Anthony Collins
solicitors

GENERAL DATA PROTECTION REGULATIONS

KEY IMPLICATIONS FOR EMPLOYERS

CONTENTS

WHAT ARE THE MAIN CHANGES INTRODUCED BY THE GDPR?

The General Data Protection Regulations (GDPR) will come into force on 25 May 2018 and bring changes to the rules governing data protection and the requirements placed on organisations, which control or process personal data. National laws, including the Data Protection Act 1998 (DPA), will no longer apply to matters falling within the GDPR's scope. This briefing summarises the main changes for employers and highlights key steps HR teams should be taking now.

Whilst many of the requirements imposed by the GDPR are similar to the current law, it will introduce some significant changes. The most relevant points for HR professionals are summarised here:

TRANSPARENCY

There is a new underlying principle of transparency, which is likely to mean employers will have to be more open with their staff about their approach to managing and processing data.

DATA SUBJECT RIGHTS

There are changes to existing rights and some new rights that employees may seek to rely on, namely:

- The right to erasure or to be forgotten.
- The right to the restriction of processing (this strengthens the existing right).
- The right to object to processing (this strengthens the existing rights)

However, there are various exceptions that will apply. There will, no doubt, be employees who will seek to use these rights to make internal disciplinary and capability procedures more difficult. It will be important to ensure your teams have a good knowledge of the exceptions, so that employees don't make your life impossible by incorrectly exercising their rights.

CONSENT

The GDPR reinforces the position that where data controllers rely on consent as a processing ground, the consent must be freely given, specific, informed, and capable of withdrawal at any time. The GDPR makes it clear that consent must also be unambiguous and that silence or pre-ticked boxes cannot constitute consent.

The new law makes it clear that where there is an 'imbalance' of power between the controller and data subject, consent is unlikely to be freely given and therefore is unlikely to be valid.

There are grounds under the new law (and under the existing Data Protection Act - DPA) that are much more likely to be valid for the processing of the 'core' personal data required by employers. For example, the contractual ground for non-sensitive personal data and the 'necessary for an employment contract' ground in relation to sensitive personal data.

It is, therefore, important that employers review the use of consent as a processing ground, bearing in mind that explicit consent may well still need to be relied upon for the processing of sensitive employee personal data in certain circumstances.

PRIVACY NOTICES

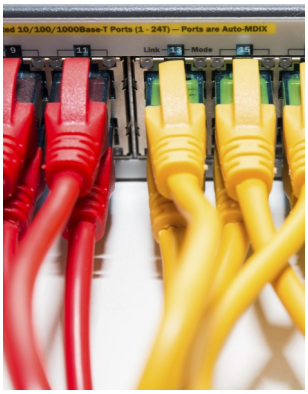
Under the DPA there is a legal requirement under Principle 1, to provide the 'fair processing' information to data subjects at the time that their personal data is first collected or whenever their personal data is disclosed to a third party. This is normally done by way of privacy notice or privacy statement, and the DPA leaves it up to data controllers how they provide the following information to data subjects:

- The identity of the data controller;
- The purposes for which the data are to be processed; and
- 'Any further information' that is necessary to ensure fair processing. The kind of information that is normally provided under this heading usually includes (i) the categories of recipients (ii) retention periods where these are known/reference to retention policy (iii) sources of data.

Under the GDPR, there will be a legal requirement to include a greater category of information within privacy notices, including the information that would fall under the 'further information' category above.

The information that must be notified to the data subject at the time of the first collection of his or her personal data includes:

- The legal basis for processing the information – as is the case now, two grounds will be required where the employee data is 'sensitive personal data';
- The length that it will be held for;
- The source of the data (unless it originates from the data subject);
- Who will receive personal data (or the categories of recipients)?;
- The period for which data will be stored, or if that is not possible the criteria used to determine the period;



Employers will have to be more open with their staff about their approach to managing and processing

- The existence of data subject rights, including subject access, rectification and erasure;
- The right to object to processing on grounds related to an employee's "particular situation", which applies if an employer relies on the "legitimate interest" or "public interest/controller's official authority" condition;
- The right to withdraw consent, if the employer is relying on consent as a legal basis;
- The right to complain to the regulator; and
- The intention of the data controller to transfer personal data to a country outside of the EEA and the legal basis (under the GDPR) for this transfer.

This information should be provided in clear and easy to understand language. The Information Commissioner's Office (ICO) has recently updated its Privacy Notices Code of Practice, which provides useful guidance on how to simplify privacy notices wherever possible. In particular, organisations are encouraged to use icons, where appropriate, to ensure that the message is accessible to those with particular needs. They are also encouraged to use 'layered notices' i.e. making reference within a more general notice where individuals may find the further information they are entitled to regarding how their information is used.

