown Prosecution Service and the enforcement division of the former Financial Services Authority.

Calum has, for a number of years, been recognised by the major UK directories for all areas of his practice. *Chambers UK* 2018 says that he is "forward thinking, technically flawless and clear-sighted" and *Chambers UK* 2019 reports that "he is a go-to on contentious regulatory matters – he has a huge wealth of experience, is very impressive intellectually and has good commercial sense".

Benjamin Scrace
Allen & Overy LLP

Ben has a broad commercial practice, including data protection, commercial contracts and non-contentious intellectual property. He has experience of multi-jurisdictional data protection matters and advises on the IP, IT and data protection considerations in corporate transactions. Ben previously spent time on secondment with the digital and data privacy legal team of a multinational electronics and technology company.

Jason Rix
Allen & Overy LLP

Jason has a varied commercial litigation practice, which includes data protection, cybersecurity, privilege, sanctions, state immunity, conflicts of laws, EU law and English contract law. A while back, Jason was seconded to BT for nine months where he helped negotiate key supplier contracts for BT's £10 billion 21st Century Network. This experience still serves as a vivid reminder of what it is like in-house. He is a member of the CCBE European Private Law Committee and sat on the FMLC working group looking at Distributed Ledger Technology and Governing Law. In 2016, he set up Compact Contract (www.aocompactcontract.com) a blog focused on English contract law.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

One Bishops Square
London
E1 6AD
United Kingdom
Tel: +44 20 3088 0000
Fax: +44 20 3088 0088

www.allenovery.com

Nigel Parker
nigel.parker@allenovery.com

Calum Burnett
calum.burnett@allenovery.com

Benjamin Scrace
benjamin.scrace@allenandovery.com

Jason Rix
jason.rix@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Belgium

Peter Van Dyck and Claire Caillol
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

The Belgian Data Protection Act (DPA) applies to (i) the processing of personal data in the context of the activities of an establishment of a controller or processor in Belgium, whether or not the processing takes place in Belgium; and (ii) the processing of personal data that is carried out in the context of the activities of an establishment of a controller or processor in a country or territory that is not a member state (whether or not the processing takes place in such a country or territory) where: (i) the personal data relates to a data subject who is in Belgium when the processing takes place; and (ii) the processing activities are related to the offering of goods or services to data subjects in Belgium, whether or not for payment, or the monitoring of data subjects' behaviour in Belgium.

The Belgian Data Protection Authority is the regulator responsible for enforcing the GDPR and the DPA. The functioning and powers of the Belgian Data Protection Authority are set out in the law of 3 December 2017 on the creation of the Data Protection Authority.

It should be noted that the answers to the following questions take the provisions of the DPA into account and that mention is made to the DPA only to the extent that its provisions differ from those of the GDPR.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Anti-money laundering

Under the Belgian Anti-Money Laundering Act of 18 September 2017 (AML Act), it is prohibited to disclose to clients and third parties the fact that information has been reported to the Belgian Financial Intelligence Unit (the CTIF-CFI) or that an analysis or investigation is being or may be carried out regarding suspicions of money laundering or terrorism financing.

As an exception, it is permitted to share such information and data with supervisory authorities or for law enforcement purposes. This information and data can further be shared, subject to certain conditions, between credit or financial institutions belonging to the same group, or between legal professionals, accountants, auditors and tax advisers belonging to the same structure or acting for the same customer and transaction, with a view to preventing money laundering or terrorism financing.

The AML Act also indicates that the processing of data under this Act is subject to compliance with the relevant data protection laws.

Bank secrecy and bank confidentiality

There are no specific statutory bank secrecy or confidentiality obligations for banks and other financial institutions in Belgium. Case law is scarce on this matter. The Belgian Supreme Court has decided that the criminal law provisions on professional secrecy in the Belgian Criminal Code do not apply to bankers (Cour de Cassation, 25 October 1978). In 2012, Febelfin, the Belgian bankers' association, published a Code of conduct setting out principles for good banking relationships with retail customers. Pursuant to this Code, banks operating in Belgium that are members of Febelfin commit to comply with the principles of secrecy, confidentiality and data protection in relation to retail clients. While adoption of this Code of conduct is voluntary, once adopted, a bank is expected to follow the Code and a breach thereof could give rise to civil action.

In the absence of a specific statutory obligation, the scope of the confidentiality principle is not entirely clear. The comments below are therefore necessarily a reasoned analysis. They are also high-level and may not reflect all the nuances or specifics of applicable Belgian rules.

Banking confidentiality is typically seen as a consequence implied into the contractual relationship between the bank and the client. This stems from articles 1135 and 1160 of the Belgian Civil Code (which are not specific to financial institutions). Article 1135 of the Belgian Civil Code provides that "contractual parties are not only bound by what they explicitly stipulate in their agreement, but also by the consequences that are implied by customs/market practice". Article 1160 of the Belgian Civil Code provides that "a contract must be completed by the usual provisions, even if these are not expressly included in the contract." Accordingly, a bank may not in principle disclose to any third party any information about a client gained in the exercise of its professional activity, regardless of whether the client is an individual or a legal person and regardless of whether any confidentiality undertaking is provided for in the contractual documentation. However, this is without prejudice to the obligations that banks and other financial institutions may have to provide specific information about their clients to comply with their legal and regulatory obligations. For example, the law of 8 July 2018 on the organisation of a central contact point for accounts and financial contracts (and its implementing royal decrees) imposes important reporting obligations for financial institutions carrying out business in Belgium. The Central Contact Point (the CCP) is a central register, held by the National Bank of Belgium, to which financial institutions must report certain information on the identity of their clients and the financial products, contracts or transactions.

Tax

Under article 318 of the Belgian Income Tax Code of 1992 (the BITC/92), the tax authorities are not authorised to gather information in the accounts, books and documents of banks with a view to taxing their clients.

Exceptions to this provision include specific provisions in double tax treaties, the presence of indications of fraud, the automatic exchange of information in the framework of Directive 2011/16/EU and if the request is made by a foreign state.

According to a certain doctrine, however, information gathered by the tax authorities in breach of the aforementioned article 318 of the BITC/92 can nevertheless be withheld if certain conditions are met. This doctrine violates case law by the European Court of Justice to the extent that the breach of article 318 of the BITC/92 at the same time implies a breach of the taxpayer's fundamental rights.

According to article 334 of the BITC/92, if a person is bound by the obligation of professional secrecy, the tax authorities are only authorised to request and gather information in relation to third persons upon approval of the relevant disciplinary authorities.

Privacy of employee communications

Privacy of employee communications is regulated by both the GDPR and Collective Bargaining Agreement No. 81 (CBA 81), which is further discussed in question 15.

Professional secrecy

Certain professions such as doctors, pharmacists or lawyers are bound by the obligation to respect professional secrecy set out in article-458 bis of the Criminal Code. This means that they cannot disclose information which they have acquired in the context of their employment unless specific derogations applies (eg, they have to testify or they are under a legal obligation to disclose information).

A breach of professional secrecy may give rise to (i) a prison sentence of one to three years, (ii) a fine up to €8,000 or (iii) both a prison sentence and a fine. In addition, specific deontological sanctions are also likely to apply.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines personal data as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data could re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural persons. It does not also cover legal persons or deceased natural persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data are obtained (unless an exemption applies). In all circumstances, this must include (articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing, and the right to withdraw any consent at any time, where consent is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data;
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16); and
- any further information necessary to make that particular processing of data fair and transparent.

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data have not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law.

Under article 10 of the DPA, personal data relating to criminal convictions and offences or related security measures may also be processed:

- by natural persons, or public or private bodies, where necessary in the context of litigation;
- by lawyers and legal advisers where necessary for the defence of legal claims;
- where the processing is necessary for reasons of significant public interest for the performance of tasks of general interest entrusted by or under a Belgian law, decree or order or European Union law; or
- where the processing is necessary for scientific research, historical or statistical information or for archival purposes.

The controller or the processor (if applicable) is required to create and maintain a list of the categories of people who have access to the data, as well as a detailed description of their functions in respect of the processing. The controller must ensure that the people with access to personal data relating to criminal convictions and offences or related security measures are bound by a legal or statutory obligation or by an equivalent contractual provision, to maintain the confidentiality of the data concerned.

Under the other data protection principles in the GDPR, controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");
- Principle 5: personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

While there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor

is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is, therefore, not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate “explicit” consent (eg, a wet ink signature or a tick box that expressly uses the word “consent”).

Consent can be obtained through a website or other electronic means.

Note that article 10 of the DPA requires consent to the processing of data relating to criminal offences to be given in writing by the data subject.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right that it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or if the processing is necessary within legal proceedings.

A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Competent authorities may be authorised to limit data subjects' rights when processing personal data for the purposes of criminal law investigation, prevention and enforcement purposes if the processing is described under articles 11 to 17 of the DPA. The requirements apply to, among others, the police, judicial authorities, the Financial Intelligence Unit, the Passenger Information Unit, customs authorities, intelligence and security services, armed forces and the coordination unit for threat assessment (OCAM).

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

In line with article 29 Working Party's Opinion 01/2010 on the concepts of "controller" and "processor", law firms are generally characterised as independent controllers when processing data in the course of legally representing their clients.

It is, however, less clear whether legal process outsourcing firms would be considered data controllers or data processors. Of course, if their work is done by lawyers, the legal process outsourcing firm must be considered a data controller for the processing involved in that work.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Requirements for financial institutions

Financial institutions in Belgium must also comply with, among other the guidelines on material outsourcing established by the European Banking Authority (EBA). The EBA's guidelines (which will apply from 30 September 2019) set out a series of

recommendations that providers of financial services must adhere to in respect of any outsourcing to the cloud, including in respect of the security of data, where geographically data is located and processed and the importance of contingency planning.

Requirements relating to monitoring of employee communications

Requirements relating to the monitoring of email correspondence differ depending on whether the correspondence concerns employee personal data or not.

The GDPR applies to all personal data, including private emails and professional emails such as those sent between an employer and employee. It also applies to the personal data of employees and other natural persons. Under Belgian law, the privacy of employee communications is regulated by both the GDPR and Collective Bargaining Agreement No. 81 (CBA 81). Although the scope of CBA 81 is not clearly defined, the general view is that CBA 81 applies to electronic communications that contain private employee information, but not emails relating solely to professional information.

CBA 81 and the GDPR provide that the data in employees' electronic communications can only be processed under certain conditions if they contain personal or private information. The following conditions apply:

- Monitoring of employees' electronic communications is only permitted for one of four legitimate purposes described by CBA 81.
- Monitoring should be proportionate to its objective.
- Certain information on the monitoring of employee communications must be provided to the individual employees and their representatives, ie, the employee representatives on the competent Works Council, health and safety committee or trade union delegation.
- The relevant employee representatives must be consulted regularly in view of the on-going evaluation of any monitoring system.
- Electronic online communications may only be individualised (ie individually identified) following a specific procedure provided under CBA 81. When electronic online communications data is individualised and irregularities are found with this data, the employer must organise a meeting with the employee.

CBA 81 does not apply to electronic communication data which solely relate to professional information. However, in that case the GDPR still applies and employers must comply with the requirements set out in the GDPR (see question 7).

Finally, as private electronic communication cannot always be readily distinguished from professional emails, the employer could also consider applying the principles of CBA 81 to the monitoring of professional emails of its employees.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission, must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;

- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

Article 48 of the GDPR provides that, without prejudice to other grounds for international transfers, a decision from third country authorities, courts or tribunals does not in itself justify the transfer of personal data to a non-EEA country. This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: "In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement."

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, amongst others:

- Consider if there is a legal obligation to respond to the request and, if so, to what extent.
- Seek further information in writing from the requesting regulator to evaluate the purpose of the request.
- If possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation.
- In accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose.
- Consider whether it is practicable to obtain data subject consent and/or give a further privacy notice.
- Put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor).
- Consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

The Data Protection Authority is responsible for receiving complaints on and investigating compliance with the DPA. Other than imposing the above-mentioned administrative fines, the actions that can be taken by the Data Protection Authority include:

- imposing a temporary or final restriction (including a prohibition) to the processing;
- requesting the rectification, or erasure of personal data; and
- involving the public prosecutor.

In accordance with Belgian criminal law (see article 5 of the Belgian Criminal Code), both legal and natural persons can incur criminal sanctions for data protection breaches (alternatively or cumulatively depending on the scenario). This means for example, that directors and officers may incur criminal sanctions (including fines) for non-compliance with data protection laws.

Criminal sanctions flowing from breaches of the DPA are pursued by the public prosecutor and the courts. The possible criminal sanctions for breaches of the DPA include fines up to €240,000 and the publication of the judgment.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside of the EEA), including any transfer to a regulator or law enforcement authority; and
- maintain a record of processing and respond to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening data controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679)
Belgian Data Protection Act (French version)
Belgian Data Protection Act (Dutch version)

Law on the creation of the Belgian Data Protection Authority:

French version
https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2017120311&table_name=loi

Dutch version
https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2017120311&table_name=wet

Collective Bargaining Agreement 81
French version
http://www.cnt-nar.be/CCT-COORD/cct-081.pdf

Dutch version
http://www.cnt-nar.be/CAO-COORD/cao-081.pdf

Peter Van Dyck
Allen & Overy LLP

Peter is a partner within the IP/IT department of Allen & Overy (Belgium) LLP.

Peter focuses on outsourcing, IT law, copyright, media law and data protection issues. He advises clients both in litigious and non-litigious matters, and regularly assists clients on the negotiation and drafting of agreements and transactions.

In addition to his client-related work, Peter lectures on intellectual property law and data protection law at the KULeuven since 2006. Furthermore, Peter Van Dyck regularly holds internal and external client seminars about his topics of expertise and is frequently contacted by the press on these topics.

Claire Caillol
Allen & Overy LLP

Claire is a junior associate within the IP/IT department of Allen & Overy (Belgium) LLP where she focuses on data protection, IT law and intellectual property issues.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy (Belgium) LLP
Uitbreidingstraat nr 72/b3
Antwerp
B-2600
Belgium
Tel: +32 3 287 7222

www.allenovery.com

Peter Van Dyck
peter.vandyck@allenovery.com

Claire Caillol
claire.caillol@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

China

Jane Jiang, Tiantian Wang and Jason Song
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

There is no specific data protection legislation in the People's Republic of China (the PRC or China, for the purpose of this article, excluding Hong Kong, Taiwan and Macau). There are a number of different laws that govern different aspects of the collection and use of personal information:

According to the PRC Civil Code issued by the National People's Congress on 28 May 2020, which will take effect on 1 January 2021 and the General Principle Rules of Civil Law[1] issued by the National People's Congress on 15 March 2017 and took effect on 1 October 2017, PRC laws protect the personal information of natural persons. Any entity or individual that needs to obtain personal information of others should do so in accordance with PRC laws and ensure its security. They should also be prohibited from illegally collecting, using, processing or transmitting personal information of others, or illegally trading, providing or disclosing personal information of others.

Under the PRC Tort Liability Law[2] issued by the Standing Committee of the National People's Congress (the SCNPC) in December 2009, "civil rights and interests" are broadly defined to include the right to one's name, reputation, honour, image and privacy. It is likely that a customer's personal information would be interpreted as concerning such "civil rights", which are to be protected by the law.

According to the PRC Law on Protection of Consumer Rights and Interests (as amended in October 2013, the Consumer Protection Law), business operators, during the course of collecting and using customers' personal information, are obligated to keep such information strictly confidential, and shall not disclose it to third parties.

According to the Decision on Protecting Internet Information issued by the SCNPC on 28 December 2012 (the Decision), electronic information that can identify individuals or involve individual privacies (Electronic Personal Information) is protected by law. No individual or entity may steal, obtain, sell or disclose such information in an illegal way. Network service providers and other entities should not collect or use electronic personal information in breach of relevant laws, regulations or consents by the information owners. Network service providers, other entities and their staff members should keep electronic personal information collected during the course of business strictly confidential, and should not disclose, modify, destroy or sell the information or illegally provide it to third parties.

The TMT and Internet Personal Information Protection Rules issued by the Ministry of Industry and Information Technology (MIIT) on 16 July 2013 (the TMT and Internet Information Protection Rules), which implement the Decision, provide, among others, that TMT business operators and internet information service providers should not collect or use personal information of users without the latter's consents. No personal information may be collected beyond the scope necessary for the provision of services, or used for purposes irrelevant to the services. No personal information may be collected or used by cheating, disguising or coercing the users, or in a way in breach of laws, regulations or agreements with users. The rule has also repeated the restrictions in the Decision described in the above paragraph on storing, using and disclosing personal information of users by TMT business operators and internet information services providers.

The Provisions on the Cyber Protection of Children's Personal Information issued by the Cyberspace Administration of China on 22 August 2019 and took effect on 1 October 2019 provide that, before collecting, using, transmitting or disclosing any personal information of a child below the age of 14, a network operator shall inform the child's guardian of such collection, use, transmission or disclosure in a conspicuous and clear manner, and shall obtain the consent of the child's guardian.

Apart from the above, the PRC Cyber Security Law issued by the SCNPC on 7 November 2016 provides two forms of data protections, one addressed to data generated and collected by network operators (defined in the next paragraph), and the other addressed to data generated and collected by CIIs (defined below).

The network operators referred to above are broadly defined as including network owners or managers and network service providers. The term "network" means systems built on computers or other information terminals and relevant facilities to collect, store, transmit, exchange or process information according to certain rules and procedures.

The PRC Cyber Security Law provides that network operators should keep user information collected strictly confidential and set up comprehensive and robust information protection systems. No personal information may be used, processed or destroyed in breach of the agreements between network operators and users. All personal information should be processed and stored according to the relevant laws, regulations and agreements with users. No personal information may be disclosed without the user's consent, unless such information has been processed to effect that no specific individual can be identified and the original information may no longer be recovered.

Further, personal information and important data generated and collected within the territory of China by operators of critical information infrastructures (CIIs) during the course of their operations should be stored within China. If such data needs to be transferred overseas due to business necessity, such transfers should be subject to security assessments according to the relevant regulations (the Data Cross-Border Transfer Rules) jointly issued by the Cyberspace Administration of China (the CAC) and other relevant authorities. The CIIs include, among others: public communications and information service systems; systems of energy, transportation, hydro (water) systems, finance, public service sectors and areas; electronic government service

platforms; and other significant industries and areas. The category also includes important information infrastructure facilities that, if destroyed, disabled or subject to data leakage, may cause significant damage to national security, national economy, people's livelihoods or public interest.

As of the date of this chapter, various consultation drafts of rules implementing the PRC Cyber Security Law have been circulated for comments but the market is still waiting for the release of the official implementation rules to clarify those equivocal requirements in the PRC Cyber Security Law such as the requirement on cross-border data transfer assessment. That said, since the PRC Cyber Security Law took effect in 2017, various national standards have been released to guide the market the "best practice" on data protection that could be expected by the regulators. For example, on 6 March 2020, the recommended national standard named Information Security Technology - Personal Information Security Specification (GB/T 35273-2020, the Personal Information Security Specification) was released, which set out the principles and security requirements on the collection, storage, processing, share, transfer and disclosure of personal data. On 10 April 2019, the Ministry of Public Security issued the Guidelines for Internet Personal Information Security Protection (the Personal Information Security Guideline), which sets out the guidelines for reference by Internet service providers on collection, storage, processing, deletion and disclosure of personal data. On 13 February 2020, the People's Bank of China (the PBOC) issued the Personal Financial Information Protection Technical Specification, which sets out the guidelines for reference by financial institutions on collection, transmission, storage and use of individual financial information (IFI). These standards, although not mandatory, partially fills the gap while those official implementation rules to the PRC Cyber Security Law are still in draft form. Compliance with the principles set out in those guidelines and standards may be useful in evidencing an entity's compliance with the relevant requirements in the PRC Cyber Security Law.

[1] According to the PRC Civil Code, the General Principle Rules of Civil Law will be abolished on 1 January 2021 when the PRC Civil Code becomes effective.

[2] According to the PRC Civil Code, the PRC Tort Liability Law will be abolished on 1 January 2021 when the PRC Civil Code becomes effective. However, "civil rights and interests" are protected by both and enjoy the same definition.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Banking secrecy

A number of different banking secrecy laws contain obligations regarding the processing and transfer of certain types of data.

Commercial Bank Law

According to the PRC Commercial Bank Law as amended on 29 August 2015 (the Commercial Bank Law), a commercial bank has a general obligation to keep its depositors' information confidential and will be liable for any damages incurred by a depositor if the bank violates its duty of confidentiality. In China, it is typical for people to conduct cross-border money transfer through their deposit account banks. When a bank provides money transfer services to its customer, it is likely that information of the customer may be interpreted as "depositor's information".

PBOC circular on IFI

The PBOC published the Circular of PBOC on the Protection of Personal Financial Information by Banking Financial Institutions (the IFI Circular) on 1 May 2011. The PBOC Shanghai branch further issued the Circular on Issues Relating to the Protection of Personal Financial Information by Banking Financial Institutions (the Shanghai Circular) on 18 May 2011. The protections under the IFI Circular and the Shanghai Circular are administrative law in nature and, therefore, cannot be waived by bank clients by consent.

Prohibition on cross-border transfer of IFI

The IFI Circular prohibits PRC banks (including PRC subsidiaries and branches of foreign banks) from disclosing IFI to an offshore entity. IFI broadly includes personal information on identity, property, bank account details, credit and financial transactions and so on, obtained by a bank during the course of its business or while accessing the PBOC's system.

The Shanghai Circular clarifies that IFI also includes any information regarding any individual (such as the legal representative) of a corporate client of the bank.

Exceptions

Certain exceptions to the above prohibitions are available under the Shanghai Circular:

A Disclosure of IFI by a bank to its offshore parent or subsidiary is allowed if (i) such disclosure is necessary for the client or individual to conduct the relevant transactions and (ii) written authorisation is obtained from the individual. The PRC bank making the disclosure must ensure that its offshore parent or subsidiary keeps the IFI received confidential.

