General Data Protection Regulations (GDPR)

Customer Awareness - Information and Guidance

FirstServ Limited

Content

Intro

The new European Union (EU) General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC (Directive). It will be wholly incorporated into UK law and applicable legislation from 25th May 2018 and incorporated into the new upcoming 'Data Protection Bill'. This bill will replace the Data Protection Act 1998 and be more encompassing than the GDPR in order to provide a comprehensive and modern framework for data protection in the UK.

The new regulation expands privacy protections and includes new obligations for FirstServ Ltd customers: that is companies that handle personal data originating in the UK/EU. And unlike the Directive, it extends the reach of the data protection law to companies who may have no presence in the EU as long as those companies process an EU resident's personal data in connection with goods or services being offered or if those companies monitor the behavior of individuals within the UK/EU.

This document offers top level background information on the GDPR and provides example questions for organisations to ask of themselves and their business which may allow for a better understanding of their preparedness for the new regulation.

Terminology

Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); there is no distinction between a person's private, public, or work roles; a person who can directly or indirectly be identified, with identifiers including name, email address, an ID number, social media posts, online identifiers (such as an IP address & cookies) and location data.
Sensitive Personal Data	Any data consisting of medical or health information, physical, physiological, or genetic information, biometric data, bank details, racial or ethnic origin, cultural identity, political opinions, religious or philosophical beliefs, trade union membership and data concerning a natural person's sex life or sexual orientation. Information about criminal convictions is treated separately and subject to even tighter controls.
Controller	Customers and FirstServ Ltd, the natural or legal person, public authority, agency or other body, which alone or jointly with others, determine the purpose and mean of processing of personal data.
Processor	FirstServ Ltd or associated brand, a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, our customer i.e. as part of the documented service requirement and agreement.
Processing	Any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Privacy by Design	This means that privacy issues are considered and embedded into the customer's engagement when scoping a solution. Taking a privacy by design approach is important for reducing privacy risks and building trust. Potential problems are identified at an early stage and increased awareness of privacy and data protection requirements.
Data Mapping	Customer's needs to map their data and information flows in order to assess their privacy risks. They need to understand the information flow, describe it and identify the key elements, where data is transferred from one location to another i.e. to and from FirstServ Ltd.
Data Protection Impact Assessment	Used for sensitive data, the customer needs to assess evaluate and document how the data is used before processing and include the measures, safeguards and mechanisms envisaged for mitigating identified risks to the rights and freedoms of natural persons.

Understanding

The GDPR regulates the collection, storage, use, and sharing of “personal data.” Where personal data is held on customer databases, in feedback forms filled out online, in email content, in photos, in CCTV footage, in loyalty program records, in HR databases etc. and where the data belongs or relates to UK/EU residents, then organisations need to comply with the GDPR. Note that personal data doesn’t need to be stored in the UK/EU to be subject to the GDPR. The regulation applies to data collected, processed, or stored outside the UK/EU if the data is tied to UK/EU residents.

The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/EC in spring 2018 as the primary law regulating how companies protect EU citizens' personal data. Companies that are already in compliance with the Directive must ensure that they’re compliant with the new requirements of the GDPR before it becomes effective on May 25, 2018. Companies that fail to achieve GDPR compliance before the deadline will be subject to stiff penalties and fines.

GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

Simply put, the GDPR mandates a baseline set of standards for companies that handle EU citizens’ data to better safeguard the processing and movement of citizens’ personal data.

Engagement

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.
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.
Communicating privacy information	You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
Processor	FirstServ Ltd or associated brand, a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, our customer i.e. as part of the documented service requirement and agreement.
Individuals' 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.
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.
Children	You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
Data breaches	You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
Data Protection by Design and Data Protection Impact Assessments	You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.
Data Protection Officers	You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
International	If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Be aware

Organisations now have to accommodate new transparency requirements and document how they detect, report personal data breaches and how they train people who have access to the data. Accordingly, customers need to begin reviewing their privacy and data management practices now.

GDPR applies to both data controllers and processors. As the controller, our customers are in charge of the data; FirstServ Ltd as a data processor, processes the data for the customer. Our customers are legally required to only use processors that take measures to meet the requirements of the GDPR. Our customers have to determine why and how to process personal data while FirstServ Ltd in accordance with the service agreement only perform operations on personal data on behalf of our customer.

Under the GDPR, FirstServ Ltd as a processor has additional duties and liabilities for noncompliance, or acting outside of instructions provided by the customer. Hence the importance of the service agreement and review. FirstServ Ltd's duties include:

- Processing data only as instructed
- Using appropriate technical and organisational measures to process personal data
- Deleting or returning data to the controller
- Securing permission to engage other processors (suppliers like DELL EMC, HP, AWS, Microsoft, Google etc.)

The greatest challenge for customers having backup and managed services with FirstServ Ltd is the GDPR entitlement that gives residents control over their personal data through a set of "data subject rights." Most notably, the right to have incorrect personal data deleted, corrected or erased in certain circumstances (sometimes referred to as the "right to be forgotten")

Customers should know that meeting compliance with the GDPR will need commitment, though adherence will be smoother for those who already operate well-built managed or cloud services and have effective data governance in place.

Sample questions for customers

Q | Do you have your main headquarters in the European Economic Area (EEA)?
The EEA includes EU member states, Iceland, Liechtenstein and Norway.

Q | Do you have a person or job function to lead the BCR process and interact with the Data Protection Authorities ("DPAs")?
An example of a job function is "Chief Privacy Officer.

Q | Is this person located in the EEA?
The lead need not be located in the EEA, but there should be some process in place due to time changes.

Q | Will your BCRs only apply to personal data transfers from the EEA?
E.g., are you only transferring personal data from the EEA? Or do you plan for the BCRs to apply to all personal data that you transfer regardless of where the data is from or going to?

Q | Do you know the country from which most of the data will be transferred out of the EEA?
I.e., which country will receive most of the data? You should also consider whether the data will go through another country for storage, even though your HQ may be in the U.S.

Q | Do you know how you will make the BCRs binding on the members of the Group?
Each company within the group must have a legally binding authority to permit enforcement. There are various ways, please pick one below. Ideally, the BCRs are adopted by the board of directors of the ultimate parent group (WP74).

Q | Do you have work employment contracts?
Work employment contracts should address following policies, being held accountability, confidentiality, etc.

Q | Do you have special training programs for employees?
I.e., training on the BCRs for personnel who have permanent or regular access to personal data, are involved in the collection of personal data or in the development of tools used to process personal data.

Q | Are employees trained to identify the data protection implications of their work?
I.e. to identify that the relevant privacy policies are applicable to their activities and to react accordingly. Applies regardless of whether or not the employees are based in the EEA.

Q | Do your BCRs deal with the issues of cooperation with DPAs?
BCRs should include a commitment that: i) members of the group will cooperate and assist each other in handling a request or complaint from an individual or an investigation or inquiry by DPAs; and i) entities will abide by the advice of the DPAs on any issues regarding the interpretation of the BCRs.

Q | Do your BCRs allow for informing other parts of the Group and the relevant Data Protection Authorities of any significant changes to the BCRs that would in principle have an effect on the authorization?
There must be a system in place for informing other parts of the organization and the DPA of any change to the rules. DPAs only need to see changes that significantly affect data protection compliance. (See WP108, s.9)

FirstServ Ltd | 3 Tabley Court | Knutsford | Cheshire | WA16 0PL | United Kingdom

t: +44 (0)20 7871 5515 | sales@firstserv.com | FirstServ.com