



Data protection and GDPR


A guide for employers –
Newly updated for 2020

Contents


Data protection and GDPR: What employers need to know	3
Checklist	7

Find out more about DWF

 www.dwf.law

 Click here to enter email@dwf.law

 www.linkedin.com/company/dwf

 [@Click here to enter twitter handle](https://twitter.com/Click here to enter twitter handle)

**Brexit
hub** www.dwf.law/brexit

Data protection and GDPR: What employers need to know



The new regime

On 25 May 2018 the General Data Protection Regulation (GDPR) came into effect across all EEA member states including the UK. The UK Data Protection Act 2018 (the DPA) received Royal Assent on 23 May 2018, and replaced the Data Protection Act 1998.

Like all other EU-derived law, the GDPR will become part of the UK law under the European Union (Withdrawal) Act 2018 at the moment of exit. In any event the UK Government has indicated that it wants the continued flow of personal data with the EU to facilitate any trade deals with Europe and the rest of the world.

The fines for breach under the GDPR are significant, compared with the UK's previous maximum fine of £500,000. Under the new regime those who breach the GDPR could be fined up to €20,000,000 or 4% of worldwide annual group turnover, whichever is higher.

The GDPR has far-reaching consequences for both businesses, and employers alike. The responsibility for GDPR compliance rests with senior management who must take active steps to ensure data is controlled and processed across the organisation in accordance with the GDPR. In this briefing we consider some of the useful steps employers should take to ensure they are GDPR compliant.

“ We're all going to have to change how we think about data protection.

Elizabeth Denham – Information Commissioner

Enhanced rights for individuals

GDPR improves and extends the existing rights of individuals in relation to their personal data:

- Right to information and transparency
- Right of access and rectification
- Right of erasure (right to be forgotten)
- Right to restriction
- Right to data portability
- Right to object to processing
- Automated decision making rights
- Right to withdrawal of consent

Employers need to ensure the business is aware of these enhanced rights and that policies and procedures are adapted accordingly. Although many of the rights already existed in some format, the GDPR introduces new concepts and tightens existing law. Employers should take proactive steps now to ensure these enhanced rights are incorporated throughout the employment life cycle.

Personal data and special categories of personal data

The definition of personal data under the GDPR is more detailed and includes information such as online identifiers (for example an IP address). The GDPR redefines "sensitive personal data" as "special categories of personal data" and includes biometric and genetic data.

Personal data	Special categories of personal data
Name/Contact details	Medical information
Bank/payroll details/NI number	Racial or ethnic origin
Salary, annual leave and benefit information	Political opinions
Next of kin/emergency contact information	Religious beliefs
Comments on CVs/records/employment notes	Trade union membership
Education/training information	Genetic data
Employment records	Biometric data
Photograph/CCTV	Sex life and sexual orientation

Lawful processing

Employers process data at every step of the employment relationship from recruitment through to references post termination. Under the GDPR employers need to consider what lawful grounds they have to process employee data. The GDPR includes six grounds for lawful processing of personal data. The key grounds on which employers are likely to rely are:

- **Consent** – which must be freely given (and capable of being withdrawn), specific, informed, unambiguous and given by a

statement or clear affirmative action. Employers can only now rely on consent in very limited circumstances.

- **Contract** – processing is necessary for entering into a contract with the individual or performing the employer's obligations under a contract.
- **Legal obligation** – processing is necessary to perform a legal obligation (other than contractual obligations).
- **Legitimate interests** - processing is necessary for the employer's legitimate interests or those of a third party.

For example: processing payroll information is likely to fall within a number of the grounds such as necessity for the performance of the employment contract, compliance with a legal obligation and necessity for the purpose of legitimate interests. It is important to select only one – we would advise performance of the employment contract.

Processing special categories of personal data

The GDPR implements strict requirements for processing special categories of personal data. In order to process such data there must be a lawful ground for processing (please see above) **and** one of a number of exceptions must be met. The most likely exceptions available for employers include:

- Explicit consent (please see the question of consent below)
- Legal obligation - processing is necessary for complying with the employer's obligations under employment law
- Necessity for reasons of substantial public interest (defined in more detail in the Data Protection Act 2018)
- Necessity in relation to legal claims
- Necessity for the purpose of preventative or occupational medicine for assessing working capacity.

An example of situations in which employers are likely to process special category data is employees' sickness absence and medical records. Employers could potentially justify processing such data for any of the reasons set out above. From a practical point of view it will be important for employers to ensure that: they are clear about their reason for processing such special category data; they are transparent with their employees with regard to the processing; and appropriate records are kept to assist with accountability. As with much of the GDPR, processes, policies and training are essential.

