# Data Processing Agreement

*This Data Processing Agreement applies if you wish to use Vikunja Cloud as a hosted Software as a Service solution and personal data is processed by us in the course of providing the services.*

*By accepting the Terms of Service as a Business Customer, you accept the terms of this Data Processing Agreement pursuant to Article 28 of the GDPR and establish it as the basis for data processing between the parties. For the sake of transparency, this Data Processing Agreement incorporates the Standard Contractual Clauses of the European Commission for data processors in the EU/EEA, which have been adapted but are otherwise unchanged, available under: https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en*

*This Data Processing Agreement can be downloaded for filing and safekeeping.*

## Standard Contractual Clauses

## SECTION I

### Clause 1 – Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

## Clause 2 – Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

## Clause 3 – Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

## Clause 4 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

## Clause 5 – Docking clause - Optional

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

# SECTION II – OBLIGATIONS OF THE PARTIES

## Clause 6 – Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

## Clause 7 – Obligations of the Parties

### 7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

### 7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

### 7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

### 7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**7.5. Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

**7.6 Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

**7.7. Use of sub-processors**

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 4 weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the

engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**7.8. International transfers**

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

## Clause 8 – Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

## Clause 9 – Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 where applicable, taking into account the nature of processing and the information available to the processor.

### 9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

**9.2 Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

# SECTION III – FINAL PROVISIONS

## Clause 10 – Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

# ANNEX I LIST OF PARTIES

**Controller(s):** The customer of the services, which accepts these clauses as part of the agreement.

Name: as stated in the agreement

Address: as stated in the agreement

Contact person's name, position and contact details: as stated in the agreement

Signature and accession date: completed by accepting the Terms of Service

**Processor(s):**

Name: Konrad Langenberg Software

Address: Willy-Brandt-Allee 31A, 23554 Lübeck, Germany

Contact person's name, position and contact details: Konrad Langenberg, support@vikunja.io

Authorized and released by Konrad Langenberg on 9 November 2026

# ANNEX II: DESCRIPTION OF THE PROCESSING

***Categories of data subjects whose personal data is processed:***

Customers, internal and external employees of the customer, and any other individuals whose personal data is provided to the services by the customer.

***Categories of personal data processed:***

Personal Master Data, address details, employment related data, project data, content data provided and uploaded by the Customer.

***Sensitive data processed:***

The services are not intended for the processing of sensitive data.

***Nature of the processing:***

Ongoing transfer, including but not limited to storage, organisation, structuring, adaption or alteration, retrieval, erasure or destruction.

***Purpose(s) for which the personal data is processed on behalf of the controller:***

For the purpose of providing the services to the Customer in accordance with the documented instructions. Vikunja Cloud is a hosted project management solution for freelancers, teams and

businesses.

***Duration of the processing***

For the duration of Customer’s use of the services.

***For processing by (sub-) processors, also specify subject matter, nature and duration of the processing***

See Annex IV

# ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

## 1. Confidentiality of Processing pursuant to Art. 32(1)(b), Variant 1 of the GDPR

### 1.1 Access Control

Access control (formerly known as entry control) refers to measures that prevent unauthorized persons from gaining access to the processing facilities used to carry out the processing.

**Technical Measures**

- Use of alarm systems for intrusion detection, especially outside working hours
- No outside windows in the data center or server room

### 1.2 Data carrier and memory control

Data carrier control refers to measures that prevent the unauthorized reading, copying, modification, or deletion of data carriers. Storage control refers to measures designed to prevent the unauthorized entry, as well as the unauthorized access, modification, and deletion of stored personal data.

**Technical Measures**

- Connection of mobile workstations (e.g. company notebooks, company smartphones) via the Internet via encrypted and cryptographically authenticated connections (e.g. encrypted VPN with authentication using strong passwords and cryptographic client certificates)

- For smartphones and tablets: mobile device management (MDM) solutions for configuring and managing the devices, the installed apps and locating/deleting them in the event of loss
- For mobile data carriers: Secure deletion of data carriers before and after use is ensured
- Use of document shredder (min. security level DIN 66399: P4 with max. 160 mm² per particle and 6 mm strip width or P5 with max. 30 mm² per particle and 2 mm strip width)
- Use of service providers for paper destruction (certified according to DIN 66399 if possible)
- Documentation of the destruction of paper

**Organizational Measures**

- Implemented deletion on development, test and production environments

**Encryption; Art. 32 para. 1 lit. A) Alt. 2 GDPR**

- Use of strong encryption of mobile end devices (smartphones and tablets) and mobile data carriers (e.g. USB sticks, hard disks)
- All encryption technologies used in production are state of the art.
- Strong encryption of data carriers in laptops & clients

### 1.3 User control

User control refers to measures designed to prevent unauthorized persons from using automated processing systems that employ data transmission facilities. This may also include protection against unauthorized system use, as well as against system intrusions and misuse via networks.