B With respect to a branch of a foreign bank using the system of its offshore headquarter or affiliate to store, process or analyse the IFI of the bank's clients outside China, the Shanghai Circular requires the following conditions to be satisfied: (1i) written authorisation is obtained from such clients; and (ii) the offshore headquarters or affiliate shall have adopted relevant security measures to safeguard the relevant IFI and the headquarters (in the name of the bank as a legal person entity) shall bear the liabilities.

Other than the above, we are not aware of any statutory exemptions that allow PRC banks to transfer IFI offshore (whether such transfer is in response to the request of a foreign authority). In a contentious context, group-wide internal investigations and reviews relating to foreign sanctions may not be considered "necessary for the client/individual to conduct the relevant transaction", meaning that exception (A) above would not apply in this scenario. This view is further supported by the ICJAL discussed below.

Judicial Assistance on Criminal Matters

On 26 October 2018, the National People's Congress of the PRC promulgated the International Criminal Judicial Assistance Law (the ICJAL). The ICJAL applies only to criminal matters, not to civil or administrative matters.

The ICJAL sets out the relevant requirements on the processes of obtaining assistance and evidence in criminal matters on a cross-border basis. More specifically, the ICJAL applies in the case where entities and individuals outside of China seek assistances from those in China, or China-based entities and individuals seek assistances from those in other countries, including service of documents, evidence collection, witness testimony, freezing, seizure and confiscation of assets, and transfer of convicted persons.

The ICJAL requires that all such assistance in criminal proceedings be routed through a "competent authority" of the assisting state pursuant to the provisions of the ICJAL[1], or, if there is already in place a judicial assistance treaty on criminal proceedings between China and the relevant state (eg, the China-US Agreement on Mutual Assistance in Criminal Matters signed between China and the United States in 2000), pursuant to the requirements under such treaty.

The purpose of the ICJAL is partially to serve as a gap-filler for countries that China does not have a judicial assistance treaty on criminal proceedings. In addition, according to the official report of the drafting commission of ICJAL and the press conference at which the ICJAL was made public, one of the main purposes of the ICJAL is to "effectively restrict foreign countries from exercising 'long-arm jurisdiction', particularly where foreign criminal enforcement authorities request information directly from China-based organisations and institutions".

The ICJAL applies to individuals and entities located in China, and activities of evidence production taking place in China.

Article 4 of the ICJAL provides among others that unless approved by relevant competent authorities, no foreign entities, organisations or individual may carry out any activities for the purpose of foreign criminal proceedings within the territory of China, and no entities, organisations or individuals located in China may provide evidential materials or assistance to any person in foreign countries.

This seems to suggest that a Chinese entity is prohibited from providing evidence, testimony or other forms of assistance in criminal proceedings initiated outside China without approval of Chinese competent authorities. The wording is sufficiently broad to include the situation where a China-based subsidiary of a multinational company provides any of such assistance to its offshore parent, including but not limited to an internal investigation scenario, if such assistance is related to any foreign criminal proceedings.

The ICJAL does not contain penalties for violations. However practically, it is possible that the PRC regulators may frame the violation under the existing regimes including such as data privacy or state secrecy and therefore impose the relevant penalties thereunder.

As the ICJAL is still at an infant stage, there is no precedent yet to provide more insight on how the PRC regulators will enforce against any violation. It is also not clear for example whether the ICJAL may imply a duty to inquire if a PRC based entity or individual provides assistance to a foreign investigation without knowing that the investigation involves or may involve criminal aspect.

State secrecy

The restrictions contained in the PRC laws and regulations on state secrecy would be triggered to the extent that the relevant personal information constitutes state secrets.

Under the PRC Law on Protection of State Secrets (the State Secrets Law) as amended on 29 April 2010, the term "state secret" is broadly defined to mean matters which are related to national security and interest, determined in accordance with legal procedures, and may only be disclosed to limited persons within a certain period of time.

The State Secrets Law provides a list of matters and information that can be classified as state secrets. Such matters and information, if disclosed, may impact China's security and interest in key areas such as politics, economy, defence and foreign affairs.

The National Administration for the Protection of State Secrets (the NAPSS) and the relevant government agencies have the power to determine and classify state secrets related to specific areas. NAPSS and the relevant governmental agencies may authorise non-governmental agencies such as state-owned enterprises (SOEs) to determine and classify state secrets generated from, received or possessed by such enterprises.

State secrets, if so determined, can be classified as "top secret", "secret" or "confidential".

According to article 16 of the State Secrets Law, no state secrets should be disclosed to any person unless the disclosure is necessary for carrying out the relevant activity and has been approved by the Relevant Authority in charge (ie, the NAPSS or the relevant governmental agencies) (the Relevant Authorities).

According to article 30 of the State Secrets Law, if an entity needs to disclose state secrets in its communication or cooperation with foreign entities, or any foreigners engaged by the entity need to know state secrets, such entity shall apply to the Relevant Authority for approval of the proposed disclosure, and sign confidentiality agreements with the recipient of the information.

According to articles 21 and 25 of the State Secrets Law, the preparation, receipt, delivery, use and reproduction of state secrecy carriers (eg, paper, optical and magnetic media) should comply with the relevant regulations on protection of state secrets. No persons may carry or transmit any state secret carriers out of China without the approval of the Relevant Authority.

Under the Implementation Provisions of PRC Law on Protection of State Secrets issued by the State Council on 14 January 2014, an entity procuring services involving state secrets must determine the class of the confidential information in accordance with PRC laws, regulations and standards, and request the service provider to keep state secrets confidential and sign a confidentiality agreement with the service provider.

Under normal circumstances, however, state secrets are highly unlikely to be involved during the course of ordinary business. However, the risk may increase where the data subject is a Chinese government agency or SOE, especially in certain industries sensitive to Chinese national security or national interests. Such sensitive industries may include infrastructure, energy and resources (including nuclear power), transportation, iron and steel, banking, export credit, technology and major equipment manufacturing.

The restrictions under the State Secrets Law cannot be waived by consent other than the approvals of the relevant authorities described above.

Blocking statute

According to the Interim Administrative Measures on Seizures over Assets relating to Terrorism Activities issued jointly by the PBOC, the Ministry of Public Security, and the Ministry of State Security on 10 January 2014 (the PBOC 2014 Notice), where a foreign authority intends to request client identity data or transaction data from certain financial institutions or designated non-financial institutions in the PRC, for reasons of anti-terrorism investigation, the relevant institutions must advise the foreign authority to make the request through diplomatic or judicial assistance channels. The institutions concerned must not provide the data to the foreign authority unless this requirement is complied with.

[1] In the case of China, five authorities are designated as the "competent authorities" according to article 6 of the ICJAL, namely the National Supervisory Commission, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security and the Ministry of State Security.

3 What can constitute personal data for the purposes of data protection laws?

There is no single definition of personal data in the PRC. The type of information that the various legislative provisions apply to depends on the nature of the activity in question.

The General Principle Rules of Civil Law does not provide a definition of "personal information".

The Consumer Protection Law applies to information collected by a business operator in the course of providing products and/or services to a consumer. This includes their name, gender, occupation, date of birth, ID number, residence address, contact information, income and assets, health situation, expenses and such other information that may make the consumer identifiable, either individually or in combination with other information.

The PRC Cyber Security Law and the PRC Civil Code define "personal information" as information recorded in electronic or other forms that, either alone or in combination with other information, may identify an individual. Such information includes an individual's name, date of birth, ID number, address, phone number, account number, passcode, and so on.

The Decision protects Electronic Personal Information as defined above. Under the Provisions on Application of Laws in Hearing Disputes relating to Tortious Activities Damaging Rights and Interests of Individuals by Using Information Networks issued by the Supreme People's Court on 21 August 2014 (the Judicial Interpretations), personal information protected under

the Decision includes personal privacy of an individual such as genetic information, medical history, physical history, criminal record, residence address, private activities and other personal information.

The TMT and Internet Information Protection Rules apply to the information of users collected by service providers during the course of providing the relevant services. This includes information that may identify the user or the timing and location of their access to the relevant services, either alone or in combination with other information. This information would include the individual's name, date of birth, ID number, address, phone number, account number, passcode.

The IFI Circulars and the Shanghai Circular protect IFIs, as defined at question 2.

4 Does personal data protection relate only to natural persons or also legal persons?

The term "personal information" is defined to refer only to information relating to natural persons (individuals). As such, to the extent that a provision refers to personal information, such reference is addressed to information relating only to natural persons (individuals). However, whether a specific provision only covers personal information or extends to information of entities should be assessed against the exact wording of such a provision. For example, the protection of the information generated and collected by CIIs under the PRC Cyber Security Law also covers other "important data"; the protection under the Commercial Bank Law covers information of "depositors", which include corporate clients of banks; the protection under the State Secrets Law and related legislations covers both individual and entity information. It is also notable that certain personal information includes personal information of individuals relating to entities, such as the IFI protected under the IFI Circular.

5 To whom do data protection laws apply?

The Consumer Protection Law applies to "business operators" that transfer personal information. A business operator is not defined in the statute, but one view is that, in practice, the relevant companies are limited to those based onshore in the PRC. However, if any offshore business operator is deemed as carrying out business in China, it would be subject to the PRC licensing regime and may also fall within the framework of the Consumer Protection Law. This is a separate topic that we will not further address here.

The PRC Cyber Security Law applies to CII operators and network operators for the relevant purposes described in question 1. Please note that for the security assessment required by Article 37 of the PRC Cyber Security Law on cross-border transfer of personal information or important data, various draft measures have been published for comments on this issue and some have extended the security assessment requirement to cover not only CIIs but also network operators in general. It is unclear whether the official rules to be promulgated will actually expand the application of this requirement.

The Decision applies to network service providers and other businesses that collect or use individual electronic information in the course of their business.

The TMT and Internet Information Protection Rules apply to "service providers". This term is defined broadly as any telecommunication or internet information service provider approved by the regulator to provide telecommunication or internet information services and that may receive personal information from customers when providing these services.

The Commercial Bank Law and the IFI Circular apply to PRC incorporated banks or foreign bank branches set up in China.

No distinction is made in any of the above provisions between data controllers and data processors.

6 What acts or operations on personal data are regulated by data protection laws?

There is no specific definition of the acts regulated in the relevant laws. They regulate all aspects of the collection and use of personal information.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

The obligations on the person controlling the data vary depending on the circumstances and the particular law that applies as a result.

Under the PRC Civil Code, the data processor's obligations are as follows:

- unless otherwise provided by applicable PRC laws and administrative regulations, it must obtain the consent of the data subject or his or her guardian with respect to a proposed processing of personal data;
- it must make the processing rules public;
- it must expressly inform a data subject of the purposes, methods and scope of the personal information processing;
- it must not breach applicable PRC laws or administrative regulations or the terms of any agreement with the data subject;
- it must not divulge or distort the personal information collected or stored by it or illegally provide it to other persons;

- it must adopt technical measures and other necessary measures to ensure the security of the personal information collected and stored by it;
- it must adopt remedial measures in a timely manner where the information is, or may be, divulged, damaged or lost.

Under the Consumer Protection Law, the business operator's obligations are as follows:

- it must expressly inform a consumer of the purposes, methods and scope of the collection and use of their personal information;
- it must be genuinely necessary to collect or use the personal information;
- the business operator must obtain the data subject's consent and must not breach the terms of any agreement by which it obtains such consent;
- the business operator and its employees must keep the consumers' personal information strictly confidential and must not transfer it to others; and
- mitigating measures must be taken immediately where confidence is broken or the personal information is damaged or lost.

The obligations of network operators to ensure the proper processing of personal information under the PRC Cyber Security Law are substantially the same as those under the Consumer Protection Law described above.

To comply with the Decision, network service providers must:

- provide the user with information on the objective, methods and scope of the collection of their data and its use, including making collection and use rules public;
- obtain the consent of the data subject to the use and collection of the information and not breach the terms of any agreement on this subject;
- ensure that all staff strictly protect the private information of the users collected in the course of their business activities and do not divulge, distort or damage the information, or illegally provide it to other persons; and
- adopt remedial measures immediately where the information is divulged, damaged or lost.

The Judicial Interpretations supporting the Decision provide that if an information network user or service provider uses the information network to disclose personal information of an individual and this use causes damage, a claim for damages should be supported by the Chinese court, unless one of the following applies to the disclosure:

(a) The individual has given written consent and the disclosure is within the agreed scope;
(b) To promote the public interest and it is within the necessary extent;
(c) For the purposes based on public interest of academic research or statistics by schools and research institutions, consented by the individual in written form, and the way of disclosure is not sufficient to identify the specific individuals;
(d) The information self-disclosed by the individual or other personal information that has been lawfully disclosed on the internet;
(e) The personal information obtained by lawful channels; and
(f) As otherwise provided by law or administrative regulations.

If personal information referred to in item (d) or (e) above is disclosed in a way that breaches public interests or morality or if it would damage the significant interests of an individual, the court should support any request from an individual that the service provider be held liable.

To comply with the TMT and Internet Information Protection Rules, a TMT business operator or internet information service provider must generally follow the principles of legality, legitimacy and necessity. It is liable for information security, where it collects or uses personal information in the delivery of the service.

Additionally, a TMT business operator or internet information service provider must:

- establish policies in relation to the collection and use of users' personal information and publish these policies on the internet and in its business locations;
- obtain the user's prior consent to the collection and use of their personal information and inform the user of the purpose, method and scope for the collection of their information, including the consequences if the user does not provide the information;
- avoid collecting personal information that is not necessary for their services or use personal information in a way that is irrelevant to their services;
- avoid collecting personal information by disguise, cheating or coercion, or in a way in that breaches laws, regulations or any agreements with the users;
- stop the collection and use of personal information from the relevant users when its provision of the service ends and allow the users to revoke their records;

- supervise any outsourcing that involves an individuals' private information to ensure that a service provider complies with these requirements; and
- ensure that all personal information is kept confidential.

One view is that any business conducting any kind of electronic service should behave as if the TMT and Internet Personal Information Protection Rules apply to it.

The obligations of banks to ensure bank confidentiality and the obligations for relevant entities to protect state secrets have been described in question 2.

Under the Provisions on the Cyber Protection of Children's Personal Information, the network operator's obligations are as follows:

it must have special rules and user agreements for the protection of children's personal information and designate a person responsible for the protection of children's personal information; when seeking for a consent of a guardian, it must provide an option to reject issuing such a consent and expressly disclose the matters related to personal information processing including (i) purposes, methods and scope of collecting, storing, using, transmitting and disclosing children's personal information, (ii) location and duration of storage of children's personal information and processing of children's personal information after such duration, (iii) security measures for children's personal information, (iv) consequence of rejection, (v) channels and methods of complaints and reports, (vi) ways and methods of correcting and deleting children's personal information, and (vii) other matters which should be disclosed, and where there is any substantial change in any of the above items (i) to (vii), a separate consent of the guardian should be obtained; and it must neither collect children's personal information unrelated to the services provided by it nor breach applicable PRC laws or administrative regulations or the terms of any agreement with the data subject.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

We are unaware of any PRC laws or regulations providing guidance on the collection of non-locally generated data to or within China. Since the Chinese data protection regime is sourced from a complex web of different legislation (as explained at question 1) each aspect of a company's the data protection obligations should be assessed separately.

The General Principle Rules of Civil Law and PRC Tort Liability Law

The right to the protection of personal information under the PRC Civil Code, General Principle Rules of Civil Law and PRC Tort Liability Law is considered a personality right in PRC law. According to the PRC Law on Choice of Law for Foreign-related Civil Relationships issued by the SCNPC on 28 October 2010, the applicable laws on an individual's personality rights should be the laws of the ordinary residence of the individual. To the extent that the data subject's ordinary residence is outside China, the protections of personal information under the PRC Civil Code, General Principle Rules of Civil Law and the PRC Tort Liability Law should not apply. However, if the data subject's ordinary residence is in China, since the right of personal information under the PRC Civil Code, General Principle Rules of Civil Law and the PRC Tort Liability Law is considered a civil law right in nature, such right may be waived by the data subject by consent.

The Consumer Protection Law, the PRC Cyber Security Law (in respect of personal information collected by network operators), the Decision and the TMT and Internet Information Protection Rules, and the Commercial Bank Law

Despite the absence of an explicit exception, it is generally believed that data generated outside China is not intended to be the focus of the protections under these rules.

The PRC Cyber Security Law (in respect of personal information collected by CII operators), the IFI Circular and the Shanghai Circular, and the PBOC 2014 Notice

For other rules regulating or restricting cross-border transfer of information from China to offshore as discussed in questions 1 and 2, the relevant provisions under these rules are aimed to regulate cross-border transfer of PRC locally generated data offshore, they should be irrelevant to collecting and transferring non-locally generated data to or within China.

The State Secrets Law

The State Secrets Law also applies to those state secrets generated outside China. In the case that any such information needs to be collected and transferred to and within China, the requirements described in question 1 should be satisfied. This means

that the collection and transfer are (i) necessary for carrying out the relevant missions, (ii) have been approved by the Relevant Authority, and (iii) assured that the carriers of state secrets complies with the requirements under the State Secrets Law.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Under the TMT and Internet Information Protection Rules, TMT business operators or internet information service providers engaging third parties to conduct marketing, technology services or other direct client fronting services involving collecting or using personal information of users should supervise and manage the safeguards of such personal information by third party service providers. No service providers that fail to satisfy the personal information safeguard requirements under the rules should be used.

In addition, certain outsourcing related legislation may apply where third parties are involved in data processing. Chinese outsourcing laws are outside the scope of this questionnaire.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

It is essential to obtain the consent of the data subject to the processing of their data. However, for any personal information collected by network operators under the PRC Cyber Security Law or collected or stored by data processor under the PRC Civil Code, redactions may be adopted as alternative solutions provided that the original information may no longer be recovered and the information can no longer identify the data subject.

Under the PRC Civil Code, the Consumer Protection Law, the PRC Cyber Security Law, the Decision, the TMT and Internet Information Protection Rules and the Provisions on the Cyber Protection of Children's Personal Information, for consent to be sufficiently informed, the data subject or the guardian (as applicable) must be informed of the purpose, method and scope of information collected and the policies that relate to data collection and usage. There is otherwise no prescribed form for the data subject's consent.

Under the IFI Circular, for consent to be sufficiently informed, the data subject must be informed of the scope of information and the circumstances under which the data processing or transfer may occur. The bank should also highlight the implications of such authorisations in noticeable places and remind clients of such alerts when the relevant contracts are entered into.

For the avoidance of doubt, the following restrictions cannot be waived by data subjects by consent: the restrictions under the PRC Cyber Security Law in respect of cross-border transfer of personal information generated and collected by CII operators, the restrictions under the IFI Circular and the Shanghai Circular in relation to cross-border transfer of IFI, the restriction on providing cross-border assistance to a foreign criminal matter under the ICJAL and the restrictions on disclosing state secrets under the State Secrets Law.

One view is that the consent of the data subject or the fact that the transfer is required by a foreign authority or for internal or external investigation purposes is not sufficient for the relevant information to be transferred to another jurisdiction. This is supported by the ICJAL in terms of foreign criminal matters. That said, for non-criminal related matters, PRC regulators may be willing to take a relatively pragmatic view in terms of the difficulties encountered by CII operators or banks in investigations on a case-by-case basis, therefore it is advisable to consult with the relevant regulators where cross-border transfer of data is necessary for the investigation.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

The consent of the data subject is usually mandatory when planning an investigation (see question 10).

12 Is it possible for data subjects to give their consent to such processing in advance?

Consent may be given through general terms and conditions or by the use of a website, as long as this is executed by the data subject, and sufficiently generic to include the relevant data processing.

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

Under the PRC Cyber Security Law, an individual has the right to request that the network operator erase his personal information if they discover that the network operator collects or uses their personal information in breach of laws, regulations

or any agreement the two have made. An individual may also ask the network operator to correct their personal information if it contains any mistakes. The network operator should remove or correct mistaken personal information at the data subject's request.

The rights of data subjects to access or verify their personal data and influence or resist the processing of their personal data under the PRC Civil Code are substantially the same as those under the PRC Cyber Security Law described above.

The PRC Cyber Security Law also requires that network operators establish policies and systems to handle cybersecurity-related complaints, and publish details of how to complain and how complaints will be received and handled in a timely manner.

Under the TMT and Internet Information Protection Rules, the channels for searching or correcting personal information, among others, should be notified to users of TMT business operators or internet information service providers for the purpose of obtaining consent by users for the collection and use of their personal information. TMT business operators and internet information service providers should also establish policies and systems to handle complaints by users, provide effective contacts for such purpose, and reply within 15 days from receipt of a complaint.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

We are unaware of any PRC legislation providing any guidance on how law firms and legal process outsourcing firms are generally characterised under Chinese law. In general PRC legislation does not distinguish between data controllers and data processors.

Disclosure to professional advisors is not explicitly set out as an exception to the data protections described above. One view is that disclosure to professional advisors, especially those based in China and subject to an obligation of confidentiality, may not breach data protection rules. Certain additional risk mitigation measures, such as anonymisation, may also be helpful when information is disclosed to professional advisers.

A separate analysis would be needed taking specific factual patterns into account in an unusual case where state secrets were involved.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

We are unaware of any additional legislation regulating the disclosure of data to third parties in the PRC for this purpose.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

Our discussions above apply equally to cross-border transfers of data to third parties.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The PRC Cyber Security Law, the Decision and the TMT and Internet Information Protection Rules generally require that network operators, network service providers or TMT business operators or internet information service providers (as the case may be) co-operate with any investigation or inspection by regulators of the TMT and cyber security sectors. Regulations in various specific industries, such as financial services, may contain similar requirements. That said, we are unaware of any generic exception on transferring personal data to PRC regulators or enforcement authorities. Such a transfer may be an implicit exception, though for prudence, one view is that consent of the data subject should be drafted in a way that is sufficiently generic to include such disclosures. A separate analysis would be needed taking specific factual patterns into account in an unusual case where state secrets are involved.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

Please refer to our comments in question 10 and our discussion of the ICJAL and blocking statute in question 2.

