



Guide to the **GDPR**



dbpdata
make the connection

Guide to the GDPR

Contents

- 03** What does the new GDPR say?
- 04** The GDPR Principles
- 04** Organisational & Technical Measures
- 05** GDPR at a glance
- 06** From May 2018 each of us have some new awesome rights!
- 07** Keeping personal information safe
- 08** Other security measures
- 08** What more can you do?
- 09** Notion of Accountability
- 10** Wider definition of Personal Data
- 10** Important new change
- 11** Stricter rules on consent
- 12** Greater transparency (notification)
- 13** Preparing for the GDPR
- 14** Exemptions and National Derogations
- 15** The key to complying with the GDPR is...
- 16** How can DBS Data help you with GDPR?



Click or tap this icon to get back to this page



Click or tap on this icon to move page



What does the new GDPR say?

The General Data Protection Regulation (GDPR) is an important new piece of legislation adopted by the European parliament and the European council and must be implemented by all EU member states by 25th May 2018.

The GDPR is actually just one part of a new set of data protection regulations due to replace the Data Protection Act in 2018. The other element is the 'Law Enforcement Directive' which is being introduced at the same time as the GDPR to facilitate the safe sharing of personal information between national police forces and security agencies in the various member states.

The purpose of the legislation is to:-

- Give greater rights and protection to EU Citizens
- Offer organisations greater clarity of their responsibilities
- Bring consistency to legislation throughout Europe
- Standardise enforcement and sanctions between Regulators
- Future-proof the legislation against new technologies
- Ensure overseas countries respect the data of EU Citizens



On the following pages we shall outline the significant rights, obligations and elements of the GDPR - you can read more at the ICO Website

Guide to the GDPR | Call us today 01245 397 570



The GDPR Principles

The GDPR is introducing some new concepts and they are outlined on the following pages. However, many basic concepts still remain and they include the following data protection principles:-

- Personal information must be processed **Fairly, Lawfully** and in a **Transparent** manner ('lawfulness, fairness and transparency');
 - Personal Information collected for **Specified, Explicit** and **Legitimate** purposes ('purpose limitation');
 - Personal information must be **Adequate, Relevant** and limited to what is **Necessary** ('data minimisation');
 - Personal information must be **Accurate** and, where necessary, kept **Up-to-date** ('accuracy');
 - Personal information must be kept for **No Longer** than is necessary ('storage limitation');
 - Processed in a manner that ensures appropriate **Security** of the personal data ('integrity and confidentiality');
- i* The Data Protection Act also had principles on the Rights of a Data Subject and for International Transfers - these are covered in the GDPR under separate Articles.

Organisational & Technical Measures

The GDPR demands that sufficient Technical and Organisational measures are taken to keep personal information safe.

This includes hardware, software, policies, procedures and people skills, including training.



Q GDPR at a glance

- **Wider definition of Personal Data** Introduction of the term 'concerning' regarding health and sexuality, plus introduction of biometrics, genetics and location data;
- **Greater rights for individuals** New rights introduced such as free access to their data, to be told how their data is being processed and why, and the right to data portability;
- **Stricter obligations on Data Controllers and Data Processors** Includes strict contractual agreements and that Data Processors are now equally liable for data breaches;
- **Notion of Accountability** You say you comply, now prove it! Record keeping is now essential to demonstrate compliance;

- **Mandatory breach reporting** The DP Regulator and Data Subjects must now be informed of serious breaches;
- **Appointment of DPO's in many organisations** If organisations are processing personal information on a large-scale they must appoint a DPO;
- **New rules on consents** Consent must now be informed, freely given and affirmative. Opt-out boxes are no longer acceptable. Explicit consent is required for sensitive or special categories of data;
- **Greater protection for Children** Over 13's and Under 16's must have parental/guardian consent to use Internet services and have greater rights to have their data erased;

- **Changes to lawful conditions of processing** Many technical changes occurred to the lawful reasons why an organisation can process personal information, for example, Local Authorities can no longer rely upon 'Legitimate Interests';
- **New rules on automated decision making and profiling** Data Subjects can have automated decisions reviewed and object to profiling
- **Tougher rules on international transfers** Organisations must be assured that overseas companies can safely protect personal information; new rules introduced on the contractual arrangements required;

 PII = Personally Identifiable Information

Guide to the GDPR | Call us today 01245 397 570



From May 2018 each of us have some new awesome rights!

