G.D.P.R

Staff Guide

H&S | UK

THINK
!nformation

Introduction to G.D.P.R

The Data Protection Act 1998has now been replaced with the General Data Protection Regulations 2018 (GDPR). This guide has been created to help you better understand what has changed and what it means when you handle customer, supplier or any third party data during your working day.

Why the change?

The Data Protection Act was introduced twenty years ago and its purpose to protect personal data from misuse by placing rules on businesses on how personal data was handled, processed and used by that business.

Twenty years on and things have changed greatly, with the introduction of more computer programmes and the holding of personal data in so many formats that the old Data Protection Act really does not offer the protection it should.

The reform comes in the form of the General Data Protection Regulations (GDPR) which takes into account the advances in new technology and media by introducing new rules on how personal data is collected, stored, used or processed.

Although the GDPR is European Legislation, a Bill on Data Protection incorporating the new requirements was laid down in front of the UK parliament and passed into legislation for the UK.

When the UK leaves Europe in 2019, the Act will become The Data Protection Regulations 2018, but the meanings and regulations will remain the same, unless they are updated in further Acts of Parliament in the future.

The regulations will continue to apply to the UK.

What has not changed?

Many aspects of the Data Protection Act 1998 have been incorporated into the GDPR. There will still be principles and conditions that require to be met before personal data can be processed; the UK Information Commissioner (ICO) will continue to be the regulator; individuals still have rights over how and when their personal data is processed; we are still required to provide privacy notices and have appropriate measures in place to ensure that we protect customers personal data.

We still need their permission before we can use their personal data, for example marketing requirements.

What's new?

The GDPR requires certain organisations, such as our business to appoint a responsible person to oversee our Data – they are known as Data Protection Officers.

More than the Data Protection Act, GDPR places a bigger emphasis on accountability and organisations must be able to demonstrate that they comply with the legislation. This means that we will need to record how we handle personal data by having appropriate procedures and policies in place and we will need to be able to demonstrate that these are adhered to.

We will also need to keep records of data breaches, general data management, information management practices and privacy impact assessments.

Individuals have been given greater powers and control over their personal data and how it is used. We will be required to make more information available to individuals about what data we hold, why we hold the data and what we are using that data for.

Previously, if there is a breach of Data Protection it was the company that was responsible for that breach, regardless of whether the processing was carried out by a supplier, printers or third party working for the business. The GDPR changes this as it will now hold both the business, third party provider and even any employee directly involved responsible and each party will be subject to fines or enforcement action. Therefore, we need to monitor what employees and third party suppliers are doing with any data we are responsible for and ensure that all are adhering to the GDPR / Data Protection rules.

What will be the benefit?

Many aspects of the Data Protection Act 1998 have been incorporated into the GDPR. There will still be principles and conditions that require to be met before personal data can be processed; the UK Information Commissioner will continue to oversee the regulations, investigate reported or potential breaches and provide enforcement under UK and EU legislation as required.

We are also now required to better explain what we will do with a customers or suppliers personal data, we will need to demonstrate that we are looking after this data correctly and also explain how they can see what data we hold on them.

Previously, if a customer requested information on the personal data we held on them, we could charge them for this and there was no regulation on what data or time line we needed to supply this data. Now it is a free service and we have 30 days to respond to any requests.

Anyone who we hold personal data on has the right to ask us to amend this data, record up to date information or remove their data from our systems.

We have deadlines, now covered by the regulations that we must met when answering personal data requests, so it is important that if you receive such a request you send the application to the Data Officer for your depot (as shown on page 3 or 4 of this guide).

If you fail to do this then you will breach the Regulations, and, so will the company.

What is personal data?

Personal data is defined as 'any information relating to and identified or identifiable natural person' (a data subject). An identifiable natural person is defined as one who 'can be identified, directly or indirectly, in particular by reference to an identifier such as name, an ID number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural, living, person.

This means that data protection applies to information that directly or indirectly identifies an individual either on its own or by linking it with any other information. This can be a person's name, address, contact number, online profile or record (for example employee HR record or customers sales record).

The information can be held in any format i.e. Paper, electronic, photo's, telephone recordings or CCTV.

The term 'processing' means the collecting, using, sharing, storing and deleting of personal data.