**Technical Measures**

- Use of an anti-virus solution or an endpoint protection system on smartphones and tablets
- Checking incoming emails using anti-malware protection
- Wireless access via Wi-Fi is supported only on current Wi-Fi routers with effective access mechanisms
- Using a Wi-Fi guest network without access to the internal network
- Documented update strategy for the operating systems, browsers, and core components in use

- Only software for which security updates are still being released in a timely manner is used.
- We use only operating systems for which the manufacturer still provides security updates.
- No mobile devices are used for which there are no security updates (anymore).
- Automatic installation of security-related updates and patches for client computer operating systems
- Proper Configuration of Software Distribution
- Timely manual installation of security updates on high-risk servers
- A standardized process for deploying security updates for browsers and core components (e.g., Java, PDF readers, remote maintenance software, and critical company software).
- Deployment and Proper Configuration of a Hardware and Software Firewall
- A security policy is in place for the use of printers, copiers, and multifunction devices (e.g., Print-to-Me, Follow-Me Print, with PIN)
- Logging at the network and firewall levels to detect and analyze unauthorized access between networks

### 1.4 Access control

Access control refers to measures designed to ensure that automated processing systems are used exclusively by authorized individuals within the scope of their access permissions, thereby guaranteeing that authorized individuals have access only to data covered by their permissions.

**Technical Measures**

- Login with user name & password
- Use of Biometric Features as a Supplementary Authentication Method
- Access to smartphones and mobile IT devices is permitted only after authentication
- Use of two-factor or multi-factor authentication methods for high-risk processing activities
- Mandatory two-factor or multi-factor authentication for administrator accounts
- Use of Strong Authentication Methods for Critical Systems

- Only strong passwords are used for the admin accounts of the IT systems (e.g., at least 16 characters, complex, and without common words).
- Non-privileged standard accounts, even for administrators, for other work outside of administrative duties.
- Mandatory use of strong passwords in accordance with current security standards (e.g., those set by BSI, NIST, and ENISA)
- Password Managers in Use

**Organizational Measures**

- Centralized Management of User Accounts and User Permissions
- Default authentication credentials provided by software vendors should be changed after installation
- Management of User Rights by the IT Administrator
- Each employee is assigned their own user profile in the domain
- Secure Delivery of Initial Login Credentials
- Measures for Detecting Compromised Passwords
- Blocking and Resetting Passwords in the Event of Security Incidents or Suspected Incidents
- No administrator credentials for users who do not perform administrative tasks.
- Number of IT administrators reduced to a minimum

### 1.5 Separability

Separability refers to measures that ensure that personal data collected for different purposes can be processed separately.

**Technical Measures**

- Implementation of client separation through separation at system level

**Organizational Measures**

- Logical client separation (on the software side)

### 1.6 Pseudonymization; Art. 32 para. 1 lit. a) Alt. 1 GDPR

Pseudonymization refers to measures for processing data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to appropriate technical and organizational measures. The application of pseudonymization to personal data can reduce the risks to the data subjects' data. Pseudonymization is sufficient if de-pseudonymization by internal users is not possible or is possible only with disproportionate effort.

- Not relevant, since pseudonymization does not take place or is not required

## 2. Data integrity pursuant to Article 32(1)(b), Variant 2 of the GDPR

### 2.1 Transmission and Transport Control

Transmission control refers to measures used to verify the recipient of a data transmission. Transport control refers to measures used to ensure the confidentiality and integrity of data during the transport of data media.

**Technical Measures**

- Sensitive information is transmitted over networks exclusively in encrypted form using recognized cryptographic methods.
- When transmitting high-risk personal data, both state-of-the-art transport encryption and content encryption are used.
- In the case of mass email campaigns, the disclosure of all recipients is prevented through technical or organizational measures.
- Unencrypted transmission protocols (e.g., FTP, Telnet) are not permitted for the transmission of personal or sensitive data.
- Remote access to clients or systems is granted exclusively via encrypted connections after the administrator has been successfully authenticated and the user has given approval.

### 2.2 Input Validation

Input control refers to measures for (retrospective) verification of which personal data was entered into or modified in automated processing systems, at what time, and by whom.

- The entry, modification, and deletion of data in IT applications are tracked in a traceable manner using personalized, unique user Ids
- Access to servers and operating systems is logged to detect and analyze unauthorized or security-related activities

### 2.3 Reliability & Data Integrity

Reliability refers to measures that ensure that all system functions are available and that any malfunctions that occur are reported. Data integrity ensures that stored personal data cannot be corrupted by system malfunctions.

- Systems, servers, and network components are configured according to recognized hardening standards
- Firewall configurations are reviewed on a regular basis
- Firewalls, network components, spam filters, virus scanners, and security-related systems are updated regularly
- IT systems and applications have defined malfunction and security alerts.
- Time Synchronization (NTP)

## 3. System availability and resilience (resilience) pursuant to Article 32(1)(b), Variant 3 of the GDPR

### 3.1 Restorability pursuant to Article 32(1)(c) of the GDPR

Recoverability refers to measures that ensure that systems in use can be restored in the event of a failure.

