ALLEN & OVERY

GDPR for litigators

2019

Virtually all evidence, whether in litigation or arbitration or relating to investigations carried out by regulators or enforcement authorities, will contain some personal data. A year on from the EU General Data Protection Regulation (universally known as GDPR) coming into force, we examine what it means for disputes and contentious regulatory/enforcement matters, focussing on three areas.

BREXIT

Given the political uncertainty surrounding Brexit, it is deliberately not addressed in the remainder of this note.

Under the Withdrawal Agreement, EU law would continue to apply, including GDPR. Transfers of data from the UK to the EU (both before and after the end of the transition period) are to be treated no differently to if the UK had not withdrawn from the EU. However, there is no express provision dealing with transfers the other way: from the EU to the UK. The Political Declaration envisages the UK being recognised as providing an adequate level of protection.

The UK government and the UK Information Commissioner's Office has published extensive guidance on what would happen in the event of a no-deal Brexit. The most significant change is that the UK would be a "third country" for the purposes of the EU GDPR by virtue of its no longer being a Member State of the EU. So a transfer of personal data from any country in the European Economic Area (**EEA**) to the UK would require a legal basis under the EU GDPR in a way that it does not at the moment.

Disclosure in all its forms

Disclosure comes in many shapes and sizes. It has nearly as many names: discovery, disclosure, production of documents, inspection and so on. It encompasses not only the specific meaning in English civil litigation under the Civil Procedure Rules (which itself is being reformed via the disclosure pilot scheme), but also whenever documents are collected, reviewed or produced in a legal, regulatory or enforcement context. This may be under compulsion or due to a desire to share those documents with another party, whether that be the opponent in litigation or arbitration or a local or foreign regulator or law enforcement agency.

When might data protection considerations arise?

The concept of personal data has always been drawn extremely widely under EU data protection laws. Under GDPR, personal data is information that relates to an identified or identifiable natural person. The identifier could be a name, an online identifier (eg an IP address or a cookie) or some other factor. A data controller is the entity which, alone or jointly, determines the purposes and means of processing. Both clients and their lawyers will usually be data controllers. The same is likely to be true of other professional advisers like accountants and consultants. Almost any interaction with personal data will amount to processing, including collecting, organising, storing, altering, retrieving, using and erasing. Given the wide scope of personal data and processing activities, data protection may touch disclosure at various stages. Chief among these are:

Personal data may, for example, relate to employees, customers or business contacts. Sensitive data (or "special category data") needs to be handled with even greater care than personal data but is probably less likely to be present in standard commercial disputes.

Sensitive data includes data revealing racial or ethnic origin or political opinions, or data concerning health, but does not include financial information (eg bank account or credit card numbers). GDPR deals separately with personal data relating to criminal convictions and offences (ie it is not part of sensitive data). Some countries have special requirements for how national identification numbers are processed.

The Data Protection Act 2018 (**DPA 2018**) contains certain exemptions that may be relevant to litigation (hidden in Schedule 2). The exemptions are from a list of GDPR requirements including notifying the data subject. The exemptions may apply, for example, where disclosure of data is required by law or an order of a court or tribunal.

Another example of when these exemptions may apply is where the disclosure is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings). While these exemptions do not remove the need for a legal basis for processing, they would be relevant, for instance, to whether a transfer may be lawful in the absence of an adequate privacy notice. They may also vary between EU Member States, notwithstanding GDPR.

Separately GDPR allows derogations in specific situations from the normal requirements for an international transfer of personal data (ie from within to outside the EEA). The one most obviously relevant to litigation is that the transfer is necessary for the establishment, exercise or defence of legal claims.

With the above in mind, on the following page we illustrate three different scenarios with some of the potential issues and possible solutions.

ENGLISH CIVIL LITIGATION

For disclosure in English civil litigation, the main risk, from a data protection perspective, is probably disclosing "irrelevant" or "non-responsive" personal data. That is, personal data that is not clearly caught by the disclosure model ordered by the court since then it cannot be said to be necessary to disclose it. This risk can be mitigated by redaction in the same way that "irrelevant" confidential data may be redacted, although this is both difficult and costly.

In particular, the definition of personal data means that redacting someone's name is unlikely, of itself, to be sufficient to remove all personal data from any given document. It is highly likely that the individual can still be identified from other data and/or the context. Redaction has a place but it is neither a wholesale solution nor required in every instance. In practice a risk-based approach is typically adopted.

U.S. DISCOVERY OBLIGATIONS ON A COMPANY IN THE EEA

Imagine a UK company is subject to extensive U.S. discovery obligations by virtue of being a party to litigation before a U.S. court. Here the main tension is between compliance with, on the one hand, the U.S. Federal Rules of Civil Procedure and, on the other, GDPR (as well as other laws, such as bank secrecy rules and "blocking statutes"). GDPR introduced a new provision (Article 48*) which provides that decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to a non-EEA country unless based on a an international agreement such as a mutual legal assistance treaty.

