DATA PROTECTION ACT 2018 AND GDPR FOR EMPLOYERS

In May 2018 the Data Protection Act was updated and incorporated the EU General Data Protection Regulation (GDPR).

Following Brexit, the EU GDPR has been incorporated into UK GDPR coming into effect on 1st January 2021, essentially meaning that EU GDPR and UK GDPR share all the same core principles, rights and obligations.

The UK GDPR sits alongside the DPA (Data Protection Act) 2018 with some technical amendments so that it works in a UK context.

Third parties which operate inside the EU will still have to comply with EU GDPR so make sure you check your data controllers and suppliers to understand where they operate and that they comply with their relevant GDPR requirements. You must also comply with EU GDPR if you provide goods or services to individuals in the EU or monitor the behaviour of individuals in the EU.

If you solely focus on UK individuals and all third parties operate inside the UK then only UK GDPR will apply to your business.

The data protection laws impose greater accountability to businesses and give more power to the individuals regarding their personal data. Also these laws give the Information Commissioner's Office the right to impose fines and penalties to businesses which do not abide by the laws. These fines can reach up to £16,840 or 4% or annual global turnover - whichever is higher (correct at the time of writing).

WHAT DATA PROTECTION PRINCIPLES HAS THE GDPR INTRODUCED TO UK LAW?

All businesses that process personal or sensitive data must put technical and organisational measures in place to ensure compliance with the following six data principles:

1. Lawful, fair and transparent processing of data.
2. The purpose for which personal data is collected must be specified, explicit and legitimate, and the data must be processed in a manner that remains compatible with the initial purpose for which it is collected.
3. Data is not excessive and remains adequate and relevant data to the purpose.
4. Accuracy of data is maintained.
5. Data is stored for no longer than is necessary.
6. Appropriate measures are taken to ensure data is processed in a secure manner.

WHAT IS PERSONAL DATA?

Personal data is defined as any data that could lead to the identification of the individual. This principle relates to customers, employees, clients, suppliers or any other identified or living individual.

An individual can be identified directly or indirectly from:

- A name
- An identification number
- Location data
- An online identifier
- Other specific factors that can identify the individual

In the context of employment even things such as minutes of a disciplinary meeting, as an employee could have a unique length of meeting, can identify an individual and therefore this data must be protected appropriately.

WHAT IS SENSITIVE PERSONAL DATA?

The GDPR refers to sensitive personal data as “special categories of personal data”

These are:

- Race or ethnic origin
- Political opinions
- Trade Union membership
- Religious or other philosophical beliefs
- Physical or mental health
- Sexual life or sexual orientation
- Unique genetic or biometric identification

Processing personal data which reveals any special categories of personal data is prohibited unless:

- The data subject has given explicit consent and there is a lawful basis for the processing
- Processing necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Processing necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided that the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject.
- Processing necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Processing necessary for reasons of substantial public interest on the basis of EU or Member State law
- Processing necessary for reasons of preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or

management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional
- Processing necessary for the reasons of public interest in the area of public health
- Processing necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

Situations could arise which mean that the employer does not need to ask for consent from the data subject. For example, if the employer is responding to a request form Jobcentre Plus to give the reasons why an individual is no longer employed at the company or if the employer is providing the individual's data to the local authorities to assist with their safeguarding investigation.

CRIMINAL CONVICTIONS

Certain circumstances can require a prospective employee or worker to do either voluntary disclosure or official criminal records checks through the Disclosure and Barring Service. Employers are not allowed to carry out criminal records checks as a matter or routine however.

The new data protection laws allow you to carry out criminal records checks only when necessary. This also applies when the employees are subject to the enhanced DBS regime for a specific role. If this does apply then the employer must comply with GDPR mechanisms. This includes having policies in place which clarify how you ensure to comply with data protection principles and outlines the special measures and safeguards that you have in place to keep the information safe. The policy must outline the amount of time to which the data will be held (only as long as necessary) and process of retention and erasure of the data.