The principles

The GDPR has six principles to ensure that personal data is collected and used appropriately. These state that personal data shall be:

1. **Processed lawfully, fairly and in a transparent manner**. This means that we must have a lawful basis for processing the data and we must inform individuals what we will do with their personal data.

Example: name and address to arrange a delivery.

2. **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. This means that we are not free to use personal data for a purpose different from the one communicated to the individual in a privacy notice.
   Example: taking details for a delivery, then marketing new products to the individual.

3. **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed. This means we should only collect the information needed for the purpose.
   Example: Asking for spouse's details when you have one name, solely to add to a database to market to.

4. **Accurate and, where necessary, kept up to date**. Every reasonable step should be taken to ensure that personal data, where inaccurate, is erased or rectified without delay. This means that we must ensure personal data is regularly reviewed and inaccurate data is rectified, where appropriate.
   Example: Ask your customer or contact to check their details whenever you serve them or speak to them.
5. **Kept in a form which permits the identification of individuals for no longer than is necessary**. This means that we should have a time limit in place for the retention of all data and ensure that it is applied.
   Example: We need to hold data for accounting / HMRC requirements for six years.

6. **Processed in a manner that ensures appropriate security of personal data**. This means that we must ensure that personal data is protected from unauthorised access, unauthorised or unlawful processing, accidental loss, destruction or damage using physical and technical measures.
   Example: Password protected systems, monitoring systems of IT, secured offices.

Processing personal data

For processing of personal data to be lawful, it must meet one of the following conditions.

Necessary for the performance of a contract. This applies when the individual has entered into a sales or order contract with us to supply a service or goods, or an employee for example for an employment contract.

Necessary to enable the company to comply with a legal obligation. For example law enforcement requests (speeding fines), HMRC requirements, Local authority tracing services.

Necessary to protect someone's vital interest. This can only be applied in a life or death situation, such as passing on an employee's health details to the NHS in an emergency.

Necessary for the performance of a task. Which is carried out in the public's interest or for a local authority or government body, for example tracing persons, social services or payment plans attached to income and earnings.

As you can see out of the for, only the first one covers all of our roles, some specialist roles within the business such as HR or senior managers may use options to comply with law enforcement or for the performance of specific tasks.

Consent

The GDPR states that consent must be 'freely given' and, as a supplier of goods, services and an employer we have to demonstrate a fair balance to show the information has been provided to us freely.

In the majority of cases and individual will be unable to access our services or purchase products from us unless they freely offer their personal data to us.

This means that we have to be very careful how we process and use any data provided to us and we must ensure that the individual is fully aware as to why and who we will use the data they have provided to us.

Consent from an individual must be 'informed' these means that pre ticked boxes on forms can no longer be used, the individual must actively put a 'tick in the box' and they must be fully informed as to why we need the data for processing, prior to them giving it to us.

We must inform them why we need the data to complete the service they are using, even if you feel it is obvious.

Special Category Personal Data

As with the Data Protection Act 1998, the GDPR states that certain categories of personal data require heightened protection and if this is collected, we must meet specific 'special category' conditions before it can be processed.

Special category data is:

- A person's race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health, genetic / biometric data
- Sexual orientation or sex life

For dealing with customers and third parties we do not collect any special category personal data, for employees we use hand scanners for payroll security, we therefore have the very latest IT security in place to protect this data.

Processing special category data

Special category data has a different set of conditions and for processing to be lawful it must meet one of the following conditions:

Necessary to carry out a specific obligation or exercise a right in the field of employment, for example payroll, for social security information and protection of pensions.

Necessary to protect an individual's vital interest. This can only be applied in 'life or death' situations, for example a medical emergency.

Necessary to establish, exercise or defend legal claims. This would apply to sharing and individual's data to support or defend a legal claim against the company.

Necessary for reasons of substantial public interest. Not required for us.

Necessary for the purposes of preventative or occupational medicine. For the assessment of the working capacity of an employee, medical diagnosis, the provision of health and social care.

Necessary for reasons of public interest in the area of public health. Not required for us

Necessary for archiving purposes in public interest. For statistical purposes, IE national audit data, it applies to documents that require permanent preservation, for example, Asbestos or certain health reports.

The personal data has been made public by the individual. It has to be obvious that the individual has made the information public, for example of social media or hard copy media.

