Contract for the processing of data
- data processing on behalf in accordance with Article 28 GDPR -

between

Company or person who has created a user account on the TAWNY platform in accordance with the terms of use or who has concluded a subscription for the Tawny platform or who is in a contractual relationship with TAWNY GmbH regulated by another contract ("Main Contract").

Controller - hereinafter

referred to as the Client

and

Tawny GmbH
Schellingstraße 45
D-80799 München

Processor - hereinafter

referred to as the Contractor -

Content

1 Preamble

In providing the services in accordance with the Terms of Use or Main Contract Terms, the Platform Operator processes personal data ("User Content") provided by the Controller for the purpose of providing the services.

This Contract establishes the data protection obligations of the contractual parties, arising from the concluded contract and the processing on behalf in the sense of Art. 28 GDPR as described in detail in the Terms of Use or Main Contract. It applies to all work connected with the contract and for which the Contractor's employees or third parties commissioned by the Contractor can come into contact with the Client's personal data.

Within the context of IT system maintenance, it cannot be ruled out that the Contractor will be able to view personal data. Although in this context the Contractor is not carrying out any data processing, because it may be possible to view personal data, a data protection agreement must be concluded which fulfils the regulations for processing agreements in accordance with Article 28 GDPR.

2 General

(1) The Contractor processes personal data on behalf of the Client in accordance with Article 4(8) and Article 28 of Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). This Contract regulates the rights and obligations of the parties in relation to the processing of personal data.

(2) Where the terms 'data processing' or 'processing' (of data) are used in this Contract, the definition of 'processing' is based on Article 4(2) GDPR.

3 Object of the Contract

The object of processing, i.e. the nature and scope of processing, the types of personal data and the categories of data subject are laid out in **Annex 1** of this contract.

4 Duration of the Contract

(1) The Contract begins with the contract concluded in accordance with the Terms of Use or Main Contact and is concluded for an indefinite period.

(2) The Contract ends automatically at the time of the deletion of the user account or with the termination of the main contract.

(3) If the Contractor is in serious breach of the applicable data protection laws or in breach of obligations arising from this Contract, or if, in violation of the Contract, the Contractor cannot or does not wish to carry out an instruction issued by the Client, or if the Contractor denies access to the Client or the competent supervisory authorities, the Client can terminate the Contract at any time and without notice.

5 Provision of services

The contractually agreed data processing shall only take place in a Member State of the European Union or in another signatory to the Agreement on the European Economic Area. All processing in a third state

requires the Client's prior consent and may only be carried out if the special requirements of Article 44 et seqq. GDPR are met.

The adequate level of data protection at Google in Ireland (EU)* is established by EU-standard contractual clauses (Art. 46 para. 2 lit. c and d GDPR).

* The sub-processor Google processes the data within the EU, implements the regulations of the EU standard contractual clauses and provides additional guarantees to comply with European data protection law.
According to the case law of the ECJ (judgment of 16.07.2020, ref.: C-311/18 ("Schrems II")), there is no adequate level of data protection for US companies. In particular, there is a risk that personal data may be processed by US authorities, despite being stored and processed within the EU, for control and for monitoring purposes, possibly also without redress.

6 Technical and organisational measures

The measures to be taken are measures relating to data security and to guarantee a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and capacity of systems. In doing this the state of the art, implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons must be considered (Article 32(1) GDPR)

(1) The Contractor guarantees the Client that he will comply with the following technical and organisational measures which are necessary in order to comply with the applicable data protection regulations. These comprise especially provisions on the security of processing from Article 28 (3)(c), and Article 32 GDPR and particularly in relation to Article 5(1) and (2) GDPR.

(2) The Contractor appends to this in Annex 4 an assessment of the state of technical and organisational measures at the point of concluding the Contract, with particular relation to the concrete implementation of processing prior to commencement. If the inspection/an audit by the Client results in a need for adjustment, this must be implemented by mutual agreement.

(3) The technical and organisational measures are subject to technical progress and development. In this respect, the Contractor is permitted to implement adequate alternative measures. The security level of the measures established may not be compromised in the process.

The parties are agreed that in order to adjust to technical and legal developments, changes to the technical and organisational measures could be necessary. The Contractor will agree any fundamental changes that could affect the integrity, confidentiality or availability of personal data in advance with the Client. Measures that only result in slight technical or organisational changes and do not negatively affect the integrity, confidentiality and availability of the personal data can be implemented by the Contractor without agreement from the Client. At any time, the Client can request from the Contractor an up-to-date version of the technical and organisational measures implemented.

