HR Data Protection Factsheet

1 Introduction

Data protection is not new. However, on 25 May 2018, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) came into force. At that time, this legislation was heralded as representing the biggest overhaul in data protection law for two decades and organisations spent some considerable time preparing for it.

Since its implementation, there has been updated guidance from the Information Commissioners Office (ICO) on how organisations must safeguard data – both in accordance with the GDPR and related legislation. Additionally, as the UK has now left the EU (the transition period having ended on 31 December 2020), there are other changes to be aware of.

This factsheet is designed to cover the key matters you need to be aware of now.

1.1 Glossary

First, a brief explanation of the key terms in the UK 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 What impact has Brexit had on the data protection regime?

Legislation was passed which has had the effect of retaining a body of European law – this includes data protection Brexit legislation. However, there have been some changes to the data protection regime as a result of the new legislation. One immediately obvious change is the renaming of the GDPR which is applicable to the UK – it is now the UK GDPR.

The data protection Brexit legislation refers to the GDPR, which continues to apply to the rest of the EU, as the "EU GDPR".

It is possible that some organisations will have to comply with both the UK GDPR and the EU GDPR.

1.3 Why is the UK GDPR important?

Many of the UK GDPR's main concepts and principles originally derived from the Data Protection Act 1998. There were, however, some new elements and significant enhancements, which meant organisations had to do some things for the first time and some things differently. It's anticipated that many of those changes will have bedded in by now.

Failure to comply with the UK GDPR could have serious implications for an organisation's reputation, attract claims by aggrieved data subjects, and expose it to fines up to £17.5m.

1.4 Does the UK GDPR apply to you?

The UK GDPR applies to all UK organisations handling personal data – this is regardless of whether the processing of that data takes place inside or outside of the UK. This is due to the change in territorial scope that was brought about by the UK GDPR.

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

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

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

2 UK 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 UK 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 UK 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 it should keep under review the extent to which it relies on consent. This is because the bar under the current data protection regime is fairly high in terms of what consent means and how it should be obtained, managed and recorded. It is now the case that 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, those organisations that historically relied on the consent in its contracts were advised to review those contracts and obtain UK GDPR compliant consents from staff.

Now is a good time to again review those consents to ensure they remain consistent with the UKGDPR.

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. If you choose to rely on consent 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:

—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; and

—genetic or biometric data processed for the purpose of uniquely identifying a natural person.

This was called 'sensitive personal data' under the data protection regime which existed before 25 may 2018. You can only process special category personal data if it satisfies at least one of ten conditions in the UK 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 these are subject to further restrictions.

6 Data subjects' rights

Under the UK GDPR a data subject rights are summarised below:

Data subject right/request	Comment
To be given access to personal data held about them	The UK GDPR expands the mandatory categories of information which must be supplied. You must provide a copy of the personal data free of charge – the right to charge £10 having been abolished in May 2018.
To have inaccuracies corrected	This right existed under the pre-May 2018 data protection regime. The only change, was that you must now notify any third parties with whom it has shared data if the data subject requests any corrections. This remains the position under the UK GDPR.

Data subject right/request	Comment
To have information erased (the right to be forgotten)	This right, which was introduced in May 2018, is for personal data to be erased under specific circumstances. You must ensure systems and procedures have been implemented to both facilitate this right and 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 Privacy Notices must provide information about the right,
To prevent automated decision-making and profiling	The only change between the pre and post May 2018 data protection regime is that, now. 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 was a right that was first introduced in May 2018 and is known as data portability.

The UK 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 likely 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 UK GDPR, you will need to continue 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 UK GDPR imposes on them in respect of this. These obligations should tie in with the Staff Handbook and/or standalone UK GDPR related policies.

This is an area that is often overlooked by employers. Since the data protection regime changes in May 2018, the ICO has imposed fines on individuals in their personal capacity where they have breached their data protection obligations whilst processing data in the course of their employment – it's no longer just the organisations that are being fined. For this reason, now is a good time for refresher style training to be given to all employees on their data protection obligations.

8 Other Considerations

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

9 Top 5 Key steps for your organisation to consider

1. Review your organisation's data map to identify where the organisation holds data, what it does with this data and what lawful basis is being relied on for processing it.
2. Review and update:
    - data protection, confidentiality and monitoring clauses in contracts,

- data protection, disciplinary and IT usage policies in handbooks, and
- Privacy Notices – recruitment and staff.

In particular ensure the correct UK GDPR terminology is used,

3. Review those consents from staff upon which the organisation bases it UK GDPR compliance on and update where necessary.
4. Review your organisation's retention policy and ensure its practices reflect this.
5. Deliver refresher data protection training to employees.

Produced: February 2021

wilson browne SOLICITORS

Area	What do we need to do	Status
1. Awareness	Make sure your employees know the: —law is changing —timescale for this change —impact these changes are likely to have	
2. Data Protection Officers	Identify the individual to be tasked with leading data privacy compliance processes.	
3. Information audit/data mapping	Document what personal data your organisation holds, where it came from and who it's shared with	
4. Communicating privacy information	Review current 3rd party privacy notices	
6. Subject access requests	Plan how you will handle requests within the new timescales and provide any additional information	
7. Legal basis for processing personal data	Look at the various types of data processing you carry out and identify and document the legal basis for carrying it out	
8. Consent	Where you rely on individuals' consent to process their data, make sure it will meet the standards required by UK GDPR. If not, alter the consent mechanisms or find an alternative to consent	
9. Data breaches	Implement processes to detect, report and investigate a personal data breach	
10. Data protection by design and data protection impact assessments	Consider whether any upcoming projects or activities present a data privacy risk that should be assessed by a DPIA	

11 Are there any other areas with my organisation that should be aware of UK GDPR?

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