CHANGES TO DATA PROTECTION REQUIREMENTS UNDER THE GENERAL DATA PROTECTION REGULATION (GDPR)

Introduction

What is the GDPR?

Key changes

- appointing a data protection officer
- the accountability principle
- the legal basis for processing and consent
- privacy notices
- subject access requests
- security breach – new notification requirements
- penalties for non-compliance
- right to compensation and liability

Getting ready: what employers need to do

Data protection principles

Glossary of terms

Further information

Useful links
Introduction

The EU’s General Data Protection Regulation (GDPR) will apply from 25 May 2018, bringing about a number of changes which will impact on how employers process, manage and store personal data.

The GDPR, together with a new Data Protection Act 2018, will replace all pre-existing provisions under the Data Protection Act 1998. These changes will continue to apply, regardless of our exit from the EU.

What is the GDPR?

The GDPR significantly updates the provisions outlined in the EU’s pre-existing data protection directive, which forms the basis of the Data Protection Act 1998. It is intended to strengthen and unify data protection for all individuals within the EU.

In addition to EU-based organisations, these requirements will also apply to any company in any country that has responsibility for processing the personal data of EU citizens, including where this relates to the delivery of goods, services or profiling.

Key changes

The provisions of GDPR will necessitate a series of changes that employers will need to consider when processing and handling employee data. These changes will require HR departments to work closely with their governance, legal and IT teams to ensure their organisations are both working to comply with the new law by 25 May 2018, and on an ongoing basis thereafter.

The key changes include:

Appointing a data protection officer

All public authorities (as defined by the Freedom of Information Act 2000) and organisations whose core activities involve the large-scale processing or processing of ‘special category’, or sensitive personal data, will need to appoint a data protection officer (DPO). This will therefore include NHS trusts and foundation trusts.

The role of a DPO has several key duties as defined within article 39 of the regulations.

— Informing and advising the organisation and its employees of their data protection obligations under the GDPR.

— Monitoring the organisation’s compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
— Advising on the necessity of data protection impact assessments (DPIAs) and the manner of their implementation and outcomes.

— Serving as the contact point to the data protection authorities for all data protection issues, including data breach reporting.

— Serving as a contact point for individuals (known as “data subjects”) on privacy matters and subject access requests.

The DPO will be required to act independently in the way they carry out their duties and will need to have a strong understanding of data protection and GDPR.

The DPO should not be a person who makes decisions within the organisation about how data is used. Although not a legal requirement, the EU’s guidelines suggest that it would not be appropriate for employers to give DPO responsibilities to chief executives, IT directors, chief financial officers, chief medical officers or HR directors, given the potential conflict of interest.

The DPO is protected under the legislation and cannot be dismissed or penalised for performing their tasks, and they should have direct report to the board.

**The accountability principle**

An explicit accountability requirement is one of the key changes under GDPR. Organisations are required to show that they comply with the revised data protection principles set out in article 5 of GDPR. A summary of the current data protection principles is provided on page seven.

Accountability concepts appear throughout GDPR and organisations need to consider the following.

— Implementing appropriate and proportionate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies. These arrangements need to be kept under review.

— Maintaining relevant documentation on processing activities.

— Implementing measures that meet the principles of data protection by design and data protection by default. Measures could include:
  — data minimisation, or reducing the amount of personal data you hold
  — pseudonymisation, or replacing identifiable fields within a data record
  — transparency
  — allowing individuals to monitor processing
  — creating and improving security features on an ongoing basis.

— Undertaking data protection impact assessments where appropriate.
From May 2018, employers will need to ensure they keep a record of all their data processing activity and the justification for it, as outlined by the accountability principle.

Pre-existing provisions under the Data Protection Act also make clear that only the necessary personal data required for each specific purpose should be collected, processed and stored. These principles continue to apply, although there is now emphasis on being able to demonstrate the justification for datasets being obtained and used.

The legal basis for processing and consent

Given the accountability principle, it will be even more important for employers to be clear about their legal grounds for collecting, using and retaining personal data.

There are various legal bases for processing personal data, including:

(i) consent
(ii) to comply with legal requirements
(iii) for the discharge of an organisation’s tasks or functions
(iv) because the processing is necessary for the purposes of a contract with the data subject (for example, the employment contract with the employee).