(4) The Contractor shall regularly review the technical and organisational measures it has implemented, also with regard to their effectiveness.

7 Rights and obligations of the Client

(1) The Client is the controller in the sense of Article 4(7) GDPR), responsible for the processing of data on its behalf by the Contractor.

(2) In the event of an obligation to provide information to third parties in accordance with Articles 33 and 34 GDPR, or where the Client is subject to another legal reporting obligation, the Client is responsible for complying with this.

(3) As controller, the Client is responsible for protecting data subjects' rights.

(4) The Client nominates the Contractor as a contact partner for any date protection queries that arise within the scope of the contract.

(5) The Client shall inform the Contractor immediately and fully if the Client has noticed that the Contractor has made errors or irregularities in connection with the processing and the use of personal data.

7.1 Authority of the Client

The Contractor may only process data of data subjects within the scope of the order and the Client's instructions, except in exceptional cases in the sense of Article 28(3)(a) GDPR.

(1) The Client has the right to issue the Contractor with instructions about the nature, scope, and procedural form of the data processing at any time. Instructions can be made in text form (e.g. by email).

(2) Regulations about any possible remuneration of additional costs, which arise through additional instructions of the Client to the Contractor, shall remain unaffected.

(3) The Client shall confirm oral instructions immediately in text form.

(4) The Client can appoint persons authorised to issue instructions. Where authorised persons are nominated, this is to be documented in text form. In the event of changes to the authorised persons nominated by the Client, the Client shall communicate this to the Contractor in text form.

7.2 Client control rights

(1) The Client has the right - in relation to the processing of personal data of the principal -to inspect the Contractor's compliance with the legislation on data protection and/or compliance with the regulations contractually agreed between the parties and/or compliance with the instructions issued by the Client at any time and to the extent necessary.

(2) The Contractor shall ensure that the Client is able to establish that the Contractor is complying with its obligations according to Article 28 GDPR. The Contractor shall guarantee the Client the necessary information when requested, insofar as this is required so as to implement inspections in accordance with Paragraph 1.

(3) The Client may request to inspect the data which has been processed by the Contractor for the Client as well as the data processing systems and programs used, to the extent that these concern the platform account or the platform projects of the client and the data protection for other clients using the TAWNY platform is preserved.

(4) The Client has the right to carry out checks in consultation with the Contractor, or to have them carried out by auditors which have no competitive relationship with the contractor to be appointed in the individual case. The Client has the right to check the Contractor's compliance with this agreement in the course of its business by means of spot checks, which should usually be announced in good time and carried out during the Contractor's regular office hours.

(5) In order to verify compliance with contractual obligations, the Contractor can provide the Client with the following evidence, not always relating to the specific order:

- current audit opinions, reports or report excerpts from independent authorities (e.g. auditors, reviewers, data protection officers, IT security department, data protection auditors, quality auditors)
- results of a self-audit
- internal company codes of conduct including external proof of compliance
- compliance with approved codes of conduct as per Article 40 GDPR
- certification according to an approved certification procedure as per Article 42 GDPR
- an appropriate certification from an IT security or data protection audit (e.g. according to BSI basic protection, ISO 27001)

(6) In the event that a supervisory authority acts against the Client in the sense of Article 58 GDPR, the Contractor is obliged to provide the necessary information to the Client, particularly in respect of information and monitoring obligations, and to allow the relevant supervisory authority to carry out an inspection on site. The Client shall inform the Contractor of planned action accordingly.

8 Rights and obligations of the Contractor

The Contractor has the right to inform the Client if it believes that an object of the order and or/any instruction constitutes unlawful data processing.

8.1 General obligations

(1) The Contractor shall process personal data exclusively within the scope of the agreements and/or in compliance with any additional instructions communicated by the Client. Excluded from this are legal regulations which may oblige the Contractor process the data in a different manner. In such an event, the Contractor shall inform the Client of these legal requirements prior to the processing, unless the law in question prohibits such communication because of a significant public interest.

(2) In addition to complying with the provisions of this order, the Contractor also has legal duties according to GDPR; as such, it guarantees in particular compliance with the following provisions.