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

For non-criminal related matters, one view is that the consent of the data subject should be sufficiently generic to include data transfer to regulators. Anonymisation and pseudonymisation are considered significant mitigation measures. The local regulator and the regulator requesting the data transfer should be consulted, to the extent reasonably practicable. Those with knowledge of the data should be kept to a minimum and should sign confidentiality undertakings, as should the relevant service providers. Facilities for the storing, processing and transferring of relevant data should be secure to safeguard such data from damage, loss or leakage.

For criminal related matters and if the request was from a foreign authority, then in addition to the above considerations, the specific requirements under the ICJAL and/or any applicable judicial assistance treaty on criminal proceedings should be followed depending on the specific assistance that is sought by the foreign authority.

20 What are the sanctions and penalties for non-compliance with data protection laws?

Criminal liability

Any collection, use or transfer of personal information in breach of the PRC Cyber Security Law, the Decision or the TMT and Internet Information Protection Rules, the Commercial Bank Law and the IFI Circular and the Shanghai Circular may constitute a criminal offence. The maximum penalty is imprisonment for up to seven years or a fine. Offences that would attract a severe penalty include selling, stealing or illegally obtaining the personal information of Chinese citizens.

There is no criminal liability for breach of the Consumer Protection Law to the extent that the breach itself is not considered a crime elsewhere in Chinese criminal law.

Unlawful collection, disclosure and cross-border transfer of state secrets may result in criminal sanctions. Article 111 of the PRC Criminal Law provides that it is a criminal offence to steal, secretly gather, purchase or illegally provide state secrets or intelligence for an organisation, institution or person outside China. Any person committed the aforementioned activities may be sentenced to between five and 10 years' imprisonment. If the offence is severe in nature, such person may be sentenced up to a life sentence. If the offence is less severe in nature, such person may be sentenced to less than five years' imprisonment, criminal detention or public surveillance.

According to article 398 of the PRC Criminal Law, if a person is in serious breach of the State Secrecy Law by deliberately or negligently disclosing state secrets, such a person is subject to no more than three years' imprisonment and, if the breach is severe, subject to imprisonment of three to seven years.

Administrative liability

Breach of the Cyber Security Law or the Consumer Protection Law can lead to correction orders, the confiscation of unlawful gains, fines, or the suspension or revocation of a business licence. Breach of the Decision or the TMT and Internet Information Protection Rules could lead to warnings, fines, the confiscation of unlawful gains, cancellation of permits, closure of websites and prohibitions on any personnel held to be liable.

The Commercial Bank Law does not expressly provide penalties specifically for the breach of banking secrecy. In practice, breach of the Commercial Bank Law generally results only in an order from the CBRC (currently the CBIRC, China Banking and Insurance Regulatory Committee) to rectify the breach. Article 89 generally provides that where a bank violates the provisions of the Commercial Bank Law (without further specifying the acts of violation), the CBIRC has a broad power to:

- temporarily or permanently disqualify the directors or senior management personnel directly responsible for the violation from their positions; or
- prohibit the directors or senior management personnel and any other persons directly responsible for the violation from holding their post for a certain period of time; or even permanently ban them from undertaking banking work (in specific circumstances).

Where the violation does not constitute a criminal offence, the directors or senior management personnel and any other persons directly responsible for the violation may be given warnings or issued with a fine of up to 500,000 yuan.

According to article 10 of the IFI Circular, the PBOC may take the following measures in the event of any violation of the IFI Circular or Shanghai Circular or any other failure by a bank to fulfill the obligation to protect IFI:

- request an explanation of the violation from the senior management of the bank;
- if possible, order the rectification of the violation by the bank;
- publicise the non-compliance within the financial sector;
- recommend that the bank punish the senior management or other personnel directly responsible for the violation; or
- submit the violation to the courts if a crime is committed.

Under article 11 of the IFI Circular, if the violation is conducted by using the relevant credit information system, payment system and other system of the PBOC and the relevant bank refuses to rectify, the PBOC may suspend the bank from using or prohibit its newly-established branch from accessing the above systems.

Breach of State Secrecy Law may give rise to administrative disciplinary penalties which are imposed on governmental agencies and their officials. However, we are unaware of legislation providing any administrative sanctions applicable to private entities and their staff members, but there may be some other relevant rules that are not available to the public. Therefore, it would be difficult to draw a conclusion that administrative sanctions will not be imposed on private entities and their staff members in breach in any event although the common position under the key legislation seems to be such.

Breach of the State Secrets Law will give rise to disciplinary actions which are primarily imposed on the relevant governmental agencies or the officials in breach. In the absence of express provision under the State Secrets Law, such actions should not be applicable to private entities or their staff members.

Civil liability

A civil claim can be made by a data subject who has suffered harm as a result of unlawful processing. Damages and injunctive relief are both available.

The ICJAL does not contain penalties for violations. However practically, it is possible that the PRC regulators may frame the violation under the existing regimes including such as data privacy or state secrecy and therefore impose the relevant penalties thereunder.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

The discussions above apply equally to the continuing obligations of the original data controller.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The discussions above apply equally to the continuing obligations of the intervening data controller.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

We are unaware of any additional materials on these topics other than the legislation set out in the questions above.

Jane Jiang

Allen & Overy LLP

Jane Jiang is a partner in Allen & Overy's Shanghai office. She is qualified in the UK and Hong Kong and has worked in London, Hong Kong, Shanghai and Beijing on dispute resolution and other cross-border matters. Jane is a fellow of the Chartered Institute of Arbitrators. Her broad-based practice, in particular her sensitivity to culture differences typically involved in a cross-border transaction are unique assets in dispute resolution involving a Chinese party. Jane is a trusted adviser for many first-tier Chinese companies for their international operations and disputes outside of China.

Benefitting from a long career with the firm and internal credibility, she also helps major Chinese SOE clients with their investment and business operations overseas, leveraging the best resources within the network. Her familiarity with the legal and regulatory environment in both China and key issues faced by Chinese clients in their outbound activities (such as regulatory approval, remittance of payment, regulatory reporting and investigation, sanctions, IP) enables her to immediately identify the relevant risks and efficiently deploy resources. Her understanding of the corporate culture of Chinese clients also puts her in a unique position to ensure that issues arising from complex transactions are well communicated and efficiently executed. She is often sought after for crisis management and praised for her ability to find the best resources in the A&O network and deliver strategic advice in simple terms.

Tiantian Wang

Allen & Overy LLP

Tiantian is a senior associate in Allen & Overy's Shanghai office. She specialises in advising clients in financial sectors on a wide range of matters, including various issues relating to in-bound and out-bound investments in financial institutions and quasi-financial institutions, cross-border portfolio investments such as QFII/RQFII, QDII/RQDII, QDLP, Stock Connect, Bond Connect, related foreign exchange issues and regulations on trading on the stock exchanges in China, fintech related regulations, and establishment of PRC onshore presences by foreign financial institutions. She also specialises in restructuring and insolvency. Tiantian obtained her bachelor degree from Tsinghua University and an LLM from University College London. She is qualified in China. Tiantian speaks Chinese and English.

Jason Song

Allen & Overy LLP

Jason is an associate in the litigation and dispute resolution department based in our Shanghai office. Jason has experience in advising financial institution clients in respect of contentious regulatory investigations and financial and commercial disputes. He has assisted in handling shareholders' disputes, including disputes relating to mainland China, mis-selling of financial products, commercial fraud, fraud investigations, FCPA issues, insolvency-related disputes and compliance issues. Jason is admitted to practise in the PRC (inactive) and the State of New York. He speaks English and Mandarin.

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy LLP
Shanghai office
15F, Phase II, Shanghai IFC
8 Century Avenue
Pudong
Shanghai
200120
Tel: +86 21 2036 7000

www.allenovery.com

Jane Jiang
jane.jiang@allenovery.com

Tiantian Wang
tiantian.wang@allenovery.com

Jason Song
jason.song@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Czech Republic

Markéta Císařová and Jakub Cech
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

Together with the GDPR, the Czech Act No. 110/2019, on Processing of Personal Data (the DPA) forms the data protection regime in the Czech Republic. Among other things, the DPA implements derogations and Czech specific exemptions, as permitted by the GDPR. Throughout this chapter, references to the GDPR shall refer to the GDPR as it applies in the Czech Republic.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Bank secrecy

Czech Act No. 21/1992, on Banks, as amended, provides that all banking trades and financial services of banks, including information on bank account balances, are subject to the principles of banking secrecy and cannot be disclosed to a third party without the consent of the client.

A bank that has outsourced some of its activities will be responsible for any breaches in relation to bank secrecy committed by the service provider to which the activity was outsourced. The conditions of the outsourcing must be documented in an agreement, usually in a written form.

Employment law

In relation to the transfer of employee email correspondence for review, the rules of Czech employment law applicable on monitoring of employees may apply. However, the provisions in employment law tend to apply to continuous monitoring, as opposed to one-off reviews of email correspondence, which means that these employment law restrictions shall not be applicable on transferring of personal data in connection with investigation.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines personal data as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data could re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not also cover legal persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (as per articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision-making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or special categories of personal data), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law.

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");

- Principle 5: personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- the controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

While there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate "explicit" consent (eg, a wet ink signature or a tick box that expressly uses the word "consent").

Consent can be obtained through a website or other electronic means.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right which it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data

subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or if the processing is necessary within legal proceedings.

A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

According to article 29 Working Party's Opinion 01/2010 on the concepts of "controller" and "processor", law firms should be generally characterised as data controllers to the extent they represent their clients in court. It is, however, less clear whether they would be regarded as data controllers also with respect to the systematic review of documents in connection with an investigation. We are of the view that law firms and legal process outsourcing firms that are involved in investigations may be, at least with respect to certain aspects of their work (eg, in the situation where a law firm or a legal process outsourcing law firm is employed by a company and receives detailed instructions from the company's in-house lawyer), also regarded as data processors.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Financial institutions that are subject to Czech Act No. 21/1992, on banks, as amended, have a general obligation to obtain consent from their clients for any disclosure of client data to third parties. Furthermore, a financial institution that has outsourced some of its activities will be responsible for any breaches in relation to bank secrecy committed by the service provider to which the activity was outsourced. In addition, these financial institutions must also comply with applicable obligations stemming from regulation of outsourcing, which involve, in particular, an obligation to enter into a written outsourcing agreement.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission, must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

This article provides that, without prejudice to other grounds for international transfers, a decision from a third country, authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country. This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: "In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement."

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, amongst others:

- consider if there is a legal obligation to respond to the request and, if so, to what extent;
- seek further information in writing from the requesting regulator to evaluate the purpose of the request;
- if possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation;
- in accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose;
- consider whether it is practicable to obtain data subject consent and/or give a further privacy notice;
- put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor); and
- consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside of the EEA), including any transfer to a regulator or law enforcement authority; and
- maintaining a record of processing and responding to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679):
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Czech DPA
https://www.uoou.cz/en/assets/File.ashx?id_org=200156&id_dokumenty=1837

Guidance of the Czech Data Protection Office to the GDPR (in Czech only)
https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

There is no specific guidance by the Czech Data Protection Office regarding internal and external investigations (disregarding domestic police and administrative investigations). We are also not aware of any relevant case law in this respect.

Markéta Císařová

Allen & Overy LLP

Markéta specialises in dispute resolution and is CEE anti-bribery and corruption coordinator. She regularly advises on anti-bribery and anti-corruption matters and has extensive experience with conducting internal investigations, money laundering and anti-bribery compliance. She also advises on a regular basis board members and senior management on criminal, administrative and civil law liability. Markéta has represented a large number of clients from various industry sectors on civil and commercial matters in both court and arbitration.

Jakub Cech

Allen & Overy LLP

Jakub regularly advises on corporate transactions. He has participated in a number of mergers and acquisitions, both domestic and cross-border, in which he represented both buyers and sellers. Jakub was involved in a cross-border merger involving a major Czech bank and he regularly participates in a number of due diligence exercises relating to acquisitions of local companies by foreign investors. Apart from his corporate expertise, Jakub specialises in intellectual property law, in particular copyright enforcement on the internet. He also provides advice on protection against unfair competition and enforcement of rights from trademarks and industrial designs. In The Legal 500 rankings for EMEA 2020 Jakub is recommended for M&A.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy (Czech Republic) LLP, organizační složka
V Celnici 4
Prague
11000
Czech Republic
Tel: +420 222 107 111

www.allenovery.com

Markéta Cisarova
marketa.cisarova@allenovery.com

Jakub Cech
jakub.cech@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Germany

Catharina Glugla, Wolf Bussian,
David Schmid and Jan Erik Windthorst
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

The German Federal Data Protection Act (the BDSG) adapts the application of the rules of the GDPR in Germany where the GDPR provides for opening clauses. It particularly regulates the processing of employee personal data and provides for exemptions to articles 13 to 15 of the GDPR. Apart from that, the majority of the provisions of the BDSG only apply to the data processing by public bodies and authorities, in which case the BDSG is further accompanied by state law regulations.

Furthermore, there are specific data privacy provisions in German laws, mainly providing for a purpose limitation. In relation to investigations, the Telecommunication Act restricting access to telecommunication data, such as business email accounts or business phones or the browsing history of internet browsers, as long as the telecommunication process is ongoing.

As far as personal data is concerned, data privacy rules have to be considered and complied with when processing personal data in internal investigations (see question 7 for more details). In practice, reliance on statutory legal grounds for processing is often the preferred option as consent can be withheld and withdrawn by data subjects at any time.

In the context of internal investigations, sections 24 and 26 of the BDSG and article 6 of the GDPR can provide valid legal grounds for processing where the personal data of employees or other third parties is concerned. However, it is mandatory to balance the data subject's interests against those of the controller (eg, the employer), and processing of personal data is only permitted if the processing is proportionate in relation to the purposes for which the data is processed and if the data subject's interests do not outweigh the controller's interest. As the controller's interest in processing personal data in the context of an investigation must be necessary, adequate and proportionate, each step of investigation should be assessed individually in terms of compliance with data protection laws.

This applies to an even greater extent where the use or communication content of email, internet or phone is reviewed as there are various requirements and restrictions that have to be considered. Such processing might even lead to criminal sanctions in Germany.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Bank secrecy

Subject to limited exemptions, credit institutions (as defined in section 1(1) of the German Banking Act) must not disclose confidential client data to (i) third parties; or (ii) persons within the same bank who are not involved with the client-bank relationship.

The German bank secrecy rules are not codified in laws but are customary law. One leading view is that bank secrecy rules constitutes an accessory obligation of the banking contract between a credit institution, bank or financial institution and its client. However, the exact scope of the obligations remains unclear.

A credit institution's duty to observe bank secrecy rules is contained in section 2(1) of the German Banks' Standard General Terms and Conditions (AGB-Banken), which a bank with a branch in Germany may or may not subscribe to. Under the German bank secrecy rules, the credit institution, bank, etc, is, in principle, not entitled to disclose the identity of its clients or any client-related information enabling the identification of the client. German bank secrecy rules apply to information relating to both individuals and corporations in connection with client relationships of (German or non-German) credit institutions, banks etc. that are governed by German law, irrespective of whether the credit institution, bank, etc, is operating via a branch or entity within Germany or validly on a cross-border basis.

Anonymised data, however, would not be included in the scope of bank secrecy rules.

Bank secrecy rules can generally only be lifted if the client consents or other justification (including under data protection laws) is given. It is accepted that bank secrecy rules shall not limit the functioning of the credit institution and, for example, not prohibit internal audits and investigations related to internal processes and matters as this would also not be in the interest of the client.

A breach of German bank secrecy rules may lead to contractual damage claims from clients. Where significant violations of bank secrecy rules impair the proper conduct of banking business, the Federal Financial Services Supervisory Authority (BaFin) could take measures to counteract such violations.

Employment Law

If a works council is established at a company, two participation rights of the works council should be considered in the context of investigations concerning employee personal data.

First, the works council has information rights under section 80(2) sentence 1 of the German Works Constitution Act (BetrVG). With respect to employees that the works council is competent for, the employer must inform the works council in a timely and comprehensive manner about its intention to access employees' emails and its intention to transfer employee data so that the works council can review compliance with relevant laws that protect the rights of employees.

The employer must inform the works council, prior to accessing employees' emails and transferring employee data, of the scope and extent of its intended access. Complex information may have to be given in writing to the works council and the works council should have time to provide feedback on the intended measures prior to their execution. In case of infringement of this information right, the works council can file a claim enforcing its information right. Further consequences or penalties are unlikely and, according to current case law, non-compliance with the information right should not impact the employer's ability to use findings of otherwise validly collected data as evidence against an employee in court proceedings.

Second, there is a co-determination right pursuant to section 87(1) no. 6 of the BetrVG. This means that the employer must not implement or use technical measures for reviewing emails, video interviews or data mining before reaching an agreement with the works council. This right is triggered easily where software or other technical measures are used for the evaluation of emails or other employee data. It does not matter whether a third party uses the software in the interests of the employer or the employer uses it itself. The scope of application is very broad according to German employment case law, but would, for example, not be triggered where already existing physical documents (print outs, letters, etc) are reviewed manually. The works council also has a co-determination right if the matter concerns the organisation of the operation or the behaviour of the employees. This would be the case if the employees' private emails are to be reviewed.

If the employer implements the measure (eg, screening the emails with new software) without the agreement of the works council, the works council can file a preliminary injunction to stop the processing.

We note that (i) one employer might have multiple works councils and also that (ii) the works council is generally not competent for employees in managerial position (leitender Angestellter). Regarding information and internal investigation, we note that the works council is only competent for Germany-based employees with a German employment contract.

Telecommunication Law

Further restrictions on data transfer in the context of an investigation may arise under the German Telecommunication Act (see question 11 for further details).

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines "personal data" as any data relating to a living individual (ie, not a legal person) who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data could re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not cover legal persons or deceased natural persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (as per articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

In Germany, lawyers are exempted from providing information due to professional secrecy rules under article 14(5) lit. d) of the GDPR, section 29(1) sentence 2 of the BDSG, section 43a(2) of the German Federal Lawyers' Act and section 203 of the German Criminal Code.

Relating to investigations, German supervisory authorities accept that the information of data subjects can be withheld to not "tip off" data subjects until the investigation is completed. This is based on the exemption that providing the information is likely to render impossible or seriously impair the achievement of the objectives of that processing under article 14(5) of the GDPR and sections 29, 33 of the BDSG. From the explicit wording or article 14(5) GDPR and sections 29, 33 of the BDSG, it is not entirely clear whether the information has to be provided once the investigation is complete (ie, whether it is an exemption to the information obligations or only a suspension). There is no judgment on this issue yet.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject. In the context of investigations, for example, pursuing or defending civil claims or preventing damages or criminal liability of both the controller as well as other group companies could serve as legitimate interest.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR and stricter organisational and technical security measures required under section 22 of the BDSG. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law. Under the legislative materials to the BDSG, section 26(1) of the BDSG provides for sufficient safeguards within the meaning of article 10 of the GDPR and can serve as a legal basis for processing criminal personal data of employees in Germany.

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");
- Principle 5: personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

Under section 24(1) of the BDSG, processing of personal data for a purpose other than the one for which the data were collected is permitted if such processing is necessary (i) to prevent threats to state or public security or to prosecute criminal offences or (ii) to establish, exercise or defend legal claims, in each case unless the data subject has an overriding interest in not having the data processed.

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (see also question 16).

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

While there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for consent under GDPR, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may, therefore, wish to obtain consent by means of an additional formality to demonstrate “explicit” consent (eg, a wet ink signature or a tick box that expressly uses the word “consent”).

Note that German employee consent has to be obtained in written form (ie, wet ink signatures) or, once the draft amendment of section 26 of the BDSG will have been implemented by German lawmakers, in electronic form (ie, qualified electronic signature, not email or ticking a box).

Consent can be obtained through a website or other electronic means.

Employee consent

Note that employee consent in Germany must be obtained in written (i.e. wet ink signatures) or electronic form (i.e. qualified electronic signature, not email or ticking a box), unless a different form is appropriate because of special circumstances, under section 26(2) sentence 2 of the BDSG.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground might sometimes not be appropriate. One reason is that consent must be capable of being withdrawn at any time (a right which it is not possible to contract out of).

However, according to the German supervisory authorities' view, consent might under certain circumstances be required for reviewing employee business email accounts. In this regard, it has to be differentiated between a scenario when the employer allows or tolerates the private use of the business email account and the opposite setting in which the private use is strictly forbidden:

- Where the employer allows or tolerates private use, German supervisory authorities regard the employer as a telecommunication provider so that employers are bound by the secrecy of telecommunication. Any processing of telecommunication data is subject to the German Telecommunication Act under which the processing of telecommunication data can only be justified in very limited cases of which none applies to reviewing emails in case of internal investigations. Processing of telecommunication data may also not be justified by the GDPR or the BDSG as such laws do not explicitly refer to the telecommunication process and the secrecy of telecommunication and can therefore not serve as a legal basis for processing telecommunication data, such as the content of an email. Note that the secrecy of telecommunication is also protected by criminal liability under the German Criminal Code. However, this rationale only applies during the telecommunication process, which scope of application and duration is, however, unclear. There is case law both agreeing and disagreeing with the German supervisory authorities' line of argumentation. Therefore, whether the employer is regarded as a telecommunication provider and as such bound by the secrecy of telecommunication remains a shade of grey area. As a consequence, it should always be assessed whether (i) private use is allowed or tolerated, (ii) the communication process is ongoing or (iii) consent from the employee should be obtained.
- If however the private use of the business email account is strictly prohibited, the secrecy of telecommunication does not apply and the general data protection rules under the GDPR and BDSG apply.