The right to be informed

You have a right to be told HOW and WHY your data is being used, who it is being shared with, and if your fundamental rights or freedoms may be affected, also told if your data was involved in a data breach.

The right of Rectification

Just the same as now, you have a right to demand that any data held on you which is inaccurate or incomplete is rectified.

The right to Restrict Processing

When you ask for processing to be restricted, organisations are permitted to store the personal data, but not further process it. They can retain just enough information to ensure that the restriction is respected in the future.

The right to Object

You have an absolute right to object to your data being used for research purposes or company's legitimate interest or public interest/exercise of official authority.

The right of Access

From May 2018 each of us can request, AT NO CHARGE, a copy of our personal information, and it must be provided within 1 calendar month after identity confirmed.

The right to Erasure

Also known as 'the right to be forgotten', is your right to request the deletion or removal of personal data where there is no compelling reason for its continued processing,

The right to Data Portability

Gives you the right to move your personal data, held in an electronic format, for example, held on social media, from one IT environment to another.

The right to object to Automated decision making & Profiling

You have a right to ask for any decision made on you which is made by a computer to be reviewed by a human being, and you can object to organisations profiling your behaviours and characteristics.



Keeping personal information safe

The Organisation invests a lot of time and resources by way of technical measures to protect personal information, but they **need your help to keep personal information safe**. Over the next few pages there are a few suggestions on how you can help fight cyber-crime, ensure information is processed in the strictest of confidence and keep sensitive information safe.

Key Responsibilities of our Organisation

- Providing a secure ICT network and encrypted remote access
- Install robust firewalls to keep out hackers and malware
- Install virus-checking on all computers and devices
- Keep computer patches up-to-date
- Taking regular back-ups
- Securely disposing of old computers and devices
- Providing a way of encrypting sensitive emails
- Provide a secure way of sending faxes
- Train all staff in their obligations and how to keep personal data safe
- Implement access controls to only allow employees with lawful reasons to access personal data
- Keep accurate audit trails of who has viewed, accessed, deleted or shared personal information.
- Having contracts or Data Sharing Agreements in place.

How employees can help keep personal information safe

- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities;
- Never use public wi-fi;
- Always follow any guidelines, policies or instructions issued by



the Organisation;

- Only access the information you need to do your job;
- Don't share passwords with your colleagues;
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen;
- Do not store data on local devices or download to USB sticks;
- Be aware of spyware and social engineering;
- Do not send personal information via unencrypted email;
- Be cautious of predictive text and allowing email to fill in email addresses;
- BCC instead of CC in emails;

- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone;
- Try not to use fax machines, but if the only option, double check the fax number you are using and if possible dial from a directory of previously verified numbers;
- Never use a Fax redial option and always include a cover sheet so contents do not need to be read;
- With email or fax always ring and ensure sensitive information arrived with recipient safely;
- Do not send sensitive information to an unprotected printer or fax in an open-plan area;



Other security measures

- Shred all your confidential paper waste;
- Check the physical security of your premises (ensure no one is tailgating you);
- Be aware of blagging (where people pretend to be the Data Subject to obtain their personal information);
- Install a firewall and virus-checking on your home computer and mobile devices;
- Keep your computer patches up-to-date'
- Install effective anti-virus and spyware software;
- Securely dispose of old computers and devices;
- If any of your devices is hacked or stolen inform IT immediately;
- Wherever possible anonymise or pseudonymise your data;

What more can you do?

To comply with the spirit of the GDPR Data Controllers and every member of the team must work together to help protect personal information.

An open, honest and non-judgemental partnership must be in place to achieve this goal. The following suggestions could further

assist the Organisation to protect personal information even further.

