HR GDPR Factsheet

1 Introduction

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. It represented the biggest overhaul in data protection law for two decades.

1.1 Glossary

First, a brief explanation of the key terms in the GDPR:

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person
Special categories of data (sensitive personal data)	Any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership Data concerning health or a natural person's sex life or sexual orientation Genetic or biometric data processed for the purpose of uniquely identifying a natural person
Data subject	A person described and identifiable by personal data
Processing	Obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, aligning or disclosing any data or information
Data controller	The person/body responsible for deciding how and why personal data is to be processed
Data processor	The person/body tasked with carrying out data processing on behalf of the controller

1.2 Why is the GDPR important?

Many of the GDPR's main concepts and principles are not new—they are familiar from the Data Protection Act 1998 (DPA 1998). There are, however, some new elements and significant enhancements, meaning organisations will have to do some things for the first time and some things differently.

Failure to comply with the GDPR could have serious implications for an organisation's reputation, attract claims by aggrieved data subjects, and expose it to fines up to €20m or 4% of the total worldwide annual turnover of an undertaking (whichever is higher).

1.3 Does the GDPR apply to You?

The GDPR applies to all EU organisations handling personal data.

It is virtually impossible to operate any business without handling personal data, so it's safe to assume your organisation is caught by the GDPR.

Both data processors and data controllers have responsibilities under the GDPR.

Broadly, in its capacity as a commercial organisation supplying services to businesses, it will be both data processor and a data controller.

2 GDPR Principles governing personal data processing

There are six principles governing the processing of personal data - namely:

- **Lawfulness, fairness, and transparency**.
- **Purpose limitation**, which means that:
  - you should only collect personal data for specified, explicit, and legitimate purposes; and
  - you should not process the personal data in a manner that is incompatible with those purposes, except under limited circumstances.
- **Data minimisation**, which means that personal data should be:
  - adequate;
  - relevant; and
  - limited to what is necessary for the purpose of processing.
- **Accuracy**, which means that personal data must be:
  - accurate and kept up-to-date; and
  - corrected or deleted without delay when inaccurate.
- **Storage limitation**, which requires that you keep personal data in identifiable form only for as long as necessary to fulfill the purposes for which it was collected, subject to limited exceptions. It is prudent that you adopt a retention policy which can double as a guidance for this.
- **Integrity and confidentiality**, which requires that you secure personal data by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

The GDPR requires a data controller to both comply and demonstrate that compliance when processing personal; data.

3 Data Protection Officer?

It is not compulsory for all commercial organisations to appoint a Data Protection Officer (**"DPO"**). This is only required in certain instances.

All organisations should, at the least, appoint a member of staff or outside consultant to carry out tasks similar to those of a formally-appointed DPO.

4 Lawful grounds for processing personal data

The driving aim of the GDPR is to protect data subjects and their data. Data subjects include both individual customers and employees.

There are 6 lawful grounds for processing – key grounds are covered in this factsheet.

Processing of personal data will be broadly lawful where the data subject has given their consent or if the processing is necessary:

—for the performance of a contract (if the data subject is a party);

—to comply with a legal obligation;

—to protect the vital interests of the data subject or another natural person;

—to perform a task carried out in the public interest; and/or

—for the pursuit of the legitimate interests of the organisation or a third party.

4.1 Consent of the data subject—lawful ground for processing

Consent has historically been the preferred lawful ground for many commercial organisations, but those organisations should look again at the extent to which consent is relied on. This is because the GDPR raises the bar on what consent means and how it should be obtained, managed and recorded. Under the GDPR consent must be freely given (this precludes the ability to offer "opt-out" in many instances), it must be granular and should no longer be included in contracts of employment. Therefore, if you have historically relied on the consent in your contracts, the contract should be reviewed and new GDPR compliant consents obtained from staff.

Wherever possible, it is advisable that other lawful grounds are relied on instead of consent.

4.2 Contractual performance—lawful ground for processing

Personal data may be processed where necessary:

—for the performance of a contract to which the data subject is party; or

—to take steps at the request of the data subject before entering into a contract.

4.3 Legitimate interests—lawful ground for processing

A commercial organisation can process personal data if it has a genuine and legitimate reason for doing so, unless this is outweighed by harm to the individual's rights and interests.