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, may for this reason be invalid. In any case it has to be assessed in detail whether the employee freely provided consent taking into account the individual case including the interests of the employee and whether the employee gains an advantage by providing consent (section 26(2) sentence 1 of the BDSG). Note that German supervisory authorities request employers to obtain employee consent for reviewing business email accounts in certain scenarios (see question 11 for further details), so that it can be assumed that employee consent can validly be obtained for such purposes in Germany.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. Therefore, if consent is hidden among other terms and conditions one might argue that the respective prerequisites are not fulfilled. So there is a risk that a generic consent provided through general terms and conditions may be regarded as not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject. According to some German supervisory authorities, it is sufficient to provide a "summary" as opposed to a "copy" of the personal data. There are exemptions to the DSAR under section 34 of the BDSG, none of which applies in the context of internal investigations (except for lawyers due to professional secrecy rules, see above). Furthermore, according to a decision from the regional labour court in Baden Wurttemberg (dated 20 December 2018, case No. 17 Sa 11/18), the employer might, in certain circumstances have an overriding interest in secrecy on which basis the DSAR may be denied. However, details as to when and to what extent this additional exemption applies are still unclear. Case law on the DSAR is evolving rapidly and should be monitored closely in relation to investigations.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. According to some German supervisory authorities, German procedural laws do not recognise a right to produce information and the DSAR should therefore not be misused for non-privacy purposes.

If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or if the processing is necessary within legal proceedings.

A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

Law firms would, in general, qualify as controllers in relation to providing legal advice and as processors when only providing document review or hosting services. External document reviewers and other legal process outsourcing firms are generally characterised as processors and, thus, a data processing agreement pursuant to article 28 of the GDPR has to be entered into.

However, exemptions may occur in practice as this depends on the service provided and the details of the individual case, particularly on whether the client issues instructions regarding the content and means of the data processing, that is, whether the external service provider or law firm:

- is free to determine the purposes, content and means of the data processing (the 'why' and 'how'), in which case it will be qualified as controller; or
- is strictly bound by concrete and binding instructions of their client regarding the processing of personal data (in which case, it will be qualified as processors).

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

The data protection officer of the controller should be involved.

It should be assessed whether processing and, in particular, the disclosure is likely to result in a high risk to the rights and freedoms of natural persons so that a data protection impact assessment has to be carried out pursuant to article 35 of the GDPR prior to disclosing personal data.

Depending on the client's business, the purposes for which the personal data can be processed might be limited under German regulatory law (eg, data that has been shared for anti-money laundering purposes) and it has to be ascertained whether processing for the purpose of the internal investigation is compatible with the purpose for which the personal data have been initially collected.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to jurisdictions within the EEA and transfers of data to other jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from Germany to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within Germany (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14 of the GDPR, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR or section 26 of the BDSG in relation to employee data.

Prosecutors, tax investigation officers and regulators such as the Federal Cartel Authority or BaFin have extensive powers to investigate (ie, to inspect corporate or private premises, to copy and/or seize documents in any form and to interview suspects

and employees). There are certain degrees of investigation powers of regulators and enforcement authorities, from individual requests to provide information on certain matters to official search orders. Investigation powers may be based, inter alia, on criminal prosecution grounds (section 94 et seq. German Code of Criminal Procedure), cartel grounds (section 57 et seq German Law Against Restraints on Competition) or administrative grounds (section 46 German Act on Regulatory Offences). The BaFin's supervisory powers include, inter alia, the right to (i) conduct an investigation in respect of a supervised entity; or (ii) appoint the German Central Bank or another third party (eg, audit or law firms) to conduct an investigation on BaFin's behalf. In all these cases, transfer of personal data to regulators or enforcement authorities within Germany is permissible.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR or section 26 of the BDSG for employee data) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are often interpreted narrowly. The additional exemptions under sections 32 to 34 of the BDSG are also interpreted narrowly and, according to German supervisory authorities, do not provide for general exemptions but only for temporary postponement of the information obligations (see question 7).

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may or may not be permissible, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details) subject to a comprehensive balancing of interests, particularly taking into account whether the data subject could face (legal) consequences; or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

This article provides that, without prejudice to other grounds for international transfers, a decision from a third-country authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country. This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: "In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement."

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, among others:

- Consider if there is a legal obligation to respond to the request and, if so, to what extent.
- Seek further information in writing from the requesting regulator to evaluate the purpose of the request.
- If possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation.
- In accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose.
- Consider whether it is practicable to obtain data subject consent and/or give a further privacy notice.
- Put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor) or data transfer agreements limiting the purpose for which the transferee can process the data and, to the extent required by supervisory authorities, put in place additional safeguards for employee personal data.
- Consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

If the secrecy of telecommunication applied to employers allowing or tolerating the private use of business systems, there is also a risk that unlawful processing of personal data will incur an administrative fine of up to €300,000 under the German Telecommunication Act. Infringement of the secrecy of telecommunication is a criminal offence in Germany, subject to five years imprisonment or a fine.

Further potential consequences in Germany are reputational damages due to press releases or articles in the activity reports of the German supervisory authorities and cease and desist order from competitors or consumer associations and respective litigation and in exceptional cases criminal liability under section 42 of the BDSG.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside the EEA), including any transfer to a regulator or law enforcement authority; and
- maintaining a record of processing and responding to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant Materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Federal Data Protection Act
https://www.gesetze-im-internet.de/englisch_bdsg/index.html

Guidance from German supervisory authorities regarding whistleblowing hotlines and other warning systems including guidance on internal investigations (dated 14 November 2018, German language only)
https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf

Guidance from German supervisory authorities regarding application of telecommunication laws to employers allowing private use of business communication systems (dated January 2016, German language only)
https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf

Catharina Glugla

Allen & Overy LLP

Catharina is a senior associate working in the German Data & Data Protection Group and assists several clients across industries with implementing the GDPR. In particular, she developed a data protection impact assessment with an automated risk assessment helping clients meet their GDPR requirements with an efficient solution. Catharina advises on crisis management of privacy violations, data breaches or cyber-attacks. Additionally, she focuses her legal advice on intragroup and international data transfers, cross-border compliance projects and data privacy matters on transactions and corporate reorganisations. Another focus of her work is the data privacy compliant drafting of data processing agreements, data transfer agreements, privacy notices and information as well as declarations of consent. By doing so, she legally secures and enhances the usability of the value "data".

In addition, Catharina has experience in advising national and international companies on all issues of individual and collective employment law. She studied law at Bucerius Law School in Hamburg, Germany, and completed a stay abroad at Waseda University in Tokyo. Catharina completed her legal traineeship at the Higher Regional Court District of Frankfurt, with our Allen & Overy employment and data teams in Dusseldorf and London and at the German Embassy in Phnom Penh, Cambodia. Prior to joining Allen & Overy, Catharina worked for several other renowned international law firms as a research fellow and as a legal trainee. Clients benefit from her vast international expertise, which Catharina further enhances during a secondment to Allen & Overy's London Data & Data Protection team from November onwards.

Wolf Bussian

Allen & Overy LLP

Wolf heads Allen & Overy's German dispute resolution practice. He focuses on litigation and investigations in the finance sector. He represents banks, asset managers, insurers, funds, accounting firms and other companies as well as governments and public institutions in disputes both in and out of court. He deals with disputes about complex finance products and tax driven transactions (for example cum/ex and cum/cum trades) on a regular basis. Wolf also frequently advises on capital market disputes and capital market-related professional indemnity claims as well as disputes in the field of payment services. He has special expertise with disputes resulting from bank crises (restructuring, resolution and insolvency) and equity substitution. He regularly deals with international civil procedural law issues (eg, service, taking evidence and enforcement abroad), in particular in relation to the UK and the United States.

A major focus of his work are investigations in the financial sector (eg, relating to allegations of tax evasion, market manipulation, fraud or insider trading), typically in multi-jurisdictional teams from several practice groups (including regulatory, tax, corporate). Wolf leads internal investigations and advises on external investigations conducted by regulators (including ECB, BaFin, SEC, DOJ, FCA), tax authorities or criminal prosecutors.

Wolf regularly publishes in legal journals as well as daily press on procedural, capital market and banking issues. He is recognised as leading expert for finance litigation and investigations in legal directories. *The Legal 500* Germany 2019 praises his finance litigation practice as market leading (Tier 1). *Chambers Global* recognises Wolf as leading expert for finance litigation since 2015 already, highlighting that he "enters the rankings on the strength of his excellent reputation for representing banks and financial institutions in litigation proceedings, often with a significant international aspect". *JUVE* 2017/2018 lists Wolf as "leading expert for investigations and disputes in the context of tax transactions like cum/ex and cum/cum deals". *The Financial Times* commended Allen & Overy as "standout" for a matter led by Wolf in the category "Innovation in dispute resolution" at the FT Innovative Lawyers Awards 2015.

David Schmid

Allen & Overy LLP

Dr David Schmid has been practising as a German lawyer (*Rechtsanwalt*) in Allen & Overy's Frankfurt office since 2013. His work focuses primarily on the field of internal investigations. In particular, he regularly advises on large-scale, cross-border internal investigations being conducted at corporates and financial institutions, both with respect to ongoing proceedings instigated by regulators or other authorities and in preventative internal investigations. His expertise in particular covers investigations relating to breaches of compliance regulations, tax-specific issues (eg, cum-ex and similar transaction structures) or matters related to antitrust law, including associated aspects of white-collar crime, such as money laundering, breach of trust, fraud, bribery and corruption in business transactions – a subject he addressed in his dissertation. David was able to broaden his experience in the context of internal investigations through a secondment to the regulatory enforcement team of a major international financial institution.

Further, David advises on national and cross-border disputes before public courts. In this context, the focus of his work lies on disputes following internal investigations as well as on financial services litigation. He regularly acts on behalf of major financial institutions and electronic payment service providers in such disputes and litigation matters and also has extensive experience in disputes concerning equity substitution law, including in constellations involving restructuring.

Jan Erik Windthorst

Allen & Overy LLP

Erik represents clients before state courts, arbitral tribunals and government agencies. He handles banking and finance litigations as well as corporate disputes (including stock corporation law proceedings, directors' liability and M&A disputes), often with a cross-border element.

Erik has extensive experience with large-scale internal and administratively imposed investigations in the financial industry and other industries. He was seconded to the Litigation and Regulatory Enforcement team of a leading international bank in Frankfurt and closely monitors the increasing nexus between regulatory and contentious issues in the financial sector.

Erik advises financial institutions, insurance companies and private equity investors as well as clients from a wide variety of industries.

Erik is recognised by leading legal directories: *The Legal 500* German language version singles Erik out as 'name of the next generation' for financial litigation. JUVE's Handbook Commercial Law Firms in Germany lists him as "frequently recommended" for litigation, citing others who describe Erik as a "lightning-quick strategist" (*JUVE Handbook 2017*), "creative, highly professional" and someone who "has full control over the proceedings" (*JUVE Handbook 2018*).

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy LLP
Dreischeibenhaus 1
Duesseldorf
40211
Germany
Tel: +49 211 2806 7000

www.allenovery.com

Catharina Glugla
catharina.glugla@allenovery.com

Wolf Bussian
wolf.bussian@allenovery.com

David Schmid
david.schmid@allenovery.com

Jan Erik Windthorst
jan-erik.windthorst@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

France

Dan Benguigui and Laurie-Anne Ancenys
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

Act No. 78-17 dated 6 January 1978 on information technology, data files and civil liberties (as modified).

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Under French law, data sharing in the context of investigation may be restricted, principally, by four other statutes, the violation of which may be subject to criminal or regulatory sanctions, and may result in civil litigation risks:

- Laws relating to banking secrecy (article L511-33 of the French Monetary and Financial Code);
- Law No. 68-678 dated 26 July 1968, as amended, governing the request, research or disclosure of information of an economic, commercial, industrial, financial or technical nature, with a view to establishing evidence in foreign judicial or administrative proceedings or in relation thereto (the Blocking Statute);
- Law No. 2018-670 dated 30 July 2018, dealing with the protection of business secrecies; and
- Law No. 71-1130 dated 31 December 1971 where article 66-5 establishes a professional secrecy covering legal advice, meeting notes and any correspondence between a French lawyer and his client, including emails.

In addition, from an employment law stance, using data of an employee (emails, files) marked as "personal" or "private" is prohibited in principle.

For files, an exception exists where (i) this access is performed with the employee present or duly convened; (ii) in case of "particular risk or event". However, this exception only covers exceptional circumstances and French courts construe it very narrowly, in consideration of an absolute emergency for the employer to access information.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines "personal data" as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not cover legal persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (as per articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;

- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision making (including profiling); and the right to lodge a complaint with a supervisory authority. In addition, under French law, the controller should inform the data subject of the right to lay down guidelines as to the fate of his or her personal data after his or her death.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law.

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");

- Principle 5: personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

While there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

Consent can be obtained through a website or other electronic means.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate "explicit" consent (eg, a wet ink signature or a tick box that expressly uses the word "consent").

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right that it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

Data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the

data subject, or if the processing is necessary within legal proceedings. A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

Law firms and legal process outsourcing firms are generally characterised as data processors.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

There are no additional requirements, beyond those specified above, that regulate the disclosure of data to third parties in France.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;

- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

Article 48 of the GDPR provides that, without prejudice to other grounds for international transfers, a decision from a third-country authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country. This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: "In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement."

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, among others:

- consider if there is a legal obligation to respond to the request and, if so, to what extent;
- seek further information in writing from the requesting regulator to evaluate the purpose of the request;
- if possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation;
- in accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose;
- consider whether it is practicable to obtain data subject consent and/or give a further privacy notice;
- put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor); and
- consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

Administrative fine

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement. Furthermore, the decision relating to the amount of this sanction will depend in particular on the degree of cooperation with the supervisory authority, to remedy the infringement and commitments to mitigate the possible adverse effects of the infringements.

Other material sanctions

As part of an inspection revealing infringements of the applicable data protection regulation, the CNIL may also issue (i) a warning; (ii) a formal order to comply with the applicable regulation; (iii) a temporary or definitive restriction to processing; (iv) a suspension of data transfers; and (v) an order to fulfil the requests of a data subject to exercise his or her rights.

In addition, every abovementioned sanction can be made public and would therefore trigger reputational damage.

Criminal sanctions: for infringing the French data protection legislation, criminal sanctions could also be levied (ie, up to five years imprisonment and up to €1.5 million for a legal entity). In practice, criminal sanctions are rather theoretical. To our best knowledge, there have been very few criminal proceedings based on the French data protection legislation.

Group action: A group action may be brought before a civil court or the competent administrative court, under certain conditions, to (i) put an end to a breach or (ii) to engage the liability of the company that caused the damage to obtain compensation for the material and moral damages suffered or for both purposes.

Civil claim

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside of the EEA), including any transfer to a regulator or law enforcement authority; and
- maintaining a record of processing and responding to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Dan Benguigui

Allen & Overy LLP

Dan is a partner in the litigation department of Allen & Overy in Paris.

Dan is a member of the Paris Bar and a graduate of both Université Jean-Moulin-Lyon-III law school (DESS Droit et finance de l'entreprise) and EM Lyon business school.

Dan began his career within a criminal law firm before working as a clerk to the judge heading the 15th Chamber of the Paris Court of Appeal (banking and financial litigation). He spent many years in house within the Global Litigation department of BNP Paribas and led the "Criminal Proceedings and Regulatory Enforcement" team of the group prior to joining the litigation practice of Allen & Overy, in 2014.

Dan now specialises in litigation work, notably in the field banking and finance. He represents private and corporate clients before all criminal, civil and commercial courts. He has a particular expertise in complex white-collar crime (market abuses, money-laundering, corruption, sanctions, etc) and commercial cases involving banks, investment service providers and large corporates.

Dan also assists clients in the implementation of internal investigations or in the context of enquiries, inspection, or enforcement proceedings initiated by financial regulators (AMF, ACPR).

Laurie-Anne Ancenys

Allen & Overy LLP

Laurie-Anne is a counsel in the corporate department of Allen & Overy in Paris, dedicated to the telecommunications, media and technology sector. She has in-depth experience in the fields of data protection, computer law and information technology. She has developed an expertise in data protection compliance projects and, more specifically, in the implementation of personal data processing, pan-European data protection strategies and international data transfers.

Laurie-Anne is also specialised in the drafting and negotiation of complex agreements related to business and technology matters. She particularly advises international clients on all specific contract issues whether dealing with licence and maintenance, IT services, hosting, integration and outsourcing.

She also assists French and international clients with e-commerce issues, in particular with the digitalisation of their activities and often as part of multi-country studies.

Laurie-Anne spent six years working in London as an avocat / solicitor in a renowned City law firm and as a legal counsel in international groups in the technology sector. Such experience is a real added-value when she takes part to multi-disciplinary cross-border transactions and contributes to complex due diligence processes.

Laurie-Anne conducts round table discussions at the Franco Chamber of Great-Britain (FCGB) in London, and regularly publishes, in particular in the e-commerce Law Reports and *French Chamber Magazine.*

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy LLP
52 avenue Hoche
Paris
75008
France
Tel: +33 1 40 06 54 00

www.allenovery.com

Dan Benguigui
dan.benguigui@allenovery.com

Laurie-Anne Ancenys
laurie-anne.ancenys@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Hong Kong

Matt Bower and Clement Sung
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The collection and processing of personal data in Hong Kong is regulated by the Personal Data (Privacy) Ordinance (the PDPO).

The Office of the Privacy Commissioner for Personal Data (the PCPD) is the regulator responsible for enforcing the PDPO.

The PCPD has expressed concern that the privacy protection laws in Hong Kong are not keeping up with international standards, given that the last major reform to the PDPO was back in 2012. The authorities and the legislature have been in discussions since early 2020 about introducing new amendments to the PDPO. The reform proposals are at a preliminary stage and no draft bill is available yet. However, the Constitutional and Mainland Affairs Bureau presented to the Legislative Council a paper proposing six key amendments to the PDPO (the Paper): (i) establishing a mandatory data breach notification mechanism, (ii) introducing a requirement to maintain a clear data retention policy, (iii) enhancing PCPD's sanction powers, (iv) expanding PDPO's reach to regulate data processors, (v) amending the definition of personal data to cover information relating to an "identifiable" natural person and (vi) prohibiting doxxing activities. Meanwhile, it is expected that further in-depth studies and consultation with relevant stakeholders will take place before a draft bill will be formulated. As with any law reform and legislative processes, it will take some time before actual changes to the PDPO will come into effect.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Providers of banking services – implied duty of confidentiality

A person providing banking services in Hong Kong has an implied duty of confidentiality to its clients under Hong Kong common law. This means that such an entity must not divulge confidential information about its client to any third party, unless the consent of the bank's client is obtained or an exemption applies. The banker's duty of confidentiality is considered to be an implied term of the contract between a banker and his or her customer, but it may be modified by express terms.

The duty applies to any information about a client (both natural and legal persons) that a banker acquires in the course of providing banking services.

There is no exhaustive definition of what constitutes banking services and therefore the precise scope of the banker's duty of confidentiality is unclear. However, examples of banking services that would trigger the confidentiality obligation are:

- keeping current accounts for customers, in which credits and debits are entered;
- accepting money from and collecting cheques for customers and placing them in credit; and
- paying cheques drawn on those accounts and debiting customers accordingly.

These essential characteristics of banking are not exhaustive and transactions that lack these characteristics may still be considered banking. As a result, the banker's duty of confidentiality may well apply to persons that do not consider themselves to be banks.

Certain exemptions apply to the banker's duty of confidentiality at common law. These include those situations where:

- the express or implied consent of the client has been obtained;
- there is a duty to the public to disclose such information;
- Hong Kong law or court order compels disclosure; or
- the interests of the bank require disclosure.

The Organized and Serious Crime Ordinance (the OSCO) is one of the major statutory exceptions to the common law duty of confidentiality. A person is required under OSCO to make a disclosure to "authorised officers" (eg, police officers) where that person knows or suspects that any property, among others, in whole or in part directly or indirectly represents the proceeds of an indictable offence. In the context of property passing through a bank account, this may require the disclosure to an authorised officer of account information subject to the banker's duty of confidentiality.

A client can claim damages for breach of confidentiality by a bank. These are usually nominal damages, unless the client has suffered financial loss. Injunctive relief is also available.

In addition to the banker's duty of confidentiality at common law, authorised institutions (ie, licensed banks, restricted licence banks, and deposit-taking companies regulated by the Hong Kong Monetary Authority (the HKMA)) (AIs) are also required to comply with regulatory guidance issued by the HKMA. That guidance includes circulars on customer data protection and a module in the HKMA's Supervisory Policy Manual regarding outsourcing (SA-2). A detailed analysis of outsourcing laws is beyond the scope of this chapter; however, in summary, where an AI engages in outsourcing, it is expected under SA-2 to: ensure that outsourcing arrangements comply with the relevant requirements (eg, the PDPO and the banker's duty of confidentiality), have controls in place to ensure that these requirements are observed and proper safeguards are established to protect the integrity and confidentiality of customer information, notify customers of the possibility that their data may be provided to another person as part of an outsourcing arrangement, and ensure that all customer data is destroyed or retrieved (as permitted by

law) where an outsourcing arrangement is terminated. AIs should discuss any outsourcing plans with the HKMA in advance and should be prepared to satisfy the HKMA that issues relating to customer data, among others, are properly addressed.

The HKMA has also endorsed the Hong Kong Association of Banks' Code of Banking Practice, which makes reference to AIs' obligations under the PDPO and the relevant codes of practice issued by the PCPD, and reminds banks to comply with the relevant requirements.