The question of consent

Under the GDPR consent must be freely given, specific, informed, unambiguous and given by a statement or clear affirmative action.

Historically (but not necessarily correctly), many employers have relied on consent contained within employment contracts to permit the processing of employee data. The use of consent and consent clauses and forms should be reviewed in light of the GDPR and updated to rely on alternative lawful grounds as needed. It can often be a difficult balance between conciseness and including all the detail required but we can help.

Consent will not be freely given if there is an imbalance in the relationship or if the individual does not have any real choice over how the data is used. Such an imbalance is always likely to exist in an employer/employee relationship and so, inevitably, since May 2018 employers can no longer rely routinely on consent for processing employment data.

When an organisation decides that consent is the most appropriate basis for processing employee data (and it will no longer be the first choice) it must ensure that it meets the new requirements.

The request for consent must be clearly distinguishable from the rest of the organisation's terms and conditions (and not buried in small print); in an intelligible and easily accessible form and in clear and plain language. The request for consent needs to be very clear. For example, do not have a page with a lot of information and an all-embracing "I consent" box at the end. This may well mean a person is consenting to more than you (or they) intended. The GDPR also requires that consent is as easy to withdraw as it is to give and that withdrawal is acted upon – this can be a technical challenge

The GDPR requires transparency. If an employee is asked to consent to data processing and subsequently withdraws their consent, it would not be transparent or fair for the employer to then say they have alternative grounds for processing and so never really needed the consent. Therefore, select the appropriate lawful basis from the start.

Privacy notices: the right to be informed

Employers are required to provide employees and job applicants with a privacy notice or "fair processing notice", which is often located in a data protection policy or in the small print on standard forms. The GDPR extends the requirement giving data subjects the right to receive more information and more detail about how their data is handled.

Privacy notices should:

- be concise, transparent, intelligible and easily accessible;
- contain basic information specifying what personal data is being collected, how it will be used and who will have access to it;
- highlight any request for consent and explain how it can be withdrawn; and
- be sufficiently brought to employees' attention and not hidden away in other contractual provisions.

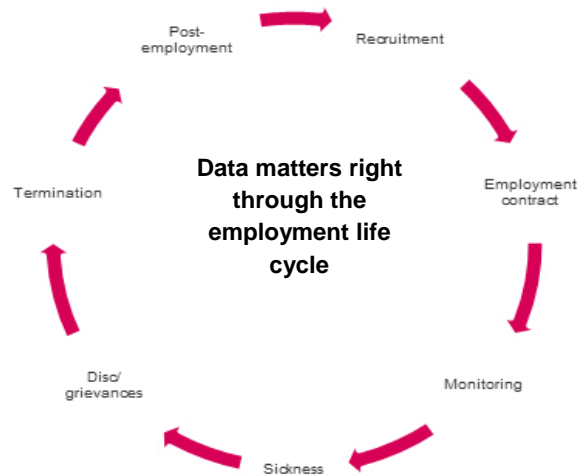
Employers need to review any existing privacy notices to ensure they are compliant with the new extended right to be informed. Employers also need to consider how any revised information should be communicated to their workforce.

"Delete it, freeze it, correct it": the right to erasure, restrict processing and rectification

Data subjects now have increased rights to be forgotten, to restrict how data is processed and to have inaccurate or incomplete personal data rectified.

Employers should ensure internal policies are clear when these rights might be applicable and when a request could be refused. These new data protection rights are already being used in a similar way to Subject Access Requests (SARs) in employment disputes. Data protection specialists in the HR team and elsewhere in the organisation should be trained on how to handle such requests to ensure your organisation complies with the GDPR, deals with requests consistently while balancing the need to protect the business and is in the strongest possible position if a request is refused or in responding to an inappropriate request.

Employees might ask for historic disciplinary warnings to be erased from their personnel files. Employers will need to consider whether they can legitimately justify retaining such information, particularly by reference to any defined retention periods in their policies. In every case employers will need to ask themselves whether they can justify retaining and continuing to process such data under the GDPR. Some rights only apply to some of the lawful bases of processing and some have exceptions, so being clear and selecting the right lawful basis is critical. It should be reflected in your record of processing/data inventory as well as your privacy notice.