This requires a balancing exercise: the legitimate interests of the organisation against the fundamental rights and freedoms of the data subject.

There are three elements to consider when considering whether you can rely on the legitimate interests basis and it helps to think of this as a three-part test;

a. Identify a legitimate interest;

b. Show that the processing is necessary to achieve it;

c. Balance it against the individual's interests, rights and freedom.

The legitimate interests test is more likely to succeed if the employees' data is being processed in a way that could reasonably be expected by them.

It will be important to assess upfront which basis is appropriate to process the personal data and document this. It may be possible that more than one basis applies to the processing because you have more than one purpose, and if this is the case then you should make the chosen basis clear from the start.

Be aware that if you choose to rely on consent initially and an employee decides to withdraw their consent at a later date, you **will not** be able to rely on a back up basis of legitimate interests after the fact, to enable you to continue processing this data.

5 Lawful grounds for processing special categories of personal data

There are three main special categories of personal data:

1. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

2. data concerning health or a natural person's sex life or sexual orientation; and
3. genetic or biometric data processed for the purpose of uniquely identifying a natural person.

This was called 'sensitive personal data' under the pre-GDPR regime. You can only process special category (sensitive) personal data if it satisfies at least one of ten conditions in the GDPR. The most relevant and likely conditions are:

—the data subject has given explicit consent;

—processing is necessary in relation to employment, social security and social protection law;

—processing relates to personal data which are manifestly made public by the data subject;

—processing is necessary for the establishment, exercise or defence of legal claims;

Some of the above are subject to further restrictions.

6 Data subjects' rights

The GDPR significantly enhances data subject rights, as summarised below:

Data subject right/request	**Comment**
To be given access to personal data held about them	The GDPR expands the mandatory categories of information which must be supplied You must provide a copy of the personal data free of charge – there is no longer the right to charge £10
To have inaccuracies corrected	This pre-existing right has not significantly changed under the GDPR However, you must now notify any third parties with whom it has shared data if the data subject requests any corrections
To have information erased (the right to be forgotten)	This is a new right to have personal data erased under specific circumstances You must implement new systems and procedures to facilitate this, and to notify affected third parties about the exercise of this right
To object to direct marketing	This is an absolute right—once an individual objects, you must stop processing their data for direct marketing purposes The main difference from the pre-GDPR regime is the need to provide information about the right, - this should be reflected in its privacy notices
To prevent automated decision-making and profiling	The GDPR preserves the previous position, with only minor changes—the explicit consent of the data subject is a valid basis for evaluation on the basis of automated profiling
To be provided with their data in an electronic and commonly used format	This is a new right (known as data portability)

The GDPR also imposes shorter deadlines for dealing with data subject requests, ie one month from receipt of the request.

7 Employees' obligations in respect of the data processing of others

All employees will have access to and will process personal data in some way as part of their job. This may be the personal data of their colleagues, customers or clients. As part of demonstrating compliance with the GDPR, you will need to ensure that employees receive training so that they understand how they are data controllers and/or processors and are aware of the responsibilities the GDPR imposes on them in respect of this. These obligations should tie in with the Staff Handbook and/or standalone GDPR related policies.

8 Other Considerations

You should pay specific consideration to the use of CCTV and tracking devices in vehicles as, whilst not prohibited by the GDPR, specific considerations should be given to these ensure continued use of them is GDPR compliant.

9 Top 5 Key HR considerations

1. Keep data mapping exercises updated to identify where the organisation holds data, what it does with this data and what lawful basis is being relied on for processing it. This is particularly important for Brexit preparations.
2. Revise:
    - data protection, confidentiality and monitoring clauses in contracts,
    - data protection, disciplinary and IT usage policies in handbooks, and
    - privacy notices – recruitment and staff.

    And keep the revisions under review to ensure terminology keeps abreast of Brexit developments.
3. Obtain GDPR compliant consents from staff only where necessary.
4. Create a retention policy.
5. Deliver training to employees – this training should be included in induction sessions as well as by way of refreshers. This training should remind employees of the potential for facing criminal prosecutions outside of their employment.

10 What other key areas should our organisation ensure are GDPR compliant?

- Commercial Terms and Conditions;
- 3rd Party Privacy Notices for your Website/Customers; and
- Marketing Activities

Please contact a member of our Employment Team for further guidance on GDPR.