- Identify new risks and Vulnerabilities;
- Inform your DPO, IT management ASAP;
- Help educate your colleagues and share hints, tips and advice;
- Report actual/suspected breaches immediately ;
- Proactively think of, and recommend ways of improving systems and protecting P11;
- Encourage a non-judgemental, blame free culture to foster openness and co-operation;



Notion of Accountability

It was implicit under the Data Protection Act that you should be able to demonstrate compliance with the legislation, the GDPR now demands that Data Controllers can demonstrate compliance with the legislation.

The Notion or Principle of Accountability has therefore been introduced.

Data Controllers are expected to put into place comprehensive but proportionate governance measures to comply with GDPR. Good practice tools that the ICO has championed for a long time include the following measures:-

- (Data) Privacy Impact Assessments and Privacy by Design (DPIA or PTA's); which are now legally required in certain circumstances;
- Create internal data protection policies such as for processing of P11, training of staff;
- Perform internal audits to confirm policies and procedures are being followed;
- Maintain relevant documentation on processing activities. This includes all details that would historically have been provided to the ICO during the notification process;
- Where appropriate, appoint a Data Protection Officer (DPO) to oversee compliance;
- Ensure robust audit trails and access logs are maintained;
- Review security features regularly and record findings;
- Keep accurate asset registers and a cradle to grave process for all devices;
- Ensure manual records and electronic devices are securely destroyed and destruction certificates are obtained;
- Have in place clear contracts and data sharing agreements with processors;



EU Data Protection Supervisory Authority

Dear Data Controller, Please prove how you can demonstrate compliance?



Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures and auditing for organisations, although many organisations will already have good governance measures in place.



Wider definition of Personal Data

The GDPR as with the DPA only applies to information from which you can (on its own, or with another piece of information) identify a living individual (natural person).

However, the GDPR's definition is more detailed and makes it clear that information such as mobile phone number or online identifier, i.e an IP address, can be personal data.

The more expansive definition of PII provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

Important new change

The Introduction of the word '**CONCERNING**' in relation to Physical or Mental Health or Sex Life

Special categories or 'sensitive' Personal data includes any data revealing:-

Personal data includes

- Name & address;
- Phone numbers
- ID numbers
- Images - CCTV;
- IP Addresses;
- Descriptions;
- Location data;
- Nicknames
- Ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data (in some cases);
- Biometric data;
- **Concerning** health;
- **Concerning** a person's sex life sexual orientation;

i Not covered in the EU GDPR - but under UK law alleged or actual criminal convictions or prosecutions, or court sentences will be 'sensitive' PII



Stricter rules on consent

The GDPR has given Data Subjects even more control over the information they receive and who can process their PII. This includes:-

- Giving individuals genuine choice and control;
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default - i.e. silence is not consent;
- Explicit consent is required for sensitive data and requires a very clear and specific statement of consent - this explicit consent is usually in writing;
- Consent requests must be kept separate from other terms and conditions;
- Be specific and granular, Vague or blanket consent is not enough;
- Be clear and concise;
- Name any third parties who will rely on the consent;
- Make it easy for people to withdraw consent and tell them how;
- Keep consent under review, and refresh it if anything changes;
- Avoid making consent a precondition of a service;



NOTE: You don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate, e.g. you must process the information because another law says so. Where possible do not just rely on consent to process.

Enforcement & sanctions

All of the enforcement powers of the UK Regulator still apply, but sanctions are increasing. Importantly, if EU Citizens are involved then an overseas Regulator could technically take action against a UK Organisation.

Maximum Fine

€20 million or for multi-national Companies 4% of global turnover

International transfers

As long as you have appropriate permissions in place, and have performed due-diligence on the data processor, you can store data safely within the EEA or a country on the white list, or where a scheme such as Privacy Shield exists. Otherwise data may only be transferred in compliance with the conditions set out in Chapter V of the GDPR.



Greater transparency (notification)

Articles 12, 13 and 14 within the GDPR includes rules on giving privacy information to data subjects. These are far more detailed and specific than in the DPA and place an emphasis on making privacy notices transparent, understandable and accessible.

Data controllers are expected to take 'appropriate measures' to explain how data is being processed. This may vary depending on the audience, reason for processing, category of data processed and so on.