HR data processors

It is common for certain HR functions to be outsourced to third parties such as payroll companies, agencies, occupational health and pension providers. The GDPR implements more specific obligations to ensure contractual guarantees are in place to protect employee data, and this applies to pre-May 2018 contracts as well.

As part of their data protection audit, employers should identify third party providers who are data processors, review their agreements with third parties and ensure they are GDPR-compliant. In most cases, it will be easy to identify whether the employer or the third party is the data controller or processor; however, certain activities conducted by third parties may need to be analysed carefully to determine whether the third party is a data controller or data processor.

Automated decision-making and profiling

The GDPR has specific rules in respect of automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate an individual). Employers who use automated decision-making or profiling must be able to demonstrate that the decision is necessary to enter into or perform a contract or based on the individual's explicit consent. For fairness, employers must provide details about the use of automated decision-making, including profiling, in their privacy notice.

Employers need to review any automated processes they have in place which have a significant impact on individuals, including recruitment, sickness absence, performance management and reward and promotion triggers. In addition, recruiters might need to re-consider automated selection procedures and profiling.

Do you need a data protection officer?

The GDPR requires public authorities and private companies who carry out large scale monitoring or large scale processing of special category data (see above) as one of their core activities to appoint a data protection officer (DPO).

The DPO must be independent and the role must not conflict with the DPO's other duties. The DPO should be trained to a high level on data protection law and practice, including the GDPR. DPOs benefit from a number of workplace protections, similar to trade union representatives: for example they must not be dismissed or penalised for carrying out their duties.

Regardless of whether you are required to appoint a DPO, it is important to ensure there are people in your business who are responsible for data protection, understand the new requirements of GDPR and report to the appropriate level.

Data breach response plan

The GDPR requires organisations to report certain breaches to the supervisory authority (in the UK, the Information Commissioner's Office) within 72 hours of anyone in the organisation becoming aware of the breach. Employers will need to ensure that:

- everyone knows how and to whom to report a breach;
- they have effective systems and processes in place for handling data breaches quickly and effectively which balance the need for a swift response with business continuity and confidentiality;
- their DPOs and senior managers are familiar with the organisation's data breach response plan, are trained to identify potential data breaches and know how to handle and report breaches quickly; and
- their data breach response plan includes factors such as taking immediate legal advice, managing PR and staff communications, safeguarding data, evidence and confidentiality, regulatory reporting and other obligations, reporting potential criminal activity to the police and any impact on other policies and procedures such as disciplinary, bribery and corruption. Being ready for potential litigation is also important with a rise in data protection-related claims and settlements.

Criminal record checks

Employers may be concerned about the extent to which criminal record checks can be carried out post-GDPR. Although the GDPR contains a general prohibition on the processing of personal data relating to criminal convictions, the DPA does allow processing in the absence of consent where it is necessary to allow employers to carry out their employment law obligations. The UK is permitted

to deviate from the GDPR under a specific derogation. Provision has also been made for enhanced criminal record checks under the DBS (when working with vulnerable adults and children). The DPA contains provisions requiring appropriate policy documents outlining compliance with the GDPR and details of retention and erasure procedures.

TIP: Only do checks when required – don't have a blanket policy of vetting everyone.

“ We're expecting more of everything. More breach reports...More complaints...Greater engagement.

Elizabeth Denham – Information Commissioner

TUPE and the GDPR

Employers deal with employee data throughout the employment cycle. One area which involves a particularly high volume of employee data is a TUPE (Transfer of Undertakings (Protection of Employment) Regulations 2006) transfer. Transferring businesses are under a legal obligation to provide employee liability information to the transferee business (though this information is provided at a late stage and is fairly limited). This transfer of information is necessary to comply with a legal requirement and this is a legal ground for processing under the GDPR. Any due diligence information about employees which goes beyond the strict legal requirement and is transferred over and above the legal obligation under TUPE should be transferred under another legal basis or should be appropriately redacted.

Even if the information is redacted, it may be pseudonymous rather than anonymous data, in which case it is still personal data and the GDPR will apply. The GDPR defines pseudonymisation as "the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information". So for example, referring to "Employee A" rather than "Joe Bloggs" would be pseudonymised data. Any additional information that identifies the individual must be kept separate from the pseudonymised data.

In practice, be aware that this is a particular problem for data disclosed early in a TUPE transfer where key staff can easily be identified by their salary level.

TIP: Keep good records of what information you disclose in the context of a TUPE transfer and how and when the information is disclosed. This will enable you to locate the data in future and potentially help protect your organisation against claims by ex-employees.

