LEWIS SILKIN

Ius Laboris Global HR Lawyers
LEWIS SILKIN

Data Protection and employment

Inside

Introduction

The General Data Protection Regulation (GDPR) is European legislation affecting all organisations that hold personal data on living individuals. It aims to ensure that organisations using and processing personal data do so fairly and lawfully and gives a number of rights to individuals in terms of how they can access their data and influence its use.

The legislation is very much relevant for employers – all of whom will process data on their staff. Data protection compliance is necessarily becoming a high priority for many organisations as there is a potential for significant fines and reputational damage where organisations fail to comply.

This In-brief looks at some of the key issues.

Basic concepts

The *"Data controller"* is the person who has control of the purposes and ways in which personal data are processed. Employers will be data controllers in respect of the data they process about their staff.

"Personal data" is data relating to an identifiable natural person (the "data subject"). A person will be identifiable if they can be identified by reference to their name but also other things such as ID numbers, location data or online identifiers, as well as information relating to the their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data can be information processed on a computer (including e-mails and documents) as well as information held within structured paper filing systems (such as a set of employee files organised by name). The old law made clear that the definition included expressions of opinion about a data subject and whilst the GDPR does not state this explicitly it is reasonable to assume expressions of opinion will still be caught.

"Processing" personal data includes obtaining, holding and using data, as well as changing and deleting it. Essentially, everything an organisation might do to data.

"Special personal data" is a category of sensitive data to which more stringent conditions apply. This includes data revealing ethnic origin, religious or philosophical beliefs, trade union membership and political opinions, genetic and biometric data and data concerning health, sex life, and sexuality.

Data protection principles

All data controllers must comply with the data protection principles. In summary, data must:

- be processed fairly and lawfully and in a transparent manner
- be obtained only for specified, explicit and legitimate purposes and must not be processed in any manner incompatible with those purposes
- be adequate, relevant and limited to what is necessary for said purposes
- be kept in a form which permits identification of data subjects for no longer than is necessary for said purposes
- be accurate and kept up to date, with every reasonable step taken to rectify inaccurate data without delay
- be processed in a manner that ensures appropriate security

Ensuring you have a legal basis for processing

Data controllers must ensure that they have a valid legal basis for processing data. This means that at least one of several statutory conditions must be satisfied. These include:

- where the processing is necessary for the performance of a contract to which the data subject is party (for example, processing an employee's bank account details for the purposes of paying them)
- where the processing is necessary to comply with a legal obligation to which the controller is subject (for example, processing an employee's NI number for tax purposes)
- where the processing is necessary for the purposes of 'legitimate interests' pursued by the controller or by a third party (for example, processing information about an employee's performance)
- where the data subject has given consent

Where special personal data is processed there are additional conditions which must also be satisfied. These include:

- where the data subject has given explicit consent
- where processing is necessary for the purpose of rights or obligations conferred by law on an employer or employee in relation to employment (this could include the employer processing sick notes for statutory sick pay purposes)
- where the processing is necessary for the establishment, exercise or defence of legal claims

Historically, employers have often relied on consent to process employee data, often in the form of very general consent wording in the employment contract. Under the GDPR, consent must be actively and freely given to be valid. Where consent is given in a written declaration that also deals with other matters, the request

for consent must be clearly distinguishable from those other matters. It must be as easy to withdraw consent as it is to give it, and if there is a clear imbalance between the parties, such as in an employment relationship, consent is presumed not to be freely given at all. It is clear from all these factors that signing an employment contract with a general consent clause is not going to be effective. Even where a valid consent can be shown, subjects have the right to withdraw this at any time. Employers are therefore advised to move away from consent and focus on other legal bases.

Data minimisation

Data must be limited to what is necessary in relation to the purposes for which they are processed. Employers must ensure that they do not process more data than they need to – for example by collecting too much extraneous information during recruitment or background checks.

Data retention

Employers should have a policy which sets out the maximum periods for which different categories of data should be stored, and should ensure this is followed. In the employment sphere it will often be necessary to retain data for the purpose of defending against legal claims and many retention periods can be based on the limitation periods for said claims – for example this could mean keeping employee contracts for six years after the employment relationship ends.

Privacy notices

Data subjects are entitled to receive significant information about their data and how it is handled. This "fair processing information" includes information about what data is processed, why, the legal basis for the processing, who has access to the data and how long it will be held for. Controllers will also have to spell out the rights of the data subject – such as the right to withdraw consent to data processing and to lodge a complaint with the ICO.

To meet transparency requirements, the notice should go into sufficient detail for each category of data. For example, an employer may need to inform employees that their bank details would be processed for the purposes of paying them and that the legal basis for this is that it is necessary for the performance of the employment contract.

Meeting the accountability principle

The accountability principle requires a data controller to be able to demonstrate compliance with the GDPR, usually by means of appropriate policies and practices. This should involve:

- undertaking internal audits of what data they process, assessing risks, implementing clear policies and procedures, ensuring these are kept under review, and training staff.
- keeping a record of processing activities carried out. This is explicitly required for employers who employ over 250 people, or who process special data (in practice this will essentially include all employers).
- appointing a Data Protection Officer ('DPO') where required, namely where a controller's core activities require systematic monitoring or the processing of sensitive data on a large scale. Even if a DPO is not required, controllers should ensure there is clear responsibility for data protection compliance within the organisation, although the title of "DPO" should be avoided save where a DPO is required.
- carrying out privacy impact assessments ('PIAs') where processing is likely to result in a high risk to individuals (see below).