- Documented Data Backup Plan
- Documented Backup Policy for Servers and End Devices
- At least one backup system is protected against immediate encryption or deletion by malware.
- A documented recovery plan for the immediate restoration of IT availability has been implemented.
- Monitoring the Data Backup Process

- Regular data recovery tests and logging of the process (recommended: quarterly)
- Backup media are physically separated from the production system and stored securely.
- At least one backup is stored outside the company or in a logically separate environment.

### 3.2 Availability Check

Availability control refers to measures that ensure that personal data is protected against accidental destruction or loss.

**Organizational Measures**

- Up-to-date equipment management and documentation are in place
- Identification of Critical Assets

## 4. Procedure for regular review, assessment, and evaluation pursuant to Article 32(1)(d), Option 3 of the GDPR

Organizations must not only implement appropriate security measures but also ensure that these measures are reviewed and evaluated at regular intervals. This process is intended to ensure that the measures taken remain effective and meet current requirements in order to minimize data protection risks.

- Entering into data processing agreements with subcontractors pursuant to Article 28 of the GDPR
- Review of Technical and Organizational Measures in accordance with Article 32 of the GDPR
- A documented process for identifying, reporting, handling, and following up on security and data protection incidents.
- Documentation of security and data protection incidents (e.g., ticket system)
- Regular review, assessment, and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing

## 5. Security of the Development Environment

### 5.1 Software Development

Data protection and security must be taken into account early on in the development of in-house software systems or when selecting software products for use within the organization.

Privacy-friendly default settings (Privacy by Design/Privacy by Default) describe measures that ensure that, by default, only personal data whose processing is necessary for the specific processing purpose in question is processed.

**Technical Measures**

- Production systems are technically and organizationally separate from development and test systems
- System and security tests are conducted regularly
- Access to the source code is restricted
- Standard software and updates are obtained exclusively from trusted sources

**Organizational Measures**

- Documentation of in-house IT applications (system description, authorization policy, interfaces, reports, data deletion policy)
- Documented coding standards and development guidelines
- No personal data or login credentials are stored in the source code management system
- Data entries are validated based on semantic criteria (semantic input validation)
- Purpose attributes have been defined and implemented for data fields and records
- No real data or personal data is processed in test and development environments
- Relevant employees have been trained on the fact that Security by Design (ensuring confidentiality, availability,and integrity) is a legal data protection requirement as a subset of Data Protection by Design and influences key design decisions (product selection, centralized vs. decentralized, pseudonymization, encryption, and the country of a service provider).
- A sufficient number of test cycles are taken into account
- There is an ongoing plan for monitoring, evaluating, and implementing updates or configuration changes throughout the software's entire lifecycle.

**5.2 Web Application Development (e.g., online stores, apps, etc.)**

Websites and web applications are typically easily accessible targets for attacks, but they can usually be well secured using established best practices.

**Technical Measures**

- Production systems are technically and organizationally separate from development and test systems
- Remote access to web servers is provided exclusively via encrypted connections and with two-factor authentication.
- A state-of-the-art HTTPS protocol is used (TLS 1.2 or TLS 1.3).
- A documented data backup plan for the online application is in place.
- A RAID system or disk mirroring is used
- Timeouts or protective measures for multiple login attempts have been implemented.
- A Content Security Policy (CSP) has been defined and technically implemented

**Organizational Measures**

- Complete IT documentation for the online application is available
- An access control policy for source code repositories and development tools has been implemented
- A transparent version and change management system has been established
- Content that cannot be found publicly is technically protected against indexing by search engines
- Data entries are validated based on semantic criteria (semantic input validation).
- Purpose attributes have been defined and implemented for data fields and records.
- Only synthetic or anonymized data is used in test and development environments
- The database is protected by appropriate firewall rules
- Automated testing tools for enforcing coding standards are used
- Access to source code management systems is granted exclusively through secure authentication mechanisms

- Sensitive data is not stored in the source code management system
- Employees have been trained to understand that Security by Design (ensuring confidentiality, availability, and integrity) is a legal data protection requirement—as a subset of Data Protection by Design—and that it influences key design decisions (product selection, centralized vs. decentralized, pseudonymization, encryption, and the country where a service provider is located).
- Documented coding standards and development guidelines

**5.3 The Lifecycle of Secure Development**

- Incorporating Safety Requirements into the Specification and Design Phases
- Secure version control with change tracking

# ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

**1. Name: Hetzner Online GmbH**

Address: Industriestr. 25, 91710 Gunzenhausen

Description of the processing: Hosting of Vikunja Cloud

**2. Name: Scaleway S.A.S.**

Address: 8, Rue de la Ville-l’Évêque 75008 Paris 8, France

Description of the processing: Mailserver, Hosting of Vikunja Cloud

**3. Name: Cloudflare Inc.**

Address: 101 Townsend Street, San Francisco, CA 94107, USA

Description of the processing: CDN and DNS services, Captcha