Data Protection Policy

October 2023

Overview

Eptura is committed to international compliance with all data protection laws. This policy defines the expected behavior and actions of Eptura employees and any Third Parties in relation to the collection, use, disclosure, transfer, retention, and destruction of any personal information of data belonging to Eptura customers, and the general public using Eptura's websites.

Personal data is any information which relates to an identifiable person. It is mandated by legal and regulatory authorities that Personal Data be secured. These legal and regulatory authorities stipulate controls and safeguards required to be in place to protect and control the personal information of an individual.

Eptura is primarily a Data Processor for personal information entrusted to us by our customers, which are the Data Controllers. On a much smaller scale and scope, Eptura is also a data controller for limited personal information obtained from its website and employees.

Eptura Commitment

Eptura's Executive Leadership Team is committed to ensuring the continual and effective implementation of this Policy. Non-compliance may lead to regulatory undertakings, fines, civil actions, and major reputational damage, including the loss of clients.

Eptura expects all employees and related Third Parties to commit to this Policy. Any deviation or breach of this Policy will be taken seriously and may result in disciplinary actions or termination of any business contract.

Scope

This Policy establishes a global Eptura standard for the processing and protection of personal information. This Policy address all national and international data protection regulation and laws, including but not limited to General Data Protection Regulation (GDPR), Australian Privacy Principles (APPs), and California Consumer Privacy Act (CCPA).

This Policy applies to all Eptura departments where personal information and data is handled and stored. This Policy applies to all processing of personal information on behalf of Eptura customers in digital or physical form and applies to the control of information entered using Eptura's websites.

Policy

Data Protection Officer

To demonstrate Eptura commitment to information and data protection the Data Protection Officer (DPO) function is the responsibility of the Chief Information Security Officer (CISO). This role functions independently from other key functions within the Eptura organization and reports directly to the Chief Technology Officer, and to the Board. The DPO will facilitate compliance to Privacy regulations by:

- Advising Eptura and its employee's details regarding data protection regulations and law
- Carrying out Privacy Impact Assessments (PIA)
- The point of contact for all Data Protection Authorities (DPAs)
- The point of contact for any Client related data protection requests
- The establishment and operation of a process to provide timely responses to Data Subject requests
- Informing senior management of any breach or potential breach of personal information or data
- Assessing and monitoring any applicable third party engaged by Eptura for compliance to this policy
- Creating training and awareness for all Eptura employees responsible for processing data to be aware of and comply with the content of this Policy.

Additional Eptura Roles and Responsibilities

Eptura responsibilities for Data Protection include:

- everyone processing personal information understands that they are contractually responsible for following good data protection practice
- everyone processing personal information is appropriately trained to do so
- everyone processing personal information is appropriately supervised
- everyone processing personal information will report a suspected or actual breach of data using the Data Protection Breach Incident procedure
- anyone wanting to make enquiries about handling personal information knows what to do
- will regularly review and audit the processes it uses to hold, manage and process Personal Data

Data Protection by Design

Privacy by design is a methodology that enables security to be 'built in' to the design and architecture of information systems, business processes and networked infrastructure. Privacy by design also applies when upgrading existing systems or processes, each of them must go through an approval process. A Privacy Impact Assessment (PIA) is to be undertaken by the DPO for all new and changed systems and processes. This includes:

- Product
- Infrastructure
- Customer Service
- Sales

Privacy by design aims to ensure that privacy is considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling of personal information. It shifts the privacy focus to prevention rather than compliance. Privacy by design features shall include:

- Proactive not reactive
- Privacy as the default setting
- Privacy embedded into design
- End-to-end Security – Full Lifecycle Protection
- Visibility and transparency
- Respect for user privacy

By following these principles, Eptura management and employees will be able to build privacy into policies, programs, and practices.

Compliance

To ensure the appropriate level of security and compliance is being achieved, the Information Security and Privacy Manager will carry out periodic audits across all Eptura areas to assess the level of compliance and protection of personal data.

Audits will include but not limited to:

- Access rights
- Data transfers
- Access logs
- Data storage and locations
- Assessment of procedures and processes with respect to personal data handling
- Personal data complaints handling

All audit findings will be addressed with a remediation plan with compliance reporting submitted to Eptura Management.

Personal Data Protection Principles

The following principles and best practices are adopted by Eptura for the protection for personal data. The seven principles apply to the collection, use, retention, transfer, disclosure and destruction of personal data.

Principle 1: Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject. Eptura must inform the data subjects and/or the data controllers (the Clients) what type of processing will occur. This can be via a privacy policy and/or agreements or contracts.

Principle 2: Purpose Limitation

Personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Eptura must specify exactly what the personal data collected will be used for and limit the processing of that data to only what is necessary to meet the specified purpose or functions.

Principle 3: Data Minimization

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. This means Eptura will only collect and store the absolute minimum fields or details required to perform its services.

Principle 4: Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data which is inaccurate or having regard to the purposes for which they are processed, are erased, or rectified without delay.

Principle 5: Storage Limitation

Personal data shall 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 is processed. Eptura will delete data no longer required or store personal data in a way that limits or prevents identification of the data subject, in line with any legal requirements.

Principle 6: Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful use or processing, against accidental loss, destruction, or damage, using appropriate security controls and organizational processes.

Principle 7: Accountability

Eptura, and its employees are responsible for and be able to demonstrate compliance with these principles at all times.

Data Collection

Eptura uses the Personal Data collected for the following processes:

- To provide services to its customers
- To provide information to general public interested in Eptura product offerings
- Eptura general running and business administration

Personal data should be collected only from the Data Subject or Client where the nature of the business purpose necessitates collection of the Personal Data from other persons or bodies which is aligned with the Eptura operating model.

