Tollers' Guide To The General Data Protection Regulation

...Talk to tollers

INTRODUCTION

The General Data Protection Regulation (often referred to as GDPR) comes into force on 25 May 2018. The purpose of GDPR is to put in place a single data protection regime that applies across the EU and it will replace all existing national data protection laws in member states.

Everyone will be affected by this new law, whether a business or an individual. In this guide we summarise the key points arising from GDPR and at the end of the guide we set out some steps you can start taking now in order to prepare for its coming into force.

WILL BREXIT AFFECT GDPR?

GDPR comes into force 10 months before the UK leaves the EU. Until Brexit actually occurs then GDPR will apply automatically. There is no need for the UK government to put in place implementing legislation as the Regulation has direct effect across all EU member states.

Following Brexit it is anticipated that a UK version of GDPR will be put in place. In the Queen's speech in June 2017 one of the key bills announced was a Data Protection Bill. The Bill has now been published and is at the start of its progress through Parliament.

Even after Brexit, GDPR will still apply to all businesses that process personal data about, or who monitor the behaviour of, living individuals in the EU.

WHAT IS PERSONAL DATA?

Personal data is any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, by reference to a piece of information such as a name, address or identification number. An online identifier such as an IP address can be personal data.

For most companies personal data will be included in your HR records, your customer lists and contact databases.

GDPR applies both to electronic/ online records and communications, and to manual filing systems. Certain categories of data are known as **Sensitive Personal Data** or **special categories of data**.

Sensitive personal data includes data relating to an individual's:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Health.
- Sex life .
- Sexual orientation.

Sensitive personal data also includes genetic data and biometric data which can be processed to identify an individual.


Even after Brexit, GDPR will still apply to all businesses that process personal data about individuals in the EU...

THE KEY PRINCIPLES

Personal data must be processed in accordance with the following principles:

1. It must be processed lawfully, fairly and in a transparent manner.

2. It must be collected for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes.

3. It must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

4. It must be accurate and, where necessary, kept up to date. Inaccurate data should be erased or rectified without delay.

5. It should be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data is processed.

6. It should be processed in manner that ensures appropriate security of the personal data including protection against unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The controller of the data (i.e. the person who decides the purposes for which data is processed and means by which it is processed) is responsible for, and is required to be able to demonstrate compliance with the above principles.

LAWFUL PROCESSING

In order to demonstrate that the processing of personal data is lawful a business must determine the legal basis for processing the data and must document this.

The legal requirements for processing personal data are:

1. The consent of the data subject.
2. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into such a contract.
3. Processing is necessary for compliance with a legal obligation.
4. Processing is necessary in the vital interests of the data subject or another person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party unless those interests are overridden by the interests, rights or freedoms of the data subject.

In addition, the conditions for processing special categories of data are:

1. You must have the explicit consent of the data subject, unless reliance on consent is prohibited by law.
2. Processing must be necessary for carrying out obligations under employment, social security or social protection law or under a collective agreement.
3. Processing is necessary to protect the vital interests of the data subject or another individual where the data subject is physically or legally incapable of giving consent.
4. Processing is carried out by a not-for–profit body with a political, philosophical, religious or trade union aim provided that processing relates only to members of that body.
5. The processing relates to data made public by the data subject.
6. Processing is necessary in relation to the establishment, defence or exercise of legal claims or in connection with court proceedings.
7. Processing is in the public interest.
8. Processing is necessary in connection with preventative or occupational medicine, for assessing the work capacity of an employee, medical diagnosis, the provision of health or social care or treatment.
9. Processing is necessary for reasons of public interest in the area of public health such as ensuring high standards of healthcare, medicinal products or devices.
10. Processing is necessary for archiving purposes in the public interest, scientific and historical research or statistical purposes.

CONSENT

Consent must be specific, informed and unambiguous. Silence or pre-ticked boxes will not constitute consent.

Data controllers must be able to demonstrate that data subjects have consented to data processing. This will mean that controllers will need to keep accurate and update to records.

If consent is given in a written document it must be distinguishable from the remainder of the document and the form of consent must be in clear and plain language.

Consent must be freely given so any requirement for consent to be given before a contract is performed, even when data processing was not necessary to perform that contract, will be subject to scrutiny.

Individuals have the right to withdraw their consent at any time.

