Data Processor and Controller Compliance Roles and Responsibilities

January 2023

Overview and Purpose

Under the General Data Protection Regulation (GDPR) both Eptura, the Processor and Eptura's customer, the Controller have certain obligations with respect to the protection of personal data belong to the Controller's workers, the Data Subjects.

This guideline is to be referred to by both, the Eptura employees and the Controller to understand our roles and responsibilities with respect to GDPR requirements and rights of the Data Subjects.

This guideline will help create a closer coordination between Controllers and Processors to ensure GDPR compliance.

Scope

The guideline refers to personal data transferred to Eptura, the Processor, by the Controller, Eptura's customer for Processing.

Personal data referred to is the Personal Identifiable Information (PII) provided by the Controller for processing as per the respective contractual agreements by Eptura, on Eptura owned or managed systems. There are no sub-processors used by Eptura.

Guideline

Roles and Responsibilities

The GDPR has particular requirements that are applicable to each, the Processor and the Controller with respect to the protection of personal data and the rights of the Data Subjects.

The Processor

- The appointment of a Data Protection Officer (DPO)
- Only process personal data on instructions from the Controller
- The Processor must ensure that any personal data that it processes are kept confidential.
- Will obtain written permission from the Controller before engaging a subcontractor
- Take reasonable steps to secure data, such as encryption, stability and uptime, backup and disaster recovery, and regular security testing
- Provide the Controller with full co-operation and assistance to enable the Controller to comply with any requests from Data Subjects
- Not disclose or release any Personal Data requested by the Data Subject or third party without first consulting with and obtaining formal approval from the Controller
- Provide in a timely notification in changes of risk
- Notify the Controllers without undue delay upon learning of data breaches
- Upon request, delete or return all personal data to the Controller at the end of contract

The Controller

- Supply the Processor with a mutual Data Processing Agreement (DPA)
- In the event of a data breach, the Controller must report the breach to the DPA without undue delay, and in any event within 72 hours of becoming aware of it.
- Notify the Processor of any Data Subject requests, such as:
- Request for information of data collected
- Request to opt out of data collection
- Deletion of all data belonging to the Data Subject

Data Subject Requests

Processor is to notify the Controller within 2 working days for any request from a Data Subject exercising their right under the GDPR. These include requests to:

- access their Personal Data
- erase their Personal Data
- disclose their Personal Data to a third party
- any objections to Processing

Any third-party requests for Data Subject Data must be formally approved by the Controller.

Process

All Personal Data is controlled by Eptura's customer, who is the Controller and the Custodian on behalf of the Data Subject. Eptura must always get approval or instruction from the Customer.

***Scenario 1 - Data Subject requests of their Personal Data from Eptura**:*

1. Data Subject request directly to Eptura, via email, or social media
2. The Data Subject may need to be contacted if further information is required
3. A ticket is raised with Customer Service (CS) team and Information Security and Privacy Manager is notified.
4. The respective CS account representative contacts the customer via email, following up with a phone call.
5. CS team member informs the Data Subject to contact their respective Data Controller (Eptura's Customer)
6. The email shall contain:
    a. relevant details of the Data Subject
    b. Details of the type and reason of request
7. The Customer's DPO shall also be informed via Eptura's Information Security and Privacy Manager
8. Eptura will await further instruction from Customer. Until then, no further action is to be taken.

Scenario 2 - Eptura Customer contacts Eptura on behalf of the Data Subject:

1. Eptura Customer contacts Eptura CS representative or Eptura's DPO.
2. Request should be in writing with the relevant Data Subject details
3. Customer to provide details on the request, such as to:
    a. provide to the Controller the Data Subject's data
    b. delete the Data Subjects
4. Ticket to be raised with CS team
5. Ticket to be raised with PRODOPS for the request to be completed
6. Confirmation of requested tasks completed

Scenario 3 – Data request from third party, such as Police, Legal request, or other regulatory authority:

1. All third-party requests are to be forwarded to the Eptura DPO
2. The respective Eptura customer will be notified of request and ask for instructions
3. Under no circumstances are details or data relating to a data subject be released without Customer approval.