HERBERT SMITH FREEHILLS

EMPLOYMENT BRIEFING

PRACTICAL STEPS FOR EMPLOYERS WHEN PREPARING FOR THE EU GENERAL DATA PROTECTION REGULATION

NOVEMBER 2016

London

The General Data Protection Regulation ("GDPR") aims to harmonise data protection procedures and enforcement across the European Union. It will apply to all EEA countries and the companies that conduct business in them from 25 May 2018. New standards for consent, enhanced information rights and greater sanctions for data processors and controllers indicate a potentially significant impact for employers; companies should take steps now to prepare for the changes. But what steps should they take in light of the referendum result and the potential UK exit from the European Union?

This briefing focuses on the implications of the GDPR in the employment sphere and the practical steps that employers should take in relation to data protection in relation to recruitment, during employment and on termination of employment.

Table of Contents

1. As a result of Brexit, is GDPR still relevant? 1
2. Why do we need to think about this now? 2
3. Recruitment: clarity around what constitutes personal data, transparency about proposed use and consider retention 2
4. Obtaining proper consent from employees and applicants 3
5. During employment: enhanced data rights for employees 4
6. On termination 6
7. Data controllers and data processors - remaining accountable 6
8. International human resources transfers 6
9. Potential for deviations across Member States 7
10. Sources 7
11. Contacts 7

RELATED LINKS

Herbert Smith Freehills' dedicated Brexit Hub

Herbert Smith Freehills GDPR briefing

1. As a result of Brexit, is GDPR still relevant?

- The UK is likely still to be a member of the EU on 25 May 2018. The Prime Minister stated that she will invoke Article 50 before the end of March 2017, so (subject to her still being able to do so given last week's High Court decision) the two-year period for negotiating an exit from the European Union will not have expired by the deadline for implementation of the GDPR. Provided that by 25 May 2018 the Brexit negotiations have not reached their conclusion, the GDPR will have direct effect in the UK without the UK government having to take any steps. Therefore companies with operations in the UK or who provide services to those in the EU which involves processing personal data of those data subjects in the EEA will need to continue preparation for GDPR compliance. The Information Commissioner's Office also announced on 31 October 2016 that the Government has confirmed that the UK will be implementing the GDPR.

- Further, if the UK does leave the European Union, it is likely to ensure that it is considered an "adequate" jurisdiction for data protection to ensure trade with the EU. This will require the UK to adopt the GDPR, or, at any rate, legislation which is substantially similar. This is consistent with the Information Commissioner's Office ("ICO") position after the Referendum: “Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to present our view that reform of the UK law remains necessary.” She more recently added that "I don't think Brexit should mean Brexit when it comes to standards of data protection”.
- In any event, it is preferable for global companies with operations across the EEA or who are providing goods or services to those in the EEA to have a consistent set of standards and approach in relation to data processing within the region.

It may be difficult for those responsible for data protection compliance to get management or board level approval for investments into systems and processes in light of a potential Brexit. However, the risk of fines of up to EUR 20 million or 4% of annual worldwide turnover for breach of the Regulation, including data protection principles, failure to comply with the conditions for consent, and breach of data subjects' rights should focus minds.

See our briefing for an overview of the key provisions and business impact of the GDPR. Set out below are the practical steps for employers to start taking.

2. Why do we need to think about this now?

It is less than 19 months until the GDPR is implemented across the EU, including (it seems) the UK. Whilst that sounds like a lot of time in which to ensure your business is compliant, in fact there are a number of steps that need to be taken, some of which require a long lead in time. For example, in order to give effect to the right to be forgotten companies will need to ensure that their IT systems have the functionality to allow them to delete data where they are required to under the GDPR. There is often a long lead in time for IT projects, so any plans for changes to IT systems should be "future proofed" for GDPR which by necessity will require steps to be taken early. Also, companies will need time to undertake an audit of their systems and procedures in order to perform a gap analysis of areas that need to be focused on and changes that need to be made, which all takes time. Ultimately, this is a business issue affecting various parts of businesses, which necessitates "buy-in" from various stakeholders internally as to changes that need to be made. Many companies are far advanced in their preparations for GDPR, are you?

