P-21: PRIVACY CODE OF PRACTICE

POLICY DETAIL REPORT

2021/04/21

P-21: Privacy Code of Practice

Owned by Compliance Department

Description

This document describes the xMatters Privacy Code of Practice. These practices are crafted in alignment to the Privacy requirements of ISO 27000 series and multiple Privacy Regulations that are relevant to xMatters business, employees and clients.

Versions

- Rev 3 published on: **2020-11-12 13:06:56** - **Active**
  Changes: Annual review
- Rev 2 published on: **2019-10-02 00:00:00** - **Retired**
  Changes: Privacy audit considerations incorporated
- Rev 1 published on: **2019-09-09 00:00:00** - **Retired**
  Changes: First Release

Privacy Code of Practice

Everything you need to know about Privacy at xMatters

Introduction

This document describes the xMatters Privacy Code of Practice. These practices are crafted in alignment to the Privacy requirements of ISO 27001 series, indutry specific privacy standards and the different Privacy Regulations that are relevant to xMatters business and clients.

xMatters design and implementation of Privacy Practices will be conducted by reviewing and incorporating the privacy laws and regulations from the regions that xMatters operates in. As well using a risk-based approach to determine the requirements of information security and organizational policies, processes and procedures to protect privacy related information. In regard to privacy data and systems that store and process personal information, industry best and accepted practices will be used to provide protection.

Scope

This Privacy Code contains principles that are applicable to xMatters as a processor of Clients' disclosed information. These principles must be observed on xMatters' products, services, processes and any subsidiaries or employees.

This Code is based on the 7 GDPR (General Data Protection Regulation) Principles and also take into considerations requirements from:

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australian privacy Principles (APPs)
- California Consumer Privacy Act (CCPA)

The scope and application of this Privacy Code are as follows:

- This Code applies to personal information about xMatters' clients and team members that is collected, used, or disclosed by xMatters.
- This Code applies to the management of personal information in any form whether oral, electronic or written.
- The Code applies to information regarding xMatters' corporate customers; however, such information might also protected by other policies and practices and through contractual arrangements.

Definitions

a) Personal Information: Any information about an identifiable individual, such as name, phone number, email, address, etc.

b) Collection: The act of gathering, acquiring, recording, or obtaining personal information from any source, including third parties, by any means.

c) Consent: voluntary agreement with the collection, use and disclosure of personal information for defined purposes. Depending on the circumstances and the geographical area where the personal information is collected, used or disclosed, consent can be either express or implied and can be provided directly by the individual or by an authorized representative. Express consent can be given orally, electronically or in writing, but is always unequivocal and does not require any inference on the part of xMatters. Implied consent is consent that can reasonably be inferred from an individual's action or inaction.

d) Customer: An individual who uses, or applies to use, xMatters' products or services, where such individual is a small business customer or a large corporation.

e) Disclosure: Making personal information available to a third party.

f) Personal identifiable information (PII): Information about an identifiable customer or team member.

g) Third party: An individual or organisation outside xMatters.

h) Use: The treatment, handling, and management of personal information by and within xMatters.

Roles & Responsibilities

Chief Executive Officer (CEO)

The CEO is identified as the ultimate asset owner for the entire organization and has accountability and responsibility for the organization in general.

Data Protection Officer (DPO)

The Data Protection Officer is identified as the owner of Privacy Policies and Procedures. The DPO has the responsibility and accountability of Privacy Compliance based on input from internal and external legal counsel and the Information Assurance (IA) team when applicable.

Information Assurance (IA) Team

The IA team is identified as the steward of the Privacy Code of Practices, including Policies and Procedures. The Information Assurance team conducts activities such as risk assessments, that include Data Protection Impact Assessment (DPIA), Privacy Assessments, etc.

Subject Matter Experts (SME)

In regards to Privacy Compliance and when necessary, advice will be sought from subject matter experts. This can include, but not be limited to, internal and external legal counsel and Privacy Auditor.

Clients (xMatters SaaS users)

The client is the provider of the data through bulk uploads, or individually via the web-based UI. The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the provider of the information (the client). Keeping in mind the interests of the client, xMatters relies on the client to keep certain personal information, such as First Name, Last Name, Email address information accurate,

complete and up-to-date. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to facilitate the business and use case of the client. Client provided information and data is always available for review by the client for accuracy via our web-based UI as the client wishes.

Legal Counsel

Specific Privacy clauses are observed in documented contracts and agreements that bind xMatters relationship with clients and vendors.

Principle 1 – Lawful, Fairness and Transparency

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

xMatters only process data when:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes as defined on agreements and contracts that bind the relationship between xMatters and its clients.