8.2 Data protection officer of the Contractor

(1) The Contractor confirms that he has nominated a data protection officer in accordance with Article 37 GDPR and/or in the case of German companies in accordance with Section 38 BDSG 2018 [German Federal Data Protection Act].

(2) The Contractor bears the responsibility for ensuring that the data protection officer has the necessary qualifications and knowledge of the area. The Contractor shall communicate to the Client the contact details for its data protection officer in **Annex 3**.

(3) The Client must be informed promptly in text form of any change of data protection officer.

(4) The obligation to confirm a data protection officer can be deemed unnecessary by the Client if the Contractor can prove that he is not legally obliged to appoint a data protection officer and operational regulations exist that ensure the processing of personal data complies with legal provisions, the regulations of this Contract as well as any further instructions from the Client.

(5) If the Contractor is located outside of the EU, he shall nominate in text form a representative in the EU in accordance with Article 27(1) GDPR.

8.3 Non-disclosure obligation

(1) When processing data, the Contractor is obliged to protect the confidentiality of all personal data received in connection with the order, as well as any other data of which he gains knowledge.

(2) The Contractor shall ensure that it is aware of the applicable provisions under data protection law and familiar with their application. In order to protect confidentiality in accordance with Articles 28(3)(b), 32(4) GDPR, when carrying out the work, the Contractor shall only engage employees who are obliged to protect confidentiality when processing personal data and have been made aware of the relevant data protection provisions as they pertain to them.

(3) Upon request, proof of this obligation shall be provided to the Client in accordance with Paragraph 2.

8.4 Binding instructions

(1) The Contractor and all persons subordinate to the Contractor who have access to personal data may only process this data in accordance with Articles 29 and 32(4) GDPR, exclusively according to the instructions of the Client as per the authorisations granted in this agreement, unless they are legally obliged to process it.

(2) The Contractor may not correct, block or delete the data which are being processed on the Client's behalf on its own initiative, but rather only according to a documented instruction from the Client. If a data subject directly contacts the Contractor with regard to this, the Contractor shall forward this request to the Client immediately.

(3) The Contractor must inform the Client immediately if he believes that an instruction breaches data protection provisions. The Contractor is entitled to defer the execution of an instruction until it has been confirmed or amended by the Client.

(4) The Contractor may inform the Client of the person(s) authorised to receive instructions from the Client. Where persons authorised are named, this is to be documented in text form.
In the event of changes to the authorised persons named by the Contractor, the Contractor shall communicate this to the Client in written or text form.

8.5 Reporting obligations of the Contractor

(1) The Contractor is obliged to inform the Client immediately of any breach of data protection provisions, contractual agreements and/or instructions from the Client that occurs during processing of personal data of the Client by the Contractor or other persons involved in processing. The same applies to any infringement on the protection of personal data processed by the Contractor on behalf of the Client.

(2) In addition, the Contractor shall inform the Client immediately should a supervisory authority begin audit procedures and measures in relation to the Contractor, in the event that this also includes an audit of processing of Clients personal data undertaken by the Contractor on behalf of the Client (in accordance with Article 58 GDPR).

This also applies if a responsible authority captures personal data in the course of administrative offence or criminal proceedings in relation to processing by the Contractor while processing the order.

(3) The Contractor is aware that it may be subject to a reporting obligation in accordance with Articles 33 and 34 GDPR, which requires a report to be sent to the supervisory authority within 72 hours of being made known. The Contractor shall assist the Client in fulfilling its reporting obligations. The Contractor shall inform the Client immediately of any unauthorised access to personal data being processed on behalf of the Client, and at the latest within 48 hours of becoming aware of the access. The Contractor's report to the Client must contain the following information in particular:

- a description of the type of breach in protection of personal data, if possible specifying the categories and the approximate number of data subjects, the categories in question and the approximate number of personal data sets affected
- a description of the measures taken or suggested by the Contractor to remedy the breach in protection of personal data and, if necessary, measures to mitigate any possible adverse effects of this

8.6 Contractor's obligation to cooperate

(1) The Contractor shall support the Client to a reasonable extent and only to the extent that is acceptable to the Contractor in complying with the obligations named in Articles 32 to 36 of the GDPR on the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. These include

- ensuring an appropriate level of protection through technical and organisational measures which consider the circumstances and purposes of processing as well as the predicted likelihood and gravity of a possible infringement by security vulnerabilities and facilitate immediate identification of relevant breach incidents
- supporting the Client in data protection impact assessments and/or supporting the Client within the scope of prior consultations with the supervisory authority

(2) The Client and the Contractor shall cooperate on request with the supervisory authority when carrying out their tasks.