If the data subject has provided permission that meets GDPR then employers are allowed to process criminal conviction data.

If information in relation to convictions and offences is requested you must also set out what type of processing will happen and the legal justification of the processing.

WHAT IS PROCESSING?

Processing occurs when any of the following activities are performed in relation to the data:

- Collection, recording, organisation, structuring or storage
- Adaptation or alteration
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination
- Restriction, erasure or destruction

WHO IS A DATA CONTROLLER OR PROCESSOR?

A data controller can be an actual person or legal entity who will either individually or jointly with others determine for what purpose the personal data is processed and the manner of which the processing takes place.

A processor is an individual or legal entity who acts on behalf of the controller to carry out the processing of personal data and is instructed by the controller.

WHAT IS A FILING SYSTEM?

A filing system is an structured set of personal data, accessible according to specific criteria held:

- Automated or by manual means
- Centralised, decentralised or dispersed
- On a functional or geographical basis

HOW TO DEAL WITH A SUBJECT ACCESS REQUEST UNDER GDPR

Initially you must identify the person making the request using “reasonable means" . If the request you receive is electronic then you should provide the information requested in a commonly used electronic format. There is a potentially controversial best practice recommendation in the GDPR that, where possible, organisations should be able to provide remote access to a secure self-service system which 4 would provide the individual with direct access to his or her information. The ICO acknowledges that this will not be appropriate for all organisations, particularly SME’s. The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

Large amounts of pergola data can be requested. When this happens the GDPR allows you to ask the individual to specify the information that the request relates to.

CHARGING FOR ACCESS

Businesses must provide the information free of charge unless the request is excessive or particularly repetitive, in these circumstances a business can charge a ‘reasonable fee’. Additionally if a client makes a request for further copies which have already been supplied then the business is again entitled to charge a ‘reasonable fee’.

REFUSAL TO COMPLY WITH SUBJECT ACCESS REQUEST

If you decide to refuse an access request then you must without delay and at the latest within a month:

- Give your reasons for your refusal to the individual.
- Inform the individual of their right to complain to the supervisory authority (ICO)
- Inform them of their right to a judicial remedy.

Data controllers can also withhold personal data if disclosing it would “adversely affect the rights and freedoms of others”.

REPLY TO SUBJECT ACCESS REQUEST IN ONE MONTH

Information should be supplied within a month of the request unless the request is complex or nyumerious. If you require an extension then you must request it within a month and explain why you need it.

WHAT INFORMATION IS THE DATA SUBJECT ENTITLED TO?

Individuals will have the following rights regarding their personal data:

- To be informed that their data is being processed
- Access to their personal data
- Rectification of inaccurate data
- Erasure of data
- Restriction of data processing
- Portability of data
- Objection of data processing
- Request a human to make a decision in some cases rather than a machine or automated profiling system.

TO BE INFORMED THAT THEIR DATA IS BEING PROCESSED

Employers must provide detailed privacy notices to employees and new applicants. The notices must inform them of how long their data will be stored and whether it will be transferred to other countries.

It will also outline the rights they have for their data to be deleted or rectified and also their right to request to see their data by making a data subject access request.

RECTIFICATION OF INACCURATE DATA

If someone requests their data to be rectified as it is inaccurate then you have to make the relevant changes within a month, unless the rectification is complex and then you are entitled to an extension of an additional 2 months. If you refuse their request you must let them know within a month and your reasoning for the denial.

Additionally you must inform them that they have the right to complain to the Information Commissioner's Office and to a judicial trial regarding their requests denial.

Where this personal data was shared with third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

ERASURE OF DATA

The right to erasure is also known as 'the right to be forgotten', it enables individuals to request the deletion or removal of their personal data when there is no legitimate reason for their data to still be held. Please note that the right to be forgotten is not an absolute right.