Breach of the HKMA's regulatory guidance or the Code of Banking Practice does not, by itself, allow a customer to claim damages. However, it may lead to disciplinary action by the HKMA against the AI concerned, which in extreme cases can include suspension or revocation of the AI's banking licence.

Other persons

Persons other than providers of banking services may also be subject to a duty of confidentiality depending on the circumstances. The most common situation in which a duty of confidentiality may arise is where information is received in the course of a relationship which a reasonable person would regard as involving a duty of confidentiality. Such relationships may include agents, trustees, partners, directors, employees and professionals, such as doctors and accountants.

Although not exhaustive, the generally recognised exemptions to this duty of confidentiality, and the consequences of breach of this duty, are the same as those that apply to the banker's duty of confidentiality, discussed above.

Official Secrets Ordinance

Persons who come into possession of official information relating to security or intelligence services, defence, international relations, or criminal investigations are, under certain circumstances, prohibited under the Official Secrets Ordinance from disclosing such information. The Official Secrets Ordinance is unlikely to be relevant to an investigation unless the person being investigated has a relationship with a government that would put that person in a position such that it is likely to receive such information.

3 What can constitute personal data for the purposes of data protection laws?

The PDPO defines personal data as any data relating directly or indirectly to a living individual, from which it is "practicable" for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable.

"Practicable" is defined as "reasonably practicable". When considering whether data is personal data, the PCPD will consider all relevant data controlled by the party in question. If it is reasonably practicable for that party to ascertain from the totality of such data the identity of the data subject, then the data is personal data and the PDPO applies. It is commonly understood that a person's name in isolation generally does not constitute personal data.

This definition has been recognised as too narrow in light of the increasing use of tracking and data analytics technology. The Paper, therefore, proposes expanding the definition of personal data to cover information relating to an "identifiable" natural person.

4 Does personal data protection relate only to natural persons or also legal persons?

Personal data protection extends only to natural living persons, not to legal persons such as companies or deceased natural persons.

5 To whom do data protection laws apply?

In relation to transfers of personal data, the direct obligations under the PDPO are only applicable to "data users". A data user is defined as a person who (either alone or jointly or in common with others) controls the collection, holding, processing or use (which includes disclosure or transfer) of the data.

A person is taken to be a data processor if he holds, processes or uses personal data solely on behalf of another person, and not for his own purpose. Under the current law, a data processor is not obliged to comply with the requirements of the PDPO in respect of any personal data for which it is a data processor. This may change if the proposal under the Paper to expand the PDPO's regulatory reach to cover data processors is adopted.

6 What acts or operations on personal data are regulated by data protection laws?

The acts regulated by the PDPO are the collection, use, disclosure and retention of personal data. There are currently no restrictions on the cross-border transfer of personal data over and above those in place for transfers of personal data within

Hong Kong. A provision has been enacted that would place extra restrictions on cross-border transfers (section 33 of the PDPO), but it has not yet been implemented (see question 16).

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

Personal data must be processed in accordance with the six principles set out in the PDPO.

- **Principle 1** is that personal data must be collected by means that are lawful and fair in the circumstances. All practicable steps must also be taken to ensure the data subject is explicitly or implicitly informed of their rights and obligations.

To comply with this principle, the data subject must be given certain information when their personal data is collected. This includes whether it is obligatory to supply the data and any consequences of not supplying the data. The data subject should be explicitly informed of the purpose for which the data is to be used and the classes of person to whom the data will be transferred. This information is usually provided by way of a written notice, which is generally referred to as a Personal Information Collection Statement. For the statement to be effective, it should be presented in a conspicuous manner and the language used should be easily understandable.

- **Principle 2** is that personal data must be accurate and, where necessary, kept up to date. Personal data shall not be kept longer than is necessary for the fulfilment of the purpose for which the data is or is to be used. As noted, the Paper suggests data users should maintain a clear retention policy specifying: (i) a maximum retention period for different categories of personal data; (ii) legal requirements which may affect the retention period (eg taxation, employment or medical requirements); and (iii) how the retention period will be counted.
- **Principle 3** is that personal data shall not be used for a purpose other than that notified to the data subject.
- **Principle 4** is that appropriate measures must be taken against unauthorised or unlawful access, processing, erasure, loss or use of personal data.
- **Principle 5** is that practicable steps must be taken to ensure that a data subject can understand the data user's policies and stay informed about the kind of personal data held by a data user and the main purpose or purposes for which it is held.
- **Principle 6** is that data subject should be able to find out whether a data user holds any of its personal data and to request access and correction of personal data where necessary.

Hong Kong law does not recognise the concept of special categories of personal data, such as sensitive personal data.

Apart from the six principles above, the PDPO also restricts the processing of personal data for direct marketing purposes.

"Direct marketing" includes offering or advertising of goods or services through 'direct marketing means' (ie, sending information or making phone calls to specific persons).

Data users who intend to use data subjects' personal data in direct marketing must (i) inform the data subjects of the data user's intention to use their personal data for that purpose and that the data user may not use their personal data for direct marketing unless the data user receives their consent, (ii) provide the data subjects with information on the intended use of their personal data for direct marketing (including the kinds of personal data to be used and the classes of marketing subjects in relation to which the data is to be used), (iii) provide a channel through which the data subjects may, without charge by the data user, communicate their consent, and (iv) obtain such consent. A data user must also notify data subjects when using their personal data in direct marketing for the first time.

The requirements for data users who intend to provide data subjects' personal data to third parties for their use in direct marketing are even stricter, and include the requirement to provide certain information (eg, whether their personal data will be provided for gain and the classes of persons to whom the data will be provided) to data subjects in writing and the requirement to obtain data subjects' consent in writing.

If at any time a data subject requests that a data user stop using, or stop providing to third parties, their personal data for direct marketing, the data user must comply without levying a charge on the data subject.

Contravening the requirements for use or provision of personal data in direct marketing constitutes one or more criminal offences (see question 20).

Currently, under the PDPO, a data user is not required, but only encouraged, to report a data breach. It remains to be seen whether a mandatory data breach notification requirement as proposed under the Paper will be added to the PDPO.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

The PDPO does not restrict the transfer of personal data into Hong Kong. Data users should, however, ensure that the transfer of personal data to Hong Kong from other jurisdictions complies with the domestic data privacy laws of the originating jurisdiction. Transfers within Hong Kong should be compliant with the principles for processing personal data under the PDPO.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

If a data user engages a local or overseas data processor to process personal data on its behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than necessary for the specified processing and to prevent the unauthorised or accidental access, processing, erasure, loss, or use of the personal data. Also see question 15.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

Whether consent is needed depends on the purposes for which the personal data was originally collected from the data subject. If the investigation falls within those purposes (which is a question of fact), no consent would be required. If the investigation falls outside those purposes, subject to a consideration of potentially applicable exemptions (see question 17), express consent would be required.

If consent is required, it must be express and not withdrawn by notice in writing served on the person to whom the consent has been given.

Express consent can be given either orally or in writing. Consent can be obtained through a website as long as the other requirements of the PDPO (see question 7) are met.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Yes, consent should be considered as an enabling action when planning out an investigation.

12 Is it possible for data subjects to give their consent to such processing in advance?

Yes, data subjects can give their consent through standard terms and conditions as long as the requirements of the PDPO (see question 7) are satisfied. Consent language should be presented in a manner that renders it easily readable and understandable in terms of its length, complexity, font size and accessibility.

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

Under Principle 6 in the PDPO (see question 7), a data subject or a relevant person acting on their behalf can ask for confirmation that a data user holds personal data for which he is the data subject, request access to this data and ask for it to be corrected if it is inaccurate.

A "relevant person" could be a parent of the data subject, a person appointed by the court, or a person authorised in writing by the individual.

Under the PDPO, the normal time period for complying with a data access request is 40 days after the receipt of such request.

There are various grounds on which the data user can refuse to comply with a data access request. The data user is entitled to refuse to comply with a request if the same is not made in the form prescribed under the PDPO. The form has been designed to make clear the following matters:

- the fact that a data access request is being made under the PDPO;
- the particular provision(s) of the PDPO under which such request is being made;

- the precise scope of the data to which the request relates; and
- the way of handling (including the time for compliance with) the request and possible consequences of failure to do so.

Another key exemption is that the data user should, where the personal data requested also contains the personal data of another individual(s), refuse to comply with the request unless consent from that person is obtained or the personal data of that other individual is erased from the data before release.

A data user is obliged to give to the requestor written notification of the refusal and reasons for the refusal.

Where the scope of the data access request is too generic (eg, "all of my data") and, in the absence of any information from the requestor to specify or to otherwise assist in locating the data requested, the data user's duty of compliance may only extend to such data as it may reasonably and practicably be expected to provide.

It is important to note that the data requester is entitled to a copy of his or her personal data only, not every document that refers to him or her.

After personal data has been provided to the requestor pursuant to a data access request, the requestor may request the correction of such data. The data user is obliged to comply with a data correction request only if it is satisfied that the personal data to which the data correction request relates is inaccurate.

As part of the investigation, if data has been disclosed to third parties by the data user, and data access and correction requests are then received, the data user should ascertain whether the third party has ceased using that data. If the data user has no reason to believe that the third party has ceased using the data for the purpose for which it was disclosed, the data user should take all practicable steps to supply the third party with a copy of the corrected personal data and a written notice of the reasons for the correction.

Exemptions are provided under the PDPO from the application of Principle 6, including where:

- data is held for the purposes of, among other things, the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, dishonesty, or malpractice, or discharging certain functions of a financial regulator; and
- the requests would either be likely to prejudice any of those purposes, or be likely to identify directly or indirectly the person who is the source of the data.

Therefore in the context of an investigation, a data user would be able to resist data access and correction requests regarding data held for the aforesaid purposes to the extent that complying with the request would prejudice those purposes or identify the source of data. A data subject would still be able to access or correct data that would not prejudice those purposes.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

Law firms and other external processing agents, if they process data on behalf of another person and not for their own purposes, are regarded as data processors. This is usually the case when law firms and other agents are engaged to provide services in the context of an investigation.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Under the PDPO, unless an exemption applies, personal data cannot be transferred to another person for a new purpose unless the consent of the data subject has been obtained. A new purpose means any purpose other than that for which the data was to be used at the time of its collection or one directly related to that purpose.

If personal data disclosed to a third party is materially inaccurate, all practicable steps must be taken to ensure that the third party is informed that the data is inaccurate and is provided with enough information to rectify the inaccuracy. See also question 13. The right to conduct the transfer remains.

As to the use by a data user of third-party data processors to process data on its behalf, see question 9.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

There is currently no restriction on the cross-border transfer of personal data over and above those in place for transfers of personal data within Hong Kong.

A provision has been enacted that would place extra restrictions on cross-border transfers (section 33 of the PDPO), but it has not yet been brought into force. Were it in force, data users would be prohibited from transferring data to a place outside of Hong Kong unless:

- the data user has reasonable grounds for believing that there is in force in that place any law that is substantially similar to, or serves the same purposes as, the PDPO;
- the data subject has consented to the transfer in writing;
- the data user has reasonable grounds to believe that the transfer is for the avoidance or mitigation of adverse action against the data subject, where it is not practicable to obtain consent but if it was practicable to obtain such consent, the data subject would give it; or
- the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if the place were Hong Kong, would be a contravention of a requirement under the PDPO.

Section 33 also contains certain exemptions to the cross-border transfer restrictions, such as for certain transfers for the purposes of preventing and investigating crime.

The transfer restrictions will not apply to transfers to jurisdictions set out by the PCPD in a notice published in the Gazette, or jurisdictions where the data user has reason to believe an equivalent law to the PDPO is in force. As at the date of this survey, there is no indication yet which jurisdictions these would be.

In May 2017, the government put before the Legislative Council preliminary findings of a business impact assessment on the implementation of section 33. As at the date of this survey, no timetable of its implementation has yet been set by the authorities.

Large corporations and financial institutions in Hong Kong tend to follow section 33 as if it were in force as a precautionary measure; the HKMA advises in SA-2 that AIs take account of section 33 and the potential impact on their plans for overseas outsourcing. Moreover, PCPD also actively promotes GDPR compliance for Hong Kong businesses when handling cross-border data transfer. The PCPD is still in the process of assessing the impact of section 33, were it in force, on businesses, and will formulate the steps forward, to bring the section in effect.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

Any transfer of personal data to regulators within Hong Kong must comply with the principles set out in the PDPO (see question 7) including, for example, that personal data shall not be used for a purpose other than that notified to the data subject.

There are, however, exemptions to the general prohibition (Principle 3) under the PDPO, including:

- where the data is used for, among other things, the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, dishonesty, or malpractice, or discharging certain functions of a financial regulator; and not disclosing the data would be likely to prejudice such purposes; or
- the disclosure is required by a law in Hong Kong.

It is, therefore, often the case that disclosure of personal data to Hong Kong regulators as part of an investigation falls within the exception to Principle 3.

For example, the Securities and Futures Commission may, during the course of an investigation and under the Securities and Futures Ordinance, issue to a bank a notice to produce certain records or documents that may contain a customer's account information. Disclosure of personal data by the bank pursuant to the notice would fall under the second exception above. Another example worth noting is the enforcement powers under the Hong Kong National Security Law (the HKNSL), which came into effect on 30 June 2020. Under the HKNSL, for the purpose of assisting an investigation into an offence endangering national security or the proceeds obtained with the commission of the relevant offence, the Secretary for Justice or police officers may apply to the court for an order to require a person or corporation that has the required information to answer questions within a specified time period, or to furnish or produce the relevant information or material (article 43(7) of the HKNSL and Schedule

7 to the Implementation Rules for article 43 of the HKNSL). It is conceivable that a corporation may be asked, pursuant to such powers, to disclose personal data for HKNSL investigations.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

Any transfer of personal data to regulators outside Hong Kong must comply with the principles in the PDPO (see question 7). As there is currently no legislative provision applying to cross-border data transfers, there are no additional restrictions relating to the transfer of data to a regulator in another jurisdiction.

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

Data users should be cautious when handling requests for disclosure from a regulator. By way of example, a bank was criticised by the PCPD for providing personal data of a police officer to the police for its internal disciplinary investigation, without the consent of the officer and without questioning the nature and purpose of the request. The PCPD considered that there was simply insufficient information available to satisfy the PCPD that the situation was serious enough to fall under the "seriously improper conduct" exception under the PDPO, hence the bank's disclosure was unjustified and in breach of data protection principles.

Faced with such requests, the data user should consider:

- the purpose for which the data is required;
- whether the data user has obtained adequate consent from the data subject, and if not, whether it could now do so, provided that seeking consent now would not breach any other law;
- whether the personal data requested can be obtained from other sources;
- how the lack of such data may prejudice the purpose of obtaining the data; and
- whether the request to provide the data was made subject to legal compulsion under Hong Kong law.

20 What are the sanctions and penalties for non-compliance with data protection laws?

Contravention of the requirements relating to the use, or provision to third parties for their use, of personal data for direct marketing constitutes one or more criminal offences. In addition, a criminal offence is committed if any person discloses personal data obtained from a data user without the data user's consent with the intent to profit financially or cause loss to the data subject, or if the disclosure causes psychological harm to the data subject. The maximum penalty for each offence is a fine of HK$1 million and imprisonment for up to five years.

The PCPD can conduct its own investigations, regardless of whether a complaint is received, about suspected breaches of the PDPO. If the PCPD, following completion of an investigation, finds that the relevant data user has contravened a requirement under the PDPO, the PCPD may issue an enforcement notice requiring the data user to remedy the contravention. Non-compliance with the notice is a criminal offence. On first conviction, the maximum penalty is a fine of HK$50,000 and imprisonment for two years, and a daily fine of HK$1,000 if the offence continues after conviction. The Paper contains proposal conferring powers on the PCPD to directly impose administrative fines for contravention of the PDPO instead of having to first issue an enforcement notice. In addition, the Paper proposes an increase in the level of fines that may be imposed for criminal liability, and linking the level of fines to the annual turnover of the data user.

If section 33 of the PDPO comes into operation, a failure to comply with the restrictions on cross-border transfer will constitute a criminal offence carrying a maximum penalty of a fine of HK$10,000. If an offence is committed by a body corporate with the consent, connivance or negligence of any director, manager, secretary or similar officer of the body corporate, that person will be considered equally guilty of the offence under the PDPO.

A data subject who suffers damage or distress in addition to damage through a breach of the PDPO by a data user may seek compensation from the data user. Compensation is awarded by the courts and not the PCPD.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

In addition to those obligations mentioned in question 15, as a matter of good practice, the PCPD further recommends the following:

- it should be made plain to data subjects when collecting their personal data that their data may be processed by data processors;
- proper records of all personal data transferred for processing should be kept; and
- inspections should be made by the data user to establish how the processor handles and stores personal data (this should be provided for in the contract).

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

Any intervening data users are obliged to observe and comply with the requirements of PDPO. Their obligations are therefore the same as the original data users.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

The website of the PCPD: https://www.pcpd.org.hk

Guidance notes issued by the PCPD: https://www.pcpd.org.hk/english/resources_centre/publications/guidance/guidance.html

Decisions of the Administrative Appeals Board: https://www.pcpd.org.hk/english/enforcement/decisions/decisions.html

Matt Bower

Allen & Overy LLP

Matt Bower is a partner in Allen & Overy's litigation and dispute resolution department. Matt advises investments banks, financial institutions and other clients in High Court litigation in England and Wales and Hong Kong and regulatory investigations. He has particular experience of disputes arising from derivative, syndicated loan and asset management complaints and extensive trial experience, having acted among other matters for six former non-executive directors of Equitable Life in defending one of the largest claims ever brought before the English Commercial Court against individual directors. Matt has advised on benchmark investigations across Asia Pacific, liaising with financial services and competition regulators throughout the region. He advises financial institutions on self-reporting obligations and the prospects of regulatory sanction.

Clement Sung

Allen & Overy LLP

Clement Sung is an associate in the dispute resolution practice in Allen & Overy's Hong Kong office. He has ample experience in debt recovery actions and general commercial litigations. Clement has also advised on various investigations initiated by the Hong Kong Competition Commission and the Office of the Privacy Commissioner. These clients include social media companies, financial institutions, manufacturers and other international conglomerates.

Clement is fluent in Mandarin, Cantonese and English.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy (Hong Kong)
9th Floor
Three Exchange Square
Central
Hong Kong
China and Hong Kong
Tel: +852 2974 7000

www.allenovery.com

Matt Bower
matt.bower@allenovery.com

Clement Sung
clement.sung@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Italy

Livio Bossotto
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

Together with the GDPR, Legislative Decree 196/2003 (the Privacy Code), as lastly amended by Legislative Decree 101/2018, constitutes the main source of the data protection regime in Italy. Among other things, the Privacy Code implements derogations and sets out specific provisions as permitted by the GDPR.

The Garante per la protezione dei dati personali (the Garante) is the regulator responsible for enforcing the GDPR, the Privacy Code and all the other data protection provisions.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Confidentiality

Under Italian law, a duty of confidentiality may arise from:

- specific confidentiality agreements;
- specific legislations, such as those governing industrial secrets; and
- principles of Italian contract law, such as the fairness principle in the execution of a contract or, according to a divergent opinion, the general principle of good faith in the performance of a contract.

Banking confidentiality

Italian laws do not contain specific provisions on bank confidentiality. However, there is a strict banks' general duty of confidentiality towards their clients in relation to the safeguarding and protection of any customer data.

It is an implied term of the contract between a bank and its client that the bank will not divulge any confidential information about its client to any third party. This duty of confidentiality arises as a result of the bank-client relationship and it applies to all Italian banks, including Italian branches of foreign banks.

This duty of confidentiality arises from:

- customary market practice and usage;
- specific confidentiality agreements in force between the bank and its client;
- specific legislations, such as those governing industrial secrets; and
- principles of Italian contract law, such as the fairness principle in the execution of a contract or, according to a divergent opinion, the general principle of good faith in the performance of a contract.

Consequently, a restriction on data disclosure is an implied term in the contract between a bank and its client. Such restriction will apply to any bank with a (pre-)contractual relationship with a client, where such relationship is governed by Italian law. Nonetheless, there are exceptions to such duty of confidentiality, as in the case where a client has consented to such disclosure, the bank has to communicate such data to public entities to comply with specific legal obligations or the bank needs to use such information to exercise a right before a court.

Legal professional privilege

Under Italian law, there is a legal professional privilege between a lawyer and his client concerning the information provided by the client or acknowledged in the course of the lawyer's mandate.

Once established, legal professional privilege is a substantive right to withhold disclosure of privileged documents and to prevent the lawyer from testifying on information acknowledged in the course of his mandate and/or during the preliminary activities before the official mandate. Italian law also provides for specific safeguards in the event of searches and seizure of documents in the lawyer's premises, or interceptions concerning the object of the mandate.

Law on whistleblowing

Under Italian law, an employer that establishes a whistleblowing system must ensure that the identity of the whistleblower is kept confidential. The identity of the whistleblower must not be disclosed during the investigations, unless s/he has previously agreed to the disclosure or, according to court judgments, unless the disclosure is essential to ensure the right of defence of the person subject to the investigation.

Other

There are other laws and regulations relating to the sharing of data and cooperation between judiciary authorities in a criminal context, which may be relevant for the purposes of an investigation depending on the specific context.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines personal data as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data could re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not cover legal persons or deceased natural persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to data controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (as per articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply, unless such application would jeopardise the investigations or it is expressly excluded by a provision of law, and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. The Privacy Code, in turn, sets out specific provisions applying to the processing of certain special categories of data (eg, genetic and biometric data) or certain processing purposes (eg, the processing is necessary for reasons of substantial public interest). In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law.

Furthermore, article 2-octies of the Privacy Code states that criminal data may not be processed otherwise than under the supervision of a public authority except where:

- there is a legal basis under article 6 GDPR; and
- such processing is authorised by a provision of law or, when provided by the law, or regulation providing for adequate safeguards for data subjects' rights and freedoms.