A key change introduced by the GDPR is the need to include, for the first time, the legal grounds for processing individuals' personal data. It is, therefore, important that employers ensure that relevant staff have a good understanding of the GDPR – something that could be covered as part of an organisation's regular and on-going data protection training for all staff.

It will become mandatory for a large number of organisations to have a designated DPO

SUBJECT ACCESS REQUESTS

Under the GDPR, organisations must process requests without undue delay and reply within one month. This can be extended by two months where the complexity of the request justifies it. Extensions may be common for employee data requests, which are, in many cases, complex to handle.

The GDPR does provide for organisations to refuse access requests where they are deemed manifestly unfounded or excessive. However, you must be able to support that decision with clear refusal policies and procedures and must be able to show that the request meets the relevant criteria in those policies.

DATA PROTECTION OFFICERS (DPO)

It will be mandatory for public authorities, or any organisation whose core activities involve systematic monitoring or large-scale processing of sensitive data, to have a designated DPO. We expect many of our housing, education, charity and health and social care provider clients to be caught by this requirement, in addition to those in the local authority sector. In any event, we consider it would be good practice for most organisations to designate a DPO to help ensure compliance, particularly in light of the increased paperwork burden that is to be imposed on both controllers and processors.

DATA PROCESSORS

You will typically rely on other data processors such as your IT, cloud provider, payroll or occupational health provider to process some employee data. It is important that you are clear about the extent to which service providers are controlling key decisions with regard to the data. There are no 'hard and fast' rules on this, and it can sometimes be tricky to ascertain whether or not a provider is a processor or a separate data controller. It is very important to be clear on this as it has significant compliance implications.

Where the service provider is to act as separate data controller, it is important that the ICO's statutory Data Sharing Code of Practice is followed. A data sharing protocol or agreement may be needed.

Where service providers act as data processors, there is already a mandatory legal requirement (under the DPA) to have a written contract that includes the requisite data processing clauses in relation to following documented instructions from data controllers and ensuring the security of the processing. This can either be accomplished by the insertion of appropriate data processing clauses within the service contract or by using a separate data processing contract.

The GDPR tightens the rules on the use of data processors, extending the formal contractual requirements needed between data controllers and processors. It will have an obligation to demonstrate compliance to the controller and to permit inspection and audit. Processors will also be obliged to delete or return all personal data to the controller at the end of the contract, assist the controller where individuals exercise their rights, and notify the controller where the processor believes that an instruction that it has received from the controller would be in breach of the GDPR.

You can, therefore, expect some additional contractual terms to become part of your contractual arrangements with third parties processing data on your behalf.

The GDPR tightens the rules on the use of data processors

DEMONSTRATING COMPLIANCE

The current requirement for data controllers to register with the ICO and pay the annual registration fee is removed under the GDPR, but the trade-off is an increased paperwork burden on organisations, particularly for those organisations (both controllers and processors) with over 250 employees or those that carry out high-risk processing. Clients who process large amounts of sensitive personal data (as set out above) are likely to fall into this category. As suggested previously, clients may find that the appointment of a DPO assists in this regard.

Clearly thought through data protection policies that take into account all the likely forms of processing will, therefore, be important. Consideration should also be given to specific policies in relation to data retention and information security, particularly for larger organisations or those who process large amounts of sensitive personal data.

Employers should also be aware of the mandatory requirement for privacy impact assessments - 'PIAs' (rebranded as 'Data Protection Impact Assessments' under the GDPR). PIAs are not currently mandatory. However, under the GDPR they will have to be carried out well in advance of any proposed new high-risk processing.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Employers will be expected to take steps to build data protection into system design. For example, when designing an online HR system. Measures must be taken to minimise data collected, ensuring it is necessary for the specific purpose for which it was obtained.

DATA BREACHES

There have been many recent examples in the press of personal data being inadvertently left in public places. Employers who discover a personal data breach must notify the regulator promptly and within 72 hours, if feasible. If the notification is not made within this time, the employer must provide a "reasoned justification" explaining the delay. The notification requirement does not apply if the breach is unlikely to result in a risk to data subjects (e.g. because all data on a laptop was encrypted).

The notification must describe what happened and set out the approximate numbers of individuals affected, the likely consequences and the measures taken or proposed. If there is a high risk to a data subject, he or she must be told.

Records must be kept of all data breaches and the action taken, including those in respect of which there was no obligation to notify the regulator.

