DATA PROTECTION POLICY
PROCESSOR

TABLE OF CONTENTS

1 Introduction

This policy describes the organizational and technical safeguards Aditro has implemented to protect Personal Data processed by Aditro as processor for our customers, in accordance with the EU General Data Protection Regulation and national data protection laws. It is the responsibility of our employees to apply the provisions of this Policy in relation to all Processing of Personal Data.

Aditro is committed to integrate Privacy in its products and services to enable our customers to be compliant in using our offerings.

2 Scope

This Policy applies to Aditro Group AB and its subsidiaries.

This Policy applies only to Aditro in the capacity of Processor for our customers. Aditro will only process personal data for the purpose of fulfilling its obligations under the relevant agreement with each customer, and as set out in this policy.

In addition to this policy, the agreement between Aditro and each customer sets out the nature of the Processing for that customer and responsibilities of the Processor (Aditro) and the Controller (Customer).

Legal requirements on archiving of payroll or accounting material of each Aditro customer are the responsibility of each Aditro customer and is outside the scope of Aditro's obligations and this policy.

This Policy may be translated to any language of a country where Aditro Group or its subsidiaries are operational, in case of discrepancies between a translation and the English version, the English version shall prevail.

3 Essential changes

Version	Change
1.0	Initial version
1.1	Additional information on privacy objectives and privacy governance, general updates

4 Approval

Approved by	
Approval date	Version 1.0. Aditro Group General Management Team, 19.9.2017 Version 1.1 General Counsel Ulrika Ersman on, 06.04.2020
Effective date	Version 1.0 25.05.2018 Version 1.1 06.04.2020

5 Glossary and acronyms

The following key terms are used in this policy. Unless otherwise stated, these terms and other terms used in this policy shall be interpreted in accordance with their definitions in the EU General Data Protection Regulation (EU 2016/679) (the "GDPR").

Term	Explanation
Personal Data	Any information relating to an identified or identifiable natural person (data subject).
Processing	Any operation or sets of operations performed on personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	The natural or legal person, public authority or other body, who determines the purposes and means of the processing of personal data, in this case Aditro's customer(s), their affiliate(s) or end customer(s).
Processor (or sub-processor)	The natural or legal person, public authority or other body that processes personal data on behalf of the data controller, in this case Aditro, including Aditro affiliates and sub-contractors.
Data Subject	An identified or identifiable natural person
Products	All Aditro products

6 Privacy objectives

Aditro recognizes the importance of Personal Data and of respecting the Privacy rights of individuals. Due to the nature of our business almost all data that we handle has its origin in the employment relationship between our customers and their employees. The data that follows from such a relationship can be sensitive and therefore deserves special care. We have committed to govern the privacy accordingly.

Aditro's privacy governance objectives are:

- ***Complying and respecting personal data privacy in services and products***
- ***Operate in transparent and compliant manner in each location by each employee***
- ***Commit to continual improvement of the privacy management system***
- ***Continuously improve and develop our processes to overcome future privacy challenges***

7 Privacy responsibilities

Aditro has defined the following privacy responsibilities.

7.1 Privacy governance

Aditro's privacy is governed by the General Management Team (GMT), supported by the Aditro Compliance Committee to align various standards and frameworks to ensure consistency and compliance in privacy governance.

7.2 Privacy management

Aditro's privacy is managed by the Group Privacy Officer & Data Protection Officer (DPO), together with the Privacy Operations Team, distributed throughout the organization. Aditro's privacy management system framework is ISO 27701:2019.

The Data Protection Officer reports to General Counsel, who is a member of the General Management Team and the Compliance Committee.

7.3 Group Privacy Officer & DPO responsibilities

Aditro has appointed a Group Privacy Officer & Data Protection Officer who is responsible for:

- Acting as a key point of contact for all internal and external related data protection queries and the reporting of breaches to controllers and/or data protection agencies
- Monitoring compliance with this and other data protection policies as well as with the General Data Protection Regulation (EU 2016/679)
- Conducting reviews of internal procedures and be part of any Data Protection Impact Assessment
- Liaising with Data Owners to deliver training, improve awareness and communicate information relating to this Policy to other employees
- Updating this Policy if necessary
- Demonstrating compliance with the General Data Protection Regulation (EU 2016/679)
- Registrations and handling contact with government agencies such as Datainspektionen, Datatylsynet and Tietosuoja
- Provide internal guidance and training

Aditro Group and its subsidiaries shall have Datainspektionen in Sweden as Lead Supervisory Authority.