3. Recruitment: clarity around what constitutes personal data, transparency about proposed use and consider retention

Definition of Personal Data

The definition of "personal data" is essentially the same as under the Data Protection Directive, and includes any information relating to an identified or identifiable person. Genetic data and biometric data have been included in the new definition of sensitive personal data. Genetic data is defined as all personal data relating to the genetic characteristics of an individual that have been inherited or acquired which give unique information about the physiology or the health of the individual, whilst biometric data means personal data resulting from specific technical processing relating to physical, physiological or behavioural characteristics which allow for or confirm the unique identification of the individual (Article 9). Employers should therefore ensure their data protection policies and procedures are updated and that there are clear communications with all employees about what information constitutes "personal data".

Fair Processing Notices

Provisions relating to the processing of personal data (Article 5) and the lawfulness of processing (Article 6) broadly reflect the current position under the Data Protection Directive but data subjects will have greater information rights in relation to how their data is processed. Employers, as data controllers, should prepare to make their procedures more transparent and accessible to employees and update their fair processing notices to reflect the additional requirements of the GDPR. This then focuses attention on how personal data is processed.

Employers must provide concise, transparent, intelligible and easily accessible information to their employees, including information about the parties involved in the processing of their personal data and how their data will be treated (Articles 12 and 13). Fair processing notices must state:

- the identity and contact details of the data controller and Data Protection Officer (where applicable);
- the purposes of processing and the legal basis for it;
- an explanation of the data controller's legitimate interests, where processing is based on this;
- the recipients of the personal data; and
- information on any cross-border data transfers outside the EEA (where applicable).

In addition, the following information should be provided to employees when personal data is collected, and we suggest providing it in a separate, dedicated document:

- the data retention period (this may be difficult to establish);
- a brief explanation of their right to erasure (i.e. have their data deleted), rectification and to object to processing;
- their right to withdraw consent to processing;
- their right to complain to a Supervisory Authority (i.e. the Information Commissioner);
- the consequences of failure to provide data in certain circumstances (e.g. where it is a statutory or contractual requirement to do so);
- the existence of automated decision-making, including profiling (where applicable).

Exemptions: the notice does not need to be provided if it is impossible or would involve disproportionate effort, the processing is required by law. Further guidance on these exemptions will be produced in due course.

Right to object

As mentioned above, employers must inform employees clearly about their right to object to the processing of their personal data. This information can be in data protection notices or other communications with the employee. It would be best practice to outline this in a separate, dedicated document.

Other practical tips

- Pre-employment checks continue to be allowed under the GDPR, along with equal opportunities monitoring processes, but both should be reviewed in light of the new requirements to ensure that all the personal data collected is essential to carry out the check and is not stored for longer than is necessary. It can be difficult to ensure data is deleted after it is no longer needed.
- Review and amend employment contractual documentation, as appropriate, to ensure compliance with new fair processing notice requirements.
- Particular care should be taken with automated processing (which could constitute "profiling"); individuals have the right not to be subject to decisions made solely by an automated process. Graduate or general HR recruitment may utilise systems to filter out candidates on the basis of university or grade. Similarly, a large scale redundancy exercise may require performance review data to be analysed in an automated system. Such systems should be reviewed to ensure that decision-making is not entirely automated (Recital 71). Information about the logic used in these systems must be made available to employees and applicants (as appropriate); with explicit consent being sought.

4. Obtaining proper consent from employees and applicants

Silent, assumed or ambiguous consent is not an acceptable standard – it needs to be "freely given, specific, informed and unambiguous" (Article 4). Employers must also ensure that employees' and job candidates' consent is given either by a statement or through clear, affirmative action to signify agreement to personal data relating to him or her being processed (Article 7).

Personal data may only be processed lawfully if one of the following applies:

- the employee has given consent to the processing of his or her data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the employee is party;
- processing is necessary for compliance with a legal obligation to which the data controller is subject;
- processing is necessary to protect the vital interests of the data subject, or another individual;
- processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the data controller; and
- processing is necessary for the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or rights of the data subject. (Article 6).

Consent must relate to the processing of personal data for a specified purpose. Guidance should clarify the meaning of "freely given" in due course but it is anticipated that pre-ticked boxes and 'opt-out' methods will not be acceptable. Under the current law there is a debate across Member States whether an employee can give consent i.e. is it truly freely given. This debate will remain under the GDPR. Further, the individual should have the right to withdraw his or her consent at any time (Article 7(3)). This means that an employer may need to rely on another lawful basis for processing.

