TRAPETS

Data Protection Policy - Trapets as Processor

2024-11-14

TRAPETS

1. Purpose and Scope

Trapets provides cutting edge services and systems to the global finance industry for monitoring of transactions, KYC, customer due diligence and fraud prevention.

This policy describes the organizational and technical safeguards Trapets has implemented to protect Personal Data processed by Trapets within our service delivery, as processor for our customers (the controllers). Trapets is committed to integrate privacy in our products and services to enable our customers to be compliant in using our offerings.

It is the responsibility of our employees to comply with this policy in relation to all processing of Personal Data.

This Policy applies to Trapets AB and its subsidiaries.

2. Owner and Version control

Owner: Ulrika Ersman, CLO and Data Protection Officer			
Version	**Date approved**	**Approved by**	**Major changes**
1.0	2023-05-08	Management team	New policy
1.1	2024-11-14	Trapets Management team	Annual review and approval, minor updates

3. Definitions

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 Trapets' customer(s) or their affiliate(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 Trapets, including Trapets affiliates and sub-processor(s).
Data Subject	An identified or identifiable natural person
KYC Screening Data	Content in the agreed and specified screening lists included in the agreed InstantWatch KYC services. Such lists can be company information and beneficial ownership lists, sanctions lists, PEP lists or other lists, as specified in the applicable customer agreement.

TRAPETS

4. Privacy objectives and responsibilities

Trapets recognizes the importance of respecting the privacy rights of individuals. In addition to the GDPR, some of the personal data we process for our customers are also covered by legislation on bank secrecy or similar legislation. We are committed to govern privacy accordingly.

Trapets' privacy management is governed by the CEO, supported by the DPO function consisting of the Data Protection Officer and CISO, as described below.

Data Protection Officer

- External contact person registered with Integritetsskyddsmyndigheten (IMY)
- Overall responsibility for privacy related policies, templates and related documentation.
- Monitor GDPR and other relevant data protection legislation for relevant changes/updates
- Review and approve/negotiate non-standard DPA's
- Support procurement process for supplier/sub-processor evaluation and contract review from a privacy perspective
- Help answer GDPR related questions and requests from Trapets' customers and employees
- Internal communication, training and awareness
- Point of contact for personal data incident process

Chief Information Security Officer (CISO)

- Coordinate privacy requirements and needs with general InfoSec/ISO requirements.

Each business function and manager is responsible to ensure compliance with defined privacy and data protection policies and practices.

Each employee, including managers, is responsible to follow all issued privacy data protection and/or information security policies or instructions, and to participate in required training.

5. Scope and legal grounds of processing

Trapets customers (or their end customers) are controllers of their personal data and utilize Trapets' services primarily for compliance with legal obligations they are subject to within prevention and detection of financial crime, within the areas of anti-money laundering and terrorism financing, market abuse and/or fraud. In relation to our customers Trapets is a processor of personal data. In this capacity, Trapets will only process personal data for the purpose of delivering our services and fulfilling our obligations under the relevant agreement, including data processing agreement, with each customer, as described in this policy.

It is each controller's responsibility to ensure there is a valid legal ground for 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. Prior to engaging Trapets as processor, the controller shall ensure that the processing by Trapets, including the technical and organizational measures described by Trapets in this policy

and other relevant documentation, fulfils the controller's requirements and comply with legal or other requirements on the controller.

Each Customer is at all times responsible to ensure it complies all applicable laws and regulations, including relevant data protection legislation, in its use of Trapets services. This includes but is not limited to Trapets Screening, Trapets KYC and Screening Data, where each Customer is responsible for obtaining all applicable permits, licenses and approvals that may be required for screening and for using and processing any Screening Data.

6. 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").

Lawfulness, fairness and transparency

Trapets as a processor does not determine the scope or purposes for the processing we perform for its customers as controllers.

Purpose limitation

All personal data processed by Trapets as processor for our customers is processed in accordance with the agreement, including Data Processing Agreement and applicable instructions, with each customer.

Data minimisation

Trapets 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. The data or categories of data that are finally processed for each customer are defined by the customer.

