iomart

General Data Protection Regulations (GDPR)

Customer Awareness

Information and Guidance

Customer Assurance

Group Integrated Management Systems

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 1998and 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 on our 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 behaviour of individuals within the UK/EU.

As a service provider, GDPR offers iomart an invaluable opportunity to engage with customers, a chance to demonstrate our experience and expertise by providing insight, understanding and guidance to a customer's service readiness for meeting requirements.

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

Terminology

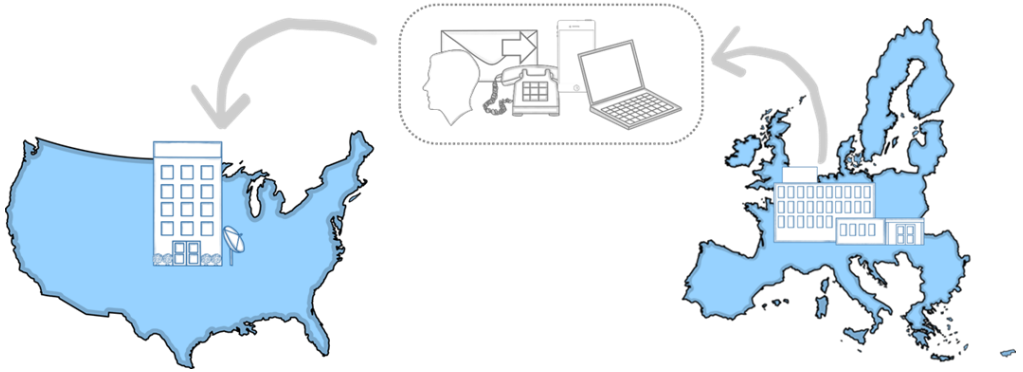
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); there is no distinction between a person's private, public, or work roles; a person who can directly or indirectly be identified, with identifiers including name, email address, an ID number, social 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 iomart, 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	iomart 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	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 iomart.
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 our customers 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.

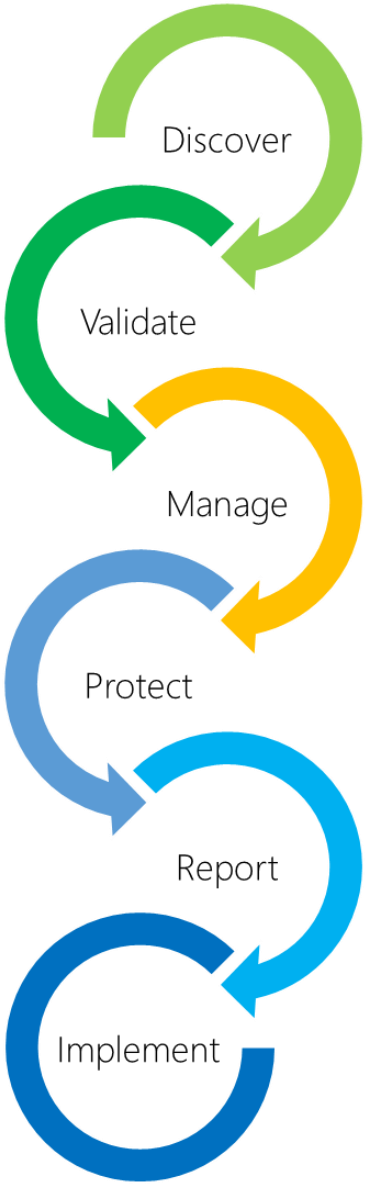


Example 1

A financial analyst firm is tasked with projecting a European company’s revenues for the next three years. The primary analyst works out of an office in the US, but uses personal data provided by the client. Because the data was collected in the UK/EU, it is subject to GDPR requirements, even though the analyst is based out of the US office and didn’t originally collect the data.

Example 2

A mobile and online website allows people to shop for, buy, and rate products. The company based outside the UK/EU that owns the retail storefront collects personal data about the people that visit and make purchases. The information is subsequently used in advertising campaigns and sales reports. If a person visits the website while they are physically present in the UK/EU, the requirements of the GDPR follow the personal data collected during that visit. That means that any website or mobile application that is accessible by and collects personal data from a person in the UK/EU will need to comply with the GDPR



Gather documentation & look at CRM
Understand the service agreement

Talk to the customer regarding their understanding of GDPR, our knowledge of their current service and future requirement that should be considered for compliance

Analyse the service with customer looking at Data governance, type of personal data, how they process data, purpose etc. and Data classification for responding to data subject requests

We can help the customer understand risks and to defend against them by putting in appropriate technical measures to protect personal data from loss or unauthorised access or disclosure

We can assist with the data processing requirement, where data is collected, used, shared, or otherwise, by maintaining systems that can track and record the use of personal data

We can provide expertise, guidance and support to ensure agreed service changes, controls and processes are delivered for GDPR compliance

Engagement

Customers as the controller must ultimately determine how GDPR will impact their business and act accordingly.

iomart can helps customers identify GDPR readiness gaps in their online service and define common-sense strategies for addressing these gaps.