7.4 Privacy and data protection in processes

Each business area and business function is responsible to ensure compliance with the agreed privacy and data protection policies and practices to ensure Aditro's privacy practices always fulfil the business objectives. Each employee is responsible to follow the issued privacy instructions.

8 General privacy principles

Personal data shall always be

- processed fairly and lawfully ("lawfulness, fairness and transparency");
- collected and processed for specific and legitimate purposes ("purpose limitation");
- adequate, relevant and limited to what is necessary for the purpose ("data minimisation");
- accurate and kept up to date ("accuracy");

- kept for no longer than is necessary for the purpose ("storage limitation");
- processed using appropriate technical and organizational measures to protect against unauthorized alteration, accidental loss, destruction or damage ("integrity and confidentiality").

8.1 Lawfulness, fairness and transparency

Aditro as a processor does not determine the scope and purposes of the processing it performs for its customers as controllers. Aditro may assist customers by providing an overview of the data or categories of data that our products or services require to perform their intended functionality. Aditro uses a purpose classification built on three pillars ("product purpose" for data required to deliver the product's intended outcome, "legal purpose" for data to be stored based on legal requirements, and "customer purpose" for data that is not required for our products or for compliance with legal obligations but that a customer may need to process for other purposes). The data or categories of data that are finally processed for each customer are defined by the customer.

8.2 Purpose limitation

Aditro enables categorization of data by purpose in its standard configuration and to some extent customer specific categorization and can therefore identify when data is used for different purposes or is used for purposes that derive their use directly from the initial purpose, such as for support and incident management. This allows for appropriate access and retention management.

Aditro may use fully anonymized or anonymous data for statistical purposes.

The Aditro Test Data Policy sets out the applicable requirements and the process to obtain customer consent for any use by Aditro outside of the initial purpose to perform Aditro's agreed service delivery to the customer.

8.3 Data minimisation

Aditro assists Controllers by

- Identifying personal data generally needed as a minimum input for each of our products, more data might be needed depending on the type of business and products purchased
- Keeping data up to date where possible, final responsibility for accurate data rests with the Controller
- We do not hold Personal Data on a 'just-in-case' basis or because it might be useful in the future, data is only processed as long as in our standard configuration or as instructed by the controller
- Where possible we do not show Personal Data when there is a legal obligation to retain data that extends beyond the data that is necessary for product functionalities

8.4 Accuracy

The data Controller should take necessary steps to ensure that the information and Personal Data sent to Aditro is correct and up to date. Some of Aditro products have a

customer interface that enables Controllers to perform the necessary checks to ensure accurate data.

8.5 Storage limitation

Aditro uses a standard configuration for those products and services that handle structured data, these include options for the safe erasure or de-identification of data. The execution of such removal processes is primarily within the domain and responsibility of the customer. Aditro standard configuration is however a complete set up that intends to offer GDPR compliance as concerns the storage limitation principle. Any deviation from the standard configuration is optional.

The Aditro Data Retention Policy contains further details on data retention and removal.

8.6 Integrity and confidentiality

Aditro uses a data classification system that ensures integrity and confidentiality, more information can be found under chapter 12 below.

9 Controller and Processor

Aditro is the processor of personal data that Aditro processes as part of our service delivery to our customers. In Aditro's capacity as processor of personal data, Aditro will only process personal data for the purpose of fulfilling Aditro's obligations under the relevant agreement with each customer, and as set out in this policy.

Each Aditro customer (or end customer) is the Controller of the personal data concerning its employees. It is the Controller's responsibility to ensure there is a valid legal ground for the processing, that the data subjects are duly informed of the processing in accordance with legal requirements and, to the extent the processing is based on consent from the data subject, that any consents are given and logged. Some of our products can assist in logging consent. Prior to engaging Aditro as processor, the controller shall ensure that the processing by Aditro, including the technical and organizational measures described by Aditro in this policy and other relevant documentation, fulfils the controller's requirements and comply with legal or other requirements on the controller.

10 Data Processing Agreement

The agreement between Aditro and its customers shall set out the subject-matter and the duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects and the obligations and rights of customer and Aditro. Unless otherwise agreed, the data processing agreement will be in the form provided by Aditro.

