sysnet global solutions

General Data Protection Regulation

The changes and the steps businesses need to take.

What is the General Data Protection Regulation?

From 25th May 2018, the General Data Protection Regulation, or GDPR for short, will come into force across all EU Member States. It will affect the processing and movement of the personal data of approximately 500 million citizens. The GDPR has the potential to impact globally: any company that offers goods and services to, or monitors the behaviour of, citizens of EU Member States will fall under its scope. These companies will therefore be liable for penalties in relation to non-compliance.

In this fact sheet we outline the GDPR and the changes it introduces and consider the steps businesses need to start taking now in order to be ready for May 2018.

GDPR Overview

Data Controllers and Processors

The Data Controller determines what, how and why Personal Data is processed.
Personal Data is information relating to an identified or identifiable living natural person. Also referred to as PII (Personally Identifiable Information).

A Data Processor acts on the Data Controller's behalf.

Key change under GDPR

Data Processors are now directly subject to, and are required to comply with, particular data protection requirements which previously only applied to Data Controllers.

Applicability

GDPR primarily apples to Data Controllers and Data Processors established in the EU.

Key change under GDPR

GDPR also applies to Data Controllers and Data Processors based outside the EU that offer goods and services to, or monitor the behaviour of, EU citizens.

Scope

GDPR applies to Personal Data. If a business holds Personal Data that falls under the scope of current data protection legislation, it will also fall within the scope of the GDPR.

Key changes under GDPR

GDPR provides a more detailed and expansive definition of Personal Data. Information such as online identifiers – e.g. an IP address or cookie identifiers – can be Personal Data.

GDPR also expands the definition of Sensitive Personal Data ('special categories of Personal Data') to include not just race or ethnic origin, political opinion, religious/philosophical beliefs, membership of trade unions, health and sex life/orientation but also genetic and biometric data. Data relating to criminal convictions and offences is also afforded special protection.

Personal Data that has undergone pseudonymisation may still be in scope, if that data could be attributed to a particular individual by the use of additional information.

GDPR does not apply to processing of Personal Data by individuals for their own exclusively personal or household activities.

Special measures are set out for the processing of Personal Data relating to a child under 13 years of age. This includes a requirement to obtain a parent or guardian's consent in order to process their Personal Data lawfully.

Rights of Data Subject

GDPR continues to maintain the rights of data subjects in relation to their Personal Data, as defined in the original Data Protection Directive.

Key changes under GDPR

GDPR creates new rights for individuals including: the right 'to be forgotten', to restrict processing, to object (to processing of their Personal Data) and to data portability.

The rights provided for individuals by GDPR:

- The right to information (on the collection and further processing of their Personal Data)
- The right of subject access
- The right to rectification
- The right to erasure (the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- The right to not be evaluated on the basis of automated decision making and profiling.

Principles

Data Controllers must ensure that the processing of Personal Data complies with the six general principles. The principles are almost identical to the obligations under the Data Protection Directive:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for public interest, scientific, historical or statistical purposes);
3. Adequate, relevant and limited to what is necessary in relation to purposes for which they are processed;
4. Accurate and, where necessary, kept up to date;
5. Kept in a format which permits identification of data subjects for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes); and
6. Processed in a manner that ensure appropriate security of the Personal Data to maintain integrity and confidentiality. Use appropriate technical or organisational measures.

Key change under GDPR

The inclusion of the accountability principle. Data Controllers must not only comply with these principles but also be able to show they comply. This can be achieved by having appropriate policies, allocating responsibilities, implementing technical measures, having effective procedures in place and training staff.

Data Security

The Data Protection Directive already required Data Controllers and Data Processors to implement appropriate technical and organisational security measures to protect Personal Data.

The obligation to keep Personal Data secure is also in GDPR and is expressed in the same general terms.

Key change under GDPR

The GDPR specifies a number of measures that may be needed to ensure a level of security appropriate to the risk including: pseudonymisation and encryption of the Personal Data; measures to maintain the security of the information systems; use of back-ups and disaster recovery to maintain availability and access to the Personal Data; regular testing and assessment of the effectiveness of the security measures.

Responsibility

Key change under GDPR

Data Controllers and Data Processors need to keep records of their processing activities. These must be made available to the supervisory authority on request. The records include:

- the name and contact details of the Data Controller;
- the purposes of the processing;
- description of the categories of data subjects and of the categories of Personal Data;
- the categories of recipients to whom the Personal Data have been or will be disclosed;
- where applicable, transfers of Personal Data to a third country or an international organisation. If applicable, including documentation of suitable safeguards;
- the envisaged time limits for erasure of the different categories of data;
- general description of the technical and organisational security measures;

Additional records for Data Processors:

- the name and contact details of the Data Processor, as well as those of each Data Controller on behalf of which the Processor is acting;
- the categories of processing carried out on behalf of each Data Controller;

Exemption: Businesses employing fewer than 250 people are **exempt from the record keeping requirements.** That is unless their processing activities are risky, frequent or includes Sensitive Personal Data.