In the absence of such provision, the Minister of Justice may issue a decree identifying the cases in which processing of criminal data is allowed.

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");
- Principle 5: personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Finally, the Garante set out a Code of Conduct for private investigations, including those performed by lawyers in the context of judicial proceedings, and Guidelines on the processing of special category of data by private investigators. Both of such sources, where applicable, may include more specific data processing provisions and instructions.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

While there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate "explicit" consent (eg, a wet ink signature or a tick box that expressly uses the word "consent").

Consent can be obtained through a website or other electronic means.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right that it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Article 119 of the Italian Bank Consolidated Act provides that the client, his or her successor and the person who takes over the management of the client's activity have the right to obtain, at their own expenses, within a reasonable time period and, in any case, no later than 90 days, copy of the documentation concerning single bank operation undertaken in the past 10 years.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or

if the processing is necessary within legal proceedings. A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

The rights set out by articles 15–22 of the GDPR are also applicable to deceased persons' data may be exercised by anyone that has an interest, acts on the data subject's behalf as his or her representative or for family reasons deserving protection (article 2-terdecies of the Privacy Code).

The Privacy Code also provides for specific limitations to the above-mentioned GDPR rights.

A Article 2-undecies of the Privacy Code provides that these rights may not be exercised by the data subject to the extent that the exercise may result in a concrete and effective prejudice to:

- the interests protected by the provisions regarding anti-money laundering;
- the interests protected by the provisions regarding support for victims of extortion;
- the activities of Parliamentary committees of inquiry;
- the activities carried out by a public entity, different from public economic bodies, pursuant to a specific law provision, for the only purposes regarding the monetary and currency policy, the payment system, the control of brokers and of the credit and financial markets, the protection of stability;
- the carrying out of defensive investigations or the exercise of a right before a court;
- the confidentiality of the identity of the whistleblower; and
- the interests protected by the provisions regarding tax evasion.

B Article 2-duodecies of the Privacy Code provides that the restriction of the rights provided for by articles 12-22 and 34 of the GDPR may occur also in case of processing for justice purposes.

In both the aforementioned situations under A and B, such rights are exercised pursuant to the related provisions of the applicable laws and regulations.

The exercise of the said rights may, under the circumstances described above, be postponed, limited or excluded by the controller through a reasoned communication provided to the data subject without delay, unless such communication undermines the aims of the limitation and as far as it constitutes a necessary and proportionate measure for the protection of the interests safeguarded by the above-mentioned set of laws.

The data subject may in any case exercise his rights by seeking a Garante's assessment or inspection. The data subject must be informed of such possibility by the data controller (eg, through the reasoned communication by which it informs the data subject of the limitation to his or her rights).

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

The National Lawyers' Council suggests that law firms are generally characterised as controllers in their own right. This is on the ground that responsibility also lies with the law firm itself as it determines what information to obtain and process in order to perform its work and because it is answerable itself for the content.

A legal process outsourcing firm is likely to be considered as a third-party processor in relation to the processing of personal data relating to its clients. This means that the conditions set out at question 9 must be complied with when contracting with a legal process outsourcing firm for the review of documents containing personal data.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Disclosure of employees' data

Article 4 of Law No. 300/1970 on remote monitoring of employees sets out some additional requirements as regards disclosure of employees' data to third parties. In particular, article 4 of Law No. 300/1970 provides that it is generally forbidden for the employer to install or implement devices or software for the exclusive purpose of remotely monitoring employees' activity at work. Accordingly, the employer may install the devices or software required only for productive or organisational needs and only upon reaching an agreement with local work councils or obtaining an authorisation with the local Labour Office, given the fact that such kinds of activities may result in employees' remote monitoring.

However, recent amendments to article 4 of Law No. 300/1970 specified that no agreement or authorisation is required with regard to devices or machinery used by employees to perform their duties as long as the main aim of the controls is not to monitor employees' activities and provided that the requirements set out by the data protection legislation are met. In this respect, article 4 of Law No. 300/1970 requires the employer to adequately inform its employees on the use of electronic devices and their business email account and on how their personal data is stored and processed through the privacy notice.

Furthermore, Garante provides that monitoring of employees' email, instant messaging and internet records can be performed only:

- incidentally and not on a continuous basis;
- if the checks are reduced to the minimum needed; and
- following the delivery of the privacy notice referred to above.

There is some Italian case law suggesting that monitoring employees' emails can be lawfully performed by an employer where it has suspicion or notice of 'misbehaviour' by an employee. However, the investigatory actions performed should be reduced to the minimum needed to establish the relevant facts.

Other

The European Banking Authority issued guidelines on outsourcing arrangements that set out a series of recommendations that providers of financial services must adhere to in respect of any outsourcing to the cloud, including in respect of the security of data, where geographically data is located and processed and the importance of contingency planning.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;

- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

While there is no specific exemption to the data transfer rules in the GDPR for transfer to a regulator or an enforcement authority within the jurisdiction, there are a number of possible exemptions and conditions that may be used for a transfer to regulators and enforcement authorities in the jurisdiction. These include where the disclosure is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

This article provides that, without prejudice to other grounds for international transfers, a decision from a third country authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country.

This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: "In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement."

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, among others:

- Consider if there is a legal obligation to respond to the request and, if so, to what extent.
- Seek further information in writing from the requesting regulator to evaluate the purpose of the request.
- If possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation.
- In accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose.
- Consider whether it is practicable to obtain data subject consent and/or give a further privacy notice.
- Put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor).
- Consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

The Privacy Code also extends the administrative fines provided by the GDPR to a series of infringements of its provisions (eg, provisions concerning the processing of data related to criminal convictions and offences or concerning the rights of deceased people).

Furthermore, there are a number of criminal offences under the Privacy Code (eg, making false statements or submitting false documents during proceedings or investigations before the Garante). The maximum penalty for criminal offences under the Privacy Code corresponds to six years of imprisonment.

Article 2-decies of the Privacy Code also establishes that data processed in violation of data protection legislation must not be further processed, except in the case where such processing occurs in the context of judicial proceedings. The processing and the usability of the related information in the latter hypothesis is regulated by the provisions of civil procedure. The Garante is responsible for enforcing the GDPR and the Privacy Code, but in certain circumstances enforcement is conducted through the courts (eg, under article 79(1) of the GDPR, data subjects have a right to an "effective judicial remedy" where they consider their rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR).

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement or data transfer agreement, or both, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside the EEA), including any transfer to a regulator or law enforcement authority; and
- maintaining a record of processing and responding to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening data controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Lawyers' Code of Professional Conduct
https://www.consiglionazionaleforense.it/web/cnf/codice-deontologico-forense

Bank Consolidated Act
https://www.bancaditalia.it/compiti/vigilanza/intermediari/Testo-Unico-Bancario.pdf

National Lawyers' Councils guidelines on GDPR
https://www.consiglionazionaleforense.it/documents/20182/445621/IL+GDPR+E+L%27AVVOCATO/ef231b75-2066-43df-8d88-570bf0ea98b3

European Banking Authority's Guidelines on Outsourcing Arrangements
https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

The Garante's Code of Conduct for Private Investigations
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069653

The Garante's Guidelines on the Processing of Special Category of Data by Private Investigators
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5803458

Livio Bossotto

Allen & Overy LLP

Livio heads the Italian employment and benefits and data protection team. He is specialised in both employment law and data protection law, advising major corporates and financial institutions on both employment-related contentious and non-contentious matters as well as on data protection matters, with a particular focus on companies' internal compliance. Livio has extensive experience in Italy and abroad on cross-border matters, multi-jurisdictional data transfers as well as due diligence activities, private equity deals, joint ventures and commercial agreements. He is a member of the European Lawyers Association (EELA), the International Bar Association (IBA) and the Italian Employment Lawyers Association (AGI). Livio has been awarded "Labour Lawyer of the Year - Rising Star 2016" at the annual Italian Legalcommunity Labour Awards. "He is always very good at finding a solution to any problem we bring to his attention." *Chambers Europe* 2018 (Employment & Benefits: Italy).

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy Studio Legale Associato
Via Manzoni 41
Milan
20121
Italy
Tel: +39 02 290 491

www.allenovery.com

Livio Bossotto
livio.bossotto@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Luxembourg

Catherine Di Lorenzo, Thomas Berger and Paul Wagner
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Banking and insurance secrecy

Under the Luxembourg Act dated 5 April 1993 relating to the financial sector, as amended (known as the Banking Law), those subject to the supervision of the Luxembourg Supervisory authority of the financial sector (the Commission de Surveillance du Secteur Financier, or the CSSF) pursuant to the Banking Law are prohibited from disclosing any information entrusted to them in the course of their professional duties to any third parties. This applies to credit institutions and other professionals in the financial sector (also known as PFS) in addition to members of their management, directors and their employees. Banking secrecy also applies to the Luxembourg branches of overseas banks.

All client data is protected by banking secrecy, irrespective of whether the client is an individual, a company, a government body or otherwise.

There are a number of exceptions to banking secrecy. Exceptions to banking secrecy include when:

- the disclosure is authorised by law, for example, under the Banking Law (as well as any law that predates the Banking Law); or
- the disclosure is made with the client's consent or its specific instruction (in a note dated 1 March 2004 issued by the CSSF's lawyers committee (the CODEJU) (annexed to the CSSF's 2003 annual report), the CODEJU describes the conditions under which a client's consent to a transfer of his or her client data may result in such transfer without violating banking secrecy as set out in the Banking Law. Please note that this concept has not yet been tested in court. Since 2018, the Banking law expressly provides for the possibility to rely on client's consent in an outsourcing context subject to certain conditions (see below).

In particular, information covered by banking secrecy may be disclosed to:

- shareholders or partners whose status or capacity is a precondition for authorisation of the financial institution in question, insofar as this is necessary for the proper and prudent management of the institution, the risk assessment on a consolidated basis or the calculation of prudential ratios on a consolidated basis;
- internal control bodies of companies forming part of the same group of companies as the credit institution or PFS may have access to information regarding specific business relations with clients, to the extent that this is needed for the global management of legal risks and risks to their reputation in connection with money laundering or the financing of terrorism (within the meaning of the law of 12 November 2004 on the fight against money laundering and terrorism financing);
- companies forming part of the same financial conglomerate as the credit institution or PFS for information that these entities may exchange between them insofar as the information is necessary for the exercise of supplementary supervision of a financial conglomerate under the Banking Law;
- the CSSF, foreign or European regulators responsible for prudential supervision of the financial sector;
- any person established in Luxembourg, subject to the prudential supervision of the Commission de Surveillance du Secteur Financier (the CSSF), the European Central Bank (the ECB) or the Commissariat aux Assurances (the CAA) and which is bound by a criminally sanctioned professional secrecy obligation, insofar as the information communicated to those professionals is provided under an agreement for the provision of services; or
- service providers providing services to the credit institution/PFS in the context of an outsourcing arrangement provided that the client has accepted the outsourcing of services, the type of information to be transmitted in the framework of the outsourcing and the country of establishment of the service provider and provided that the service provider having access to confidential information is subject by law to professional secrecy or bound by a confidentiality agreement.

In accordance with articles 7 and following of the Law of 7 December 2015 on the insurance sector, those subject to the prudential supervision of the CAA or a foreign supervisory authority for the exercise of an activity covered by that law, including insurance and reinsurance undertakings and pension funds, are subject to insurance secrecy.The requirements on insurance secrecy largely mimic those on banking secrecy, including their exceptions (mutatis mutandis).

A breach of banking or insurance secrecy is subject to an imprisonment from eight days to six months and a fine of €500 to €5,000 and may lead to administrative sanctions.

The answers to the questions below are subject to the above developments regarding banking and insurance secrecy and an analysis of whether these secrecy requirements may affect each of the responses must be made.

General professional secrecy

Article 458 of the Luxembourg Criminal Code is the general basis for professional secrecy in Luxembourg. It provides that doctors, surgeons, health officers, pharmacists, midwives and all other persons who are custodians, by state or by profession, of the secrets entrusted to them, and who, except in cases where they are called upon to testify in court and where the law obliges them to make these secrets known, have revealed them, shall be punished by imprisonment from eight days to six months and a fine of between €500 and €5,000.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines "personal data" as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data could re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not cover legal persons or deceased natural persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (as per articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision-making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under Article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law.

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");
- Principle 5: personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

Although there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate “explicit” consent (eg, a wet ink signature or a tick box that expressly uses the word “consent”).

Consent can be obtained through a website or other electronic means.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right that it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or if the processing is necessary within legal proceedings. A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

Although it is not considered a special category of data under the DP Act, personal data collected by any activity that, carried out using technical means, consists of observing, collecting or recording the personal data of one or more individuals concerning their behaviour, movements, communications or the use of electronic equipment is subject to heightened restrictions. Personal data collected on employees in the course of their employment, such as e-mails, internet usage, log files on systems and documents accessed, access badges and CCTV data, could be considered monitoring data.

Specifically, in the employment context, the processing of such data is subject to additional compliance steps.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

No.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;

- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

This article provides that, without prejudice to other grounds for international transfers, a decision from a third-country authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country. This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: "In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement."

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, amongst others:

- Consider if there is a legal obligation to respond to the request and, if so, to what extent.
- Seek further information in writing from the requesting regulator to evaluate the purpose of the request.
- If possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation.
- In accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose.
- Consider whether it is practicable to obtain data subject consent and/or give a further privacy notice.
- Put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor).
- Consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside the EEA), including any transfer to a regulator or law enforcement authority; and
- maintaining a record of processing and responding to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Catherine Di Lorenzo

Allen & Overy LLP

Catherine specialises in information technology with a particular focus on data protection (ranging from advice on compliance steps or the use of mobile applications, cookies or similar techniques to assistance in case of investigations performed by the data protection authority), IT contracts and negotiations, e-commerce, advertising (including targeted advertising), media and telecommunications, intellectual property and regulatory issues (notably regarding IT outsourcing in the financial sector). She has been active in these areas in Luxembourg since 2006. In the past years, Catherine has also lectured IT law at the University of Luxembourg.

She is a member of APDL (the Luxembourg association for data protection), FedISA (the Luxembourg chapter of an international electronic archiving community) and ITechLaw. Catherine is also a member of Fedil ICT (the Luxembourg industry federation and local chapter of BusinessEurope), IAPP (International Association of Privacy Professionals) and Girls in Tech Luxembourg. She participated in the preparation of a position paper and amendment suggestions on the draft EU data protection regulation as well as in a presentation on net neutrality made to a delegation of the Luxembourg Parliament. Catherine has been on secondment twice with a major e-commerce company where she mainly worked on general commercial and data protection aspects.

Catherine is a member of the Data Protection Forum, the ICT Forum, and of the Trust and Cybersecurity Forum of the Luxembourg Bankers' Association (ABBL).

She is also an active member of our FinTech task force, supporting clients from established financial institutions, incumbents and start-ups in developing innovative products.

Thomas Berger

Allen & Overy LLP

Thomas heads the litigation department. He specialises in domestic and cross-border litigation and pre-litigation matters within the realm of civil, commercial and corporate law. He has a particular focus in banking law, including on professional liability in the financial sector, finance litigation, money laundering, "white-collar" criminal law aspects, etc. He also assists clients facing dawn raids. Thomas also specialises in regulatory matters involving professionals of the financial sector. In this context, he regularly advises on issues related to AML, PSD, MIFiD and banking secrecy.

Thomas is a member of the Legal Forum, the Payment Forum, the MiFID Forum and the Payment Services Directive II working group of the Luxembourg Bankers' Association (ABBL).

He is also an active member of our FinTech task force, supporting clients from established financial institutions, incumbents and start-ups in developing innovative products.

Paul Wagner

Allen & Overy LLP

Paul Wagner, associate, is a member of the IP/IT practice and advises on IP, IT and data protection matters. Paul specialises in data protection with a focus on internet-related topics, including online advertising, cookies, and connected devices. He further advises clients on data protection and privacy matters at the workplace, such as IT monitoring, data access, video surveillance and employee authentication measures.

Paul has experience in both contentious and non-contentious matters. He has notably assisted clients in defending them against trademark infringement actions and investigations from data protection authorities. Complementary to the IP and IT practice, Paul also advises on Luxembourg contractual law and other general civil law-related matters.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy
33 avenue J.F. Kennedy
L-1855 Luxembourg
PO Box 5017
L-1050
Luxembourg
Tel: +352 44 44 55 1

www.allenovery.com

Catherine Di Lorenzo
catherine.dilorenzo@allenovery.com

Thomas Berger
thomas.berger@allenovery.com

Paul Wagner
paul.wagner@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Poland

Justyna Ostrowska and
Krystyna Szczepanowska-Kozłowska
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

In relation to the GDPR, the new Act on Personal Data Protection of 10 May 2018 (New PPDA) entered into force on 25 May 2018, which, among other things, establishes a new authority competent for the data protection in Poland (ie, the President of the Office for Personal Data Protection).

On 4 May 2019, supplementary legislation amending a number of Polish laws to ensure the application of GDPR, including the Labour Code, the Banking Law and insurance regulations, entered into force.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Banking secrecy

The Polish banking law of 29 August 1997 (the Banking Secrecy Law) prevents banks from disclosing bank secrecy information to a separate entity. Bank secrecy information includes all information concerning banking operations and other parties to the contract concluded with the bank, obtained in the course of negotiations or during the conclusion and performance of the contracts on the basis of which the bank performs its operations. It is not only banks that are bound by the obligation of banking secrecy, it also covers bank employees and anyone through whom the bank performs banking acts.

There are some exceptions that allow the information covered by banking secrecy to be disclosed to third parties, in particular:

- where the client has consented in writing to the transfer of specific information to specified entities;
- where information is provided to the counterparty of any outsourcing agreement, to the extent necessary to perform that outsourcing agreement; and
- disclosure of information covered by banking secrecy to qualified lawyers.

Blanket authorisation is not permissible. The Banking Secrecy Law can still apply if there are already copies of the data outside Poland.

A similar obligation of secrecy applies to insurance undertakings, investment firms, pension societies, management companies, payment institutions and electronic money institutions as well as individuals obtaining information in connection with the provision of financial services.

Telecommunication secrecy

The Telecommunication Act of 16 July 2004 also limits access to and processing of information subject to telecommunication secrecy, such as: personal data of user, location data, transmission data and the content of sent messages.

Classified information

Additional limitations also apply to sharing of information that is classified as confidential under the Classified Information Act of 5 August 2010, which applies not only to governmental authorities, state legal persons and state organisational units but also covers entrepreneurs wishing to apply for or enter into contracts for access to classified information or performing such contracts, or performing tasks related to access to classified information under the law.

Other

There are other laws and regulations relating to the sharing of data in a criminal context, which may be relevant for the purposes of an investigation depending on the specific context. These include the Act of 14 December 2018 (as amended in 2019) on the protection of personal data in connection with the prevention and combating crime and the Code of Criminal Proceedings.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines personal data as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be “personal data” for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data could re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not cover legal persons or deceased natural persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under Article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or

- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law.

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");
- Principle 5: personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

While there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate “explicit” consent (eg, a wet ink signature or a tick box that expressly uses the word “consent”).

Consent can be obtained through a website or other electronic means.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right which it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or if the processing is necessary within legal proceedings.

A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Note that where data is processed by the controller performing a public task, pursuant to articles 3-5 of the New PPDA certain rights of data subjects are excluded or restricted. For example, data subjects have no right to object to processing by a controller for this purpose. Moreover, data subjects' rights to receive information, rights of access, rights to rectification and rights to erasure or restriction may be limited or restricted where necessary and proportionate, if the provision of such information renders impossible or seriously impairs the proper performance of a public task or undermines the protection of non-public information.

In addition, the controller that obtained personal data from a subject performing a public task have to refrain from performing the obligations referred to in article 15(1) to article 15(3) of GDPR, in the case where the subject transferring the personal data made a demand in this scope due to necessity to correctly perform the public task aimed at:

1 preventing crime, detection or prosecution of torts or enforcing penalties, including protection against hazards to public safety and preventing such hazards;

2 protecting economic and financial interests of a state covering in particular:
- collection and pursuing tax proceeds, proceeds from fees, non-tax budgetary dues as well as other dues;
- enforcement of administrative execution of receivables and execution of security of cash and non-cash receivables;
- prevention of using banks' and financial institutions' activities for purposes involving fiscal frauds;
- disclosing and recovery of the property threatened by forfeiture as a result of offences;
- conducting inspections, including customs and revenue inspections.

Finally, the competent authorities processing personal data for criminal law enforcement purposes must adhere to slightly different requirements under Part 4 of the Act of 14 December 2018 (as amended in 2019) on the protection of personal data in connection with the prevention and combating crime. For example, with regards to Principle 1 (transparency of the processing),

these authorities are entitled to limit or restrict the data subjects' rights to receive information, rights of access, rights to rectification and rights to erasure or restriction where necessary and proportionate in order to, for example, protect national or public security, or avoid prejudicing a criminal investigation or prosecution.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

Law firms are generally characterised as data controllers.

In certain circumstances legal process outsourcing firms may act as data processors depending on their independency in determining the purposes and means of data processing.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

The Labour Code of 10 June 1974 (Labour Code) introduces restrictions with respect to email correspondence monitoring conducted by the employers. Monitoring of email company accounts may be introduced when it is necessary to ensure proper use of the working hours by an employee and proper use of equipment provided to the employee. However, such monitoring cannot infringe the secrecy of correspondence and the personal rights of the employees (such as privacy). For this reason, review of the content of such email correspondence by the employer and disclosure of such information to third parties may be difficult in practice.

Under the Labour Code, the employer is obliged to regulate the purposes, scope and the method of use of the monitoring of email correspondence in collective agreements with trade unions or in the internal workplace policies. The above rules should be described in a notice addressed to the employees if there is no collective agreement or the employer is exempted from the obligation to set workplace regulations. The above information has to be provided in writing to each employee before the employee starts work. The employer is also obliged to inform employees on the actual introduction of the email correspondence surveillance within two weeks before the launch of such monitoring.