(3) If the Client for its part is subject to control by the supervisory authority, administrative offence or criminal proceedings, a liability claim from a data subject or third party or another claim in connection with order processing by the Contractor, the Contractor must provide support to the best of its ability.

(4) The Contractor shall regularly check its internal processes as well as technical and organisational measures in order to guarantee that the processing within its remit occurs in accordance with the requirements of the applicable data protection legislation and that the protection of data subject rights is ensured.

(5) The Contractor shall support the Client to a reasonable extent and only to the extent that is acceptable to the Contractor in its obligation in accordance with Articles 12-23 GDPR to provide

information to the data subject and to process requests for exercising data subject rights, and will in this connection provide the Client with all relevant information promptly. The provisions in **clause 8.7** this Contract apply.

(6) The Contractor shall collaborate in drawing up lists of processing activities undertaken by the Client upon request of the Client. The Contractor shall provide the details necessary for this in an appropriate manner.

8.7 Protection of data subject rights

(1) The Client alone is responsible for protecting data subject rights. The Contractor is obliged to support the Client to a reasonable extent and only to the extent that is acceptable to the Contractor in its obligation to process data subject requests in accordance with Articles 12-23 GDPR. In this context, the Contractor bears particular responsibility for ensuring that any necessary information is shared with the Client promptly, so that the Contractor can comply with his obligations arising from Article 12(3) GDPR.

(2) To the extent that the Contractor is required to assist the Client in the safeguarding of the rights of the data subjects, especially in relation to information, corrections, blocking or erasure, the Contractor shall take the measures necessary in each case, as instructed by the Client. Where feasible, the Contractor shall support the Client with appropriate technical and organisation measures, so that the Client can comply with its obligation to respond to requests from those seeking to exercise their rights as data subjects.

(3) Regulations about any possible remuneration of additional costs, which arise for the Contractor through participatory services in connection with the exercise of data subject rights relating to the Client, shall remain unaffected.

9 Subcontracting relationships

(1) Subcontracting relationships in the sense of this provision include services which relate directly to the provision of the main service. Services that the Contractor makes use of from third parties as a simple supplementary service in order to exercise its business activity are not to be considered subcontracting relationships. These include for example cleaning services, simple telecommunication services without a specific link to services that the Contractor performs for the Client, post and courier services, transport services, guard services.

The Contractor is, however, obliged to guarantee the protection and security of the Client's data in connection with outsourced supplementary services by adopting appropriate, legally compliant contractual agreements as well as control measures to guarantee the protection of personal data.

(2) The maintenance and upkeep of the IT system or applications constitutes a subcontracting relationship and also processing on behalf requiring agreement in the sense of Article 28 GDPR, if it relates to the maintenance and inspection of IT systems which are being used as part of a service provision for the Client, and, if in maintaining the system personal data can be accessed which is being processed as part of the Client's order.

(3) The Contractor must select the subcontractors carefully and, before commissioning them, check that they are able to comply with the agreements made between the Client and the Contractor. In particular, the Contractor must check in advance and at regular intervals for the duration of the contract that the

subcontractor has taken the technical and organisational measures required in accordance with Section 32 GDPR to protect personal data. The outcome of the inspection must be documented by the Contractor and a copy is to be forwarded to the Client upon request.

(4) The Client agrees to the commissioning of the subcontractors listed in Annex 2, under the condition of a contractual agreement according to Article 28 Paragraphs 2-4 GDPR.

Outsourcing to further subcontractors or changes to existing subcontractors are permitted, if

- the Contractor informs the Client in writing or text form of such outsourcing to subcontractors in good time beforehand and
- the Client does not object in writing or text form to the planned outsourcing before the handover of the data to the Contractor and
- a contractual agreement according to Article 28 Paragraphs 2-4 GDPR is used as a basis.

(5) The Client's personal data may only be forwarded to the subcontractor and the latter may only start work once all requirements for subcontracting have been met.

(6) Further outsourcing by the subcontractor requires the express consent of the Client in text form.