From a GDPR perspective the company should therefore consider arguing for the U.S. discovery to proceed through the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (1970). Historically this has not always been palatable from a U.S. perspective due to the delays, costs and uncertainty of obtaining the evidence.

U.S. courts have begun to consider the impact of GDPR in civil litigation and, to date, have concluded that it does not trump U.S. discovery obligations. Interestingly, in one case the party seeking discovery from a non-party was required to pay the cost of the non-party's compliance with GDPR and indemnify it for any data protection breaches.

Other considerations include:

– negotiating the scope of discovery (not necessarily that easy);

– seeking a Protective Order from the U.S. court to afford some level of protection to any data transferred (this is not a panacea); and/or

– redaction of personal data (likely to be difficult and costly).

* In 2016 the UK government stated that the text of what was to become Article 48 "restricts a Member State from enforcing a judgment requiring the transfer or disclosure of personal data where there is no international agreement or treaty." As a result it stated that it had decided not to opt-in to those parts of Article 48 which trigger the UK's rights under the protocol it has for EU matters relating to justice and home affairs. Presumably for the same reason, the UK government has indicated that in the event of a no-deal Brexit Article 48 will not apply to the UK.

U.S. REGULATOR/LAW ENFORCEMENT AUTHORITY

In this example, a UK company receives a letter from the U.S. Securities and Exchange Commission (**SEC**) seeking voluntary assistance. The UK company is keen to cooperate with the SEC as far as possible.

Some of the issues from a GDPR perspective are:

– the lack of compulsion as a matter of English law; and

– the fact that the data is to be transferred from the UK to outside the EEA.

As well as considering redaction and negotiation of the scope of the assistance with the SEC, from a GDPR perspective, at least, the UK company wants the request to be made from the SEC to the Financial Conduct Authority (**FCA**) and then for the FCA to require provision of the information under its statutory powers.

IMPACT OF GDPR

The tension between data protection laws and disclosure in all its forms has existed for some time with companies frequently caught between a rock and a hard place, especially where foreign (typically U.S.) regulators and enforcement agencies are involved. Historically, companies have generally been more fearful of requesting agencies than the data protection authorities in EU Member States, although there have been recent examples of companies attempting to resist demands from U.S. law enforcement agencies.

The level of potential fines under GDPR (up to 4% of annual worldwide turnover) has meant that data protection receives more attention than it did previously, but, in the absence of enforcement by a data protection authority in this area the balance is likely to remain tipped in favour of requesting agencies. So while GDPR has not changed fundamentally the factors that banks and corporations must consider, it has made the decision more acute.

Data subject access requests

Data subject access requests (**DSAR**s) are the means by which individuals are entitled to obtain confirmation that their data is being processed, and access their personal data as well as certain other information (eg about the purposes of processing and whether the data will be given to any other organisations).

The information that can be obtained by DSARs is limited to personal data, and so is less wide-ranging than discovery/disclosure in civil litigation. However, actual and potential litigants often use DSARs as a tactic in litigation or as a "fishing expedition" to obtain either pre-action disclosure or disclosure whilst proceedings are on-going.

In *Dawson-Damer v Taylor Wessing*, when considering a DSAR made during on-going litigation, the UK Court of Appeal held that the motivation behind a DSAR is irrelevant. Provided the DSAR is not an abuse of the court's process or 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.

However, in light of the Court of Appeal's decision in *Ittihadieh v 5-11 Cheyne Gardens* and *Deer v Oxford University*, the "absence of a legitimate reason" for a DSAR may still be relevant to whether the court exercises its discretion to order compliance with that DSAR (even though a collateral purpose of assisting in litigation was held not to be an absolute bar). Further, a reduction in the costs awarded to a data subject may also be ordered where DSARs are "essentially antagonistic" or amount to "low level attritional warfare" against the data controller.

IMPACT OF GDPR

GDPR introduced a number of changes to the procedure for making a DSAR. These were generally data subject-friendly and may have made it more burdensome for organisations receiving DSARs:

- **No fees:** In most cases organisations cannot charge a fee.
- **Unfounded or excessive requests:** Where a DSAR is "manifestly unfounded or excessive", the organisation can charge a reasonable fee or refuse to respond. The burden is on the organisation to show that the DSAR was manifestly unfounded or excessive in character.
- **Time limit for response:** An organisation must respond to a DSAR without undue delay and, in any event, within one month of receipt. The one-month period can be extended to three months, taking into account the complexity and number of DSARs, in which case the data subject must be informed of the extension (including reasons) within one month of receipt of the DSAR.
- **Content of response:** As well as access to the data subject's personal data, the right of access extends to other information, including: the envisaged storage period for the personal data; the right to request rectification, erasure or restriction of processing; the right to lodge a complaint with the Data Protection Authority; and, if automated decision-making is used, meaningful information on the logic involved.
- **Electronic DSARs:** It must be possible to make DSARs electronically and, unless otherwise requested by the data subject, the organisation must provide the information in a commonly used electronic form.