The above obligations are without prejudice to the obligations regarding data subjects' rights set forth in articles 12 and 13 of the GDPR.

Certain additional requirements have been set by the Polish courts and the former data protection authority (General Inspector for Personal Data Protection) for such monitoring to be lawful:

- the monitoring must be proportionate (ie, if there are less restrictive means enabling the employer to accomplish the same objective, such less restrictive means should be used instead);
- the employer should have clear evidence of the employees having fully read and understood the policy with regards to possible monitoring; and
- the monitoring must respect employees' dignity. It would be hard to justify a review of emails marked as 'personal' and which are obviously personal in nature as this may be regarded as not respecting the employee's dignity and right to privacy. Respecting the personal rights of workers is a basic obligation of the employer.

These rules remain valid also under the GDPR.

Financial institutions in Poland must also comply with, among other requirements:

- the guidelines on material outsourcing, the guidelines concerning the management of information technology and ICT environment security and communication of 23 January 2020 concerning the processing of information by supervised entities in a public or hybrid cloud, established by the Polish Financial Supervision Authority (UKNF). These principles require financial institutions to take various measures to protect client and employee data.
- the guidelines on material outsourcing established by the European Banking Authority (EBA). The EBA's guidelines (which will apply from 30 September 2019) set out a series of recommendations that providers of financial services must adhere to in respect of any outsourcing to the cloud, including in respect of the security of data, where geographically data is located and processed and the importance of contingency planning.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

This article provides that, without prejudice to other grounds for international transfers, a decision from a third country authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country.

This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: “In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.”

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, among others:

- Consider if there is a legal obligation to respond to the request and, if so, to what extent.
- Seek further information in writing from the requesting regulator to evaluate the purpose of the request.
- If possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation.

- In accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose.
- Consider whether it is practicable to obtain data subject consent and/or giving notice as it may be possible, in some cases, to obtain a valid consent from individuals to undertake a particular disclosure and transfer.
- Put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor).
- Consider transfer via domestic authority as, in some cases, it may be possible to request that the requesting regulator request data via a domestic regulator of the data controller.
- Consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

New PPDA provides for criminal sanctions for prohibited and unauthorised processing and for jeopardising or impeding an inspection by the supervisory authority.

A criminal fine, restriction of personal liberty or imprisonment of up to two years (three years if processing concerns specific categories of data) can be imposed on an individual as a result of unlawful data processing (ie, processing of personal data even though its processing is not admissible or without authorisation).

A criminal fine, restriction of personal liberty or imprisonment of up to two years may be also imposed on persons hindering inspection proceedings.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid; and
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside of the EEA), including any transfer to a regulator or law enforcement authority; and
- maintaining a record of processing and responding to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679):
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Justyna Ostrowska

Allen & Overy LLP

Justyna has many years of experience covering consultancy related to new technologies law, intellectual property rights and data protection, as well as electronic trade and international commercial contracts (including sponsorship deals, distribution, and agency and franchising agreements). Justyna represents clients in contentious cases carried out by the Polish Patent Office and Polish common courts, covering enforcement of the protection of intellectual property rights and fair competition principles, and coordinates intellectual property rights customs protection programmes. She assists clients (both service providers as well as end users) in managing the implementation of IT systems, outsourcing solutions and cloud projects, by negotiating agreements concerning services, maintenance, implementation and licensing for IT solutions. She also advises clients on the cross-border use of personal data in capital groups, processing personal data in electronic business, and conducts internal audits in this respect.

Krystyna Szczepanowska-Kozłowska

Allen & Overy LLP

Professor Krystyna Szczepanowska heads Warsaw's Litigation and Intellectual Property practice. She specialises in litigation, both in intellectual property law and in business and arbitration disputes, representing clients before the common courts and administrative courts. She also advises clients on non-contentious matters, especially in civil law, intellectual property and new technologies law. Moreover, professor Krystyna Szczepanowska-Kozłowska has been listed as an arbitrator of the Court of Arbitration at the Polish Chamber of Commerce since 2003 and has taken part in numerous international cases as counsel or arbitrator. Professor Krystyna Szczepanowska–Kozłowska is also a member of the Faculty of Law at the University of Warsaw where she heads the Department of Intellectual Property Law and Intangible Assets. She is the author of numerous academic publications.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

Allen & Overy, A. Pędzich sp. k.
Rondo ONZ 1
34 floor
Warsaw
00 - 124
Poland
Tel: +48 22 820 6100

www.allenovery.com

Justyna Ostrowska
justyna.ostrowska@allenovery.com

Krystyna Szczepanowska-Kozłowska
krystyna.szczepanowska-kozlowska@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Slovakia

Michal Porubsky and Zuzana Hečko
Allen & Overy Bratislava, s.r.o.

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The EU General Data Protection Regulation (2016/679) (the GDPR) is directly applicable in this jurisdiction.

Additionally, alongside GDPR, Act No. 18/2018 has been adopted, which provides further details regarding data processing for situations not captured by the GDPR. The Act also sets out further details that the GDPR left for EU member states to govern.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Regulations that may prevent data sharing in the context of an investigation are not specifically set out in the GDPR. The process described in questions 17 to 19 needs to be followed. Whether the data may be shared or not will depend on the circumstances of each individual case.

Bank secrecy

Financial institutions in Slovakia are subject to a duty of confidentiality.

Bank confidentiality is a statutory duty that a bank has towards its customers. Save for limited purposes set out under Act No. 483/2001 on Banks as amended (the Banking Act); client data can be transferred by a bank only with the client's prior written consent or upon an explicit written instruction by the client given for a specific purpose and within the terms and limits of such consent or instruction.

Similar rules apply to transfers of client data by other financial institutions. These rules are contained in specific legislation applicable to certain types of financial institutions, for example:

- the Securities and Investment Services Act (in respect of stock brokerage firms);
- the Payment Services Act (in respect of payment institutions and e-money institutions);
- the Insurance Act (in respect of insurance and reinsurance undertakings);
- the Collective Investment Act (in respect of collective investment undertakings); and
- the Pension Savings Act (in respect of pension fund managers).

The transfer restrictions under the Securities and Investment Services Act, the Payment Services Act and the Collective Investment Act also apply to foreign stock brokerage firms (MiFID investment firms), payment institutions and collective investment undertakings when carrying out their activities in the Slovak Republic on a cross-border basis.

The restrictions under these laws are broadly similar to the restriction in the Banking Act (subject to certain exceptions).

The confidentiality rules under these laws apply to all information about clients that is not publicly accessible. This includes information on balances or assets on customers' accounts and information on any transactions entered into with, or for, the customers.

In general, a financial institution is allowed to transfer client data without a client's written consent or instruction in certain circumstances, including where:

- the data is already publicly available and therefore not confidential;
- the transfer is necessary for proper provision of payment services and settlements through a designated legal person by a payment service provider;
- the transfer of the data is to the Slovakian authorities in certain circumstances;
- the transfer is in compliance with obligations under anti-money laundering or sanctions rules; or
- the transfer is in connection with litigation or court proceedings, or to obtain legal advice, if this is either in the interests of the bank or under compulsion by order of court, but only if the relevant dispute concerns the client or its assets.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines "personal data" as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data could re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not also cover legal persons or deceased natural persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (as per articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision-making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller; or

- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law.

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");
- Principle 5: personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

Although there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate “explicit” consent (eg, a wet ink signature or a tick box that expressly uses the word “consent”).

Consent can be obtained through a website or other electronic means.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right that it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or if the processing is necessary within legal proceedings. A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

No local guidance has been provided on this subject. The assessment will therefore have to be made separately for each case. Nevertheless, it appears that law firms do not set the purposes and means of data processing, hence it does not appear that they would have a position of a data controller. Our assessment is that they should have a role of a data processor.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Not applicable.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers; or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

While there is no specific exemption to the data transfer rules in the GDPR for transfer to a regulator or enforcement authority within the jurisdiction, there are a number of possible exemptions and conditions that may be used for a transfer to

regulators and enforcement authorities in the jurisdiction. These include where the disclosure is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

While there is no specific exemption to the data transfer rules in the GDPR for transfer to a regulator or enforcement authority within the jurisdiction, there are a number of possible exemptions and conditions that may be used for a transfer to regulators and enforcement authorities in the jurisdiction. These include where the disclosure is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

This article provides that, without prejudice to other grounds for international transfers, a decision from a third country authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country. This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: “In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.”

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, amongst others:

- Consider if there is a legal obligation to respond to the request and, if so, to what extent.
- Seek further information in writing from the requesting regulator to evaluate the purpose of the request.
- If possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation.

- In accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose.
- Consider whether it is practicable to obtain data subject consent and/or give a further privacy notice.
- Put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor).
- Consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside the EEA), including any transfer to a regulator or law enforcement authority; and
- maintaining a record of processing and responding to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Slovak Data Protection Authority: https://dataprotection.gov.sk/uoou/

FAQ published by the Slovak Data Protection Authority:

https://dataprotection.gov.sk/uoou/sk/main-content/metodiky-faq (in Slovak only)

The Slovak Data Protection Authority has published (very limited) information regarding cross-border data transfers, however, the guidance contains little added value compared with the wording of the GDPR itself.

https://dataprotection.gov.sk/uoou/sk/main-content/cezhranicny-prenos.

Michal Porubsky

Allen & Overy Bratislava, s.r.o.

Michal joined Allen & Overy Bratislava in 2012. Prior to the joining Allen & Overy Bratislava, Michal earned his LLB degree from the Queen Mary University of London in 2011 and his LLM degree from King's College London in 2012. He also earned a diploma in Chinese law from Tongji University, Shanghai, China in 2010. In parallel, Michal also earned his law degree at Pan-European University in Bratislava.

Michal specialises in data protection law, dispute resolution and white-collar crime. Michal regularly engages in corporate investigations, especially in the life sciences industry.

Zuzana Hečko

Allen & Overy Bratislava, s.r.o.

Zuzana Hečko specialises in protection of personal data and intellectual property law. She is a member of Allen & Overy global team for protection of personal data and a first vice-chair of the data protection working group in The American Chamber of Commerce in Slovakia.

Zuzana was seconded to privacy teams on a temporary basis in the following companies: Standard Chartered Bank Singapore, PayPal Europe (Luxembourg) and Fox International Channels.

Prior to the joining Allen & Overy Bratislava, Zuzana worked at the European Commission in Brussels and undertook traineeship in an international law firm in Hong Kong.

According to *Chambers Europe 2017* (Intellectual Property), Zuzana Hečko is widely appreciated by her clients and she is described as "very direct and honest, and she has a strong charisma and brings a lot of clarity and authority when negotiating". She is praised by another source as "extremely responsive and a pleasant conversational partner".

ALLEN & OVERY

As an international law firm, our overriding goal is to work alongside our clients as a trusted adviser, providing the support they need to thrive in this dynamic economic environment.

And as our clients have moved to maximise commercial opportunities in new markets, so have we. We continue to invest in a growing network of international offices that covers Europe, Asia Pacific, the Middle East, the Americas and most recently Africa. With 42 offices in 29 countries, our presence is amongst the largest of any legal practice. Nearly 70 per cent of our work involves Allen & Overy offices in two or more jurisdictions and more than 50 per cent involves at least three. These figures are a testament to our ability to provide seamless advice to clients on their most complex, multi-jurisdictional matters.

But our presence is only half of the story. Our 5,000 staff, including over 500 partners worldwide, work together in a highly integrated manner to leverage their expertise and experience for our clients' benefit. In a proud 80-year history, we've fostered creative, independent thinking within a collaborative culture, to ensure that outstanding things happen when the best minds work together. As a result, our lawyers are involved in many of the most influential commercial ventures and are known for providing clients with pioneering solutions to the toughest legal challenges. This, above all, explains why Allen & Overy remains a leader in its field.

Allen & Overy Bratislava, s.r.o.
Pribinova 4,
811 09 Bratislava,
Slovakia
Tel: +421 2 5920 2400
Fax: +421 2 5920 2424

www.allenovery.com

Michal Porubsky
michal.porubsky@allenovery.com

Zuzana Hečko
zuzana.hecko@allenovery.com

GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

United Kingdom

Nigel Parker, Calum Burnett,
Benjamin Scrace and Jason Rix
Allen & Overy LLP

NOVEMBER 2020

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The UK formally withdrew from the EU on 31 January 2020. Under the European Union (Withdrawal) Act 2018 (as amended), the EU General Data Protection Regulation (2016/679) (the EU GDPR) remains directly applicable in the UK during the transition period and data transfers between the UK and EU are treated no differently to if the UK had not withdrawn from the EU. At the end of the transition period (which will end on 31 December 2020 unless extended), transfers between the EU and UK will be restricted in the absence of an agreement to the contrary.

The Political Declaration (setting out the framework for the future relationship between the EU and the UK dated 19 October 2019) envisaged that the European Commission would assess and (subject to certain conditions being satisfied) adopt an adequacy decision in relation to UK data protection by the end of the transition period. As at the date of this questionnaire, the European Commission has not yet published a decision in relation to the UK and it is uncertain whether an adequacy decision will be adopted by the end of the transition period.

The UK government has passed the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 to ensure that, following the transition period, the EU GDPR will be incorporated into UK law with certain changes to tailor provisions to the UK (the UK GDPR). The key principles, rights and obligations under the UK GDPR will broadly reflect those under the EU GDPR.

Together with the EU GDPR, the UK Data Protection Act 2018 (DPA) currently forms the data protection regime in the UK. Among other things, the DPA implements derogations and UK specific exemptions, as permitted by the EU GDPR. Following the transitional period, the UK GDPR will sit alongside the DPA. Throughout this guide, references to the GDPR shall refer to the EU GDPR as it currently applies in the UK.

The Information Commissioner's Office (the ICO) is the regulator responsible for enforcing the GDPR and the DPA in the UK.

As the status of the EU-UK adequacy decision is uncertain, this questionnaire deliberately does not address the UK data protection regime following the transition period (including in relation to international data transfers to and from the UK). The UK government and the ICO have published extensive guidance on what would happen in the event of a no-deal Brexit (in the absence of an adequacy decision). The most significant change is that the UK would be a "third country" for the purposes of the GDPR by virtue of it no longer being a member state of the EU. Therefore, a transfer of personal data from any country in the European Economic Area (EEA) to the UK would require the implementation of safeguards under the GDPR (unless a derogation applied in certain circumstances). Transfers from the UK to the EU would not be restricted.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Confidentiality

A duty of confidentiality may arise under the common law, which protects confidential information. In order for such a duty to arise:

- the information to be disclosed must have the "necessary quality of confidence" (i.e. it must not be something that is public knowledge); and
- it must have been disclosed in circumstances importing an obligation of confidence.

Generally, the person in possession of confidential information must not make use of it to the prejudice of the person who provided it, without obtaining their consent.

The confidentiality obligation can be breached by either unauthorised disclosure or unauthorised use of the confidential information.

Banking confidentiality

There is also a common law duty of confidentiality between a "banking business" and its clients. This implied duty means that a bank may not divulge confidential information about its client unless the client in question has consented or an exemption applies.

The meaning of a "banking business" relates to the business carried on by the entity instead of any regulated status. The three main factors that indicate a banking transaction are:

- keeping current accounts for customers, in which credits and debits are entered;
- accepting money from and collecting cheques for customers and placing them in credit; and
- paying cheques drawn on the relevant account and debiting customers accordingly.

The general duty of banking confidentiality can therefore apply to any business engaging in these activities, even if that institution does not consider itself to be a bank.

The implied duty applies to any information about a client (both natural and legal persons) that the bank acquires in the course of providing services.

Client consent to a transfer of confidential information should be informed but may be obtained via a website or standard terms and conditions.

Exemptions to the common law duty of banking confidentiality have been found in certain limited circumstances, including where:

- there is a compelling public interest reason for the disclosure;
- there is compulsion by law;
- the disclosure is under compulsion by order of court; or
- disclosure is necessary in the interests of the bank.

Legal professional privilege

There are two types of legal professional privilege under English law: legal advice privilege and litigation privilege. While neither acts to prevent the sharing of personal data, when considering whether confidential communications should be disclosed more generally it is important to consider whether privilege may arise.

Legal advice privilege applies to confidential communications that pass between a lawyer and his or her client and that have come into existence for the dominant purpose of giving and receiving legal advice about what should be prudently and sensibly done in the relevant legal context. The English courts have held that the "client" for the purposes of legal advice privilege is those individuals authorised to seek and receive legal advice. Litigation privilege applies to confidential communications between (i) a client and a lawyer, (ii) a lawyer and a third party, or (iii) a client and a third party, that were made for the dominant purpose of seeking or obtaining legal advice or evidence in connection with the conduct of (adversarial) litigation where that litigation was pending, reasonably in prospect or existing. In recent years there have been a number of decisions of the English Court of Appeal considering both legal advice and litigation privilege.

Once established, legal professional privilege is a substantive right to withhold disclosure of privileged documents from various third parties.

Other

There are other laws and regulations relating to the sharing of data in a criminal context, which may be relevant for the purposes of an investigation depending on the specific context. These include: the Proceeds of Crime Act 2002; the Crime (International Co-operation) Act 2003; Part 49 of the Criminal Procedure Rules 2015 (SI 2015/1490); the Criminal Justice (European Investigation Order) Regulations 2017; and the Crime (Overseas Production Orders) Act 2019.

3 What can constitute personal data for the purposes of data protection laws?

The GDPR defines personal data as any data relating to a living individual who can be identified directly or indirectly from that data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data that are truly anonymised will not be "personal data" for the purposes of the GDPR, as they do not identify the individual. Data are not truly anonymised if the data may re-identify the individuals to which the data relates by reasonably available means.

4 Does personal data protection relate only to natural persons or also legal persons?

Under the GDPR, personal data protection only extends to natural living persons. It does not cover legal persons or deceased natural persons.

5 To whom do data protection laws apply?

The direct obligations under the GDPR apply primarily to controllers. A controller is defined in the GDPR as a person who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data are processed.

However, the GDPR also imposes certain direct obligations on processors. A processor is defined in the GDPR as a person who processes personal data on behalf of the controller.

6 What acts or operations on personal data are regulated by data protection laws?

The GDPR applies to "processing", which is defined broadly and includes any activity in relation to personal data (whether or not by automated means). A number of examples are provided in the GDPR, including the collection, use, disclosure and destruction or erasure of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

A privacy notice should be provided to the data subject at the time the personal data is obtained (unless an exemption applies). In all circumstances, this must include (as per articles 13 and 14 of the GDPR):

- the identity and contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes and legal basis for the processing (including any legitimate interests relied upon where this is the legal basis for processing);
- the categories of personal data concerned;
- any recipients or categories of recipients of the personal data; and
- where applicable, the fact that the controller intends to transfer personal data to a third country, the existence (or absence) of an adequacy decision by the European Commission and, if there is no adequacy decision, the safeguards used for the transfer of that personal data (see question 16).

The controller should also inform the data subject of the period for which their personal data will be stored; the existence of the right to request access, rectification or erasure; the right to restrict the processing; the right to object to the processing; the right to data portability; the existence of automated decision making (including profiling); and the right to lodge a complaint with a supervisory authority.

If the personal data has been obtained directly from the data subject, article 13 of the GDPR will apply and the controller must also inform the data subject whether the provision of personal data is subject to a statutory or contractual requirement and of any potential consequences of failing to provide that personal data.

It may be the case in an investigations context that personal data has not been obtained directly from the data subject. If this is the case, article 14 of the GDPR will apply and the fair processing information given to data subject must also include the categories of personal data processed, the source of personal data and details of any personal data obtained from directly accessible sources.

The GDPR sets out a number of data protection principles that controllers must comply with. The first principle is that personal data must be processed "lawfully, fairly and in a transparent manner". This means that data cannot be processed unless there is a legal basis under article 6 of the GDPR. The following legal bases are available:

- the data subject has given his or her consent to the processing for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for performing tasks in the public interest or in the exercise of official functions by the controller (further clarification on this point is set out in section 8 of the DPA); or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where the processing is unwarranted by reason of prejudice to the interests and fundamental rights and freedoms of the data subject.

In respect of sensitive data (or "special categories of personal data"), the processing must also comply with one of the stricter legal bases set out in article 9 of the GDPR and section 10 and Schedule 1, Part 1 of the DPA. Sensitive data is defined as information relating to: racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and sex life and sexual orientation. In an investigations context, relevant conditions for the processing of sensitive data may include where:

- the individual has given their explicit consent to the processing for one or more specified purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- the processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, where this is proportionate to the relevant aim and safeguards the rights and interests of data subjects.

The processing of data about criminal convictions and offences is dealt with separately to sensitive data, under article 10 of the GDPR. This provides that such data can only be processed where authorised under national law (for the UK, this would be the DPA). The DPA provides further information on what is considered the "public interest" in the UK and limits the application of certain provisions of the GDPR where personal data is processed for the detection or prevention of crime or the operation of the justice system (see question 17 for further details).

Controllers must comply with the following data protection principles:

- Principle 1: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency", see above for further details on transparency requirements);
- Principle 2: personal data should be obtained only for specified, explicit and legitimate purposes and should not be further processed in any manner incompatible with those purposes ("purpose limitation");
- Principle 3: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- Principle 4: personal data should be accurate and, where necessary, kept up to date ("accuracy");
- Principle 5: personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- Principle 6: personal data should be processed in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"); and
- The controller must also be able to demonstrate compliance with each of these principles ("accountability").