- processing is necessary for the performance of a contract, including the use of xMatters SaaS platform and provision of Technical Support

- processing is necessary for compliance with a legal obligation to which the controller is subject making sue the individual has access to their information and execute its rights

Transparency

xMatters Privacy Notice is available on the Internet https://www.xmatters.com/trust/privacy/privacy-notice/.

Clients must always know the means of gaining access to personal information held by xMatters. A description of the type of personal information held by xMatters, including a general account of its use, is disclosed on agreements and legal documents, as well as directly on the clients' instance on the SaaS platform where client can always have access to their controlled information, as well as logs for auditing purposes.

xMatters provides every corporate client and individual the right of access to personal information held about them. This includes individuals about whom a file is held (e.g. service users), or any other individual who is referred to directly in that file. It is most often used by individuals who want to see a copy of the information an organization holds about them. However, the right of access goes further than this, and when an individual makes a written request, xMatters will:

- Inform them whether any personal data is being processed.

- Provide them with a description of the personal data, the reasons it is being processed, and whether it will be given to any other organizations or people.

- Provide them with a copy of the information comprising the data.

- Provide them with the details of the source of the data (where this is available).

xMatters has a Subject Access Request procedure in place that guarantees a standard and documented process for all access requests received by Technical Support Team.

Principle 2 – 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.

xMatters limits the collection of personal information to that which is necessary for the purposes identified by xMatters, primarily, from its customers for the provision of the service, or team members, for employment purposes. The information collected from clients about their employees (system users) is governed by a data map/inventory of data.

Classification and Labelling

One of xMatters privacy purpose is to limit the collection of information. Information assets of the organization are classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset.

The level of security will be identified based on the information classification performed. xMatters' client information is always classified as confidential and the appropriate safeguards are used to handle it.

Information Handling

Information handling must be based on the classification of data, as described on xMatters Security Code of Practice.

The owner or creator of information will assign an appropriate label to the information, and the user or recipient of this information will consistently maintain an assigned label to make sure information is secure.

Opt-Out Preferences

xMatters provides clients with opt-out preferences for system communication and tracking technologies.

Principle 3 - Minimization

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

xMatters ensures that only the minimum data is collected to conduct business Prior to any new process or project applicable to xMatters services, the Information Assurance team analyses the data requirements to ensure that only the minimum required information is collected and used.

DPIAs are conducted annually or prior to each project in order risks can be identified and assessed regarding the collection and use of PII and that you minimize its use as a risk mitigation strategy. xMatters has a Risk Assessment process in place as a mandatory aspect of any asset, including client data.

Data Minimization principle ensures that:

- xMatters only collects personal data it actually need for our specified purposes related to the provision of services.
- xMatters has sufficient personal data to properly fulfil those purposes.
- xMatters periodically review the data it holds, and deletes anything that is not needed.

Principle 4 - 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').

Personal information used by xMatters must be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about a client or team member. xMatters will update personal information about clients and team members as and when necessary to fulfill the identified purposes or upon notification by the individual.

xMatters take reasonable steps to confirm the accuracy and relevance of PII. xMatters SaaS users are responsible for logging their own data and have the total control over the accuracy of their data. Besides that, xMatters has Subject Access Request (SAR) process that guarantees xMatters deletes and amends the data not only from our SaaS platform but also our backups upon request.

Principle 5 – 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').

Privacy Data Retention

xMatters will use client supplied data to provide contracted services only. Any data processed by xMatters or transferred to it's suppliers is done as a part of xMatters service delivery. Suppliers are bound by contractual agreements to process data for xMatters only for xMatters business needs.

Data retention policy is defined on service agreements and data deletion clauses can be found on the same documents.

Data Controlled by Our Clients

xMatters acknowledges that clients have the right to access their personal information and revoke our permission to store it. xMatters has no direct relationship with the individuals whose personal data it processes. A client who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct their query to the xMatters' Client (the data controller).

Data controllers can contact xMatters directly thought technical Support Team and exercise their right of deletion of PII and/or any data hold by xMatters. In that case, Technical Support will initiate an

operational process of data deletion (including backup deletion) and a certificate of Deletion can be issued to the client, upon request.

Datacenters

The following are the primary locations where client data is stored and processed, and secondary locations for back up redundancy, for xMatters Cloud Based Software as a Service (SaaS) emergency communications.