Accountability

Organisations should designate someone with the appropriate knowledge, support and authority to take responsibility for data protection compliance.

Key change under GDPR

Some Data Controllers and Data Processors are required to designate a Data Protection Officer:

- public authorities;
- those carrying out systematic monitoring of individuals on a large scale;
- those processing special categories of data or data relating to criminal convictions and offences on a large scale.

Data Protection Impact Assessments

Key change under GDPR

While often recommended by supervisory authorities, such as the UK Information Commissioner, GDPR now requires a Data Protection Impact Assessment to be carried out when processing is likely to result in a high risk to the rights and freedoms of individuals, such as large scale processing of Sensitive Personal Data. A Data Protection Impact Assessment must include:

- a description of the processing and its purposes and any legitimate interest pursued by the Controller;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the individuals; and
- the measures taken to address those risks, to ensure the protection of the Personal Data and demonstrate compliance.

Notification

Under existing data protection legislation, Data Controllers already have a duty to provide certain minimum information about their processing activities to individuals, such as the identity of the Data Controller and how their Personal Data will be used.

Key changes under GDPR:

The information to be contained in privacy notices has been expanded. The information to be provided to data subject now includes: the legal basis for the processing; the data retention period; the individual's rights to complain, to object, to erasure; details of any automated decision making. These privacy information notices must also be "concise, transparent, intelligible and easily accessible" and use clear and plain language, especially if addressed to children.

Legal Basis for Processing

For processing of Personal Data to be lawful, the Data Controller must satisfy at least one legal basis (or processing condition) for each processing activity. The conditions for processing in the GDPR (Article 6) are broadly the same as those in the Data Protection Directive:

1. Consent - the data subject has given consent to the processing for one or more specific purposes
2. Contractual Necessity - processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
3. Legal Obligation - processing is necessary for compliance with a Member State or EU legal obligation to which the Data Controller is subject
4. Vital Interests - processing is necessary to protect the vital interests of a data subject or another person
5. Public Functions – processing is necessary for the performance of a task carried out in

the public interest (functions arising from Member State or EU law)

6. Legitimate Interests - processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights and freedoms of the data subject.

At least one additional processing condition must be satisfied for any processing of Sensitive Personal Data, e.g. the data subject has given explicit consent, processing is necessary for healthcare or public health purposes, is necessary for compliance with employment law.

Consent

One of the six processing conditions a Data Controller can rely on is consent. Typically, consent is the legal basis used when processing is optional. The Data Protection Directive defined an individual's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to Personal Data relating to him being processed".

Key change under GDPR:

Consent should now be "given by a clear affirmative act" as a freely given, specific, informed and unambiguous indication of the individual's agreement to the processing. The GDPR explicitly states that silence, pre-ticked boxes or inactivity do not constitute consent. Explicit consent from the data subject is required:

- if Data Controllers intend to make decisions about the data subject based solely on automated processing, including profiling;
- to authorise transfers of Personal Data to a country or international organisation that does not provide an adequate level of protection

Explicit consent is different to unambiguous consent "given by a clear affirmative act". As FieldFisher explains, for explicit consent "nothing short of an opt-in tick box or declaratory consent statement will do". The Data Controller must keep records of how and when consent was given.

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

Data Controllers may not need to obtain fresh consent from individuals for the processing of their Personal Data, if there is a record of that consent and the consent given meets the new requirements under the GDPR.

Transfers outside the EU

The Data Protection Directive prohibited the transfer of Personal Data to a third country that did not ensure an adequate level of protection and set out provisions for exemptions.

GDPR continues to prohibit transfers of Personal Data outside of the EU, unless certain conditions are met as set out in Chapter V. For example, the organisation receiving the Personal Data provides adequate safeguards.

Data breaches and notifications

Key change under GDPR:

The requirement to report Personal Data breaches is a new obligation under GDPR. A 'Personal Data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data".

Data Controllers are obliged to notify their supervisory authority within 72 hours of becoming aware of a breach. Data Processors must report Personal Data breaches to Data Controllers without "undue delay". Not all data breaches have to be reported. Supervisory authorities only need to be notified if the breach is likely to result in a risk to the rights and freedoms of the affected individuals. For example, where the breach leaves the individual open to financial loss or identity theft.

Data Controllers may also be obliged to directly notify affected individuals, without "undue delay", if the breach is likely to result in a high risk to the rights and freedoms of the affected individuals. The GDPR does not provide a definition for 'high risk' to individuals in this context. Data Controllers may be exempt from notifying affected individuals if:

- appropriate technical and organisational protection measures were applied (such as encryption of the Personal Data), or
- subsequent measures have been taken to ensure the high risk is no longer likely to arise, or
- it would involve disproportionate effort (a public communication to inform data subjects would be required instead).

Failing to notify a Personal Data breach when required to do so may result in a fine up to 10 million EUR or 2 per cent of annual worldwide turnover.