The threshold for valid ‘consent’ for the purposes of processing personal data is higher than in pre-existing data protection requirements. Using consent as the legitimising condition also entitles individuals to certain additional rights under GDPR. Consent is therefore unlikely to be the most appropriate legitimising condition for personal data processing in the context of managing the employment relationship.

Organisations should spend time now establishing what personal data they collect, what purposes it is put to, and the legal basis for processing the information. Multiple legitimising conditions may apply to the same personal data, depending on the circumstances.

The general legal bases for processing ‘special category’, or sensitive personal data, is defined by the GDPR and new Data Protection Act 2018. This provides that, in some circumstances, for example, in equalities monitoring, it may be necessary for employers to have an appropriate policy document which clearly outlines the need for processing that data.

Privacy notices

This provision relates to ensuring that individuals are informed and understand how their personal data may be used, and who it is shared with.

Under the pre-existing data protection law, employers are required to make available to employees and job applicants with a privacy notice setting out certain information.
In future, under the GDPR, employers will need to ensure they provide more
detailed information within their privacy notice(s), such as:

— the identity and contact details of the employer

— contact details for the data protection officer

— who data will be shared with, including any information that may need to be
  shared with other professional bodies either in the UK or across countries

— how long data will be stored for

— the individual’s right to have personal data deleted (the right to be
  forgotten) or rectified in certain circumstances (see further details in the
  paragraph below)

— the individual’s right to make a subject access request (see section below)

— any information provided to individuals including employees in this regard
  must be clear, concise, transparent and easily accessible. Consideration
  should be given to identify the best way, or ways, to present information to
  employees and prospective employees.

Employers are advised to review all documents which require a self-declaration
from job applicants and employees to ensure that the new requirements and the
rights of individuals are made expressly clear.

Where consent is used as the legitimising condition for processing the personal
data, it will also now require employers to request an affirmative opt-in. An
individual’s consent, in regard to the specific usage of their personal data, can no
longer be assumed on the basis that they have indicated ‘yes’ using a pre-ticked
box or have provided a signature or agreement for a range of activities.

Subject access requests

Subject access requests are already an established process under current data
protection laws. However, under GDPR employers will no longer be able to insist
that data will only be provided on payment of a fee. From 25 May 2018, the data
must be passed to the employee or individual for free in the first instance.

A fee can be charged where a request for information is considered manifestly
excessive or unfounded, or, where multiple copies of the same information is
asked for. There is currently limited guidance on what might constitute a
‘manifestly excessive or unfounded’ request, and therefore relying on this
provision should be considered with caution on a case by case basis.
Organisations should ensure that individuals making subject access requests are
made aware of their right to raise a complaint with the ICO or courts if they feel
the manifestly excessive or unfounded provision is unreasonably relied upon.

Organisations will have up to one month to respond to a request. This period can
be extended for up to a further two months where it is considered necessary for
them to present the information because of its complexity. The organisation must
notify the individual that an extended period is required, within the first month of
the request being made. Employers will need to review their subject access request policy and procedures to ensure they reflect these changes.

The Data Protection Act 2018 will outline the potential exemptions to disclosure that will be available to organisations.

**Security breach – new notification requirements**

The GDPR imposes a new mandatory breach reporting requirement. Where there has been a high-risk data breach (such as, an accidental or unlawful loss, or illegal disclosure of personal data which poses a risk to the rights and freedoms of individuals), the employer will need to notify and provide certain information to the ‘supervisory authority’ within 72 hours or, if this is not the case, as soon as possible. In the UK, the supervisory authority is the Information Commissioner’s Office (ICO).

The GDPR requirements for the reporting of information governance incidents in England remain very similar to those outlined in pre-existing guidance on information security incidents issued by NHS Digital.

Also, if the breach has, or is likely to have, a significant negative impact on the rights and freedoms of individuals, employers have a duty to notify those individuals. An example of this is where an individual may be subject to some form of discrimination, or suffer significant reputational/financial damage, or may be placed at a social disadvantage as a direct result of any such breach.

**Penalties for non-compliance**

Organisations can be subject to significant penalties from the ICO where they are found to be in breach of GDPR requirements, as well as face legal claims from individuals or employees whose data protection rights have been infringed.