North America (NA)

- Google Cloud Platform (GCP) region datacenters (3 buildings) at Moncks Corner, South Carolina (US East)
- Google Cloud Platform (GCP) region datacenters (3 buildings) at Council Bluffs, Iowa (US Central)

Europe- Middle East- Africa (EMEA) – European Economic Area (EEA)

- Google Cloud Platform (GCP) region datacenters (3 buildings) at London (Europe-West2)
- Google Cloud Platform (GCP) region datacenters (3 buildings) at Germany (Europe-West3)

Asia Pacific- Japan (APJ)

- Google Cloud Platform (GCP) region datacenters (3 buildings) at Sydney Australia (Australia-Southeast1)
- Google Cloud Platform (GCP) region datacenters (3 buildings) at Singapore (Asia-SouthEast1)

Principle 6 - 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').

Information Security Requirements for Privacy

xMatters information security program will have its requirements provided for compliance and client contractual agreements for privacy and information security. All processes and requirements to assure the confidentiality, integrity and authenticity of data are documented as part of the xMatters Information Security Management System , such as:

- Access Control
- Protection of Data in Transit
- Data Encryption
- Monitoring and Reporting
- Vulnerability Management
- Training and Awareness

Client provided data is administrated by client's in regard to emergency communications and must be kept updated by clients by way of system integration or manual administration using xMatters Web Based User Interface (WebUI). xMatters employee data must be updated by employees.

xMatters Human Resources (HR) department has employment contracts that contain confidentiality and non-disclosure agreements that all employees and contractors read, agreed to and sign. xMatters employees are required to report any change in state as indicated by the xMatters Employee Handbook. xMatters Acceptable Use Policy is distributed by Human Resources (HR) which is required to be read, signed and tested on, annually, by every employee.

xMatters ongoing compliance requirements are in regard to confidentiality, integrity and availability. xMatters is audited and certified by TRUSTe/TrustARC for data transfer. As well xMatters is fully GDPR compliant having migrated to Google Cloud Platform (GCP) and leveraging Google's infrastructure. xMatters shall periodically remind it's employees of the importance of maintaining the confidentiality of personal information. xMatters employees are required to act in accordance with xMatters Ethics policy as a requirement of employment. This includes keeping personal information strictly confidential.

Principle 7 – Accountability and Compliance

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 Data Protection Officer. xMatters shall have policies and procedures to respond to the questions and concerns ('compliance').

xMatters is responsible for Personal Information under its control and has a designated Data Protection Officer who is accountable for xMatters compliance with this Privacy Code of Conduct. xMatters keeps a data map and uses an Access Control Process overlaid with Role Base Access Control (RBAC) for separation of duties and segregation of roles.

Onward Data Transfers (ODT)

xMatters must ensure, by way of Contract/Master Service Agreement (MSA) Terms, that any supplier receiving client provided data that is classified as Personally Identifiable Information (PII), must only be stored and processed as outlined by xMatters. Suppliers must not data mine, create meta data, transfer, share, sell or in any way shape or form handle xMatters provided data for any reason.

xMatters has created and implemented policies to:

- Establishing procedures to receive and respond to inquiries or complaints
- Establishing procedures to identify, communicate, manage, respond and notify Privacy breaches
- Establishing procedures to safeguard confidential and PII
- Implementing procedures to protect PII
- Training and communicating to employees regarding xMatters policies and practices
- Developing public information explaining xMatters policies and practices.

In order to do that, xMatters has implemented procedures to protect personal information and to oversee compliance with this code:

- Customer Success and Technical Support Teams have established procedures to receive and respond to inquiries or complaints .
- HR maintains a consistent onboarding program and continual communicating to team members about policies and practices .
- Developing public information to explain xMatters' policies and practices.

- Annual compliance audits as part of the Privacy Program.

Privacy Training

xMatters uses the following awareness and training methods for distributing information that directly or indirectly supports the xMatters Privacy Code:

- xMatters Employee Contract (Contains: Confidentiality and Non-Disclosure Agreements)
- xMatters Employee Handbook
- xMatters Human Resources Code of Conduct
- xMatters Acceptable Use Policy and Procedures
- Data Incident Response Test
- Privacy Training Videos and digital material

xMatters employs continuous monitoring using OSSec and monitoring with logs to a centralized Security Informational and Event Management (SIEM), for correlation, analysis, reporting and storage. Any anomalous activity reported to a human operator for investigation. In the event of a confirmed data breach, client contact will be initiated by xMatters Support or Client Success Management (CSM) team within 24 hours and no more than the required 72 hours.

Privacy Communications & Privacy Incidents/Complaints

xMatters has established communications channels and resolution paths for any comments, concerns or complaints in regards to privacy. There channels are available on xMatters website and xMatters Support Portal.