ARE YOU PREPARED FOR GENERAL DATA PROTECTION REGULATION?

How will the GDPR affect your business?

Novatel

Deutsche Telekom Group

Summary

THE EU GENERAL DATA PROTECTION REGULATION

- This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

By 25 may 2018, business must comply with the new GDPR or they could face fines up to £20 million or 4% of annual turnover in case of a data breach.

The General Data Protection Regulation (GDPR) is one of the most controversial and anticipated pieces of legislation conceived in the EU in recent years. It's a game-changer for businesses, as it represents a fundamental shift in the risks associated with data protection — and more importantly with a data breach. The current legislation, the Data Protection Directive (95/46/EC), was agreed in 1995, before the mainstream adoption of the Internet and the World Wide Web, and more than 10 years before Facebook and Twitter were founded. The world has changed, but data protection legislation has not. Moreover, the existing rules are based on a directive, the significance of which is that each of the 28 EU member states interprets and implements the rules in its own way.

The European Commission set out, in 2012, its Data Protection Principles and the draft text for a new regulation. The regulation will apply equally and simultaneously to all 28 member states on its enactment. After more than three years of discussion and debate (and not an inconsiderable degree of disagreement) the final version of GDPR was agreed in May 2016. The new law comesinto force on May 25, 2018.

At the heart of GDPR is the goal of defining data protection rights afforded to all EU citizens. The focus of the regulation is on mandating those rights, no matter what organization is processing a citizen's personal data, or where it is taking place. Therefore core elements of the GDPR detail a number of "Rights of EU Citizens" with respect to how their personal data are used. The list is extensive, and will require significant changes to applications, policies and procedures to attain compliance.

Beyond the rights of citizens, GDPR defines a set of "principles" that govern all processing of personal data. The idea is to define the conditions on which data processing is permitted. If an organization can't show they are operating within those conditions, then their activities may be considered unlawful under the GDPR.

A key principle is that data can only be collected "for specified, explicit and legitimate purposes", which means it won't be acceptable to collect data first and figure out how it could be used later. Furthermore only the minimum amount of data necessary to perform these tasks may be collected. And organizations cannot hold onto the data in a format that allows easy identification of the people involved after it is no longer needed for the original purpose.

Definition of personal data

The most common and useful explaination is **:** „any information relating to an identified or identifiable natural person" . Identification can be direct or indirect, and includes such identifiers as "a name, identification number, location data, online identity, one or more factors specific to the physical, physiological, genetic, mental, cultural or social identity of that person" but it also include assessing a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
The definition is technology neutral. It does not matter how the personal data is stored – on paper, on an IT system, on a CCTV system etc.

Sensitive personal data means personal data consisting of information as to:

- ✓ the racial or ethnic origin of the data subject,
- ✓ his political opinions,
- ✓ his religious beliefs or other beliefs of a similar nature,
- ✓ whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- ✓ his physical or mental health or condition,
- ✓ his sexual life,
- ✓ the commission or alleged commission by him of any offence,
- ✓ any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Personal data shall be:

- ✓ processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- ✓ 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.
- ✓ adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- ✓ 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 ('accuracy');

- ✓ 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

Data protection by design and by default

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Data protection officer

You should 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.

- ✓ The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The GDPR will require some organisations to designate a Data Protection Officer (DPO), for example public authorities or ones whose activities involve the regular and systematic monitoring of data subjects on a large scale. The important thing is to make sure that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively. Therefore you should consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements.

A DPO reports to management, but is expected to work independently and without direction. His primary concern is protecting data and enabling compliance, not facilitating shortcuts or finding legal loopholes in the Regulation. The DPO is, obviously, the person who directs and oversees all data protection activities within a company.. The DPO keeps management informed regarding their obligations under the Regulation, and is the primary contact point for supervisory authorities.

Data breaches

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

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The **notification** shall at least:

- ✓ describe the nature of the personal data breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- ✓ communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- ✓ describe the likely consequences of the personal data breach;

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

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 reason for its continued processing.

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

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

A person can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- ✓ to exercise the right of freedom of expression and information;
- ✓ to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- ✓ for public health purposes in the public interest;
- ✓ archiving purposes in the public interest, scientific research historical research or statistical purposes;
- ✓ the exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forum

Compliance Auditing and Record Keeping

Companies processing personal data are obliged to keep detailed records of the data they hold, as well as the details of the processing conducted on that data. You should document what personal data you hold, where it came from and who you share it with. You may need to organize an information audit, across the organization, or within particular business areas.