The exemptions mentioned earlier (DPA 2018, Schedule 2) may also be relevant to DSARs.

Group litigation/ Representation of data subjects

In *Various Claimants v WM Morrisons*, the UK Court of Appeal found an employer to be vicariously liable for a rogue employee's breach of the pre-GDPR UK data protection law, the Data Protection Act 1998 (**DPA 1998**).

Vicarious liability

BACKGROUND

The decision followed a rogue employee's intentional disclosure of payroll data relating to around 100,000 employees.

The employee was convicted of criminal offences under the Computer Misuse Act 1990 and the DPA 1998, and was sentenced to eight years' imprisonment. A group litigation claim was brought against the employer by around 5,500 employees under the DPA 1998 and at common law (for breach of confidence and misuse of private information) seeking compensation for distress.

DECISION

The appeal relates only to vicarious liability. The first instance finding that the employer bore no primary liability stands. The Court of Appeal held that the DPA 1998 does not exclude vicarious liability. It then looked, first, at the employee's "field of activities". His role was to receive, store and disclose payroll data. The court determined that the fact he chose to disclose it to other (unauthorised) third parties was "nonetheless closely related to what he was tasked to do".

The second question was whether there was a sufficient connection between the employee's field of activity and the wrongful conduct. The employer argued that there was insufficient connection because the unlawful disclosure by the employee had been done at home, on his own computer, outside of working hours, and several weeks after he had originally downloaded the data. The court disagreed, holding that:

- The cause of action was already established when the employee was at work when he improperly downloaded the data, rather than when he subsequently disclosed it online.
- Vicarious liability does not only apply if the employee is "on the job"; although the time and place when the act occurred are relevant, they are not conclusive.
- It approved the trial judge's findings on sufficient connection: an unbroken thread linked the employee's employment to the disclosure as a "seamless and continuous sequence of events"; the employer intentionally entrusted the employee with the data during the course of his employment; and the employer tasked the employee with receiving, storing and disclosing the data; therefore his actions (albeit unlawful) were closely related to the task he was given.

COMMENT

Although the case was decided under the DPA 1998, the principles are equally applicable under the Data Protection Act 2018 and GDPR. Permission has been granted for this case to go to the UK Supreme Court.

IMPACT OF GDPR

The advent of data breach group litigation in the UK has coincided with GDPR coming into force. There are a variety of factors in play including increasing data subject awareness, greater publicity of breaches, litigation funding and no win/no fee arrangements as well as proactive claimant lawyers.

The question of quantum in the UK remains unpredictable. It is clear that it is not necessary to prove financial loss but the amounts that can be claimed for distress have varied under the DPA 1998 from a few hundred pounds to the low thousands.

A case involving Google's alleged secret tracking of the internet activity of certain Apple iPhone users gives potential defendants some cause for optimism (*Lloyd v Google*). The High Court held that compensatable damage had not been suffered: "Not everything that happens to a person without their prior consent causes significant or any distress. Not all such events are even objectionable, or unwelcome. Some people enjoy a surprise party..."

The same case shows the English court's unwillingness to allow a U.S. "opt out" class action to be brought under the Civil Procedural Rules for representative actions. The court held that it was not possible to say each claimant had the "same interest" and with a class of nearly five million and the passing of time there was no way to be sure that all claimants were properly members of the class.

Under GDPR provision has been made for data subjects to mandate a consumer protection body to exercise their rights and bring claims on their behalf for breaches of GDPR. To date this has not been exploited in the UK.

FOR MORE INFORMATION, PLEASE CONTACT:

This note provides general information and should not be relied upon without seeking specific legal advice. If you do require legal advice in respect of issues mentioned in this note, please do not hesitate to contact one of the editors or your usual contact at Allen & Overy. Further information on the restrictions and requirements affecting cross-border transfers of data can also be found on aosphere's Rulefinder Cross Border Data Transfer (aosphere.com/aos/cbdt).

London

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel +44 20 3088 0000
Fax +44 20 3088 0088

Editors

Calum Burnett
Partner
Tel +44 20 3088 3736
calum.burnett@allenovery.com

Brandon O'Neil
Partner
Tel +44 20 3088 4187
brandon.oneil@allenovery.com

Jason Rix
Senior Professional Support Lawyer
Tel +44 20 3088 4957
jason.rix@allenovery.com

Nigel Parker
Partner
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Hugo Flaux
Associate
Tel +44 20 3088 2675
hugo.flaux@allenovery.com

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (cooperation office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Yangon