Our typical customer engagement process breaks GDPR readiness activities into six phases, each with clear objectives and deliverables (see illustration).

The initial communication takes the form of a questionnaire to be completed with the customer by the iomart consultant and checks GDPR readiness. It is an assessment of whether a customer knows of, understands how the GDPR applies to their service hosted with iomart.

Talking to customers and reviewing their service will give significant insight and understanding as to the type of data the customer has, the measures they have in place for protecting and managing the data and where it resides etc. The collection, storage, use, and sharing of the “personal data.”

When understands a customer’s solution you should consider that GDPR describes encryption as an appropriate technical or organisational measure in some cases, depending on the risk. Recognised as a protective measure that renders personal data unintelligible when it is affected by a breach.

From this exercise, a customer should gain a greater understanding as to whether their service is robust enough for the collection and processing of the data they collect and will be able to compile the required data map, showing where personal data is stored, on what platforms hosted and/or managed, agree what processing activities they want from iomart as well as how long data should be retained.

Be aware

Before you speak to a customer, remember that GDPR contains many requirements about how personal information is collected, stored, and used as well as how data is identified and secured on information systems, in the cloud etc. Customer 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; iomart 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 iomart in accordance with the service agreement only perform operations on personal data on behalf of our customer.

Under the GDPR, iomart 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. iomart'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 iomart 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 | Who in the company is leading (or will be leading) your GDPR compliance effort?

Given that GDPR has a number of requirements regarding how you collect, store, and use personal data.

Q | From your managed, cloud or backup service with iomart, can you tell me how much personal data you store?

Given that GDPR enables the rights of data subjects.

Q | Do you classify your customers or your companies personal data?

Q | Does your company have a data governance program in place that meets the demands of the GDPR?

Given that GDPR requires our customers to be transparent with their data subjects, the intended processing of personal data.

Q | Do you have a data retention period for your backups or criteria for determining the retention period?

Given that GDPR requires our customers as controllers processing personal data to give data subjects a way to submit requests to rectify, erasure or transfer their personal data.

Q | Have you considered how this will be accomplished with your managed, cloud or backup service with iomart?

If you were to receive a request from a data subjects invoking their 'right to portability'

Q | Could you provide any data in a structured, commonly used, and machine-readable format and would you require iomart to assist with as part of a managed service?

Data protection and privacy by design are central to GDPR requirements and require customers as the controller to ensure that activities and supporting technology are built to include data protection and data privacy principles.

Q | Would you say your managed, cloud or backup service meets this standard today?

To maintain a high standard of security, GDPR identifies encryption as one potential tool that may be appropriate to secure personal data.

Q | How much of the personal data controlled by your company is currently encrypted with your iomart service?

With GDPR, assuring confidentiality, integrity, and availability of personal data requires that customers as the controller must implement appropriate technical and organizational measures to secure personal data. Those measures must be appropriate for the risk in question.

Q | Would you say that your companies approach to securing personal data under its control meets this standard today?

The GDPR requires customers as the controller to maintain appropriate technologies and/or processes to secure personal data and defend against personal data breaches. If a personal data breach were to occur, the customer may be required to quickly notify regulators and may also be required to notify affected data subjects. We need to keep customer contact data relevant and current.

Q | Who should iomart notify in your company, so that you can provide information to regulators with in the obligatory time scale?

In order for the customer to meet the GDPR requirement to protect personal data, they should regularly test and assess secure it is by evaluating the effectiveness of their technical and organizational measures.

Q | What testing measures do you have in place i.e. ASV or Pen Test?

With GDPR customers as controllers must map where their data held including, what, where, why, how the data is kept and with sensitive data conduct a Data Protection Impact Assessment (DPIA), evaluating, among other things, the impact of the proposed processing activity, the protection of personal data and to consider appropriate mitigation measures. If the customer has a schematic of their managed service from iomart, this can help with this process.

Q | Have you mapped your data or conducted a DPIA on your managed, cloud or backup service with iomart?

Compliance Department | Lister Pavilion, West of Scotland Science Park, Glasgow, G20 0SP | email: safety@iomart.com | Tel: +44 (0)141 931 6400