Accuracy

The Controller should take necessary steps to ensure that the information and Personal Data sent to Trapets is correct and up to date.

Trapets provides KYC Screening Data "as is", it is therefore incumbent on the Customer to check that the KYC Screening Data is of high enough quality for its use of the Customer.

Storage limitation

Depending on the product, Trapets offers a standard configuration and/or the possibility for each Controller to define customized deletion routines or to request deletion on an ad hoc basis in accordance with the Controllers' internal retention policies.

Integrity and confidentiality

Trapets uses a data classification system that ensures integrity and confidentiality. All personal data processed by Trapets as a Processor is subject to the highest level of security and access is restricted to employees with a need for such access for the performance of Trapets' services. All Trapets employees are bound by confidentiality undertaking

7. Data Processing Agreement

The agreement between Trapets and its customers shall include a data processing agreement that covers 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 Trapets. Unless otherwise agreed, the data processing agreement will be in the form provided by Trapets.

8. Categories of Personal Data

In the course of service delivery for its customers, Trapets will process personal data of the following categories of data subjects.

- Transaction Monitoring, Fraud: end customers and transaction counterparties
- Customer Due Diligence: end customers (incl. prospects)
- Screening, Trapets KYC and Trapets Real Estate: end customers (incl. prospects) and counterparties (as applicable)
- Persons listed on Screening Lists (Screening Data)
- Users in the InstantWatch platform
- Beneficial owners and representatives with connection to end customers
- Market & Trade Surveillance: end customers and trading participants in

A categorization of each data field has been made if it contains personal data or not in the indata specification for the data being processed.

The detailed indata specifications for each product are found on Trapets documentation site: https://devportal.instantwatch.net/.

If the Data Controller has another interpretation than Trapets regarding categorization of personal data for one or more data fields, the alternative categorization shall be included in the applicable data processing agreement or otherwise documented.

Should the Controller or its Users add or upload any other personal data belonging to a special category of personal data, or otherwise deemed sensitive, into any solution hosted or managed by

Trapets, Trapets will not assume any liability for the processing of such personal data outside of its general obligations of security.

9. Privacy by Design

Trapets applies conventional and proofed security measures and applies other privacy enhancing techniques based on their state of the art and maturity. Trapets implements privacy by design through active involvement of those involved in the design and early phases of development and implementation of new product or system functionalities.

10. Receipt of Personal Data

Trapets may receive personal data from the customer (controller), directly from the customer's end customer or its representative (data subject) or from a third party.

With the exception of Screening Data received from a public source or third-party vendor engaged by Trapets, Trapets 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.

11. Records of processing

Trapets maintains records of processing activities carried out on behalf of its customers. Such records include information regarding the name and contact details of the Trapets 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 Trapets.

12. Use of Sub-Processors

Trapets 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 Trapets customer, that sub-contractor is also a processor (sub-processor).

Under Data Processing Agreements in place with controllers, Trapets must not engage other sub-processors than the ones listed in the Data Processing Agreement to perform all or part of the processing of personal data, as defined in Section 8 above, unless the Controller has given its prior general or specific approval.

Prior to engaging a sub-processor, Trapets will evaluate such sub-processor to secure sufficient guarantees to implement appropriate technical and organisational measures for the processing to meet applicable requirement, and enter into 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 Trapets and the sub-processor.

Upon request, Trapets will also 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.

13. Transfers of data to third countries

Unless otherwise agreed in writing Trapets will only store and process personal data processed by Trapets as processor within the EU/EEA area.

14. Data subject rights and other controller obligations

Data subject requests

A request by a data subject concerning right for access, rectification (correction), erasure or data portability shall be directed to the relevant controller. Where Trapets is a processor for its customer (controller), Trapets will not respond to requests directly from a data subject. Instead, in case a data subject directs a request to Trapets, Trapets will refer the data subject to the relevant customer.

Upon request by the customer and depending on the nature of service delivery by Trapets to our customer, Trapets will assist the customer (controller) to respond to requests from that controller's data subjects. It is the responsibility of the controller to determine the legality of the data subject's request. Any assistance by Trapets outside the scope of the services agreed under the relevant customer agreement will be charged by Trapets at the then current rate applied by Trapets.

