

APRIL 2018

# GENERAL DATA PROTECTION REGULATION (GDPR) – FREQUENTLY ASKED QUESTIONS

## Introduction

This document aims to assist HR colleagues in fielding any queries they may have or may receive about requirements under the General Data Protection Regulation (GDPR), which comes into effect from 25 May 2018.

The frequently asked questions below are intended to provide clarity on the changes which have a specific impact on the data collected and retained as part of local recruitment and employment check processes. They are not intended to provide legal advice or cover the wider governance issues. Employers are recommended to seek their own legal advice to ensure they are fully compliant with new data protection requirements.

Employers may find it useful to refer to our factsheet on the [Changes to data protection requirements under the General Data Protection Regulation \(GDPR\)](#) which can be found on the NHS Employers website.

## FAQs

### 1. As a HR professional in the NHS, where should I start with GDPR?

In preparing for GDPR, you will need to understand what data you hold and the way that this data is currently being processed. Working with your HR staff to understand the various data processing activities they use is important.

It's also important to work with other colleagues across the organisation, including in your communications department and local staff side, to ensure staff understand their duties and rights under GDPR and share good practice.

The Information Commissioner's Office's (ICO) [12 steps to take now](#) document is a useful read to get you started. The ICO also provide [useful guidance on documentation](#), including templates you can use to document your processing activity.

You may also want to work closely with your organisation's information governance lead, and additional NHS-specific guidance may be published by the NHS Information Governance Alliance.


## 2. I've seen a lot of key terms, but what do they mean in a HR context?

Term	HR use of word
Data controller - Who determines the purpose and processing of data	The employer
Data processor - Processes personal data on behalf of the controller	Pension provider, benefit provider, payroll provider.
Data subject - Person whom the data relates to	Candidate, employee, ex-employee.
Personal data - Information related to an identifiable living individual	Name, address, date of birth.
Processing - The collecting, recording, storing, retrieving of data.	Recruitment, appraisal, health and safety.
Special category of personal data - Biometric data, health information, race or ethnicity, sexual orientation.	Diversity monitoring information, sickness and absence data.

## 3. What do I need to do regarding appointing a Data Protection Officer (DPO)?

If you work for a public authority for the **purposes of the Freedom of Information Act**, your organisation will need to appoint a Data Protection Officer (DPO), and may have done so already. Many other organisations are also likely to need to appoint a DPO. Some key responsibilities of a DPO are as follows:

- to inform staff across the organisation about their responsibilities under GDPR
- to monitor compliance with GDPR issues
- to report to the board of the organisation
- to provide a point of contact for data subjects and the regulator (the ICO) in the event of a breach
- to train staff where necessary.



The DPO could be an external appointment or a current member of staff, but they should not have a role that might lead to a conflict of interests, for instance they should not be a member of the HR team who processes a lot of information. There are no specific required credentials, but they should have knowledge and practical experience of data protection.

For further information, the ICO has produced useful [guidance around the profile of a DPO](#).

#### **4. Will we need to update all employment contracts to comply with GDPR?**

Providing employment contracts are already in compliance with pre-existing data protection laws, any changes employers need to make should be relatively minimal.

Employers should consider and review the lawful basis for their activities relating to processing employee data and determine what the most appropriate basis is, for example, it could be compliance with legal obligations, contractual necessity or consent. These different legal bases may be applicable to different aspects of how/when data is processed.

#### **5. What is the difference between explicit and unambiguous consent?**

The conditions for consent have been strengthened under GDPR.

'Unambiguous consent' refers to ensuring the expression of consent is clear and could not be interpreted as being agreement for something else. This means that requests for personal data are written in clear, plain language as opposed to being in legalistic terms, so that the person giving the consent has absolute clarity about how information will be processed. It is possible for 'unambiguous' consent to be implied through a course of action. For example, someone putting their email address into an optional field (where there is a clear explanation of how their email address will then be used) is 'unambiguous'; it's affirmative action and it's implied but it's not explicit.

'Explicit consent' is one of the possible legitimising conditions for processing 'special category' or sensitive personal data (although alternative conditions, including the specific 'employment' condition may be more appropriate).

The term explicit consent refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement, but alternative methods or approaches may also be possible.

## 6. What does 'special category' or 'sensitive personal data' refer to?

Sensitive personal data is not a new concept but is referred to as 'special category personal data' in GDPR. Data concerning the racial or ethnic origin, sexual orientation, religious beliefs, health data (including information about mental health or disabilities), trade union membership or political opinion may be classed as sensitive data, alongside any genetic/biometric information that could uniquely identify the person in question. Personal data concerning criminal activities or convictions continues to be regarded as 'sensitive' under the new legal regime.