Practical tips

- Amend the process and timing for seeking and recording consent to data processing by employees and job applicants. For example, obtain consent within a separate form instead of including a clause in the employment contract which must be agreed to if the candidate is to take up employment. This will give the employer a better argument that the consent is freely given, specific, informed and unambiguous.
- The use and processing of personal data within recruitment processes, during employment and indeed post-employment should be made clear to employees together with the specified purpose for the processing. Consider carefully all purposes that the data may be used for and try to capture them in the consent form; a generic description may not be enough.
- If consent is given in the context of a written declaration which also concerns other matters, the request for consent should be clearly distinguishable from the other matters (Article 7(2)), and in an intelligible and easily accessible form using clear and plain language. This will not be an issue if this is in a separate form.
- An employment contract which contains a provision seeking consent for the processing of an individual's personal data (notwithstanding the above) should make clear that if the individual does not consent to the processing then the employer will not go ahead with processing that person's personal data and will consider appropriate alternatives, to the extent that this is possible.
- Care should be taken to ensure that each issue is considered, and consented to as a separate matter. This right should be made clear to individuals: it should be as easy to withdraw consent as to give it.
- Employers should be wary of making the performance of a contract conditional on an individual giving consent to the processing of personal data when that is not necessary for the performance of the contract. There will likely be more scrutiny of the conditions relied on for processing. "Necessity" is likely to be looked at narrowly.
- There is a statutory requirement for a data protection policy, where proportionate in relation to the processing activities being undertaken (Article 24(2)). Review any existing policy to ensure it is fit for purpose under the GDPR. Check if it is readily available to employees and if they are aware of it and its contents.

5. During employment: enhanced data rights for employees

More transparency and accountability

Employees will have a greater right to transparency with respect to the processing of their personal data. Employers should consider their systems for processing employee data and ensure that there are procedures in place for retrieving data swiftly, enabling rectification and deletion of data, as well as restricting the processing of data. In addition, they will need to ensure they have complied with the GDPR in terms of having a permitted basis for processing the personal data.

The GDPR will require employers to tell employees (like other data subjects) about how their personal data has been processed for example, whether it intends to transfer the personal data outside the EEA and the permitted basis for the transfer, how long it has been retained for and details about the legitimate basis for the processing of their data and their rights. In response to a subject access request the employer will need to notify the employee of: their right to rectification or erasure or restriction of processing and to object to the processing, that they can withdraw any consent they have given and their right to complain to the Information Commissioner. This is more likely to result in those rights being exercised and employees challenging the basis for their personal data to be processed.

Data subject access requests

Fees will be abolished for subject access requests, and new timescales introduced (one month, rather than 40 days, extended to two "where necessary") (Article 15, Article 12(3)). No guidance has been provided as to when this will be. There is no express carve-out for requests made in contemplation of litigation, although employers may refuse consent where a request is "manifestly unfounded and excessive" (Article 12(5)). There is no guidance to date on what may constitute such a request. We expect employers will have to establish a clear policy regarding subject access requests, including limits on the scope of such requests (perhaps the scope of searches or timeline) and data retention periods. This is in line with current ICO guidance. It will likely be necessary for an employer to attempt to narrow the scope of the request with the employee before it can legitimately refuse to action it on the basis that it is manifestly unfounded or excessive. Alternatively, employers may charge a "reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested". Guidance on these points would be welcomed.

Practical tips

- Ensure you have appropriate records in order to be able to answer the questions regarding the legal basis for processing the personal data, how long the data will be held and whether it is transferred outside of the EEA.
- Introduce systems for responding to requests from data subjects for rectification or erasure of their personal data.
- Update your processes for dealing with subject access requests to ensure that you meet the new deadlines for responding to a subject access request and also to provide the additional information requested.
- Consider if any changes need to be made to IT systems in order to respond promptly and effectively to subject access requests under the GDPR.
- Train teams and ensure manager awareness of key aspects of the GDPR.

Data breaches

The GDPR will introduce a new mandatory requirement for data controllers to notify the regulatory authority of personal data breaches, if data is lost or subject to a cyber-attack and there is a risk to individuals. This must be done within 72 hours. The company may also potentially have to notify employees (Articles 33 and 34). Employees should be notified without undue delay when a personal data breach is likely to result in a high risk to their rights and freedoms and their employer has not been able to take steps to ensure that this risk is no longer likely to materialise or to render the personal data unintelligible, for example by encrypting it.