The GDPR states that the information you provide to people about how you process their personal data must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

Privacy Notice information

- Identity and contact details of the controller, or representative and DPO;
- Purpose of the processing and the legal basis for the processing;
- If Controller is relying upon the legitimate interests or public function condition;
- Categories of personal data;
- Any recipient or categories of recipients of the personal data;
- Details of transfers to third country and safeguards;
- Retention period or criteria used to determine the retention period; = The existence of each of data subject's rights;
- The right to withdraw consent at any time, where relevant;
- The right to lodge a complaint with a supervisory authority;
- The source of personal data and if came from publicly accessible sources

i Remember to use just in time notices for mobile apps and some services.



Preparing for the GDPR

The 12 steps recommended by the ICO are:-

01 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

02 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

03 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary.

04 Individual's rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

05 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

06 Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

07 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

08 Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

09 Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design & Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers

Private organisations should now designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 International transfers

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you to do this.



Exemptions and National Derogations

Exemptions and National Derogations will be of particular interest to local and central government and public authorities, however, some elements will also apply to some commercial organisations.

Article 23 enables Member states to introduce derogations to the GDPR in certain situations. These are similar to the existing exemptions from rights and duties in the DPA.

Member states can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- National security
- Defence
- Public Security
- The prevention, investigation, detection or prosecution of criminal offences;

OR

- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- The protection of judicial independence and proceedings;
- Breaches of ethics in regulated professions;
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence other important public interests or crime/ethics prevention;
- The protection of the individual, or the rights and freedoms of others; or
- The enforcement of civil law matters.
- Using data for domestic purposes (personal use)



The key to complying with the GDPR is...

- To have in place robust technical measures;
- Train your team to the appropriate level and explain the 'why' as well as the 'how';
- Be curious, vigilant, proactive and always look for vulnerabilities;
- Foster an open, blame-free culture and welcome suggestions for improvement;
- Create a values not rules driven culture;
- Follow the procedures collectively agreed, and if they don't or can't work, agree together how to change them. Working together you can protect Personal Data, Data Subjects and your Organisation;



Life after Brexit

In preparation for BREXIT, the GDPR and the EU Law Enforcement Directive are being merged into a new Data Protection Act. The Data Protection Bill is currently going through the Parliamentary process.

Guide to the GDPR | Call us today 01245 397 570



How can DBS Data help you with GDPR?

Our consultants are experts in marketing data compliance and are able to provide expertise around Data Protection, Information Governance and Data Compliance so that you can be confident that your data practices are compliant and responsible. We are able to consult, audit and train to meet the requirements of DPA 1998, PECR, ICO Guidance and GDPR in detail.

Information Governance is a fiduciary responsibility of Directors and CEO's and we are here to support the delivery of those legal duties by providing the expertise in this area that your business probably does not hold.

Our consultants work hand in hand with our clients providing advice, support, guidance and encouragement ensuring that you have a data compliance policy and practice within your business that is relevant, achievable and ensures

that you meet all the requirements of current data legislation.

DBS Data are able to consult, audit and train to meet the requirements of DPA 1998, PECR, ICO Guidance and GDPR including:- Data capture points, FPN's and privacy policies and how well suited they are to their proposed use of data

- **Age of customer & inquirer data and retention policies**
- **Database protocols, governance and security**
- **DP info held against each record (original consent date and statement, dates of engagement, consented uses and categories)**
- **Suppression policies and processes**
- **DP Security**
- **Use of 3rd party data**
- **Audits**

Our compliance audits will identify risks in your business before they become a problem. We offer both light touch or in-depth audits depending on your business circumstances and need.

Training

Our marketing data compliance trainers are specialists in their field bring expertise, experience, passion and enthusiasm to an area which is often seen as dull and boring. We will turn data compliance into fun and engaging subject that your employees will enjoy and will benefit from ensuring that your people know and understand their data legislation responsibilities without it being a chore.

To find out more about how we can help with the GDPR please contact us on 01245 397 570 or email thesalesteam@dbldata.co.uk