Examples of when it will apply include:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR)
- The personal data has to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

If the processing causes damage or distress to an individual it would make the request for erasure stronger. However there are circumstances where the right to erasure does not apply and you can refuse a request. For example:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation
- If it's necessary or the performance of a public interest task or exercise of official authority
- Archiving purposes in the public interest, scientific research historical research or statistical purposes
- The exercise or defence of legal claims

You are required to tell third parties about the erasure of data, unless it is impossible to do so or it would take a disproportionate amount of effort.

Businesses who make personal data public online should inform other organisations who process the personal data to erase links, copies or replication of the data in question. For example, if you process personal data online you must comply with these requirements.

RESTRICTION OF DATA PROCESSING

Under the GDPR you'll be required to restrict the processing of personal data in the following four circumstances:

1. Where there is a dispute over the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data
2. Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual
3. When processing is unlawful and the individual opposes erasure and requests restriction instead
4. If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must also inform individuals when you decide to lift a restriction on processing.

OBJECTION OF DATA PROCESSING

Individuals can block or suppress their data being processed. In this circumstance you can store the data but not process it. You are able to have enough information about the individual to ensure that the restriction is maintained in the future.

PORTABILITY OF DATA

Also known as data portability. This means that the data subject can request the movement of their data between data controllers. An example of when a request may arise could be in relation to an employee asking for their automated payroll or pension data to be sent to another data controller. The request must be adhered to within one month, the latest 2 months if the request is complex. The data transfer must be free of charge.

REQUESTING A HUMAN

If your business uses algorithms during the recruitment process or does any other form of automated profiling, you should be aware that the individuals who are subjected to machine profiling or any other form of automated decision, have the right to request that the assessment should be performed by a human.

Trimming down HR processes to automated systems to sift through applications may still be permissible but businesses should ensure that as and when requested a human is at hand to review the application or any other automated decision.

DATA BREACHES

WHAT TYPE OF BREACH WILL TRIGGER A NOTIFICATION TO THE ICO?

If there is a risk to the rights and freedoms of the individuals then you must notify the ICO (Information commissioner's office). A breach will arise if there is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Essentially, it's a breach that is more than just losing personal data.

It means if you were to do nothing then the breach is likely to have a significant detrimental effect on the individual(s).

The ICO gives the following examples of significant detrimental effect on the individual(s): result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This has to be decided on a case by case basis. Businesses are able to have a small window to investigate personal data breaches and to decide whether to report it or not, to either the ICO and/or their customers.

If the breach is deemed reportable then a business has 72 hours to report it. If it is a report which needs to go out to the public then it should be done with no delay. If you fail to report a breach which should have been reported then you could receive an ICO fine.

Fines can reach up to £8.4 million or 2% of the company's global annual turnover, whichever is higher.

DETAILS OF A BREACH NOTIFICATION

The notification should include the following information:

- The nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned;
    - the categories and approximate number of personal data records concerned
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

WHAT SHOULD YOU DO TO PREPARE FOR BREACH REPORTING?

You should train your staff on what constitutes a data breach for notification purposes, and that this is more than a loss of personal data.

Alongside this, create an internal breach reporting procedure. This will facilitate decision-making about whether you need to notify the ICO or the public.

HOW TO DEMONSTRATE COMPLIANCE WITH THE GDPR

This is a non-exhaustive list of what the ICO suggests you can do to demonstrate compliance with the GDPR:

- Implement measures that meet each of the principles of data protection
- Establish appropriate governance policies and audits to ensure and demonstrate that you comply with the principles
- Keeping relevant internal records of your processing activities
- Appoint a data protection officer (where needed).

WHAT INFORMATION SHOULD YOU INCLUDE IN A DPIA?

Your DPIA should focus on three main areas:

1. Employees (i.e. as they are likely to control and process the data)
2. Your processes (i.e. how you obtain the data and process it, where you store and send it)
3. Risk reduction measures (i.e. IT and cyber security issues, data encryption etc.).