Link: Aditro Data Processing Agreement Templates (Aditro internal)

11 Personal Data

In the course of operation for its customers Aditro receives both structured and unstructured data, data that is required as a minimal input for the product or services purchased but also creates data that is to be treated as sensitive. In order to safeguard data, Aditro can only properly classify data where it is aware of its intended content. Unstructured data or data provided by the customer which is not needed for the products

or services purchased but that is to be considered as personal or sensitive data needs to be identified by the customer, so that Aditro is able to take preventive measures.

Aditro can provide each customer with a list of data entries that form a necessary input for the products or services purchased as well as data that the customer is required to provide by Member State laws. This data has been classified by Aditro as data relating to a natural person either indirectly, directly or as sensitive personal data. Aditro uses this classification in combination with a risk assessment for identifying appropriate techniques, strategies and organizational measures to safeguard personal data.

12 Categories of Personal Data

To ensure that appropriate safeguards are used to protect personal data Aditro operationalizes a Personal Data Category where data or sets of data are categorized according to the intended type of Personal Data contained. As our customers are able to use our products for processing other types of data they should ensure that fields or data classes are appropriately classified. For some other products, no classification is performed due to the context independent nature of the product.

Level	Personal Data Category	Corresponding security classification
0	No Personal Data	
1	Personal Data relating indirectly to an Identifiable Person	Semi-Confidential
2	Personal Data relating directly to an Identifiable Person	Confidential
3	Sensitive Data	Highly confidential

Directly identifying categories of personal data include Personal Identification Numbers, Names, Addresses, IP Addresses, E-Mail addresses.

Sensitive categories of personal data include personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Aditro's services may include the processing of special categories of personal data (mainly concerning health or trade union membership), however only as included in the relevant service and as described in the applicable service description.

Processing of special categories of personal data (or "sensitive data") is subject to additional restrictions and security measures.

Should the Controller or its end users otherwise add or upload any personal data belonging to a special category of personal data, or otherwise deemed sensitive, into any solution hosted or managed by Aditro, Aditro will not assume any liability for the processing of such personal data outside of its general obligations of security.

13 Privacy by Design

13.1 Privacy Enhancing Technologies

Aditro uses privacy enhancing technologies, strategies and organizational measures to protect personal data. The identification of relevant measures is done according to the sensitivity level of the personal data, the duration for which data is saved, the risk involved in the processing and frequency of use. Please see for more information the data categories under chapter 12.

Aditro applies conventional and proofed security measures such as end to end encryption towards data subjects most sensitive data and applies other privacy enhancing techniques based on their state of the art and maturity.

The classification can determine which Privacy Enhancing Technologies are applied to the data. Where a standard requirement for Level 3 data may be end to end encryption a requirement for Level 2 may be pseudonymizing. The categorization also enables Aditro to specify how Personal Data is safely removed. For Level 3 this may be deletion and for Level 2 this may be anonymization. Level 0 and Level 1 data should never lead to identifiability if Level 2 and Level 3 are successfully de-identified. The Privacy Enhancing Techniques are applied product specific.

13.2 Design Principles

Aditro will implement Privacy Design through active involvement of those involved in the design and early phases of implementation of new product or system functionalities. Aditro uses a core team of Privacy trained system architects to promote Privacy throughout relevant development areas of our company. In doing so we aim to adhere foundational privacy principles of

- Proactively adopting strong privacy practices, early and consistently
- Privacy as a default where possible
- Privacy embedded into design
- Without impairment on functionality
- Lifecycle protection
- Visibility and Transparency
- Respect for User Privacy

More information can be found in the Aditro Privacy by Design Policy.

14 Privacy Impact assessments and risk management

In addition to a general risk management framework, described in the Aditro Risk Management Policy, Aditro has defined a process for registration and privacy impact assessment of new personal data processing operations, in order to secure that privacy risks are identified and mitigated as needed.

This process is further described in the Aditro Privacy Impact Assessment Policy.

15 Receipt of Personal Data

Aditro may receive personal data from the customer (controller), directly from the customer's employee (data subject) or from a third party.

