ADDLESHAW GODDARD

GDPR

Guidance on Employee Personal Data

Introduction

The General Data Protection Regulation (**GDPR**), due to come into force on 25 May 2018, will impose significant new burdens on organisations across Europe including a substantial amount of additional reporting requirements and increased fines and penalties. It is understood that post-Brexit, the UK will continue to adopt a similar standard for data protection as set out in the GDPR. This guide sets out the key changes under the GDPR and the considerations and actions to take in relation to employee personal data.

Why implement new legislation?

The aim of the GDPR is to bring a unified approach to data privacy law in line with modern use of and the international transfer of personal data.

The GDPR is not intended to restrict the processing of personal data, but rather align it to the modern digital world and ensure that such processing is done in a way that protects data subject's rights. For example many organisations outsource services to third parties (e.g. payroll or training services), use cloud hosting services (rather than onsite data racks) and engage with data subject (e.g. through training/surveys) to collect and analyse workforce demographic, knowledge and expertise. Such behaviour will need to be reviewed (but not necessarily restricted) in light of the upcoming GDPR.

What is the scope of the GDPR?

Many of the existing core concepts under the Data Protection Act 1998 (**DPA**) which implements the EU Data Protection Directive 95/46/EC (**Directive**) are reflected in the GDPR. Familiar concepts of personal data, data controllers, and data processors are broadly similar in both the DPA and the GDPR. HR teams will be well aware of how the broad definition of processing under the DPA captures their retrieval, management, transmission, destruction and retention of employee personal data and this will be the case under the GDPR as well.

Under the GDPR **personal data** now includes information relating to a living person, who can be identified directly or indirectly by such information (e.g. name, ID number, location data, an online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that person). Under the GDPR, **sensitive personal data** (which has a higher threshold of protection) will include genetic data, biometric data and data concerning sexual orientation in addition to the previous categories such as race/ethnic origin, trade union membership, health and criminal records.

The GDPR extends the obligations and territorial reach of current data protection legislation. Going forward, data processors who process personal information on behalf of a data controller will have direct statutory obligations. Specific processing terms set out in the GDPR will need to be incorporated in any written agreements between data controllers and data processors. Additionally the GDPR will apply to non-EU companies processing EU individual's personal data for example by selling to, or monitoring the behaviour of, EU citizens.

From a human resource/employment team perspective, the first step is to understand the flow of personal data within the business. For international organisations this will require a further understanding as to how such data flows across borders within the group. For example where employers outsource a particular function, perhaps data hosting (which includes HR data) and/or management of payroll service, such services will be subject to the more stringent obligations under GDPR. Moreover, non-EU affiliates using shared resources and/or centralised functions are likely to be directly affected by the GDPR given its further territorial scope. Organisations should review their existing contracts in light of GDPR, assessing current policies and procedures in place in light of the flow of data across the business. Going forward, the increased obligations and liability under GDPR should be considered in future negotiations to ensure an adequate risk allocation with suppliers. In general, businesses should expect more lengthy and difficult negotiations with suppliers as they try to address their new exposure under GDPR.

Can consent be relied on?

Similar to the DPA, the GDPR also requires the processing of personal data to be in accordance with certain **conditions of processing**. One of these conditions, which is often relied on, is the data subject's consent, with wording in privacy notices and/or employment contracts confirming the employee's consent to the processing of their personal data. The strength of such consent is already questionable under the DPA due to the imbalance of the employer and employee relationship. Furthermore, the consent is often obtained in conjunction with the employment, i.e. to get the job, the employee must sign the employment contract and consent to the processing of personal data.

The GDPR introduces a higher burden for **consent** - it must be freely given, specific, informed and clearly indicated by a statement or positive action. If consent is given through a written declaration it must be clearly distinguishable from other matters and easy to understand.

To obtain specific consent, when processing has multiple purposes and consent is being relied on for each purpose, consent needs to be obtained each purpose. Additionally, prior to giving consent, the employee must be informed they have the right to withdraw consent at any time.

Employers should review the justifications that are relied on for processing employee data and, where relevant, consider whether it will still be appropriate to rely on consent. This should be considered in light of that, even if freely given, consent can be withdrawn. An alternative would be for an employer to rely on the condition that the processing is necessary for legitimate interests (for example when processing personal data for administrative purposes). It is not yet clear as to the higher threshold for sensitive personal data of **explicit consent**, however, it is understood that this will also be required to be freely given, specific, informed and unambiguous.

What is a fair processing notice?

The **transparency** requirements under the GDPR require companies to provide individuals with extensive information about how their personal data is collected, stored and used. This information must be easily accessible, transparent and presented using clear and plain language. In practice, this means that companies will need to include more information in their privacy policies and fair processing notices, as well as retaining more detailed records of their data processing activities in relation to its employees.

In accordance with the concept that personal data must be processed fairly and lawfully, the GDPR requires employers to provide employees and job applicants with detailed fair processing notices. These notices should set out the personal data collected, the type of processing that occurs, retention periods, any international transfer of data; data subject rights such as subject access requests, right to data rectification, erasure, objection to processing and data portability.

GDPR compliance requires an ongoing assessment of processing activities. Any fair processing notices and privacy policies will need to be kept under review to ensure they accurately capture any new types of data collected or any additional or different processing of such data.

Are there additional employee rights?

The rights of future, current and former employees, as data subjects, are extended under the GDPR, presenting greater obligations on employers and HR teams. For example, employees will have a new right of portability, a right to erasure and additional rights in relation to subject access requests.

Right of portability

Data subjects will have the right to request that their personal data be provided to them (or a third party) in a machine readable portable format free of charge. Employers should consider how and where the personal data is held and if such data can be easily transferred in a safe, secure manner without impacting the usability of such data by the data subject. The employer will need to comply with such requests without undue delay, and in any event within one month.