(7) All contractual regulations in the contractual chain must also be imposed on additional subcontractors.

(8) If the subcontractor provides the agreed service outside the EU/the EEA, the Contractor must take appropriate measures to ensure the permissibility of its actions under data protection law, in accordance with Chapter V GDPR.

10 Termination/erasure and return of data

(1) After completion of the contractually agreed work, or earlier at the Client's request - at the latest on termination of the Service Agreement - the Contractor must on the decision of the Client either hand over to the Client all documents which have entered its possession, processing and usage results it has produced and data files connected to the order relationship, or destroy them in accordance with data protection law according to prior agreement. The same applies to test and sample material. Erasure is to be documented appropriately, with a report of the erasure to be provided upon request.

Data carriers must be destroyed if the Client requests their erasure and at a minimum this should comply with security level 3, DIN 66399; proof of the erasure must be provided to the Client in accordance with DIN 66399.

(2) Copies or duplicates of the data shall not be produced without the Client's knowledge. This excludes backups, if they are necessary to guarantee proper data processing, as well as data that is necessary to comply with the legal obligations to retain records or other obligations relating to the storage of data.

(3) Documentation which serves as evidence of contractual and proper data processing is to be retained by the Contractor in accordance with the respective retention periods beyond the end of the Contract. The Contractor may hand them over to the Client at the end of the Contract to discharge this duty.

(4) The Client has the right to check that the Contractor has returned all of the data or completely erased it. This can also take place by inspecting the data processing systems at the Contractor's operating sites.

The Client must provide appropriate notice of at least two weeks before performing an on-site inspection.

10.1 Right of retention

The parties agree that the defence of right of retention by the Contractor (in accordance with Section 273 BGB [German Civil Code]) cannot be made where it relates to processed data and the corresponding data carriers.

11 Liability and compensation

(1) The Client and Contractor shall otherwise be liable to the data subjects according to the regulation made in Article 82 GDPR.

(2) The limitations of liability agreed in the main contract apply to the internal relationship between the Client and the Contractor.

(3) Furthermore, it is agreed that the client shall indemnify the contractor from liability if he proves that he is in no way responsible for the circumstance by which the damage occurred to a data subject.

12 Confidentiality obligations

(1) Both parties undertake to indefinitely treat all information which they obtain in connection with executing this contract as confidential and to use it only to execute the contract. Neither of the parties may use this information, in full or in part, for purposes other than those just mentioned or disclose this information to third parties.

(2) The above obligation does not apply to information if it can be proven that one of the parties has obtained this information from a third party where there is no obligation to maintain confidentiality or if this information is public knowledge.

13 Final provisions

(1) Should the Client's data in the Contractor's possession be endangered by seizure or confiscation, by insolvency or settlement proceedings or by other events or actions of third parties, the Contractor shall immediately inform the Client. The Contractor shall immediately inform all those responsible in this respect that the sovereignty over and ownership of the data exclusively belongs to the Client as the 'controller' within the meaning of the GDPR.

(2) Amendments and additions to this Annex and all of its components - including any guarantees of the Contractor- require a written agreement which shall expressly indicate that it involves a change or addition to this Contract. This also applies for the waiver of this formal requirement.

(3) In the case of any objections, the provisions of this arrangement relating to data protection will take precedence over those in the main contract. Should individual parts of this Annex be invalid, this will not affect the validity of the remaining provisions.

Place, date _____ Munich, date _____

- Client - - Contractor -

Annex 1 - Definition of content

(1) Nature and purpose of the processing

The nature and purpose of the processing of personal data by the Contractor for the Client are:

- Provision, operation and maintenance of a platform for the analysis of images, videos, audio data or physiological data with regard to the content contained therein, in particular the emotions and behaviour shown by the persons recorded.

