Distinct IT
Nobody Does I.T. Better

Distinct IT General GDPR Guidance Summary

This is a summary of information we have collected from various websites including and primarily from the Information Commissioners Office ico.org.uk There are various official websites that can offer more in depth guidance on GDPR. The information in this document is designed to give you some general guidance on how to start becoming GDPR Compliant. The GDPR guidelines are still evolving and changing so its important to make sure that you keep up to date regards changes to GDPR from official sources. Distinct IT take no responsibility or make no guarantees for your GDPR compliance and the responsibility is that of the individual to ensure that compliance is met and upheld.

Distinct IT
Nobody Does I.T. Better

What is GDPR

- GDPR stands for **General Data Protection Regulation** and is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).
- The regulation was adopted on 27 April 2016 and It becomes enforceable from 25 May 2018 and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.
- The GDPR aims primarily to give control back to citizens and residents over their personal data.
- Even though the UK is leaving the EU it has been agreed that the UK will adopt and comply with this regulation and all businesses and individuals that process personal data MUST comply.
- Companies that fail to comply could face fines of up to 20 Million Euros or 4% of their annual worldwide turnover
- GDPR aims to ensure that data is held and processed legally and responsibly and that the IT network infrastructures that host this data is managed properly and follows best practice strategies regards security, frameworks and policies.

Distinct IT
Nobody Does I.T. Better

Who does the GDPR apply to?

The GDPR applies to all Companies and Individuals who Control (Controller) or Process (processor) personal data.

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Distinct IT
Nobody Does I.T. Better

What information does the GDPR apply to?

Personal data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
- The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
- Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data"

- The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
- Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Distinct IT
Nobody Does I.T. Better

Data Protection Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The controller shall be responsible for, and be able to demonstrate, compliance with the principles

Lawful basis to store and process data

All businesses must have a valid lawful basis to process personal data. There are 6 available lawful bases for processing and no single basis is better or more important than any of the others.

- You must determine your lawful basis before you begin processing and you should document it.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If no lawful basis applies to your processing, your processing will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully.
- For all data that you store / process you will need to document the valid lawful basis that applies.

The 6 Lawful Basis categories are as follows and you need to determine which one applies to every set of data that you hold. They will be explained in more details on the following slide.

1. Consent
2. Contract
3. Legal Obligation
4. Vital Interests
5. Public Task
6. Legitimate Interest

Distinct IT
Nobody Does I.T. Better

Lawful bases for processing

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Distinct IT
Nobody Does I.T. Better

How do we decide which lawful basis applies?

- Many of the lawful bases for processing depend on the processing being “necessary”. This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means
- It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose
- You must not adopt a one-size-fits-all approach. No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the GDPR
- Several of the lawful bases relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone’s vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first
- If you are processing for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many cases you are likely to have a choice between using legitimate interests or consent
- It is vitally important that you document your decision making process in identifying which lawful basis applies to each item of data that you hold

Distinct IT
Nobody Does I.T. Better

Rights for Individuals

GDPR provides the following rights for individuals:

The right to be informed

The right to be informed encompasses your obligation to provide ‘fair processing information’, typically through a privacy notice. It emphasises the need for transparency over how you use personal data. The information you supply regards the personal data you hold should be concise, transparent, intelligible and easily accessible.

Right of Access

Individuals have the right to access their personal data and supplementary information. Information should be provided within 1 month of request.

Right to Rectification

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. This must be done within one month of it being requested.

Right to Erasure

The right to erasure is also known as 'The right to be forgotten’. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling or legal reason for its continued processing.

Distinct IT
Nobody Does I.T. Better

Rights for Individuals Continued…

Right to Restrict Processing

Individuals have a right to 'block' or suppress processing of personal data where you are permitted to store the personal data, but not further process it.

Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Right to Object

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing and processing for purposes of scientific/historical research and statistics.

Automated Decision making/Profiling

The GDPR has provisions on automated individual decision making and profiling of an individual where processing is done without human involvement through automated means. If your software package / systems do this you should investigate this point in more detail.