If you are dealing with children under the age of 16 consent must be given or authorised by the legal guardian and there is a requirement that the controller verifies that the person giving consent is in fact the legal guardian. Member states can reduce the age limit from 16 to 13 so controllers processing data from across the EU need to be aware that different age limits may apply in different jurisdictions.

If controllers cannot obtain valid consent then consider if it is possible to rely on an alternative legal basis for processing. If this is not possible then you must stop processing the personal data.

DATA PROTECTION OFFICERS

If you carry out large scale systematic monitoring of individuals or you carry our large scale processing of special categories of data or data relating to criminal convictions or you are a local authority then you must appoint a data protection officer (DPO).

Any organisation or group of companies can appoint a DPO and even if you do not appoint a DPO you must ensure that you have staff who are trained in relation to GDPR and can discharge your obligations.

The DPO's role is to:

- Inform and advise the organisation and its employees about GDPR;
- To monitor compliance with GDPR; and
- To be the first pint of contact with the supervisory authorities (In the UK this is the Information Commissioner).

PRIVACY IMPACT ASSESSMENTS

Privacy impact assessments/data privacy impact assessments /PIAs/DPIAs – these terms all refer to the same thing. A privacy impact assessment is an audit tool to help an organisation identify the most effective way to comply with its data protection obligations and to meet individual's expectations of privacy. A PIA is an integral part of taking a privacy by design approach and will enable an organisation to systematically and thoroughly analyse how a project or system will affect the privacy of the individuals involved.

A PIA will enable problems to be identified and corrected at an early stage. A PIA is not a requirement under GDPR but the Information Commissioner is promoting the use of them as good practice.

DATA PROTECTION BY DESIGN

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. This has always been an implicit requirement of the data protection principles under the Data Protection Act 1998 but the GDPR makes it an express legal requirement.

THE RIGHT TO BE INFORMED

Data subjects have the right to be informed about the intended purpose of the processing at the point at which the data is collected. The information that must be supplied is:

- The identity and contact details of the data controller and, where applicable, any third party representative of the controller and, if there is one, the data protection officer.
- The purpose of the processing and the legal basis for it.
- The legitimate interests of the controller or the third party.
- If the data is not obtained directly from the data subject, the categories of personal data to be processed.
- Any recipient of the data.
- If the data is to be transferred to another country and, if so, details of the safeguards in place.
- How long the data will be retained or the criteria used to determine the retention period.
- The existence of the data subject's rights.
- The right to withdraw consent at any time.
- The right to complain to a supervisory authority.
- Whether there is a statutory or contractual requirement to provide the data and the consequences of failing to do so.
- The existence of any automated decision making or profiling, information about how decisions are made and the significance and consequences of this.
- The source from which the data was obtained and whether it came from publically accessible sources.

The information notice must be concise, transparent, intelligible and easily accessible and it must be provided free of charge.

SUBJECT ACCESS REQUESTS

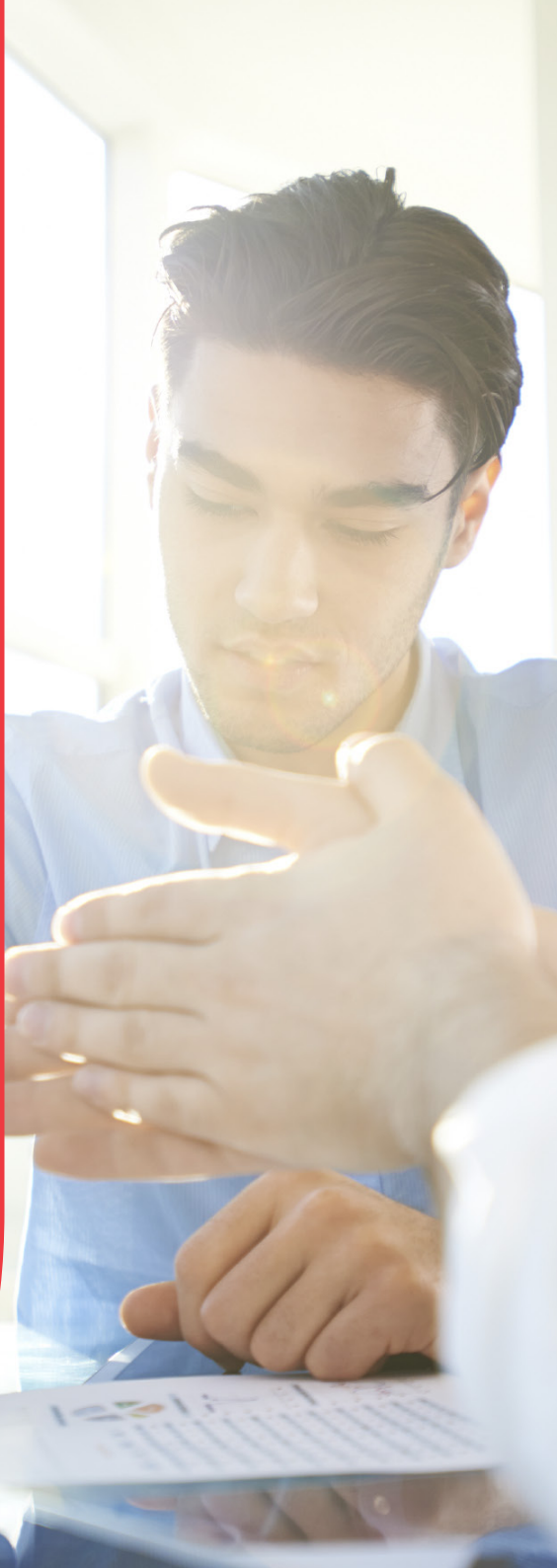
As under the Data Protection Act there will be a right of access for data subjects to confirm that their data is being processed.