Eptura will ensure that data is collected within the restrictions described in this Policy. This applies to data that is collected in person, electronically or by completing any forms. It applies to any location that is being used by staff or contractors to deliver Eptura related business.

When collecting data, Eptura will ensure, wherever possible, that there is a fair processing notice in place and that the Individual:

- clearly understands why the information is needed
- understands what it will be used for

- understands who the data may be shared with and why
- has the option to agree to sharing the data
- gives explicit consent to contact via email

Eptura does not collect any Sensitive Personal Data from its customers.

Data Subject Consent

There are instances within Eptura where implicit/implied consent is assumed for collecting data, for example information given when using Eptura website and completing information requests online. The Privacy Policy clearly explains this situation.

External Privacy Notices

Eptura public website includes an online SaaS Privacy Policy and Website Privacy Statement, fulfilling the requirements of the applicable laws and regulations.

Data Processing for Marketing Purposes

If the data subject contacts Eptura to request information (e.g. request to receive information material about a product), data processing to meet this request is permitted. Personal data can be processed for advertising purposes, if this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the type of use their respective personal data for these purposes.

If the Data Subject refuses the use of their respective personal data for marketing purposes, it can no longer be used for these purposes and must be blocked from use.

Data Storage

Information and records relating to individuals will be stored securely and will only be accessible to authorized staff. Information will be stored for only as long as it is needed or required by law or regulation and will be disposed of securely.

Data Use

Eptura will Process Personal Data in accordance with all applicable laws, regulations, and applicable Client contracts. More specifically, Eptura will not process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given consent to the controlling and/or processing of their Personal Data
- Processing is necessary for the performance of a contract to which the Data Subject is a party.

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected.

When planning for a new purpose for processing, guidance and approval must be obtained from the DPO before any such processing commences.

Data Access and Accuracy

All Individuals have the right to access the information Eptura holds about them. A Data Subject may request to access and/or correct the personal data currently in our possession or control by submitting a written request to Eptura. Eptura will require the relevant information to firstly identify the requestor as well as the nature of the request.

Once the identity of the requestor is verified and the relevant information is provided, Eptura will respond within 30 days. If unable to respond with the 30 days, a notification will be provided at the soonest practical.

Security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. Before the establishment of new systems or processes for data processing, technical and organizational measures to protect personal data must be defined and implemented. The relative person can consult with the DPO for any guidance and compliance related assistance.

Data Protection Incidents

All employees and contractors must inform their manager, the DPO, Security, or Legal Counsel immediately when a breach has occurred or there is a suspicion of a data breach.

In cases of:

- Improper transmission of personal data to third party
- Improper access by unauthorized party
- Loss of personal data

The incident must be reported immediately so that any reporting requirements under the privacy laws can be complied with.

Complaints Handling

Data Subjects with an issue about their Processing of their Personal Data should email the Eptura DPO. Once the email is received, an assessment will be made to classify the complaint followed by an investigation. The DPO will inform the Data Subject of the status of the complaint, with an outcome provided within a reasonable time.

If the Complaint cannot be resolved between the Data Subject and Eptura, then the issue can be escalated to the data protection or privacy regulatory authority within the relative jurisdiction.

Breach Reporting

Any individual, whether an Eptura employee, customer, or Data Subject, suspects a breach of Personal Data due theft or exposure, must immediately notify the Eptura DPO. The individual reporting should have the relevant details of what has occurred. The incident can be reported by email privacy@eptura.com or by calling Eptura offices or customer contacts.

The DPO will immediately investigate the breach as soon as the notification is received and confirm if in fact a breach has occurred, or if there was unauthorized access.

Once a breach is confirmed, Eptura will enact its Data Breach Incident Response Procedure to coordinate and manage handling of the event.

Definitions

Anonymizing	*Data modified in such a way that no individuals can be identified from the data by any means or by any person.*
Client or Customer	*Organizations who use the Eptura applications via commercial agreement*
Consent	*Any freely given notification by a person by which he or she, by a statement or action which signifies agreement to the processing of personal information relating to him or her.*
Data Breach	*A breach of security controls or processes leading to the accidental or unlawful destruction, loss, modification, unauthorized disclosure of, or access to, personal information transmitted, stored or otherwise processed.*
Data Controller	*A person or organization determines the purpose and how Personal Data is processed. Within this Policy, the organization is the Eptura Customer.*
Data Processor	*An organization which processes personal information on behalf of a Data Controller. Within this Policy, it's Eptura.*
Data Processing	*Any operation performed on personal information or on sets of personal data, using manual and/or automated means. Operations performed may include collection, recording, structuring, storage, modification, retrieval, use, destruction, or disclosure by transmission, dissemination or otherwise making available.*
Data Protection Officer (DPO)	*Are responsible for overseeing data protection strategy, implementation and compliance to personal data regulation.*
Data Protection	*The process of safeguarding personal information from unauthorized or illegal disclosure, access, modification, processing, transfer or destruction. This involves controls based on people, process and technology.*
Data Subject	*The identified or identifiable real person to which the data refers.*
Encryption	*Is the process of encoding data or information in such a way that only authorized parties can access it and those who are not authorized cannot.*
Personal Identifiable Information *(PII)*	*Any information that can be used to distinguish or trace an individual's identity*
Personal Data	*Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.*
Redacting	*Removes personal information from records and forms from an individual's account*

Sensitive Personal Data	*Is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.*
Third Party	*An organization or person, other than the data subject, controller, processor under the direct authority of the processor to provide services to Eptura*
Website user	*A person who uses Eptura's public websites*