ALLEN & OVERY

In focus

EU proposed data protection Regulation

UK employer challenges: EU data protection shake-up

Against the backdrop of UK plans to cut red tape and scale back employment rights, the European Commission's proposals for data protection reform could complicate life for employers. As data controllers, they would face a considerably higher compliance bar, and the risk of significant fines for slip-ups. Data processors, such as outsourced payroll functions and benefit plan administrators, would also be directly accountable under EU law for the first time.

We highlight some potential challenges for UK employers, if the proposals (which take the form of a draft Regulation) are to become law.

Managing without consent

Employers could no longer rely on employee consent to process employees' personal data or send it outside the EEA in many circumstances, as the Regulation suggests that consent is not "freely given" in an employment relationship. It is possible that this would not apply to all situations of data processing or indeed to all employees, for example in relation to senior employees where there is arguably more equal bargaining power. This restriction of the consent route comes as no real surprise. The UK Information Commissioner flags concerns about employee consent in the Employment Practices Code, as does the European data protection advisory committee in its own guidance.

In practice, employee consent is often used. For employers, it's seen as a safe option, reducing the risk that employees will assert a breach later down the line. What would be Plan B? Without employee consent, employers could still legitimately process employees' data on other grounds – including meeting employment contract obligations, complying with a legal requirement, or pursuing their own "legitimate interests", provided they are clear with employees upfront about the justification for processing and their rights to object, and document the legitimate interests in question.

They could also process "sensitive data" (such as that relating to race or ethnic origin, political opinions, religion or belief, health, sex life or criminal convictions) to meet employment law obligations, subject to any specific safeguards in EU or national rules.

Specific challenges in relation to consent arise for pension schemes and pension scheme trustees (as data controllers). For further information, please refer to our separate article on the impact of the EU proposals for UK pension schemes.

Cross-border data transfers

Whilst employee consent would be unlikely to be a basis for sending employees' data outside the EEA, employers could benefit from a "legitimate interests" addition to the permitted grounds for cross-border data transfers. This would be available – assuming the data transfer isn't "massive" or "frequent" and they comply with certain documentary and notification hurdles – to supplement other options such as transfers using binding corporate rules or pre-approved contractual clauses.

Other permitted grounds for transferring employees' data outside the EEA would continue to include transfers necessary for the establishment, exercise or defence of legal claims, which could be invoked, for example, in the context of litigation.

Stronger subject access rights – but scope to manage broad requests

Data subject access requests are a means for employees to ascertain whether or not their data is being properly processed, but are often used tactically in employment disputes. Employers would be required to establish a formal process for responding to subject access requests. A response to a request would have to be given within one month (a tighter timeframe than the 40-day limit allowed under UK rules) and no administration fee could be charged, subject to some exceptions for multiple or excessive requests.

Employers would also have to respond with more detailed information, including the length of time for which the data would be stored, the individual's right to complain to the data protection authority and the significance and likely consequences of processing particular types of data such as that used to evaluate their performance, economic situation, health, personal preferences, reliability or behaviour.

On the plus side, the Regulation doesn't incorporate the European data protection advisory committee's opinion on the meaning of "personal data", which gives a broad interpretation of the type of personal data that employees could legitimately expect to see about themselves in a subject access request. Employers could therefore continue to justify taking a robust approach to wide-ranging requests, as permitted in current UK case law (*Ezsias v The Welsh Ministers*), by limiting disclosure to information where the employee is the focus.

More security for employees – less for processors

Data processors, such as external administrators, would be directly responsible for keeping employees' data secure and they would be at risk of fines for security breaches. Currently employers (as data controllers) bear the burden of ensuring that employees' data is kept secure. They must ensure contractually that their data processors do the same. Extra care would be required when negotiating administration and other processor agreements, to assess security risks and measures upfront and apportion potential liabilities (including fines). Added to the "heightened security" approach is a system which would require them to report security breaches, such as unauthorised disclosure of employees' data, within strict time limits.

Compliance and penalties

An extensive paper trail would be required, as well as other appropriate measures (for example training), to demonstrate to the Information Commissioner that processing activities are compliant on an ongoing basis. Processors would be caught by the documentation requirements too. Whilst well-intentioned – to relieve the burden of notification – this could be costly and resource-draining for employers. But as compliance steps are a factor to be considered when determining fines, cutting corners would not be an option.

Employers are likely to be concerned by the severe penalties for breach of the proposed rules. Fines are proposed of up to EUR1 million, or 2% of annual worldwide turnover (considerably higher than the current maximum GBP500,000 penalty in the UK, although higher penalties may be levied in other EU countries) for breaches in relation to consent, security measures, compliance measures, international transfers and reporting of breaches. Inadequate replies to subject access requests or gaps in documentation could attract fines of up to EUR500,000, or 1% of turnover.

Conclusion

Whilst the Regulation is not yet in a final form, the current draft gives a flavour of the key challenges faced by employers. However, much of the implementation detail would be fleshed out in national rules. Member States could adopt specific rules on data processing for employment purposes, in particular for recruitment, employment contract compliance, management, planning and organisation of work, health and safety, employee benefits and employment termination. Hopefully, the Information Commissioner would use this opportunity to allow employers some flexibility in stricter areas of the EU rules and greater clarity than exists in some areas of the current regime.

Mark Mansell
Tel +44 20 3088 3663
mark.mansell@allenovery.com

Mark Mansell is a Partner in the London office of Allen & Overy.

Felicity Gemson
Tel +44 20 3088 3628
felicity.gemson@allenovery.com

Felicity Gemson is a Senior Professional Support Laywer in the London office of Allen & Overy.

FOR MORE INFORMATION, PLEASE CONTACT:

Belgium

Tom De Cordier
Counsel, Brussels
Tel +32 2 780 25 78
tom.decordier@allenovery.com

Czech Republic

Prokop Verner
Senior Associate, Prague
+420 222 107 140
prokop.verner@allenovery.com

France

Ahmed Baladi
Partner, Paris
+33 1 40 06 53 42
ahmed.baladi@allenovery.com

UK

Jane Finlayson-Brown
Partner, London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Germany

Bettina Enderle
Counsel, Frankfurt
+49 69 2648 5942
bettina.enderle@allenovery.com

Hungary

Balázs Sahin-Tóth
Counsel, Budapest
+36 1 429 6003
balazs.sahin-toth@allenovery.com

Italy

Lydia Mendola
Senior Associate, Milan
+39 02 2904 9713
lydia.mendola@allenovery.com

UK

Mark Mansell
Partner, London
Tel +44 20 3088 3663
mark.mansell@allenovery.com

Luxembourg

Cyril Pierre-Beausse
Counsel, Luxembourg
+352 44 44 55 515
cyril.pierre-beausse@allenovery.com

Netherlands

Hendrik Jan Biemond
Partner, Amsterdam
+31 20 674 1465
hendrikjan.biemond@allenovery.com

Poland

Magdalena Bartosik
Senior Associate, Warsaw
+48 22 820 6131
magdalena.bartosik@allenovery.com

UK

Nigel Parker
Senior Associate, London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Romania

Radu Diaconu
Associate, Bucharest
+40 31 405 7777
radu.diaconu@rtprallenovery.com

Spain

Rafael Beneyto
Associate, Madrid
+34 91 782 98 00
rafael.beneyto@allenovery.com

Slovakia

Zuzana Hecko
Associate, Bratislava
Tel +42 12 5920 2438
zuzana.hecko@allenovery.com

UK

Charlotte Mullarkey
Senior PSL, London
Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com