The ICO has a range of tools available to investigate and take enforcement against non-compliance. The most serious of breaches could potentially result in fines of up to 20 million Euros or 4 per cent of turnover, but a range of other enforcement powers are available to the ICO. The ICO will be required to publish new guidance on how it proposes to exercise its powers.

**Right to compensation and liability**

Article 82 of the regulation sets out provisions to enable any person who has suffered material or non-material damage, including financial loss, distress or other adverse effects, due to an infringement of the GDPR requirements, to claim compensation from the controller and any outsourced data processor. In such cases, the controller and data processor will initially be held jointly liable for any such infringements. Direct liability of data processors is a new concept under the GDPR.

The exception to this provision is where the controller or processor can evidence that they are in no way responsible for the event giving rise to the damage. Currently there is no case law as to how “in no way responsible” will be interpreted. However, it is anticipated to prove difficult to defend.
Getting ready: what employers need to do

There are some important steps for HR departments to take now to prepare for GDPR.

— Identify and meet with the organisation’s data protection officer. You may also need to provide support in developing their job description and the terms of their engagement.

— Carry out a data audit of current HR and other data related processes to identify what data is held, the reasons for which it is processed, and to whom it is disclosed.

— Undertake a gap analysis between existing processes and the new GDPR requirements. Use of the ICO self-assessment toolkit provides a simple starting point.

— Ensure the legal grounds for processing personal data are understood. Where consent is currently relied on, check whether it continues to meet the GDPR requirements.

— Where outsourced data processing providers are used, ensure that the need for due diligence is placed on them, and that contracts with them are updated to reflect the further requirements of GDPR.

— Ensure there are processes in place to ensure that Data Protection Impact Assessments are undertaken where exceptional or high risk uses of personal data apply.

— Review current privacy notices and other forms of processing information and update them to comply with the more detailed information requirements.

— Ensure changes are widely communicated and understood by all staff.

— Consider the organisation’s approach to GDPR training.

Data protection principles

There are eight explicit principles to remember under pre-existing data protection law. These principles, with the addition of a new accountability principle (outlined on page three), continue to be a useful touchstone for handling information under the GDPR.

In summary, personal data must:

1. be fairly and lawfully processed, with a legal basis for processing identified

2. be processed for limited purposes, and not processed in a way incompatible with those purposes

3. be adequate, relevant and not excessive

4. be accurate and kept up to date
5. not be retained longer than necessary
6. processed in line with the data subjects’ rights
7. kept secure, through technical and organisational measures
8. not be transferred to other countries without adequate protection.

Glossary of terms

The following terms are commonly referred to in GDPR and the various responses to it, and are summarised below.

— **Consent of the data subject**: this refers to the specific, informed and unambiguous indication of the data subject’s wishes. This could be by them issuing a statement of their wishes or by clear affirmative action which signifies their agreement to the processing of personal data relating to them.

— **Data subject**: this refers to the person the personal data relates to.

— **Information Commissioner’s Office (ICO)**: this is the independent authority with responsibility to uphold information rights in the public interest.

— **Information Governance Alliance (IGA)**: this is the established body with responsibility for improving information governance across health and social care services. Its members include the Department of Health, NHS England, NHS Digital and Public Health England.

— **Processing**: this refers to any operation or set of operations which is/are performed on personal data. This is regardless as to whether this is by automated or manual means and includes: collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

— **Personal data**: this is any data that relates to an identifiable living person [data subject]. For example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

— **Supervisory body**: where data breaches occur in the NHS in England, this refers to the Information Commissioner’s Office (ICO).
Further information

✓ Further guidance will be signposted on the NHS Employers website as more information becomes available from NHS Digital.
✓ Employer queries may be emailed to us at regulation@nhsemployers.org

Useful links

✓ NHS Digital General Data Protection Regulation guidance
✓ Information Governance Alliance guidance on changes to data protection legislation and why this matters to you
✓ Information Commissioner’s Office key areas to consider
✓ European Digital Rights key issues explained

Contact us
NHS Employers
2 Brewery Wharf
Kendell Street
Leeds LS10 1JR
Published December 2017
© NHS Employers 2017

www.nhsemployers.org
enquiries@nhsemployers.org
www.soundcloud.com/nhsemployers

Twitter: @nhsemployers
LinkedIn: NHS Employers