Aditro will deem personal data received directly from a data subject or from a third party as received from the controller. The controller will always remain responsible to ensure there is a valid legal ground for the processing, that the data subjects are duly informed of the processing in accordance with legal requirements and, to the extent the processing is based on consent from the data subject, that any consents are given and logged.

16 Records of processing

Aditro maintains records of processing activities carried out on behalf of its customers. Such records include information regarding the name and contact details of the Aditro entity or entities and sub-contractors that process personal data, the name of the controller or controllers, the categories of processing carried out for each controller, any transfer to a third country, and a general description of the technical and organizational security measures undertaken by Aditro.

Aditro continuously makes the relevant records available at https://aditro.com/gdpr/rop/.

17 Use of Sub-Processors

In addition to Aditro affiliates, Aditro also uses sub-contractors within the delivery of products and services to our customers. Where a sub-contractor is engaged in any processing of personal data on behalf of an Aditro customer, that sub-contractor is also a processor (sub-processor).

Unless otherwise agreed with a specific customer, the agreement between Aditro and its customers include a general written authorization for Aditro to use sub-processors. Aditro will make available to its customers an up-to-date list of its sub-processors, including information on the processing activities performed by each sub-processor. This list can be found at https://aditro.com/gdpr/rop/entities-involved-in-the-processing-of-data/.

Prior to engaging a sub-processor, Aditro will enter in to a contract with that sub-processor that sets out the subject-matter and the duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects and the obligations and rights of Aditro and the sub-processor.

18 Data transfers to third parties

Aditro's delivery of services may include a transfer of personal data to third parties, other than Aditro affiliates or sub-contractors, however only as specified and agreed for the relevant service and as described in the applicable service description. Examples of such third parties are national tax authorities, banks, statistical authorities, etc.

Such transfers will only be made to the extent and for the purposes stated in the agreement between Aditro and the customer, and in the manner specified and agreed. The relevant Controller remains liable for the legality of the personal data processing, including the transfer to the third party.

Aditro's response to information requests by public authorities or other third parties, outside of the agreed service delivered by Aditro to its customer, is described in section 22 below.

19 Transfers of data to third countries

Unless otherwise agreed in writing Aditro will only store and process personal data within the EU/EEA area. In certain situations, as described on https://aditro.com/gdpr/rop/, Aditro or its sub-processors may transfer personal data to a sub-processor located outside of the EU/EEA.

Where a transfer of personal data by Aditro, or by a sub-processor, to a sub-processor outside the EU/EEA takes place, Aditro shall ensure that transfer is only made to a country deemed by the Commission to have an adequate level of protection, to entities having committed to the EU-US Privacy Shield, or that has entered into standard data protection clauses or provided other appropriate safeguards.

20 Rights of the data subjects and other obligations of controllers – assistance by Aditro

20.1 Request for access

Every data subject has a right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, if it is, access to the personal data and certain information about such processing.

20.2 Request for rectification (correction)

Every data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. A request for rectification from a data subject shall be directed to the Controller. Aditro will not respond to requests directly from the data subject. Instead, in case a data subject directs a request for access to Aditro, Aditro will refer the data subject to the Controller.

20.3 Request for erasure

Provided the personal data is no longer necessary for the purpose for which they were collected or processed, the processing is based solely on consent by the data subject and the data subject withdraws such consent, the data subject objects to processing as described in Article 21 of the GDPR, or the personal data has been unlawfully processed, the Controller is legally required to erase the data without undue delay upon request by the data subject. Aditro can comply with requests to delete data if such a request is directed from the Controller. The data that will be deleted does not include data that needs to be retained to comply with legal provisions according to Member State law.

20.4 Request for data portability

Where processing is based on consent or on a contract between the Controller and the data subject, and the processing is carried out by automated means, a data subject has the right to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the Controller to which the personal data has been provided.

20.5 Aditro's handling of requests by data subjects

A request by a data subject as described under 20.1- 20.4 shall be directed to the relevant controller. Aditro will not respond to requests directly from a data subject. Instead, in case a data subject directs a request to Aditro, Aditro will refer the data subject to the controller.

Upon request by the customer, and depending on the nature of service delivery by Aditro to our customer, Aditro will assist the customer (controller) to respond to requests as described in 20.1- 20.4 from that controller's data subjects, as regards personal data

processed by Aditro as processor for that controller. It is the responsibility of the controller to determine the legality of the data subject's request. Any assistance by Aditro outside the scope of the services agreed under the relevant customer agreement will be charged by Aditro at the then current rate applied by Aditro.