The time limit for dealing with a subject access request has been reduced and the information must now be provided within 1 month of the date of receipt of the original request. The information must be provided free of charge – you may no longer require payment of the current fee of £10. If the request is unfounded or excessive then it is possible to charge a "reasonable fee" particularly if the request is made repeatedly.

The information may be supplied electronically unless the data subject requests otherwise.

Where possible, organisations should provide remote access to a secure self-service system allowing individuals direct access to his or her information. This will not be appropriate or possible in every sector.

Organisations need to put in place a process for dealing with subject access requests so that on receipt of such a request time is not wasted.



RECTIFICATION

If personal data is found to be inaccurate or incomplete then a data subject is entitled to have it rectified.

If the data has been disclosed to third parties then the third party should be advised of the rectification and the individual should be informed about the third parties to whom data has been disclosed.

The time limit for compliance is 1 month which can be extended to 2 months if the rectification is complex.

THE RIGHT TO BE FORGOTTEN

This is also known as the right to erasure. This right applies when

- personal data is no longer necessary in relation to the purpose for which it was originally collected.
- the individual withdraws consent.
- the individual object to the processing and there is no overriding reason to continue.
- the personal data was processed unlawfully.
- the personal data must be erased to comply with a legal obligation.
- the personal data is processed in relation to the offer of information society services to a child.

The data subject making an application for personal data to be removed does not have to demonstrate that the continued processing would cause unwarranted damage or distress.

It is possible to refuse to deal with a request of this nature on certain limited grounds such as exercise or defence of legal claims, public health purposes and the exercise of the right to freedom of expression and information.

If data has been disclosed to third parties then the organisation must inform the third parties about the erasure of the personal data unless it is impossible or would involve a disproportionate effort to do so. In the on-line environment links, copies or replication of the data should be removed.

CAN AN INDIVIDUAL RESTRICT YOUR ABILITY TO PROCESS DATA?

Yes. An organisation must restrict the processing of data if:

- the data subject claims that the data is inaccurate. Until you have verified the accuracy of the data, processing should stop;
- the processing is unlawful;
- you no longer need the data but the individual requires access to it in connection with any claim;
- whilst you consider a request to stop processing by a data subject.

DATA PORTABILITY

Individuals have the right to have a copy of their personal data in a commonly used electronic format that allows it to be transferred to another processor in a safe and secure way.

The time limit for complying with a request is 1 month but this can be extended to 2 months if the request is complex

RIGHTS IN RELATION TO AUTOMATED DECISION MAKING

If your organisation is engaged in automated decision making (such as reviewing loan applications) you must make sure that data subjects are able to obtain human intervention in that process; express their point of view; and obtain an explanation of the decision and challenge it.

The above does not apply if the processing is based on explicit consent; it is authorised by law; or it is necessary in relation to the performance of a contract between the organisation and the data subject.

Profiling is any form of automated processing of data to evaluate matters such as performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements.

TRANSFERS OF DATA OUTSIDE THE EU

Transfers of data within the EU are permitted but transfers outside the EU are subject to controls in much the same way as under the existing Data Protection Act.