Other assistance

Upon request by a customer, Trapets will upon reasonable notice and to a reasonable extent considering the nature of the processing by Trapets, 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 Trapets outside the scope of the services specified and agreed under the relevant customer agreement will be charged by Trapets at the then current rate applied by Trapets.

Audit requests

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

Privacy Impact Assessments

In addition to its general risk management framework, Trapets conducts privacy impact assessments for our services, in order to secure that privacy risks are identified and mitigated as needed and in order to provide information required by our customers in their assessment. Risks identified within a privacy impact assessment are fed into Trapets' general risk management process.

15. Security measures

Trapets has technical and organizational measures in place, including but not limited to information security policies and regular training in secure handling of personal data. Trapets is certified according to ISO 27001 Standard in Information Security Management, which confirms Trapets ability to uphold a high level of information safety and security. More information can be found in Trapets' Information Security Policy and other documentation made available by Trapets.

16. Training

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

17. Personal Data Breach

When Trapets becomes aware of a Personal Data Breach affecting personal data processed by Trapets in our capacity as processor, Trapets shall notify the affected controller(s) without undue delay. Trapets' 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 Trapets who can provide additional information, and a description of the measures taken by Trapets to address the personal data breach and to mitigate its consequences.

18. Information requests

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

a) Log all requests for disclosure of information
b) Verify the identity of the entity and person making the request
c) Verify that the demand follows a valid legal process, e.g. it must be accompanied by a written warrant, court order or likewise for disclosing personal data for a specific data subject (or data subjects).
d) Trapets will attempt to redirect the request to the controller
e) Unless prohibited by law, Trapets will inform the relevant data controller of the request

f) If legally obligated to disclose personal data, Trapets will aim to limit the scope of the personal data disclosed
g) Trapets 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) Trapets might challenge a government request for information if the request is contrary to Trapets principles for disclosing information, Trapets believe that the request is beyond the jurisdiction, of the requesting government or agency, or the demand is not signed or appropriately authorized, includes errors, or is overly broad, the information requested seems to be excessive and out of scope for the purpose of the request.
i) Trapets 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.

To approve a disclosure, the following applies:

a) A request or demand for disclosure of information, outside of an agreement, is always reviewed by Trapets Chief Legal Officer.
b) Decisions on the disclosure of information at the request from a public authority, can only be authorized by the Trapets CEO.
c) Decisions on the disclosure of any Customer Data, at the request from a commercial third party, can only be authorized by the Customer or the Data Subject.

19. Use of extracted anonymized data

Always subject to agreed terms and conditions on data usage in the relevant customer agreement, Trapets may use anonymized data extracted from Customer Data, in connection with development and testing of Trapets' systems and services, discussions and demonstrations with existing and potential customers, and in algorithms for monitoring and other functionality that may be shared with other users of Trapets' services and products. For such extracted data, it will not be possible to trace it to any end customer or any other individual or entity connected to a certain Customer or to any Customer. The extracted data is no longer Customer Data or personal data.

The conditions for Trapets' use of data extracted from Customer Data is that it is distorted (anonymized), including some or all of the measures below:

a) All personal data is deleted or distorted so it cannot be recovered and cannot in any way be linked to an individual or legal entity.
b) All customer identifiers and account numbers are distorted so it is not possible to derive from it the original customer identifier or account number.
c) Unique names or codes entered by the Customer e.g. transaction types, customer types, account types and agreement types etc. that make it possible to associate these to a particular Customer are replaced so this is not possible.
d) Transaction dates are changed.
e) Any text field containing text entered manually are removed.

Trapets is a software company that provides products and solutions for financial crime prevention, including Anti-Money Laundering (AML), Know Your Customer (KYC), and Market Surveillance.

Founded in 2000, Trapets has helped organizations meet regulatory needs for business success and fight financial crime for decades. We are trusted by over 500 companies ranging from small financial institutions to regulatory entities and earned recognition as one of the top 100 RegTech companies globally.

Trapets has more than 80 employees based in Stockholm, Hanoi, and London.

For more information, please visit www.trapets.com.