20.6 Other assistance to controller

Upon request by a customer, Aditro will upon reasonable notice and to a reasonable extent considering the nature of the processing by Aditro, as agreed with that customer, assist the customer (Controller) in ensuring compliance with the Controller's obligations, including assistance in data protection impact assessments. Any assistance by Aditro outside the scope of the services specified and agreed under the relevant customer agreement will be charged by Aditro at the then current rate applied by Aditro.

20.7 Audit request

Aditro will upon request make available information necessary to demonstrate compliance with the agreement between Aditro and a customer, and will allow for audits by the customer or a third party auditor mandated by the customer. Unless otherwise agreed, Aditro shall be entitled to charge the customer on a time and materials basis for time spent and costs incurred due to the audit.

Aditro may also provide the controller with an audit report by a third-party auditor and may make certain information or documentation continuously available to our customers on the Aditro customer portal and/or Aditro website.

Please consult our Global Audit Policy and the applicable data processing agreement for further information.

21 Personal Data Breach

When Aditro becomes aware of a Personal Data Breach of a sufficient severity level, Aditro shall notify the affected controller(s) without undue delay. Aditro's notification shall include a description of the nature of the personal data breach, where possible the categories and number of data subjects and the categories of personal data concerned, the name and contact details of the DPO or other person in Aditro who can provide additional information, and a description of the measures taken by Aditro to address the personal data breach and to mitigate its consequences.

More details on Aditro's process in case of Personal Data Breach can be found in the Aditro Personal Data Breach Policy and the Aditro Incident Management Process description.

22 Information requests

Should Aditro receive a request for information by a public authority or other third party outside of requests covered by a service delivered by Aditro for a customer, then Aditro will:

a) All requests for disclosure of information will be logged and stored by Aditro.

b) Verify the identity of the entity and person making the request

c) The demand should follow a legal process, e.g. it must be accompanied by a written warrant, court order for content or likewise for disclosing personal data for a specific data subject (or data subjects).

d) Aditro will attempt to redirect the request to the controller

e) Unless prohibited by law, Aditro will inform the data controller of the request

f) If legally obligated to disclose personal data under a request, Aditro will aim to limit the scope of the personal data disclosed

g) Aditro does not provide any direct access to our customers' data, and do not provide any government with means to break our data protection principles.

h) Aditro might challenge a government request for information if the request is contrary to the Aditro principles for disclosing information, Aditro believe that the request is beyond the jurisdiction, of the requesting government or agency, or the demand is not signed or appropriately authorized, contains the wrong dates, is not properly addressed, contains material mistakes, or is overly broad, the information requested seems to be excessive and out of scope for the purpose of the request.

i) Aditro is not in a position to prevent a request for information, but can decide to challenge any request so that it is handled properly and according to law.

j) Any Request for disclosure of information need to be filed in Aditro's Incident Management System before it can be processed.

To approve a disclosure, the following applies:

a) A request or demand for disclosure of information, outside of an agreement, is always reviewed for validity by the Aditro Legal Department. The Legal Department determines whether the requests are valid, rejects those that are not valid, specifies data that should be provided etc.

b) Decisions on the disclosure of Customer owned information, at the request from a commercial third party, can only be authorized by the Customer or the Data Subject.

c) Decisions on the disclosure of information, at the request from government, can only be authorized by the Aditro CEO, or its representatives.

23 Training

Aditro employees receive onboarding training as well as a mandatory general annual training in the area of privacy. In addition, more detailed training on processes and procedures are provided for various target groups, as needed or on a regular basis.

24 Monitoring, measurements and KPI's

Aditro monitors the number of logged and reported Personal Data Breach incidents, the number of data subject access requests received and managed, and customer use of data deletion functionality in Aditro's applications.

The Aditro DPO reports to the General Management Team twice a year (typically in March and in October) and the Aditro General Counsel reports to the Board of Directors annually (typically in September).

25 Referenced Information

- Aditro Test Data Policy
- Aditro Privacy by Design Policy
- Aditro Privacy Impact Assessment Policy
- Aditro Risk Management Policy
- https://aditro.com/gdpr/rop
- Aditro Personal Data Breach Policy
- Global Audit Policy