Right to be forgotten (right to erasure)

Data subjects have the right to request for the removal or erasure of personal data, for example if it is no longer necessary, the individual objects to such processing and/or the individual withdraws consent. Not only will employers need to comply with such requests, but it will need to ensure that any third party with whom such employee data was shared, also deletes such data.

Data subject access requests

Under the GDPR the right of data subjects to request information about the personal data processed by employers remains largely the same. However, under the new regime employers must respond without undue delay and in any case within one month of receipt of the request. Additionally, the £10 fee for making a request will also be abolished.

The new data subject rights may present practical issues for employers and HR teams, especially where employee data is spread across multiple or complex systems. Employers will need to update the relevant policies and procedures to reflect the new GDPR requirements. HR teams should review existing procedures in place when responding to data subject access requests to ensure the new time scales can be met.

What is privacy by design and default?

The GDPR requires data controllers to implement appropriate technical and organisational measures to protect a data subject's rights. This can include anonymising or pseudonymisation of data and restricting the amount of personal data processed, the access granted and/or any retention period. Coupled with this, there is an **accountability** principle under the GDPR requiring organisations to be able to demonstrate how they comply with the GDPR.

This requires a cultural shift in approach to personal data protection going forward rather than something that can be done in isolation or as a one-off. HR teams should encourage across the organisation a focus on awareness and training in relation to the new GDPR requirements. Documenting current processing activities on an ongoing basis, conducting **data privacy impact assessments** where necessary and auditing third party providers to ensure that the GDPR requirements are being met.

What are the consequences of breach?

Under the GDPR organisations will be required to report a **personal data breach** within 72 hours to the Information Commissioner. In line with the accountability requirements, all data breaches must be recorded along with details of actions taken. Employers should appoint a data breach response team, outline a response plan and set out a detailed reporting procedure in the updated privacy policy detailing how, when and to whom employees should report data breaches. Employers should also review any reporting requirements and assistance set out in outsourced services agreements.

Depending on the type of GDPR breach, a fine can be imposed of up to the greater of **€20,000,000 or 4% of the total worldwide annual turnover** of the preceding financial year. This is significantly higher than the maximum fine under the DPA of £500,000 for serious breaches.

In addition there may be financial liability to the individual in damages for losses suffered and/or criminal liability.

Lastly, it is worth remembering additional costs that can be incurred as well. Similar to a breach of current data protection legislation, a breach of the GDPR could expose organisations to substantial internal resource spent on responding to requests for information, enforcement notices, internal and external press releases and minimising any negative PR. In relation to employee personal data, HR teams will have to be able to respond quickly and effectively to minimise any exposure of the business.

Next steps

Please see below our GDPR Action Points for HR Teams which will provide you with a useful starting point when considering your organisation's approach to GDPR compliance.

GDPR Action Points for HR Teams

1. Ensure **awareness** within the organisation and amongst key stakeholders as to implications of the upcoming GDPR.

2. Given the broader definition of personal data (including sensitive personal data) and processing and the emphasis on accountability, **document the personal data processed** (e.g. by making an inventory of such data) with particular focus on:

    - what personal data is processed;
    - why such data is processed;
    - where it is located;
    - to and from where it is transferred (internally, externally and outside the EEA); and
    - how long it will be retained.

3. Adopt a **privacy by design approach** and conduct a **Data Protection Impact Assessment**

4. Understand the **legal basis for processing** the different types of personal data. Check fair processing notices, employment contracts and privacy policies. Consider if, as an employer, you are relying on employee consent alone. For example, when obtaining employee health records, we recommend that you outline the reasons for processing, being as transparent as possible through privacy policies and processing notices.

5. **Communicate the privacy information** (such as an updated privacy policy and/or fair processing notice) to employees, providing further detail as required under the GDPR.

6. If you are part of an **international organisation**, consider which jurisdiction you fall under in terms of data protection. Would Binding Corporate Rules or the EU Model Clauses be the right approach for you?

7. Consider **reviewing the organisation's** policies, such as email usage, social media and IT.

8. Given the increased number of **data subject rights**, ensure that operationally the business can comply with individuals' rights and that such rights are communicated to them (for example the right to be forgotten and that copies of personal data must be provided in a portable format). Plan **how to respond to and process subject access requests** in light of the GDPR amendments to requests for fees and response times.

9. Teams should be given **training** as to the changes coming into force.

10. Appoint a **data protection officer** if relevant.

11. Given the new timeframes for breach response, put in place a **data breach reporting plan and response plan/team**.

12. Review the organisation's **data security** (including the security measures adopted by third parties).

The Addleshaw Goddard Team

If you have any further questions or require additional support please feel free to contact AG. In addition to providing you advice, we can arm you with various documents such as GDPR compliant fair processing notices templates and/or privacy policies.

Data Protection and Information Team

HELENA BROWN
Partner
helena.brown@addleshawgoddard.com
0131 222 9544
07407 735118

BEATRICE DUKE
Associate - Leeds
beatrice.duke@addleshawgoddard.com
0113 209 2019
07730 320881

Employment Team

MALCOLM PIKE
Partner
malcolm.pike@addleshawgoddard.com
0161 934 6443
07775 586433

ROSIE KIGHT
Managing Associate
rosie.kight@addleshawgoddard.com
0161 934 6595
07753 627991

Scotland

KIM PATTULLO
Partner
kim.pattullo@addleshawgoddard.com
0131 222 9556
07795 600 446

DAVID HUGHES
Partner
david.hughes@addleshawgoddard.com
0131 222 9837
07740 910 671

addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hong Kong, Leeds, London, Manchester, Muscat, Singapore and Tokyo*

*a formal alliance with Hashidate Law Office