The three-day time frame means that employers will need to have clear policies on how they handle a breach.

The three-day time frame means that employers will need to have clear policies on how they handle a breach.

CONSEQUENCES OF A BREACH OF THE GDPR

The maximum level of fines under the GDPR is €20 million or 4% of the undertaking's annual worldwide turnover, whichever is higher.

Given the substantial fines for non-compliance, it is clear that data protection is likely to be brought to the forefront and move up the agenda of many organisations. With the implementation date of 25 May 2018, organisations will need to be planning now and ensuring good practice is in place from then.

10 TIPS TO GET YOU STARTED

There will be numerous steps to be taken across organisations - these should help you get started.

1. Decide who is taking overall responsibility for compliance in your organisation and make sure they are given sufficient time to plan and implement any changes needed. Will they be appointed as the DPO? It is important to bear in mind that the DPO role is a statutory one and where one is appointed, the requirements for this role under the GDPR must be adhered to.

2. Carry out an audit to identify all the existing data systems used and the types of personal data processed. This audit may include considering questions such as:

- Why is that data being held?
- Have we considered all personal data that we hold – in both structured paper filing systems and electronic format (including CCTV footage, emails, text messages, audio recordings, photos, data held on USB sticks, CD/DVD, digital cameras and portable hard drives?
- What is the legal basis for processing?
- Do you keep records of disclosures – particularly where exemptions are applied?
- How was it obtained?
- How long will it be retained for? Do you have a Data Retention Policy or schedule? Do you regularly cleanse your systems of data that is no longer needed in accordance with your policies?
- How secure is it (both regarding access and encryption)?
- Is the data ever shared with third parties? If so, on what basis? Do you have contracts in place with data processors that contain the requisite data protection clauses?
- Where you share data with third-party data controllers are you clear on the legal grounds for this sharing? Have you followed the ICO's statutory Data Sharing Code of Practice?
- Do you have current procedures in place to deal with data subjects' rights e.g. in relation to Section 10 objections and subject access? Do your current data privacy notices reflect the actual data collection and processing practices?
- Where you process personal data in the cloud (e.g. staff records) are you clear on where the servers of your cloud provider are located? If outside of the EEA, you will need to consider the DPA requirements for international data transfers under Principle 8.

3. Use the audit as the basis for an employee information asset register which records the outcome of the audit and sets out the legal basis that would be used for processing different types of data. Ensure this is regularly reviewed.

CARRY OUT AN AUDIT OF ALL YOUR CURRENT DATA SYSTEMS AND UNDERSTAND WHAT IS BEING PROCESSED

4. Use the audit process to identify what will need to change to comply with the revised regime. For example, where the business uses consent to justify processing, it is likely that the 'necessary for a performance of a contract' ground will justify the processing of non-sensitive employee data (i.e. data without which the employee could not be employed). The 'legitimate interests' ground may apply in the processing of some non-sensitive and 'non-core' employee personal data (e.g. the posting of an employee's picture on the staff intranet). Please note that there are additional conditions that apply to the use of this processing ground.

5. Regarding sensitive personal data, you will need to find an additional legal ground. The most likely one here is the 'necessary for the performance of an employment contract' ground. Develop and implement a policy on retention and storage of data, including emails.

6. Review any privacy notice or fair processing information given to employees (and job applicants). Consider what additional information will need to be included. For example, what "legitimate interests" are relied on for processing?

7. Review contracts of employment, handbooks and policies to see whether and how they deal with data protection (and in particular, whether contractual "consent'' is sought) and, where necessary, introduce an explicit consent form.

8. Establish a policy (with a timeline) for handling data breaches. Obtain a full picture of exposure to potential data breaches by ensuring that breaches and loss are reported to whoever is responsible.

Where data is being processed by third parties, the starting point is to establish whether they are acting as data processors or separate data controllers. It is important that third parties are clear that they are not able to 'contract out' of the DPA and, regardless of what any service contract states, their identity as controller or processor will be a question of fact in the particular circumstances. A data-processing contract will be required with processors, and a data-sharing protocol or agreement may be needed when sharing with separate data controllers.

FOR MORE INFORMATION

For more information about the impact of the GDPR and what your organisation can do to prepare, please get in touch.

Jane Burns
Solicitor & Data Protection Specialist
Tel: 0121 212 7462
Email: jane.burns@anthonycollins.com

Anthony Collins Solicitors LLP 134 Edmund Street | Birmingham | B3 2ES
www.anthonycollins.com | https://newsroom.anthonycollins.com

Anthony Collins
solicitors