Data security and data breaches

Under the GDPR data controllers have a responsibility to ensure the security of the personal data they hold. A range of measures will be appropriate ranging from physical security measures (locks, access controls) to sophisticated technological solutions. Ensuring that the workforce receives targeted training and guidance about their responsibilities when handling personal data is a pre-requisite. Third party processors also need to be vetted and certain contractual obligations imposed on them.

Where a data breach occurs, a data controller must document the facts relating to the breach, its effects and the remedial action taken. Where the breach is likely to lead to a risk to the rights and freedoms of individuals (this could include theft or fraud, reputational damage, loss of confidentiality or other disadvantages) the controller must notify the ICO within 72 hours. Because of the tight timeframe, controllers should have a taskforce trained and ready to respond to a breach and a clear and well publicised policy informing staff of what to do.

Privacy impact assessments

The GDPR imposes a new obligation on data controllers to carry out a privacy impact assessment (PIA) where a processing activity is 'high risk'. An activity will always be considered high risk in the case of large scale monitoring of a publicly accessible area, large scale processing of sensitive data, and some types of automated decision making. However, guidance suggests that other factors will also point to activities being high risk. These include where the processing includes: evaluation or scoring (this would include evaluation of an employee's performance at work); systematic monitoring (which could include routinely monitoring employees' emails or computer use); or processing special data (such as sickness records) or the data of vulnerable data subjects (which, notably, includes employees). The guidance indicates that where two or more factors are present, a PIA will be necessary. As such it is likely that employers will need to carry out a number of PIAs in respect of the processing activities they undertake.

A PIA should describe the processing activity, its purpose, and consider why it is necessary. It should then consider the risks posed in respect of affected data subjects and (i) any existing measures to address these and (ii) whether any further measures could be implemented to reduce the risks.

Transfers of data outside the EEA

Data must not be transferred outside the EEA unless there is adequate protection in the receiving state. Transferring for this purpose includes the hosting of data on servers outside the EEA. Since very few countries outside the EEA have adequate protection (not even the USA), there are certain exceptions that permit disclosure. Your organisation's approach to, and reliance on, these exceptions should be given careful thought and it is again important not to overly rely on consent in this context. The transfer of data outside of the EEA can also be

legitimised by implementation of particular legal safeguards, such as putting into place EU approved contracts between the person sending the data and the person receiving it.

Data subject rights requests

The GDPR has expanded on the rights data subjects have in relation to their data. These now include (subject to certain exemptions):

- a right to access personal data and be given certain information about the processing
- a right to have inaccurate data restricted
- a right of erasure of personal data in certain circumstances, such as where there is no longer a purpose for the processing, or where consent is withdrawn and there is no other valid legal basis
- a right to restrict (freeze) processing in certain circumstances, such as where the subject has contested accuracy or objected
- a right to receive data in a machine-readable format
- a right to object to an act of processing based on the controller's legitimate interest (unless the controller can show compelling legitimate grounds for the processing)

Handling a data subject access request

A data controller receiving a request must make sure that the request comes from the person who is purporting to make it. They must then comply with a subject access request within one month of the request. This time period may be extended by two months in complex cases or if there are a number of requests from the same source. In certain circumstances the controller can refuse to comply. The controller needs to write explaining his position if he is going to refuse or take two months and must do this within one month of receipt of the request.

Where requests are manifestly unfounded or excessive, data controllers may either charge a reasonable fee based on their administrative costs, or refuse to act on the request. There is currently no guidance on when a request will be manifestly unfounded or excessive. In practice our advice is that a dialogue should be established with the data subject to explain the excessive and complex nature of the request and the consequences which flow from that. In many cases it may be unwise to refuse to deal with it altogether and better to seek to narrow the scope of it.

What information to provide

An individual is entitled to be given a copy of information constituting personal data of which s/he is the subject. Although it is normally easiest to supply a copy of the documents, it is permissible to create new documents setting out all the information constituting personal data. Where the data subject makes the request by electronic means such as email the data should be provided in electronic form unless otherwise agreed. The data subject must also be given specific information about the source of the data, how long it will be kept for, who it might be disclosed to, etc.

Third party information

There are complex rules about a subject access request which might result in disclosure of information relating to another individual (a "third party"). If they do not consent, or if it is impracticable or inappropriate to seek consent in the first place, the controller should disclose the information if it is reasonable to do so in all the circumstances. There are certain (though rather rare) circumstances where it may indeed be reasonable to disclose without consent – for example, where the third party is the data subject's line manager, and the data consists of comments made about the subject in a work context. Controllers should always be careful when dealing with third party information as getting this wrong can have serious consequences. If the data controller decides it must withhold the third party information it should still supply as much of the subject's data as it can, redacting where necessary.

Good places to start

Helpful information can be found at www.ico.gov.uk. In addition you should:

- audit the data you hold and what you do with it, who has access to it and how secure it is, how long you keep it, and why, who it is shared with, and why, and so on
- provide privacy notices to employees as above
- audit IT usage policies, BYOD and social media policies, to check sufficient information is given
- audit contracts to ensure that a generic consent is no longer relied upon
- put in place training for employees
- consider how to log, track and comply with subject access requests
- ensure data is kept securely and put in place a data breach protocol
- consider which of your processing activities may be 'high risk' and carry out PIAs where necessary
- audit your contracts with third party providers

For further information on this subject please contact:

Alexander Milner-Smith
Partner
+44 (0) 20 7074 8196
alexander.milner-smith@lewissilkin.com