(2) Type(s) of personal data

The types/categories of data for the processing of personal data by the Contractor for the Client are:

- Emotion analysis
  - Pictures, videos, audio recordings and physiological data of subjects
  - Pseudonymised name of proband (if applicable, also name)
  - Evaluation data, Analysis data/-results
- Protocols
  - Platform user interface
  - Platform API
- User account data
  - Name
  - Email address
  - Password (encrypted)
  - Company
  - Field of activity

(3) Categories of data subject

The categories of data subjects are:

- Test subjects
  - Persons recruited by the user by consent to participate
  - Persons for whom the user has a verifiable right to use the video.
- Platform users

Annex 2 - Approved subcontractors

Subcontractor	Address/Country	Web-Address	Service
Hetzner Online AG	Stuttgarter Str. 1 91710 Gunzenhausen Germany	https://www.hetzner.com/de/	Provision of computing services (hosting, data processing, storage)
Google Ireland Limited	Gordon House, Barrow Street Dublin 4 Ireland	https://cloud.google.com/gcp/?hl=de	Provision of computing services (hosting, data processing, storage)
Hyve AG	Schellingstr. 45 80799 München Germany	https://www.hyve.net	Provision of computing services (hosting, data processing, storage)

Annex 3 – Contractor data protection officer

Contractor data protection officer

First name, last name	Dr. Eddie Kohfeldt
Email address	datenschutz@tawny.ai
Telephone	+49 8133 9179310

Annex 4 - Technical and organisational measures

Technical and organisational measures for data security

For the TAWNY platform, the following technical and organisational measures (TOM) for data security within the meaning of Art. 32 GDPR have been taken. The protective measures for data processing in customer projects via the TAWNY platform are applied in addition to those for the internal IT infrastructure. They apply to all activities in which TAWNY employees or commissioned third parties (subprocessors) process personal or sensitive data of the client.

Technical basis:

The services provided by TAWNY are delivered via two data centre infrastructures:

Google Cloud Platform

Some of the services provided by TAWNY are geo-hosted within the EU on the Google Cloud Platform (GCP). The operator is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (hereinafter "Google").

The GCP data centre and network architecture meets very high requirements that are necessary for the secure operation of TAWNY: This ensures confidentiality, integrity, availability and resilience as well as rapid recoverability. The GCP is certified according to ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 1-3, PCI DSS and CSA STAR, among others. These are internationally recognised standards for IT operations and information and data security.

Hetzner Online AG

Part of the services provided by TAWNY is hosted in a secure data centre within Germany (Nuremberg, Falkenstein). The operator is Hetzner Online AG, Stuttgarter Str. 1, 91710 Gunzenhausen (hereinafter "Hetzner").

Hetzner Online is certified according to DIN ISO/IEC 27001. The internationally recognised standard for information security certifies that Hetzner Online GmbH and Hetzner Finland Oy have implemented a suitable information security management system, ISMS for short. The ISMS is applied at the Nuremberg and Falkenstein locations as well as Helsinki under the scope "The scope of the information security management system includes the infrastructure, operation and customer support of the data centres". The corresponding certification procedure was carried out by FOX Certification GmbH.

The certificate proves adequate security management, the security of data, the confidentiality of information and the availability of IT systems. It also confirms that the security standards are continuously improved and sustainably controlled.

1. Pseudonymisation

Pseudonymisation is not currently applied. The application of pseudonymisation procedures is the responsibility of the client.

2. Confidentiality

Access control - No unauthorised access to data processing facilities

The physical security of the respective data centre is provided by the operators Google and Hetzner.

Access control - No unauthorised system use

Control of access to data processing facilities with client projects is ensured by the following measures.

Technical measures:

- Access to the TAWNY platform is only possible with a password-protected user account.
- Access to the administration tools of the backend systems is only possible via administrator accounts specially secured with 2-factor authentication.
- Access to the underlying server infrastructure is only possible via SSH with public/private key authentication (with additionally encrypted keys via passphrase).
- The logging of access to the systems of Google and Hetzner takes place via the logging functions of the respective provider.
- Logging of access to Linux servers is done via the local syslog.

Organisational measures:

- The creation of a user account on the TAWNY platform requires the validation of the email address used.
- Administrator rights are reserved for a few core developers of the contractor
- The number of these administrators is kept as small as possible.
- The administrators are specially instructed on how to handle these access options and are of course obliged to maintain confidentiality.

Access control - no unauthorised reading, copying, modification or removal within the system

Controlled access to personal data according to the "need-to-know" principle is ensured by the following measures:

Technical measures:

- Access to a project on the TAWNY platform (and the data it contains) is only possible with a password-protected user account, which must have the appropriate permissions. The enforcement of these rules is ensured via the mechanisms of the underlying databases and storage servers.
- Access to the client's data directly via the administration tools of the backend systems is only possible via administrator accounts specially secured with 2-factor authentication.
- Access to the client's data directly via the underlying server infrastructure is only possible via SSH with public/private key authentication.