The GDPR will provide for two tiers of sanctions, with maximum fines of up to EUR 20 million or 4% of annual worldwide turnover, whichever is higher (Article 83(5)). Further, all data subjects will have the right to obtain compensation from the relevant controller or processor for damage suffered (including injury to feelings) as a result of processing carried out in breach of the GDPR. The penalties must be applied in a proportionate manner and consistent with due process. The potential for such large fines fundamentally alters the risk profile for data protection compliance.

Practical tips

- Ensure that adequate procedures are in place to detect, report and investigate personal data breaches.
- Assess the potential risk of sanctions for data protection breaches.

6. On termination

Right to be forgotten

Employers will have duties to ensure their systems enable them to amend incorrect information, delete or restrict the processing of personal data and that such rights are communicated to the data subject (Article 17). The GDPR will give data subjects the right to have their personal data erased without undue delay where the personal data is no longer necessary in relation to the purposes for which they were collected, or the individual withdraws their consent on which the processing was based and there is no other legal ground for the processing. This could be particularly relevant in the employment context where data is stored in relation to, for example, a person's disciplinary record or a grievance about them where there is a dispute about whether the information is correct and/or needs to be held on their personnel file, as well as how long it should be held on the file.

Practical tips

- Assess adequacy of data retention policies, particularly in relation to HR files. Information that is no longer needed should be removed from these files (e.g. on backup tapes) where they need to be deleted.
- Consider if any changes need to be made to IT systems to ensure that items are permanently deleted and a digital footprint of them does not remain in the company's possession.

7. Data controllers and data processors - remaining accountable

The GDPR gives statutory recognition to best practice concepts such as data protection by design, imposing greater accountability on data controllers, as well as placing data processors on the hook for certain regulatory liability for the first time. Employers should review processes against this higher standard of best practice and improve where necessary.

The GDPR may require employer's data processing systems to be fundamentally amended, or new systems established. Technical and organisational measures should be in place to keep data secure. This is obviously more difficult when an employer is reliant on outsourced HR functions.

Practical tips

- The use of outsourced HR functions such as payroll may be impacted by new accountability measures focussing on both processors and controllers of data. Processors are likely to seek changes to their contracts with controllers.
- Consider whether the appointment of a data protection officer is required. This will be necessary where the core activities of a company involve large scale regular and systematic monitoring of data subjects or processing of sensitive personal data. Guidance on what constitutes core activities is expected.

8. International human resources transfers

Generally, the GDPR maintains the position of the Data Protection Directive on acceptable international destinations for personal data (inside the EEA is unrestricted; the general prohibition on transfers outside of the EEA remains, albeit slightly amended). Data transfer agreements, and European Commission adequacy decisions continue to feature, and binding corporate rules are given statutory recognition for the first time (Articles 44-49).

Criteria for adequacy decisions are set out, and new possibilities for adequate protection are provided in the form of codes of conduct and certifications. Employers who rely on storing employee data outside the EU should assess compliance with the requirements of the GDPR.

As mentioned above, the GDPR also has extra-territorial effect as it extends to data controllers located outside of the EU who offer goods and services to EU citizens or monitor their behaviour. Non-EU companies which process personal data about EU data subjects in connection with offering goods/services or "monitoring" are in the GDPR's scope for the first time.

Practical tips

- Multinational clients should include details of data transfers outside the EEA and recipients of the data in fair processing statements.
- Take care with the international transfer of employee data where HR resources are outsourced, particularly if they operate remotely or are located within another jurisdiction. At this stage, model clauses that have already been approved by the Commission and have been contractually adopted will continue to apply, as long as consent is appropriate. Note that the legality of model clauses is currently being challenged.
- Consider risks around the international transfer of data when drafting employment contracts and service agreements and ensure clear communications with employees about the use of their data.
- Bear in mind that subject access requests from employees will require employers to notify the employee in the response to the subject access request about any transfer of their data outside the EEA and the justification under the legislation for doing so, so be prepared with that information.

9. Potential for deviations across Member States

- The GDPR allows Member States to provide for more specific rules to ensure the protection of rights and freedoms of employees' personal data in the context of employment (Article 88). This covers all aspects of the employment relationship, including hiring, performance management, terminating employment as well as monitoring systems at the workplace. This may mean that instead of a harmonised approach to the treatment of employee personal data Member States choose to put in place their own rules which are more protective of employee personal data.

