PRO-10: GDPR PRINCIPLES

PROGRAM SUMMARY

2019/11/13

Effective From	2019/09/16	**Standards**	GDPR Principles
Effective To	2020/09/30		
Report Date	2019/11/13		

Description

The GDPR sets out seven key principles:
• Lawfulness, fairness and transparency
• Purpose limitation
• Data minimisation
• Accuracy
• Storage limitation
• Integrity and confidentiality (security)
• Accountability

These principles should lie at the heart of your approach to processing personal data.

Why are the principles important?
The principles lie at the heart of the GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the GDPR.

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

Scope

What are the principles?

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) 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 or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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');

(e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

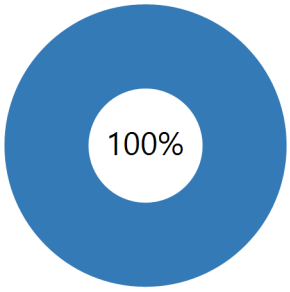
Notes

What is personal data?

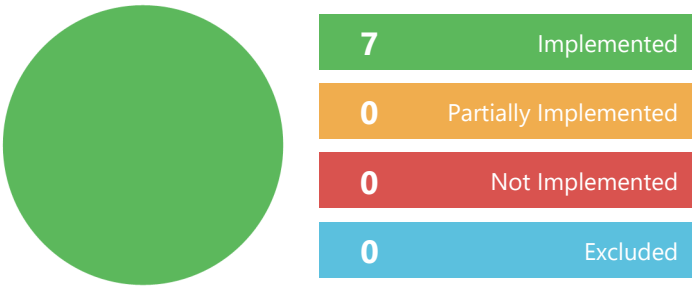
- Understanding whether you are processing personal data is critical to understanding whether the GDPR applies to your activities.
- Personal data is information that relates to an identified or identifiable individual.
- What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.
- If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
- If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.
- Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.
- When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.
- It is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller. Information which has had identifiers removed or replaced in order to pseudonymize the data is still personal data for the purposes of GDPR.
- Information which is truly anonymous is not covered by the GDPR.
- If information that seems to relate to a particular individual is inaccurate (ie it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

Reference: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

Overall Progress



Implementation Status



Total Controls/Policies

20

Number of Requirements

7

Requirements Per Standard

Requirement	Status	Date	Owner
GDPR PRINCIPLES			
Data Privacy			
Principle 1	**Implemented**		Information Assurance Department

Lawfulness, fairness and transparency
All information is processed lawfully, fairly and in a transparent manner in relation to individuals.

Satisfied By
- **Policy:** Privacy Code of Practice
- **Policy:** Privacy Policy
- **Policy:** ISMS Policy

Notes
We keep our clients informed on how, when and what data is used to perform our services. xMatters Privacy Notice, Security and Privacy articles and whitepapers ensure clients are up to date with our data governance processes. xMatters Operations and Support Teams consist of highly capable and vetted personnel. xMatters only access client data and client instances when they have been explicitly permitted to do so by the client in order to address client requests (e.g. problem ticket) and for support purposes, there is no casual data access.

Principle 2	**Implemented**		Legal Counsel

Purpose limitation
Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Satisfied By
- **Policy:** Privacy Code of Practice
- **Policy:** Privacy Policy
- **Policy:** Information Security Code of Practice
- **Control:** Service Level Agreements (SLA)
- **Control:** Data Processing agreement

Notes
Client data collected by xMatters is for specified, explicit and legitimate purposes, which depends on client's Business and Use case. All client provided data is used for service delivery as per contracted terms and agreements to facilitate emergency communications.

Principle 3	**Implemented**		Privacy Officer

Data minimisation
Collection adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

Satisfied By
- **Control:** Data Processing agreement
- **Control:** Data Map

Notes
xMatters has minimum data requirements that is a constituent receiving emergency communications: First Name, Last Name, and Email Address. Any further information provided by clients are up to the complete discretion of the client and to support their Business Case and Use Case toward the use of xMatters.

Principle 4 **Implemented** Technical Support Department

Accuracy
Data must be 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').

Relates To
- **Asset:** Software as a Service (SaaS)
- **Asset:** Mobile Applications
- **Asset:** Technical Support

Satisfied By
- **Policy:** Subject Access Request (SARS)
- **Control:** MSA (Master Service Agreement)

Notes

xMatters provides all clients with complete control over their own data. All clients have a Web Based User Interface (WebUI) access to xMatters SaaS for control and data entry, deletion and modification. xMatters has no control over the accuracy of client data inputted into the system.

Principle 7 **Implemented** Privacy Officer

Accountability
xMatters shall make available specific, understandable information about it's policies and practices relating to the processing of PII ('accountability'). Clients shall be able to direct questions concerning xMatters compliance to the xMatters Privacy Officer. xMatters shall have policies and procedures to respond to the questions and concerns ('compliance').

Relates To
- **Control:** ISMS Roles and Responsibilities
- **Program:** PRO-5: xMatters Privacy Compliance Program (GDPR, PIPEDA, CCPA, APP)

Satisfied By
- **Control:** Subject Access Request (SAR) Register
- **Control:** List of Legal, Regulatory, Contractual and Other Requirements (A1811)
- **Control:** Risk Register
- **Control:** Data Breach Register
- **Policy:** Breach response Process
- **Policy:** Acceptable Use Policy

Data Security

Principle 5 **Implemented** Infrastructure Department

Storage limitation
Data must be 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Satisfied By

- **Policy:** Data Deletion Policy
- **Control:** MSA (Master Service Agreement)
- **Control:** Data Processing agreement
- **Control:** Data Loss Protection (DLP)
- **Control:** Service Level Agreements (SLA)

Notes

xMatters data retention period is governed by the contractual agreement with the client.

Principle 6 **Implemented** Privacy Officer

Integrity and confidentiality
Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Satisfied By

- **Policy:** Data Privacy Impact Assessment Process (DPIA)
- **Control:** Data Loss Protection (DLP)
- **Control:** Access Control SaaS
- **Control:** Role Base Access Control (RBAC)
- **Policy:** Acceptable Use Policy

Notes
xMatters makes sure that client personal data is processed in a manner that ensures industry-standard security of personal data. xMatters stores and processes all client data in Google Cloud Platform (GCP) datacenters and utilizes GCP's industry leading security services. xMatters protects client data against unauthorized or unlawful processing and against accidental loss, destruction or damage.
xMatters does not 'share' or 'sell' any data. All client provided data is used for service delivery as per contracted terms and agreements. Any data transferred to suppliers is done so as a part of xMatters service delivery. Suppliers are bound by contractual agreements to process data for xMatters only for xMatters business needs.