Transfers are permitted where the EU Commission deems the level of data security to be adequate. Currently the following countries are deemed to have adequate data security:

- Andorra
- Argentina
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay

If a country is not included in this list then transfers may be made subject to compliance with one of a number of requirements including:

The informed consent of the data subject;

Binding corporate rules are in place;

Standard contractual clauses are adopted by the relevant parties;

There is an approved code of conduct or an approved certification mechanism.

It remains to be seen if the UK will be added to the list of countries deemed to have adequate data security protection following Brexit.

WHAT IF THERE IS A BREACH?

A breach is defined as any data security breach leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

A breach must be reported to the Information Commissioner if it is likely to result in a risk to the rights and freedoms of the individuals affected. This has to be assessed on a case by case basis but the notification must be made within 72 hours of the organisation becoming aware of the breach. Notification must include the name of the DPO or person responsible for data protection compliance in your organisation and details of the breach.

If the breach is likely to result in a high risk to the data subjects concerned the organisation must notify them directly and any breach which is sufficiently serious must be notified to the public without delay.

IF YOU GET IT WRONG

The maximum level of fine is increasing from the current £500,000 to €20 million or 4% global turnover (whichever is the higher).

This level of potential fine obviously increases the risk to organisations and makes it more important to prepare for the introduction of GDPR.

COMPANY POLICIES AND EMPLOYMENT CONTRACTS

Companies should have a Data Protection Policy, which is stored in a staff handbook or on the staff intranet. This policy should deal with the Company's processing of sensitive personal data.

It is advisable that employee contracts contain a clause stating that under the contract of employment, the employee agrees with the Company's Data Protection Policy when handling personal data in the course of employment including personal data relating to any employee, customer, client, supplier or agent of the Company or Group Company. It is therefore clear that the employee is bound by the policy upon entering into the employment contract.

The employment contract should also deal with the issue of consent, as set out above. The employment contract should expressly state that the employee consents to the Company or any Group Company processing data relating to the employee for legal, personnel, administrative and management purposes and in particular to the processing of any sensitive personal data. Once Brexit actually happens, this consent will need to be reviewed depending upon what the UK's new legislation requires and the relationship agreed with the EU.

MARKETING AND PROSPECTS

In future it is going to be more difficult to build a database of "prospects". Given that you cannot hold personal data for longer than is necessary and that you cannot process data without consent, the days of storing indefinitely the contact details of people that you meet are gone.

The indiscriminate storing of personal data in not allowed. If you want to store personal data about new contacts then a positive opt in is required so you will have to contact the individuals to ask their permission to include them on your CRM system.

WHAT SHOULD ORGANISATIONS BE DOING TO PREPARE?

Appoint one person within your organisation to take ownership of the preparations for GDPR and for future compliance. Even if technically you do not need to appoint a DPO this person will effectively have that role.

The decision makers in the organisation need to be aware that GDPR is coming and the date it comes into force.

Provide an employee awareness programme relevant to your staff.

Carry out an information audit to find out what data you hold, where it came from and who, if anyone, you share it with.

Consider who your external suppliers are and whether as part of their services you share data with them.

Document the results of your audit so that you have a readily accessible record of this information. This is important given the GDPR's accountability principle.

Data that is no longer required should be deleted from your systems or destroyed. Consider how you are going to do this – this may involve an upgrade to your IT systems.

Privacy policies and notices should be reviewed and updated to comply with the information requirements that GDPR imposes.

Make sure you have clear policies in place to deal with requests by individuals including subject access requests; information requests; the right to be forgotten; the right to rectification; and the right to restrict processing of data. Make sure that key members of your team are aware of these policies, what needs to be done and the timescales for action if such a request is received.

Don't panic. If you would like to talk to Tollers about how to prepare for GDPR please call 01604 258558 and ask to speak to Liz Appleyard in our Commercial Team.

All information in this guide is correct as of September 2017.

Northampton 01604 258558 | Milton Keynes 01908 396230 | Corby 01536 276727
Kettering 01536 520111 | Oakham 01572 756866 | Uppingham 01572 821184
Stevenage 01438 901095 | Kempston 01234 857014

email: enquiries@tollers.co.uk

tollers solicitors

Northampton | Milton Keynes | Corby | Kettering | Oakham | Uppingham | Stevenage | Kempston

www.tollers.co.uk