10. Sources

The General Data Protection Regulation - Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. To view a copy of the final text, please click **here**.

Information Commissioner Annual Report 2015/16 is here

Information Commissioner's 28 June 2016 Response to the Referendum is here.

11. Contacts

Andrew Taggart, Partner

T +44 20 7466 2434
M +44 7917 461269
andrew.taggart@hsf.com

Peter Frost, Partner

T +44 20 7466 2325
M +44 7919 327049
peter.frost@hsf.com

Tim Leaver, Partner

T +44 20 7466 2305
M +44 7809 200370
tim.leaver@hsf.com

Christine Young, Partner

T +44 20 7466 2845
M +44 7809 200725
christine.young@hsf.com

Tara Grossman, Senior Associate

T +44 20 7466 2797
M +44 7809 200 907
tara.grossman@hsf.com

Jemima Coleman, Professional Support Lawyer

T +44 207 466 2116
M +44 7809 200639
jemima.coleman@hsf.com

If you would like to receive more copies of this briefing, or would like to receive Herbert Smith Freehills briefings from other practice areas, or would like to be taken off the distribution lists for such briefings, please email subscribe@hsf.com.

BANGKOK
Herbert Smith Freehills (Thailand) Ltd
T +66 2657 3888
F +66 2636 0657

BEIJING
Herbert Smith Freehills LLP Beijing Representative Office (UK)
T +86 10 6535 5000
F +86 10 6535 5055

BELFAST
Herbert Smith Freehills LLP
T +44 28 9025 8200
F +44 28 9025 8201

BERLIN
Herbert Smith Freehills Germany LLP
T +49 30 2215 10400
F +49 30 2215 10499

BRISBANE
Herbert Smith Freehills
T +61 7 3258 6666
F +61 7 3258 6444

BRUSSELS
Herbert Smith Freehills LLP
T +32 2 511 7450
F +32 2 511 7772

DOHA
Herbert Smith Freehills Middle East LLP
T +974 4429 4000
F +974 4429 4001

DUBAI
Herbert Smith Freehills LLP
T +971 4 428 6300
F +971 4 365 3171

DÜSSELDORF
Herbert Smith Freehills Germany LLP
T +49 211 975 59000
F +49 211 975 59099

FRANKFURT
Herbert Smith Freehills Germany LLP
T +49 69 2222 82400
F +49 69 2222 82499

HONG KONG
Herbert Smith Freehills
T +852 2845 6639
F +852 2845 9099

JAKARTA
Hiswara Bunjamin and Tandjung
Herbert Smith Freehills LLP associated firm
T +62 21 574 4010
F +62 21 574 4670

JOHANNESBURG
Herbert Smith Freehills South Africa LLP
T +27 11 282 0831
F +27 11 282 0866

LONDON
Herbert Smith Freehills LLP
T +44 20 7374 8000
F +44 20 7374 0888

MADRID
Herbert Smith Freehills Spain LLP
T +34 91 423 4000
F +34 91 423 4001

MELBOURNE
Herbert Smith Freehills
T +61 3 9288 1234
F +61 3 9288 1567

MOSCOW
Herbert Smith Freehills CIS LLP
T +7 495 363 6500
F +7 495 363 6501

NEW YORK
Herbert Smith Freehills New York LLP
T +1 917 542 7600
F +1 917 542 7601

PARIS
Herbert Smith Freehills Paris LLP
T +33 1 53 57 70 70
F +33 1 53 57 70 80

PERTH
Herbert Smith Freehills
T +61 8 9211 7777
F +61 8 9211 7878

RIYADH
The Law Office of Nasser Al-Hamdan
Herbert Smith Freehills LLP associated firm
T +966 11 211 8120
F +966 11 211 8173

SEOUL
Herbert Smith Freehills LLP
Foreign Legal Consultant Office
T +82 2 6321 5600
F +82 2 6321 5601

SHANGHAI
Herbert Smith Freehills LLP Shanghai Representative Office (UK)
T +86 21 2322 2000
F +86 21 2322 2322

SINGAPORE
Herbert Smith Freehills LLP
T +65 6868 8000
F +65 6868 8001

SYDNEY
Herbert Smith Freehills
T +61 2 9225 5000
F +61 2 9322 4000

TOKYO
Herbert Smith Freehills
T +81 3 5412 5412
F +81 3 5412 5413