VALITOR
In partnership with VISA

GDPR.

Getting ready for the General Data Protection Regulation

Introduction.

Trust and integrity are core values of Valitor. Therefore, safeguarding the data we are entrusted with is of utmost priority. This brochure provides an overview of some important enhancements and changes to our privacy and information security programs, in order to follow new privacy and information security principles and to keep up with technological developments.

Important facts.

What is GDPR?

The General Data Protection Regulation (GDPR) regulates processing of personal data of individuals in the European Union and the activities of Data Processors and Data Controllers.

When is GDPR coming into force?

25th May 2018.

What's being introduced?

The key changes that GDPR will enforce from May 25th include: new rights for people to access their personal information held by Processors and Controllers; the ability to make certain requests pertaining to such information; obligations for management of data and a new regime of fines. GDPR will most likely impact you as a participant in the Card ecosystem, therefore, we would like to provide you with an overview about the legislation and what GDPR means for you.

Overview.

In January 2012, the European Commission set out plans for a data protection reform across the European Union in order to make Europe 'fit for the digital age'. Almost four years later, agreement was reached on what that involved and how it will be enforced. The new framework applies to organisations in all member-states and for companies processing data on EU citizens.

From social media companies, banks, retailers, and governments - almost every service we use involves the collection and analysis of our personal data. Your name, address, and more are all collected, analysed and perhaps most importantly, stored by organisations. GDPR aims to harmonise regulation across Europe to reflect the current data exchange landscape. In essence, GDPR is a new set of rules designed to give people more control over their data and to ensure companies protect the personal data they process.

What does GDPR mean to you?

GDPR applies to processing personal data of EU citizens. This means that companies and individuals based outside the EU that sell goods and services to individuals living in the EU will also need to comply with the new law. GDPR applies to controllers, joint controllers and processors,but the distinction is important, as the obligations for each differ.

Are you a Controller, Joint controller or Processor?

Responsibility under GDPR depends on your role. The data protection law has three categories: Controller; Joint Controller and Processor.

Controller

A Controller is the entity (a person or a company) that determines the purpose and means of processing personal data. Whether the entity makes that determination alone or with others.

Joint Controller

Where two or more companies jointly determine the purpose and reason for the processing of personal data e.g. they jointly decide the purpose, reason, occasion, nature, scope and objectives of the processing.

Processor

The person or group that processes the data on behalf of the Controller. Processing for example is obtaining, recording,adapting or holding personal data.

The same entity can be both a Controller and Processor, depending on the circumstances. For example, a technology company that provides data analytics to online merchants, is the processor and the merchant is the controller. However, if that technology company packages the same personal data to provide targeted customer segments to advertisers for its own purposes,it is acting as a controller.

Important changes.

Key changes that may impact your organisation include:

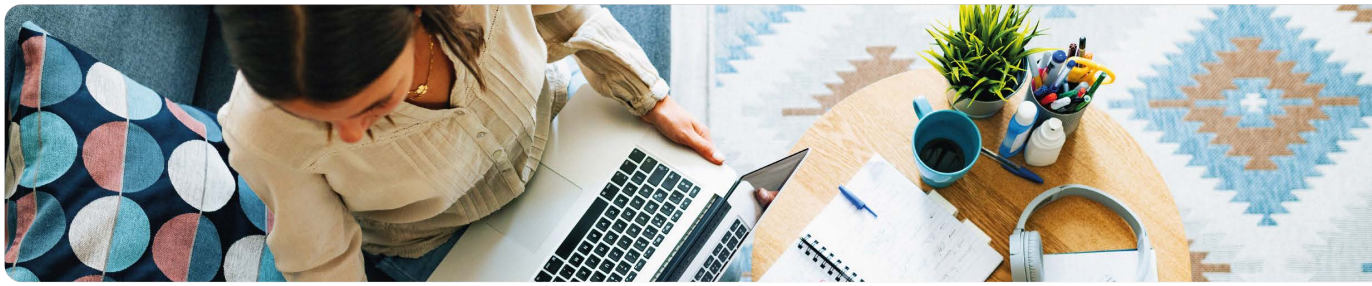
Privacy-by-design
Data protection must be built into business processes and systems.

Mandatory breach notification
Any breaches of personal data must be reported to authorities and affected individuals without delay.

Penalties for non-compliance
GDPR allows for fines of up to €20 million or 4% of the company's annual global turnover,whichever is the greater.

Enhanced rights of Data Subject
Such as, forgotten data, access to own data, to request rectification of data, to object to processing and request correction, and to have data transmitted to a new Controller.

Whilst all these rights are subject to important limitations, they reflect the importance of individual rights.



How to prepare for GDPR.

There's no 'one size fits all' approach to preparing for GDPR. Each business will need to examine what needs to be achieved to comply. Most importantly, you will need to understand whether you are a data Processor, Controller or Joint Controller. Most companies are likely to be both depending on the nature of their data processing.

Preparation

- Start by getting an understanding of what personal data is being held and who has access.
- Limit access based on business needs and implement monitoring to detect any unauthorised access.
- Perform an assessment of what compliance and security controls you have in place to collect and protect the data, how effective they are, and any gaps.
- Develop a plan to improve your security program, looking at people, processes and technology.
- Put in place a data breach notification process, including incident detection and response capabilities.
- Some organisations must also have a Data Protection Officer (DPO).

Considerations

- Establish a programme of work to gather a coherent inventory of your processes that relate to personal data.
- Create a Data Inventory and do privacy impact assessments where necessary.
- Assess your information security program as it relates to personal data, including third parties you share data with.
- Be compliant with the Payment Card Industry Data Security Standard (PCI DSS) for baseline security around cardholder data.
- Understanding of where and how you share personal data with third parties and ensure that you have the correct contracts in place.
- If applicable, ensure the information and the consent language you provide to your customers is transparent, clear, unambiguous, and written in plain language.
- Process in place by which you risk assess your data.
- Outline a plan for compliance with the more complex rights of the data subject, including rights of access, rights of correction, rights of rectification, rights of data portability, and rights of erasure.
- Establish a mechanism to identify if, when, and where any breach takes place and how you will handle it.
- It may be advisable to have a PCI Forensic Investigator (PFI) available for the event of a card data breach.

How can PCI help you?

The GDPR does not set out in detail a security framework, but The Payment Card Industry Data Security Standards (PCI DSS) provides a useful framework to enhance security of your payment data. PCI DSS compliance is required of all entities that store, process or transmit Visa and/or Mastercard cardholder data, including financial institutions, merchants and service providers. Importantly, PCI DSS does not cover everything set out by the GDPR or make you GDPR compliant but provides a useful starting point to address data security and reduce your overall risk.

Goals	PCI DSS Requirements
Build and maintain a secure network	• Install and maintain a firewall configuration to protect cardholder data. • Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data	• Protect stored cardholder data. • Encrypt transmission of cardholder data across open, and public networks.
Maintain a vulnerability management program	• Use and regularly update anti-virus software or programs. • Develop and maintain secure systems and applications.
Implement strong access control measures	• Restrict access to cardholder data by business need-to-know. • Assign a unique ID to each person with computer access.
Regularly monitor and test networks	• Restrict physical access to cardholder data. • Track and monitor all access to network resources and cardholder data.
Maintain an information security policy	• Regularly test security systems and processes. • Maintain a policy that addresses information security for all personnel.