## 7. Does GDPR change how long documentation should be kept on file, for example interview and recruitment information, or personnel files after an employee has left the organisation?

There is no specific timeframe in GDPR that employers must keep data for or must delete data after. The legislation states that personal data should not be kept longer than it is needed for (as per the government's website section on [data protection](#)), and employers should regularly check the data they hold to see whether they still need to retain it, as outlined on the Information Commissioner's Office's (ICO) webpages on [retaining personal data](#).

The NHS has a [standard records retention schedule](#) (including for HR records) which could form a helpful starting point or basis for internal policies.

Like much of the GDPR, adopting a sensible and justifiable approach should be sufficient, for example, a former employee could sensibly have their emergency contact details removed but the organisation would want to retain enough information to know they worked there and still provide a reference if requested. Likewise, interview and recruitment information for unsuccessful candidates should be retained to cover a potential legal challenge around the selection process, but not held further than that.

## 8. We still use quite old technology within our organisation. If problems are caused by not updating technology, for example, a security incident, could we be liable?

Employers could be liable and under GPPR, they will need to show that all appropriate measures to avoid the problem were in place, including technical and organisational measures (although costs can be a factor to take into account in working out what measures need to be put in place). In the event of a security breach, employers will need to show they acted swiftly and had a response plan in place to minimise the damage caused.

Employers need to make sensible and timely decisions as to the severity of any breach. Data breaches should be reported to your supervisory authority (in the UK, this is the Information Commissioner's Office) within 72 hours. In many cases, the individuals affected will need to be notified as well, if the breach is likely to result in 'high risks' to their 'rights and freedoms' (for instance because of the confidential nature of the information involved in an incident, or because there is

a high risk of identity fraud). In assessing whether or not an incident should be reported, guidance can be found in NHS Improvement's own [serious incident framework](#), and [guidance from the ICO](#). Guidance on the kinds of incidents that should be reported is set out in the [Article 29 Working Party's guidance](#) on breach reporting.

However, if the controller has implemented appropriate technical measures to protect the data involved in the incident, for example, encryption, then the ICO and individuals will not need to be notified.

In some circumstances it may take a disproportionate amount of effort to inform everyone affected. In such cases, it may be necessary to give a public notification, for instance on the trust's website and/or in the press to inform those affected.

### **9. When an employee asks for their data to be deleted, what considerations do we need to make?**

The 'right to (ask to be) forgotten' is likely to present employers with grey areas. The onus is going to be on employers to justify any decisions around deleting or not deleting data, for example if a HR department no longer requires data or (where consent is relied on to process the data in question) consent is withdrawn and there is no legal reason to retain it.

There may be a public interest to retain data, such as for income tax/auditing obligations, or where there is an ongoing or possible legal challenge, such as a legal investigation or claim involving an employee. Employers should treat each right to be forgotten request on merit.


### **10. What should be included in a privacy notice?**

A privacy notice should be defined as all the privacy information that an employer makes available or provides to individuals when it collects data about them.

Information supplied within it must be written in clear and plain language, and be concise, easily accessible and provided free of charge. The ICO website provides a checklist of what [privacy information must be supplied](#), as well as their own, comprehensive privacy notice for reference.

It is a good idea to test privacy notices by involving employees or public participation groups in drafting and reviewing notices.

Consideration should also be given to how best to present this information. It may be included in a range of notices specific to the particular processing activities, detailed in the employee handbook, and/or on the organisation's intranet and website.



## 11. Should employers consider their liability for any data processing activity carried out by third parties on their behalf, for example, an agency who carries out employment checks or has access to staff data?

Employers need to choose data processors that provide guarantees that they will meet GDPR requirements. Employers should make sure they conduct due diligence.

Existing contracts should already have clauses around making sure data is secure and processed only on the organisation's instructions. However, GDPR obligations are more extensive and contracts should be updated to cover off these further requirements where possible. The ICO have published guidance on [contracts and liabilities between controllers and processors](#) which you may find useful, and the NHS has also produced revisions to the [NHS standard contract](#) for goods and services which are a helpful starting point.

## 12. Where can I find more advice?

Employers are recommended to seek their own legal advice to ensure they are fully compliant with new data protection requirements.



## Contact us

NHS Employers  
2 Brewery Wharf  
Kendell Street  
Leeds LS10 1JR  
Published April 2018  
© NHS Employers 2018

[www.nhsemployers.org](http://www.nhsemployers.org)  
[enquiries@nhsemployers.org](mailto:enquiries@nhsemployers.org)  
[www.soundcloud.com/nhsemployers](http://www.soundcloud.com/nhsemployers)

 @nhsemployers

 NHS Employers