The document should contain a description of your processing, why it is necessary, an assessment of the risks associated with the data processing and the measures your company will have in place as to minimise risks.

Training staff on how to properly process data is essential to avoiding breaches etc. Having clear policy and enforcing it is an effective way to ensure data is being processed appropriately. You should investigate which risk management measures you can implement to show your business's compliance with the GDPR.

KEEPING RELEVANT INTERNAL RECORDS OF YOUR PROCESSING ACTIVITY

You must maintain processing activity records if your company has more than 250 employees. If your company has less than 250 you are only required to keep records of processing activities that:

- Are not occasional
- Could result in high risk to the rights and freedoms of individuals; or
- If you process special categories of data or criminal convictions.

Here is a list of typical items you should record:

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer)
- Purposes of the processing
- Description of the categories of individuals and categories of personal data
- Categories of recipients of personal data

- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
- Retention schedules
- Description of technical and organisational security measures

WHAT CONSTITUTES HIGH RISK?

ICO examples of data processing with high risk:

- Profiling and evaluation resulting in decisions that have a legal effect (or similar effect) – meaning extensive processing activities or system driven activities
- Large scale processing of special categories of data
- The use of large scale and/or systematic monitoring of public areas (CCTV)

PRIVACY IMPACT ASSESSMENT (PIA)

A PIA assessment helps you identify and reduce risks involved in projects and processes which you perform in your business. Benefits of doing a PIA include reducing risks of harm due to misuse of personal information, it will also aid in you design more effective and efficient policies and processes for handling personal data.

You do not have to do a DPIA and if you choose not to you still need to do the following:

1. Assess your data handling activities
2. Find out more and share the knowledge through training
3. Policies, plans and procedures
4. Identify who in your business will be responsible for handling subject access requests and make sure that they are properly trained.
5. Create internal procedures for subject access requests and communicate this to your staff
6. Create a standard response letter that ensures compliance with the GDPR
7. Consider how you can improve your systems to respond to specific requests and to provide the information in a format that complies with the GDPR
8. Investigate if you need a secure remote access portal and the benefits it may give your business

ASSESS YOUR DATA HANDLING ACTIVITIES

- Do an internal audit
- Ensure your system store data appropriately
- Securely delete unnecessary data
- If involving children, use clear and plain language that they will understand. If you supply “information society services” to children you must show you have processes which verify age and get parental/guardian consent where needed.

- Consider appointing a Data Protection Officer or Data Representative

POLICIES PLANS AND PROCEDURES

- Ensure that all data security, handling and processing arrangements are set out policies or procedures and are regularly reviewed and updated
- Prepare a plan/policy for handling subject access requests or requests for additional information under the GDPR and communicate your plan/policy to your staff
- Prepare a security framework and an emergency preparedness plan which outlines clearly how personal data is to be handled and secured, and what employees should do if there is a breach
- Review and amend your privacy policies for your customers/suppliers/third party data controllers
- Evaluate and review your data consent processes in preparation for the GDPR
- Consent under the GDPR must be: freely given, specific, informed and unambiguous.
- You must not only get consent to send commercial emails but you must also keep records of this consent
- On all new projects or where you are using new technologies where the processing is likely to a result in a high risk, do a Data Protection Impact Assessment
- If your buy data or buy a client database from a third party make sure that you obtain documentation to show compliance with the GDPR
- Businesses that carry out cross-border processing should identify their main supervisory authority and record this information

UK EMPLOYERS THAT RECEIVE PERSONAL DATA FROM THE EU FOLLOWING BREXIT

The EU has adopted ‘adequacy decisions’ for the UK. This means that there is still free flow of personal data from the EU/EEA to the UK. This is due to the European Commision deciding that the UK offers an equivalent level of protection to data as the EU does. This means personal data can be sent from country to country in the EU or UK without further safeguards required.

USEFUL LINKS:

- ICO guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- Data Protection Guidance: https://www.gov.uk/data-protection

Save trees, save paper. Please consider the environment before printing this document.