Distinct IT
Nobody Does I.T. Better

Accountability and Governance

The GDPR includes provisions that promote accountability and governance. You are expected to put into place comprehensive but proportionate governance measures. These measures should minimise the risk of breaches and uphold the protection of personal data.

You are expected to be able to demonstrate your compliance of this by the following means:

- You must implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies
- You must maintain relevant documentation on processing activities
- You must where appropriate, appoint a data protection officer
- You must implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  - data minimisation;
  - Pseudonymisation (key coded with artificial identifiers to make a record less identifiable);
  - transparency;
  - allowing individuals to monitor processing; and
  - creating and improving security features on an ongoing basis.
- You must use data protection impact assessments where appropriate.

Distinct IT
Nobody Does I.T. Better

Accountability and Governance Continued…

Contracts

Whenever a controller (*the person or Company that determines the purpose and means of processing personal data*) uses a processor (*the person who processes data on behalf of the controller*) it needs to have a written contract in place.

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

Distinct IT
Nobody Does I.T. Better

Accountability and Governance Continued…

Documentation

The GDPR contains explicit provisions about documenting your processing activities. You must maintain records on several things such as processing purposes, data sharing and retention.

You may be required to make the records available to the ICO on request.

- If you have 250 or more employees, you must document all your processing activities.
- There is a limited exemption for small and medium-sized organisations. If you have less than 250 employees, you only need to document processing activities that:
  - are not occasional; or
  - could result in a risk to the rights and freedoms of individuals; or
  - involve the processing of special categories of data or criminal conviction and offence data.

You must document the following information:

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of your processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

There are documentation templates available from the ico.org.uk website or that I can send you if you contact Distinct IT

Distinct IT
Nobody Does I.T. Better

Accountability and Governance Continued…

Data Protection Impact Assessment

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage.

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals such as:
  - systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
  - large scale processing of special categories of data or personal data relation to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity.
  - large scale, systematic monitoring of public areas (CCTV).

The DPIA should contain:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Distinct IT
Nobody Does I.T. Better

Accountability and Governance Continued…

Data Protection Officers

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in the following circumstances.

- You are a public authority (except for courts acting in their judicial capacity);
- You carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- You carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

The minimum tasks of a Data Protection Officer are to:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Distinct IT
Nobody Does I.T. Better

Security and IT

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

These include having and maintaining the following IT measures:

- Business Firewalls
- Antivirus
- Antispam
- Secure communications
- Encryption (where appropriate such as laptops and memory sticks)
- Business Network Policies
- Disaster recover plan and backups
- Operating System update/patch policies
- Device patches and updates
- Password Policies
- Intrusion detection and data analysis tools
- The above list is not exclusive and each business needs evaluating. Business can seek certification such as Cyber Essentials to demonstrate their commitment to cyber security.

You also need to ensure physical security of the premises and devices where data is held and implement staff policies and guidance regards the protection of data, using portable media for storage and their general responsibility of data regards the guidelines set out in the GDPR

The processor should also be monitored to ensure that the data is being processed in the correct and legal way.

Distinct IT
Nobody Does I.T. Better

International Transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Adequate legal advice should be taken before attempting any international transfer of data even simple data in an email.

Distinct IT
Nobody Does I.T. Better

Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The GDPR introduces a requirement for all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Distinct IT
Nobody Does I.T. Better

Personal Data Breaches

What breaches do we need to notify the ICO about? (Information Commissioners office – ico.org.uk)

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

For Example, the theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

Failing to notify a breach when required to do so can result in a significant fine up to 10 – 20 million euros or 2 - 4 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Distinct IT Contact Information

We hope you have found this document useful. GDPR is something that we all need to take very seriously and with all the hype and clear uncertainty, concern and lack of knowledge around this area that we have witnessed from our clients we wanted to produce a simplified document that includes all the key elements to get you started. For more information regards the next steps that you need to take or for more information and guidance, please contact Distinct IT using any of the methods below.

Telephone 01633 670603

Email: billy@distinctit.co.uk

Website: www.distinctit.co.uk