Organisational measures:

- The basic organisational unit for client data on the TAWNY platform is a "platform project". The client can create any number of such projects and define the subsequent measures individually per project.
- Managing access rights to a platform project and the data it contains is the responsibility of the project owner, i.e. the client.
- In the basic state, only the project owner himself has access to the project with his user account.
- The project owner can explicitly grant other user accounts access to a project (and thus the data contained therein) and also revoke it again.
- TAWNY employees who may be given access to the project for support purposes must also be explicitly given clearance for the project by the project owner via the same mechanism.
- In principle, it is possible to access the client's data via the backend systems and the server infrastructure by circumventing the rules described above. However, the administrator rights required for this are reserved for a few core developers of the contractor, whose accounts are specially secured with 2-factor authentication and/or public/private key authentication (with additionally encrypted keys via passphrase).
- The number of these administrators is kept as small as possible.
- The administrators are specially instructed on how to deal with these access options and are, of course, obliged to maintain confidentiality.

Transfer control

The confidentiality of personal data during electronic transmission or during its transport is ensured by the following measures:

Technical measures

- The electronic transmission of data is exclusively encrypted according to the state of the art (SSL, SSH, etc.).

Organisational measures

- The transport of data on physical data carriers (USB stick, external hard drive, etc.) is only permitted in exceptional cases.
- When transporting data on physical data carriers (USB stick, external hard drives), the data is always encrypted.

3. Integrity

Measures to ensure the integrity of the systems and services related to the processing on a permanent basis.

Technical measures:

- Changing data in a platform project is only possible with a password-protected user account that must have the appropriate permissions.
- Essential activities within platform projects are automatically logged (incl. type of action, time stamp and executing user).
- Changing the client's data directly via the administration tools of the backend systems is only possible via administrator accounts specially secured with 2-factor authentication.
- The modification of the client's data directly via the underlying server infrastructure is only possible via SSH with public/private key authentication.

Organisational measures:

- Administrator rights are reserved for a few core developers of the contractor, whose accounts are specially secured with 2-factor authentication and/or public/private key authentication (with additionally encrypted keys via passphrase).
- The circle of these administrators is kept as small as possible.
- Administrators log any changes to the principal's data that have been made via administrator access rights.
- Automated changes to the client's data (e.g. as part of rolling out a new platform software version) are tested beforehand on test and staging environments to check that the integrity of the data is maintained.

4. Availability and resilience

Measures to ensure the availability and resilience of the systems and services related to the processing on a permanent basis

Technical measures:

- The data centres used meet international standards (e.g. ISO/IEC 27001, for others see listing above).
- The TAWNY platform data is stored in multi-region buckets geo-redundantly across the European Union.
- The TAWNY platform uses the possibilities of automatic scaling of resources in the data centres to maintain availability even during peak loads.
- The TAWNY platform is operated on virtualised systems in order to be as independent as possible from underlying hardware / hardware faults.
- Backups are automated and created regularly.

Organisational measures:

- Response times in the event of faults are based on the working hours of the TAWNY platform support team (Mon-Fri 9am-6pm) and the availability of Google and Hetzner technical support.

5. Rapid recoverability

Measures to quickly restore the availability of and access to personal data in the event of a physical or technical incident.

Technical measures:

- The databases of the TAWNY platform can be restored automatically from backups.
- The platform software or certain parts of it can be redeployed automatically in a different environment (e.g. new cloud instances).

Organisational measures:

- Process, responsible persons and reporting channels are defined.

6. procedures for regular review, assessment and evaluation

Measures to regularly review, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of processing.

- Regular review of the technical measures and possible improvements to these based on the state of the art as part of the further development of the TAWNY platform.
- Peer review of concepts and implementations of technical measures within the development team.
- Regular evaluation of measures with external data protection officer.

7. List of processing activities for processors (Art. 30 (2) GDPR)

- Directory of processing activities within the meaning of Article 30 (2) of the GDPR is available.
- The processing of personal data in accordance with instructions is carried out at the contractor by means of a service agreement with a clearly defined scope for the type and purpose of the intended processing. This is documented in the contract on commissioned data processing in accordance with Art. 28 GDPR.

Status: 01.08.2021