Non Compliance

Under the Data Protection Directive, penalties for non-compliance and data breaches are determined by Member State law. In the UK, the Information Commissioner imposed its largest ever fine of £350,000 in February 2016; whereas, in Germany a fine of €1.3 million was imposed in 2014.

Key change under GDPR:

Under GDPR supervisory authorities will be able to impose significantly larger fines; these fines can be imposed on both Data Controllers and Data Processors. There are two tiers (Article 83): Fines of up to €10 million or 2% of worldwide annual turnover, whichever is the higher, for breaches such as:

- failing to obtain consent for the processing of children's Personal Data;
- failing to implement appropriate technical and organisational measures;
- Controllers failing to comply with obligations in relation to the engagement of and

processing carried out by Data Processors
- failing to notify a Personal Data breach;
- failing to complete a data protection impact assessment, when one is required;
- failing to appoint a Data Protection Officer, if one is required.

Fines of up to €20 million or 4% of worldwide annual turnover, whichever is the higher, for infringements of GDPR provisions, including:

- the basic principles for processing, including conditions for consent;
- the data subjects' rights;
- transfers of Personal Data to third countries or international organisations

Supervisory authorities are required to consider factors such as the "nature, gravity and duration of the infringement", whether the breach was intentional or negligent, the categories of Personal Data affected, etc. when deciding on the amount of a fine.

Steps to Prepare for GDPR

Understand Your Role

- Understand if and how you fall under the scope of GDPR.
- Understand if your business is a Data Controller and/or a Data Processor.
- If you are a Data Processor, consider your new data protection obligations under GDPR.

Raise Awareness

- Make sure that key people in your business are aware GDPR is coming (e.g. decision makers, marketing teams, system developers/designers, etc.).
- Make sure these key people understand the changes it brings and the potential impact on your business.
- Make sure your suppliers (Data Processors) are aware of GDPR and have a plan to comply.

Personal Data Held

- Review your business operations and data handling processes.
- Review your reliance on third party service providers and suppliers, identify your Data Processors.
- Document:
    - The Personal Data you capture and hold;
    - Where and how you receive that Personal Data;
    - Where the Personal Data resides and how long you keep it for;
    - Who you share the Personal Data with, including any international transfers;
    - The security measures protecting the Personal Data.

Your Legal Basis for Processing

- Check that you can explain your legal basis for each Personal Data processing activity.
- If you rely on consent:
  - Review whether your current method of obtaining and recording an individual's consent meets the GDPR requirements;
  - If needed, refresh the consent obtained from individuals.

- If you hold Personal Data relating to children, consider if you need processes to verify an individual's age and obtain parental or guardian consent.
- Consider if you can or should rely on another legal basis for processing (e.g. contractual necessity). This may be more straightforward; no need to maintain records of consent or to respond to individuals who withdraw consent.

Update Privacy Notices

- Check your privacy notices and privacy policies:
  - Are they concise, transparent and in plain language meeting all of the GDPR requirements?
  - Do they address the expanded GDPR notification requirements, including the legal basis, the data retention period, etc.?
- If required, update your privacy notices and privacy policies.

Provide for the Enhanced Rights of Individuals

- Check that your data protection policies and procedures cover all of the rights individuals have under GDPR.
- Update your policies and procedures so that you know what to do and how to respond when individual's exercise their rights:
  - Make sure you have processes for new rights, e.g. have processes to identify and delete Personal Data under the 'right to be forgotten';
  - Review and update existing processes, e.g. make sure your subject access request process meets the amended rules (shorter timescales, additional information to be provided, changes relating to fees, etc.).

Show your Compliance with the Principles

- Review and update your data protection policies, procedures and documentation to make sure you can show that you are compliant.
- Check that responsibilities have been allocated:

    - If required, appoint a Data Protection Officer;
    - Even if not required, consider creating this role so that overall responsibility for data protection compliance is assigned.
- Check that your technical and organisational security measures are appropriate to safeguard the categories of Personal Data you hold.
- Make sure that your staff are trained and aware of your data protection policies and procedures.

Be Prepared for Data Breaches

- Assess the categories of Personal Data you hold so that you know which would require notification if there was a breach.
- Review your ability to detect and respond to a Personal Data breach. Could you identify a breach? Would Personal Data breaches be reported? Do you have a plan to respond to and notify a breach?
- Put in place an Incident Response Plan so that you can quickly react to a breach and, if necessary, report to your supervisory authority. A template plan can be downloaded from the Sysnet website.

Keep Up to Date

- In the run up to May 2018, when GDPR comes into force, various bodies will be developing guidelines, tools and procedures to help Data Controllers and Data Processors prepare.
- Look out for guidance issued by your national supervisory authority.
- Regularly check the website of the EU's Article 29 Data Protection Working Party.

References and Further Reading

- http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr
- http://www.linklaters.com/pdfs/mkt/london/TMT_DATA_Protection_Survival_Guide_Singles.pdf
- http://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection
- https://www.macroberts.com/ip-technology-commercial/eu-general-data-protection-regulation/actions/#1470841878902-585d2e74-9f7c