In addition, under Chapter V of the GDPR personal data may not be transferred to a country or territory outside the EEA unless the European Commission has decided that the third country or territory ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Finally, note that competent authorities processing personal data for criminal law enforcement purposes must adhere to slightly different requirements under Part 3 of the DPA. For example, with regards to Principle 1, there is no requirement for processing to be transparent (given the possibility of this prejudicing an investigation). Additionally, with regards to processing of sensitive personal data, competent authorities must have in place an appropriate policy document explaining how they ensure compliance with these requirements (in addition to there being an appropriate lawful basis for the processing).

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

While there are no specific steps required under the GDPR, it is advisable to check that non-locally generated data was transferred to, or within, the jurisdiction in compliance with relevant data protection laws and regulations. This may include:

- ascertaining what data has been transferred to, or within, the jurisdiction and the natural and/or legal persons to which that data relates;
- reviewing the privacy notice provided to data subjects;
- ascertaining the legal basis for the processing (see question 7); and/or
- determining whether a contract or other safeguard applies to the transfer of that data (eg, a data processing agreement, data transfer agreement or binding corporate rules, as appropriate).

In particular, the above may inform whether certain restrictions may apply to further processing of that data.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

Additional provisions of the GDPR apply where the data are processed by a processor on behalf of the controller. The primary factor considered is control of the data rather than its possession, so the controller must ensure that the third-party processor is complying with the requirements on the security of data set out in the GDPR. A written contract to this effect must be entered into between the processor and controller (article 28 of the GDPR). This contract must include a description of the data processing activities and require the processor, among other things, to:

- act only on the documented instructions of the controller (including with regard to international transfers of data to a third country);
- ensure that persons who process the data have committed to confidentiality or are under a statutory duty of confidentiality;
- implement appropriate security measures in accordance with the GDPR;
- engage a sub-processor only with the prior authorisation of the controller;
- assist the controller in carrying out its obligations to respond to requests by data subjects to exercise their rights under the GDPR; and
- assist the controller in ensuring its compliance with its data security obligations.

Where a processor engages a sub-processor, the contract between them must reflect the same data protection obligations as set out in the contract between the controller and the processor.

These provisions of the GDPR apply to processors within the same corporate group in the same way as to other third-party processors.

The GDPR also imposes certain direct obligations on processors. These include an obligation to: (i) maintain a written record of processing activities carried out on behalf of each controller; (ii) designate a data protection officer where required; (iii) appoint a representative (when not established in the EU) in certain circumstances; and (iv) notify the controller without undue delay on becoming aware of a personal data breach.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

The consent of the data subject is one legal basis for processing of personal data under the GDPR. Data subject consent is therefore not mandatory for the processing of personal data, but consent must be obtained if no other legal basis exists.

There is no prescribed form for the consent, but it should be freely given, specific, informed and unambiguous. In addition, to the extent relied upon as a basis for international transfers, consent must also be explicit (see question 16). Consent can also be withdrawn at any time and must be as easy to withdraw as to give.

In the case of sensitive data, where consent is relied on to provide a legal basis under article 9 GDPR, it must also be explicit. A controller may therefore wish to obtain consent by means of an additional formality to demonstrate "explicit" consent (eg, a wet ink signature or a tick box that expressly uses the word "consent").

Consent can be obtained through a website or other electronic means.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may be considered as an enabling action when planning an investigation. However, obtaining consent to the processing of personal data can be practically challenging, and proceeding with processing of personal data in reliance solely on this ground is rarely appropriate. One reason is that consent must be capable of being withdrawn at any time (a right that it is not possible to contract out of, which would be difficult to manage in the context of the investigation).

12 Is it possible for data subjects to give their consent to such processing in advance?

Whether consent given in advance, such as through general terms and conditions or account opening information, is sufficient for the purposes of the GDPR depends, among other things, on the balance of power between the controller and data subject. Consent is not freely given (and so is invalid) if a data subject has no genuine or free choice or cannot refuse or withdraw consent without detriment, or there is a clear imbalance between the parties. Consent included within an employment contract, or obtained generally by an employer from an employee, is unlikely to be valid for this reason.

Written requests for consent must be clearly distinguishable from other matters, be intelligible, be easily accessible and use clear and plain language. This means that consent should not be hidden among other terms and conditions. In any event, there is a risk that a generic consent provided through general terms and conditions is not specific and informed, and so not validly given by the data subject.

The controller should also consider the requirement for consent to the processing for sensitive data to be explicit (see question 7).

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

A data subject has a right to request information regarding whether their personal data is being processed, known as a data subject access request (DSAR). The information that can be requested includes a description of the data, the purpose for which it is being processed and to whom it may be disclosed. The controller must also provide a copy of the personal data to the data subject.

Following decisions of the English Court of Appeal under the Data Protection Act 1998, the motive behind a DSAR (eg, if it is made to assist in litigation) does not affect a controller's duty to respond to it. Provided the DSAR is not an abuse of the court's process and does not result in a conflict of interest, the court will not use the purpose of a DSAR as a reason to limit the exercise of its discretion to compel an organisation to respond. Privileged material can be withheld, although privilege is narrowly construed to English law only and the English Court of Appeal has held that privileged material must still be searched.

A controller is not required to provide personal data in response to a "manifestly unfounded or excessive" request from a data subject (article 12(5) of the GDPR). If relying on this exemption, a controller should retain evidence to demonstrate why it considers the request to be unfounded or excessive. If a controller refuses to act on a request, they must also inform the data subject of the reason why and tell the data subject that they can complain to their relevant supervisory authority and enforce their right through judicial remedy.

Data subjects have the right to request rectification of any personal data relating to them that is inaccurate, and completion of any incomplete data, including by way of a supplementary statement. There is an obligation on a controller under the GDPR to ensure the personal data it keeps is accurate (see question 7).

Data subjects have the right to obtain from the controller the erasure of their personal data without undue delay if one of the specified grounds applies. This includes where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or where the data subject has withdrawn consent (and there is no other legal ground for the processing).

In certain circumstances, such as when a controller is relying upon their legitimate interests (or those of a third party) or the processing is necessary for performing tasks in the public interest or in the exercise of official functions (see question 7), data subjects have a right to object to the processing of personal data concerning them at any time. A controller must adhere to this objection unless it can demonstrate a legitimate basis for the processing that overrides the interests of the data subject, or if the processing is necessary within legal proceedings. A data subject also has a right to obtain a restriction of processing from the controller where it believes the relevant personal data is inaccurate, the processing is unlawful or the controller no longer needs the data for the purposes of the processing. If the latter is the case, the data subject can require the controller to limit the processing to that required in the context of legal proceedings.

Note that where data is processed by competent authorities for criminal law enforcement purposes pursuant to Part 3 of the DPA, certain rights of data subjects are excluded or restricted. For example, data subjects have no right to object to processing by a competent authority for this purpose. Moreover, data subjects' rights to receive information, rights of access, rights to rectification and rights to erasure or restriction may be limited or restricted where necessary and proportionate to, for example, protect national or public security, or avoid prejudicing a criminal investigation or prosecution.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

ICO guidance suggests that law firms (and other professional service providers) are generally characterised as controllers in their own right. This is on the grounds that responsibility also lies with the law firm itself as it determines what information to obtain and process in order to perform its work and because it is answerable itself for the content. The ICO cites the fact that lawyers control the detailed content of their advice and also have their own professional responsibilities (in areas such as record keeping and confidentiality of communications) as suggestive of lawyers being controllers in their own right.

A legal process outsourcing firm is likely to be considered as a third-party processor in relation to the processing of personal data relating to its clients. This means that the conditions set out at question 9 must be complied with when contracting with a legal process outsourcing firm for the review of documents containing personal data.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Financial institutions in the UK must also comply with, among other requirements:

- the Principles and the Fundamental Rules set out by the Financial Conduct Authority (the FCA). These high-level principles require some financial institutions to take various measures to protect client data. They are applied on a case-by-case basis.
- the guidelines on material outsourcing established by the European Banking Authority (EBA). The EBA's guidelines (which will apply from 30 September 2019) set out a series of recommendations that providers of financial services must adhere to in respect of any outsourcing to the cloud, including in respect of the security of data, where geographically data is located and processed and the importance of contingency planning.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The GDPR distinguishes between transfers to other jurisdictions within the EEA and transfers of data to jurisdictions outside the EEA.

Within the EEA

A transfer of personal data from this jurisdiction to a processor or controller in another EEA member state must comply with the same requirements as if the transfer was made within the jurisdiction (see question 7).

Outside the EEA

Personal data subject to the GDPR cannot be transferred to a country or territory outside the EEA unless that third country or territory provides an adequate level of protection for personal data.

The European Commission has determined that certain non-EEA countries and recipients ensure an adequate level of protection for personal data and so a transfer can be made to such countries in compliance with the rules that provide restrictions on transfers outside the EEA. Currently, these countries are Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

Alternatively, the controller as transferor could ensure an adequate level of protection through:

- entering into standard contractual clauses approved by the European Commission for both controller-to-processor and controller-to-controller transfers (note that it is expected that the ICO will adopt its own UK model clauses post-Brexit); or
- for transfers within the same group, adoption of binding corporate rules.

In a judgment issued on 16 July 2020, the CJEU held that the standard contractual clauses should be viewed as offering only the basic level of protection and they may only be used where the protection provided by the contract is not undermined in the particular circumstances. This means that controllers exporting personal data and looking to rely on standard contractual clauses approved by the European Commission must assess on a case-by-case basis whether additional safeguards are needed to remedy any identified deficiency and ensure adequate data protection.

The European Commission had issued an adequacy decision for recipients registered under the EU-US Privacy Shield framework in respect of their handling of personal data. However, in the judgment dated 16 July 2020, the CJEU held the European Commission's adequacy decision to be invalid and so data transfers cannot currently be made to the US on the basis of the EU-US Privacy Shield.

Data can otherwise be transferred if one of the following derogations, among others, applies:

- the data subject has consented to the transfer (as noted above, this consent should be explicit as well as freely given, specific, informed and unambiguous);
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion of a contract between the controller and a person other than the data subject, which is entered into in the data subject's interests;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or
- the transfer is necessary to protect the vital interests of the data subject.

Where none of the above derogations is available, a transfer to a third country may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller (which are not overridden by the interests or rights and freedoms of the data subject), and the controller has assessed all the circumstances surrounding the transfer and has, on the basis of that assessment, provided suitable safeguards with regard to protection of personal data. This ground for processing may only be relied upon where no other legal basis is available. The controller shall inform the supervisory authority of the transfer and, in addition to providing the information referred to in articles 13 and 14, shall inform the data subject of the transfer and on the compelling legitimate interests pursued. As such, this derogation is unlikely to be of practical application in the context of an investigation.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators and enforcement authorities within the jurisdiction must comply with the GDPR in the same way as any other processing (see question 7). In particular, a legal basis must be established under article 6 GDPR.

There are exemptions from certain GDPR provisions that may apply. In particular, Schedule 1 of the DPA sets out the conditions for processing of sensitive data to be considered in the "public interest" for the purposes of article 9(2) GDPR. These include that the processing is necessary for:

- the prevention or detection of an unlawful act, or for taking steps to establish whether an unlawful act has been committed;
- protecting the public against dishonesty or malpractice;
- the purpose of, or in connection with, legal proceedings (including prospective legal proceedings); or
- the prevention of fraud.

Additionally, Schedule 2 of the DPA disapplies certain provisions of the GDPR where the disclosure of personal data is necessary for the prevention of crime or where disclosure is required by a court or tribunal. The disapplied provisions include the rights afforded to data subjects and the requirement to provide a privacy notice.

When processing personal data for the purposes of criminal law enforcement purposes, competent authorities must adhere to Part 3 of the DPA. The requirements in Part 3 apply to the police, criminal courts, prisons and non-policing law enforcement, including the FCA, HMRC, SFO, NCA, CMA, ICO and the DPP, and other public bodies exercising statutory powers for law enforcement purposes. The processing must be for the primary purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, in order for Part 3 to apply.

The UK and US governments have entered into a bilateral agreement for accessing electronic data in cases of serious crime (the UK-US BDAA). The UK-US BDAA envisages UK and US domestic criminal law enforcement authorities to obtain electronic data directly from a range of telecommunications companies in the other country – without any need to go through the domestic authorities in the recipient country, a mutual legal assistance treaty (MLAT), or existing alternative routes currently used. The UK government can, therefore, issue an order directly to a telecommunications company covered under the UK-US BDAA once it has obtained a court order. The UK-US BDAA has not been implemented in the US but has been implemented in the UK via the Crime (Overseas Production Orders) Act 2019 (COPO).

The COPO states that any person subject to an overseas production order is not required to do anything that would contravene data protection legislation (such as GDPR and the DPA). Though the UK-USA BDAA states that the processing and transfer of data under the agreement are compatible with the parties' respective applicable laws regarding privacy and data protection, the UK Investigatory Powers Commissioner will be responsible for providing independent oversight of the UK's use of the UK-US BDAA to ensure standards of data protection and privacy safeguards.

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The provisions applying to cross-border data transfer generally (see question 16) also apply to the transfer of data to regulators and law enforcement authorities out of the jurisdiction. Any transfer to an overseas regulator would have to comply with the GDPR in the same way as any other processing.

Any disclosure of personal data to an overseas regulator or law enforcement authority would engage the first data protection principle (including the requirement to establish a legal basis under article 6 GDPR) and prohibitions on cross-border

transfers of personal data. In particular, the first principle provides that processing of personal data must be fair, lawful and transparent.

Any transfer of personal data to an overseas regulator or law enforcement authority may breach this principle on the basis that this is not a purpose about which the data subjects will have been sufficiently informed. The GDPR sets out exemptions to providing a privacy notice where this is impossible or would involve disproportionate effort on the part of the controller, but these exemptions are interpreted narrowly.

The cross-border transfer of personal data would additionally require safeguards for the relevant transfer and a legal basis for processing. There is no clear exemption or derogation from either the first principle, the requirement for a legal basis for processing, or the prohibition on cross-border transfers that will routinely cover requests for data by a foreign regulator or law enforcement authority.

The transfer may lack a legal basis, depending on the circumstances of the processing. The possible legal bases that a controller may rely on in this context include:

- the consent of each affected data subject to the disclosure and transfer. However, as noted above, this can be problematic to obtain, can be withdrawn at any time and (in the case of sensitive data) consent must be explicit;
- that the processing is necessary for the establishment, exercise or defence of legal claims, depending on the circumstances;
- that the processing is in the legitimate interests of the controller (see question 16 for further details); or
- that the processing is necessary for the performance of a task carried out in the public interests (see question 7 for further details on the application of this basis to the processing of sensitive data).

The prohibition on cross-border transfers provides that personal data should not be transferred to a country outside the EEA that does not provide an adequate level of protection, unless an exemption applies or safeguards for the personal data are in place. Article 49 of the GDPR provides for derogations to the requirement for an adequacy decision or implementing safeguards in certain circumstances, including where the transfer is necessary for important reasons of public interest or for the establishment, exercise or defence of legal claims.

The UK decided not to opt in to article 48 of the GDPR to the extent that it triggers the UK's rights under the protocol it has for EU matters relating to justice and home affairs. This article provides that, without prejudice to other grounds for international transfers, a decision from a third-country authority, court or tribunal does not in itself justify the transfer of personal data to a non-EEA country.

This is the case unless the transfer is based on an international agreement, such as a mutual legal assistance treaty. The European Data Protection Board guidelines state, in relation to article 48: "In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement."

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

The recipient of such a request may consider taking the following steps, amongst others:

- Consider if there is a legal obligation to respond to the request and, if so, to what extent.
- Seek further information in writing from the requesting regulator to evaluate the purpose of the request.
- If possible, negotiate the scope of the request: for example, to target the specific information required for the purposes of the regulatory investigation.
- In accordance with principles of data minimisation and anonymisation, limit the scope of any data disclosed and transferred to that necessary for the purpose.
- Consider whether it is practicable to obtain data subject consent and/or give a further privacy notice.
- Put in place a data processing agreement if data will be transferred to an affiliate or third party (acting as a processor).
- Consider transfer via an MLAT as, in some cases, it may be possible to request that the requesting court or regulator requests data via an MLAT or other international agreement.

20 What are the sanctions and penalties for non-compliance with data protection laws?

There is a tiered approach to penalties for breaches of the GDPR. This permits data protection authorities to impose fines for some infringements of up to the higher of 4 per cent of annual worldwide turnover and €20 million (eg, for breach of requirements relating to cross-border transfers or the principles for processing, such as conditions for consent). Other specified infringements attract a fine of up to the higher of 2 per cent of annual worldwide turnover and €10 million.

The GDPR contains a list of points to consider when imposing fines, such as the nature, gravity and duration of the infringement.

The ICO is responsible for enforcing the GDPR, but in certain circumstances enforcement will be conducted through the courts (eg, under article 79(1) of the GDPR, data subjects have a right to an "effective judicial remedy" where they consider their rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR).

There are a number of criminal offences under the DPA (eg, the re-identification of personal data that has been "de-identified" or making a false statement in response to an information notice). A failure to comply with the provisions on cross-border transfer is not in itself a criminal offence, but the ICO may issue an enforcement notice ordering a remedy (and failure to comply is a criminal offence). The maximum penalty for criminal offences under the DPA is an unlimited fine.

Where any offence under the GDPR is committed by a body corporate with the consent or approval of an officer such as a director or other employee, that person will also be guilty of the offence and will be liable to punishment under the DPA accordingly.

The ICO may also:

- serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- issue undertakings committing an organisation to a particular course of action to improve its compliance;
- serve enforcement notices and "stop now" orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- prosecute those who commit offences under UK data protection laws;
- serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice; and
- report to the UK Parliament on issues of concern.

A data subject who suffers material or non-material damage as a result of a breach of the GDPR by a controller may bring a civil claim for compensation. The DPA extends this to include any other data protection legislation in the UK and clarifies that "non-material damage" includes distress.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

A controller's obligations under the GDPR are continuing for as long as it remains a controller. As a result, it should ensure compliance with the GDPR, where applicable, at all stages of the investigation.

Practical steps that a controller should follow include:

- ensuring that any third-party processing data on behalf of the controller signs a data processing agreement and/or data transfer agreement, as applicable;
- ensuring that all personal data processed is accurate and, where applicable, that the consent of data subjects remains valid;
- complying with the restrictions on the transfer of data to third parties set out at question 16 (whether within or outside the EEA), including any transfer to a regulator or law enforcement authority; and
- maintain a record of processing and respond to data subject requests.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

The original and intervening controllers should ensure that a written agreement is in place between them and follow the steps to address their continuing obligations set out at question 21.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

EU General Data Protection Regulation (2016/679):
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

UK Data Protection Act 2018:
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

ICO 'Guide to the General Data Protection Regulation'
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

ICO guidance on international transfers:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

ICO guidance on exemptions under the GDPR:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

ICO guidance on data protection and Brexit:
https://ico.org.uk/for-organisations/data-protection-and-brexit/

ICO guidance on the difference between controllers and processors:
https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

ICO 'Guide to Law Enforcement Processing'
https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing-1-1.pdf.

Nigel Parker

Allen & Overy LLP

Nigel specialises in data protection and privacy, commercial contracts and intellectual property law. He works across a wide variety of business sectors, including financial services, technology, media and life sciences.

Nigel regularly advises on multi-jurisdictional data protection matters. He advises companies across various sectors on strategic issues relating to personal data management and new technologies such as privacy impact assessment and privacy by design, international data transfers (including BCRs) as well as crisis management (eg data breaches) and data protection authority investigations.

Nigel is recognised in *Chambers* and *The Legal 500*, and was named one of the "Top 40 under 40" data lawyers by Global Data Review. *The Legal 500* cites Nigel as an expert in the field of data protection, privacy and cybersecurity, describing him as "a technical expert while also being extremely strategic and forward thinking" (*The Legal 500*, 2020). He is the contributing editor of the ICLG cross-border guide on cybersecurity and an editor of A&O's Digital Hub blog.

Calum Burnett

Allen & Overy LLP

Calum Burnett is head of the UK Litigation & Investigations Group. He is experienced in acting for financial institutions, corporations and individuals in domestic and international criminal and regulatory investigations and in conducting internal investigations. He also advises financial institutions on litigation and risk management issues. Calum has previously spent time on secondment with the fraud division of the Crown Prosecution Service and the enforcement division of the former Financial Services Authority.

Calum has, for a number of years, been recognised by the major UK directories for all areas of his practice. *Chambers UK* 2018 says that he is "forward thinking, technically flawless and clear-sighted" and *Chambers UK* 2019 reports that "he is a go-to on contentious regulatory matters – he has a huge wealth of experience, is very impressive intellectually and has good commercial sense".

Benjamin Scrace
Allen & Overy LLP

Ben has a broad commercial practice, including data protection, commercial contracts and non-contentious intellectual property. He has experience of multi-jurisdictional data protection matters and advises on the IP, IT and data protection considerations in corporate transactions. Ben previously spent time on secondment with the digital and data privacy legal team of a multinational electronics and technology company.

Jason Rix
Allen & Overy LLP

Jason has a varied commercial litigation practice, which includes data protection, cybersecurity, privilege, sanctions, state immunity, conflicts of laws, EU law and English contract law. A while back, Jason was seconded to BT for nine months where he helped negotiate key supplier contracts for BT's £10 billion 21st Century Network. This experience still serves as a vivid reminder of what it is like in-house. He is a member of the CCBE European Private Law Committee and sat on the FMLC working group looking at Distributed Ledger Technology and Governing Law. In 2016, he set up Compact Contract (www.aocompactcontract.com) a blog focused on English contract law.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the US and Europe.

One Bishops Square
London
E1 6AD
United Kingdom
Tel: +44 20 3088 0000
Fax: +44 20 3088 0088

www.allenovery.com

Nigel Parker
nigel.parker@allenovery.com

Calum Burnett
calum.burnett@allenovery.com

Benjamin Scrace
benjamin.scrace@allenandovery.com

Jason Rix
jason.rix@allenovery.com