Privacy notices

Remember, we must inform individuals why we need their data and how we will use this, if we want it for marketing purposes they must freely and actively join our marketing list, this is done by completing the required form.

We must be able to provide the individual with:

- Who the Data Controller is and how to contact them
- Why the data is needed and how it will be used
- What conditions (see previous pages) are being replied upon
- Whether the information will be shared and if so with whom and the grounds around this
- How the data will be kept
- Whether the data will be used for profiling or to make any automated decisions
- How they can make a complaint.

Most of this information is contained within our data policy and on our posters and websites, however, you as an employee, must be able to inform any customers of this.

Individual Rights

As mentioned throughout this handbook, individual's rights have been enhanced and new one introduced with GDPR.

These rights are:

- To be informed how their data will be used – through privacy notices and staff knowledge
- To have access to their personal data – within 30 days, if the request is complex this can be increased to 3 months.
- Have inaccurate data amended
- Object to certain types of processing
- Restrict processing that involves automated decision making and profiling
- Have data deleted – in certain circumstances
- Data transferred to another organisation in certain circumstances

Although some of these rights described above can only be applied in certain circumstances, we are still required to respond to the individual within 30 days even if it does not apply. Staff should pass any request to their depots Data Controller as soon as they receive the request, you can e-mail this to the respective data privacy e-mail address or ask the customer if they would prefer to do this.

The request will be logged, and the individual updated within the legal time frames.

Data breaches

A data breach is when an organisation in its handling of personal data fails to comply with the data protection principles resulting in the loss, destruction or unauthorised access of personal data. They can be a result of human error, failure to follow procedure or by not having appropriate procedures or controls in place.

All staff must ensure they are trained and aware of the company's policies and procedures concerning GDPR. For new staff, it must be part of their first day induction.

Under GDPR it is mandatory to report some serious breaches to the ICO within 72 hours of identification of the breach and failure to do so could result in the company being fined.

The individuals affected may also need to be notified, if this is the case the company Data officer will complete this task, employees are not to make contact.

All potential breaches of GDPR must be reported to your depots data officer without delay, these will then be recorded.

Enforcement

The Information Commissioner will continue to be the regulator for Data Protection. As the Regulator, the ICO has investigative and corrective powers to ensure that Data Protection Legislation is adhered to by organisations.

Under GDPR, fines the ICO can issue for breaches of Data Protection have significantly increased to 10,000,000 euros or 2% of annual turnover (group turnover) for breaches that concern failure to report a breach, carry out a DPIA or to keep appropriate records of processing.

This increased significantly to 17,000,000 euros or 4% of annual turnover for breaches that concern individual rights, the principles or non-compliance with an enforcement notice.

Whilst the ICO has reported that is sees fines as a last resort, it will normally issue enforcement notices, they remind businesses that they have this power and where required fines will be issued.

An enforcement notice would inform us what remedial actions we must take and the time frame we must complete them within.

Enforcement notices are published on the ICO website, so our customers, suppliers and third parties would all be able to see these, therefore an enforcement notice alone can be very damaging to the business.

Further help & advice


PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA
UNDER THE GDPR
Lawfully
Process personal data only when there is an appropriate legal basis or legislative measure under the GDPR, EU, or Member State Law.
Fairly
Taking into account the specific circumstances and context in which the personal data is processed, provide all the information necessary to ensure fairness and transparent processing.
Transparent
Ensure that all risk, rules, safeguards, and rights concerning the processing are informed to the data subject in a concise, easily accessible and easy to understand manner.
Purpose
Personal data may only be collected for specified (defined), explicit (clear) and legitimate purposes (legal basis) determined up-front and, be processed in a manner compatible with it. Exempt. Art. 6(4) and 89(1)
Minimisation
Process personal data only when it is adequate (appropriate), relevant (pertinent) and limited to what is necessary for the purposes for which they are processed (not excessive). Focus on storage limit.
Accuracy
Take every reasonable step to ensure that personal data are accurate and up to date concerning the specific purposes for which they are processed.
Storage Limit
Keep the personal data as far as necessary to identify the data subjects for the purposes established; otherwise, should be erased. Exempt. Art. 89(1)
Integrity
and Confidentiality to process personal data in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and accidental loss, destruction or damage.
Accountability
refers to the duty to comply with the principles and be able to demonstrate that processing is performed in accordance with them.