Checklist



Issue	Action	✓
Audit		
<ul style="list-style-type: none">– Consider and implement the key action points outlined above. Data mapping should be prioritised - what data you process, the purpose of processing, with whom you share it , where you send it and how long you keep it. There are limited exceptions to the duty to keep records if the employer has fewer than 250 employees.– Review all existing privacy notices, data protection policies, procedures and contracts. Consider current Data Subject Rights Requests (DSRRs) procedures and ensure those handling DSRRs (including Subject Access Requests) are appropriately trained.– Review existing contracts with third party data processors and update to be GDPR compliant if not already.– If your business operates internationally consider the data flows and which data laws are applicable and ensure compliance. Where data is to be transferred outside the EEA ensure that those transfers are lawful and GDPR compliant. Capture this information through the data mapping exercise.	<ul style="list-style-type: none">– Data mapping– Policy, contract, procedures review– As a minimum review annually. Identify and implement actions.	
Data Protection Impact Assessments (DPIA)		
<ul style="list-style-type: none">– Consider where in the business it might be necessary to conduct data protection impact assessments. DPIAs are required under the GDPR when high-risk processing is taking place, for example systematic and extensive automated decision-making (as referred to above), large scale processing of special categories of data or large scale systematic monitoring of public areas (CCTV).	<ul style="list-style-type: none">– Identify DPIA necessity– Conduct DPIA– Discuss DPIA tool with DWF	
Training		
<ul style="list-style-type: none">– Training is key. Consider who in the business needs training and at what level of detail. Some employees will need a thorough knowledge of the GDPR and its impact on the business, whereas others will just need a basic overview and an understanding of the importance of keeping data safe and their own personal responsibility and accountability. Creating a culture of data understanding is ideal.– Use the training as an opportunity to communicate the revised data protection policies and procedures. Ensure there is a widespread understanding of the difference between "personal data" and "special categories of personal data". List the key GDPR stakeholders and organise a training programme to bring them up to speed.	<ul style="list-style-type: none">– Training plan– Implement training and awareness programme– Communicate revised policies and procedures– Keep records of training attendance and provision. Ensure everyone who handles personal data has training specific to their role	

Everyone in the business should be alive to when personal data is created (emails, lists, text messages etc.) – training and policies are essential.

We can help with all of the above.

Remember 25 May 2018 was just the initial implementation of the GDPR. Data protection requirements are continuing and evolving; it was the starting point, not the finish line. Employers need to put ongoing processes, procedures and reviews in place to ensure they continue effectively manage the employee personal data they process. The ability to demonstrate accountability will be key in the future. Please note that these requirements also apply to your organisation's commercial specialties. Data is an ever-evolving project; having the right structure in place is essential. We understand the challenges businesses are facing and that remaining compliant is a top priority.

A data protection audit

We can offer your business a data protection audit/gap analysis. This would include reviewing your existing contracts, policies and processes, highlighting areas of risk and providing updated, GDPR-compliant documentation. We can also help you implement the changes into your business with a focus on on-going compliance and employee engagement.

Training on GDPR

We can provide a bespoke training programme to suit the needs of your business ensuring the key stakeholders are up to speed on the GDPR and what they need to do to comply. From a high level overview to a step-by-step GDPR practical implementation plan, we will tailor the training to you.

If your business needs help implementing and evolving GDPR please contact your usual DWF contact or one of our team below.

Contacts



JP Buckley

Partner

T 0161 603 5039

M 07513 121 776

E JP.Buckley@dwf.law



Helga Breen

Partner

T 020 7645 9521

M 07730 6616738

E helga.breen@dwf.law



Joanne Frew

Partner

T 0161 603 5099

M 07796 174538

E joanne.frew@dwf.law



Kirsty Rogers

Partner

T 0161 603 5094

M 07808 975877

E Kirsty.rogers@dwf.law



Kate Meadowcroft

Director

T 0333 320 3171

M 07738 985344

E kate.meadowcroft@dwf.law



Charlotte Lloyd-Jones

Professional Support Lawyer

T 0161 838 0478

M 07715 423551

E charlotte.lloyd-jones@dwf.law



Beyond borders, sectors and expectations

DWF is a global legal business, connecting expert services with innovative thinkers across diverse sectors. Like us, our clients recognise that the world is changing fast and the old rules no longer apply.

That's why we're always finding agile ways to tackle new challenges together. But we don't simply claim to be different. We prove it through every detail of our work, across every level. We go beyond conventions and expectations.

Join us on the journey.