Data Processing Terms

Version 2025.3-UK

Article D1 Definitions

In these TinQwise Data Processor Terms, several definitions are used by capitalized words. These definitions have the meaning given to them in the TinQwise General Terms & Conditions. In addition, the following definitions are used:

1.1. **Autoriteit Persoonsgegevens (AP)**: The Dutch data protection authority and the independent administrative body that has been established by law in the Netherlands as a supervisor for the supervision of the processing of personal data.
1.2. **Controller**: the Party that has the role of Controller for the Processing of Personal Data, as stated in the GDPR, in this case Client; the Controller determines the purpose and means for using Personal Data.
1.3. **(Data) Subject**: the person to whom a Personal Data relates. In this the Users.
1.4. **Data Protection Officer**: the person within TinQwise who is appointed to take care of the sound maintenance and execution of the Data Protection Policy.
1.5. **Data Protection Policy**: The most accurate description of the policy within TinQwise on how TinQwise handles all data in a consistent and safe way. This includes the way the data is stored, who has access to the data, how data is retained and how data is deleted when obsolete.
1.6. **Personal Data**: all information about an identified or identifiable natural person, which the Processor processes for the benefit of the Controller in the context of the Agreement.
1.7. **Personal Data Breach**: the intentional or unintentional release of Personal Data to third parties who are not authorised to have access to that data and which leads to the destruction, loss, alteration or unauthorized disclosure of or unauthorized access of Personal Data that is being processed.
1.8. **Processing**: all activities, whether or not carried out by automated processes, that the Parties may carry out on Personal Data, from collecting through to destruction, including recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, making available, combining, alignment, restriction, erasure or destruction.
1.9. **Processing Agreement**: this present Data Processing Terms including its Appendices.
1.10. **Processor**: The organisation (in this case TinQwise) to whom the Controller has outsourced Data Processing.
1.11. **Regulation**: Regulation (EU) 2016/679 of the European Parliament and the Counsel of April 27, 2016 on protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
1.12. **Sub-processor**: a Processor's Subcontractor that, as a Subcontractor, also Processes the Personal Data.

Article D2 Object of this Processing Agreement

2.1. This Processing Agreement encompasses the Processing of Personal Data by Processor for execution of the Order Confirmation and all related documents, together being the Agreement.
2.2. Processor guarantees using fitting technical and organisational measures, so Processing meets the requirements of the Regulation and protection of the rights of the Subject is ensured.
2.3. Processor guarantees to meet the requirements of applicable laws and regulations concerning Processing Personal Data.

Article D3 Commencement and duration

3.1. This Processing Agreement commences when Parties have signed the Order Confirmation.
3.2. This Processing Agreement ends when Processor has deleted or returned all Personal Data in accordance with Article D10 and the Agreement has ended.
3.3. None of the Parties can end this Processing Agreement in the meantime.

Article D4 Scope of processing jurisdiction Processor

4.1. Processor will Process Personal Data solely on behalf of Controller after written instructions, save deviating legal regulations applicable to Processor.
4.2. When an instruction as meant in paragraph 1 is, according to Processor, in violation of a legal requirement relating to data protection, he will notify the Controller of this prior to Processing, unless a legal requirement prohibits this notice.
4.3. When Processor is legally required to provide Personal Data, he will inform Controller immediately, when possible, prior to disclosure.
4.4. Processor has no say in purpose and means of Processing Personal Data.

Article D5 Securing the Processing

5.1. In addition to Article 15 of the TinQwise General Terms and Conditions and notwithstanding Article D2.3, Processor will take technical and organizational measures as described in Appendix 3.
5.2. Parties acknowledge that ensuring a suitable level of security can force the need for taking further security measures. Processor ensures a level of security suited to the risk.
5.3. Processor does not Process Personal Data outside the European Union, unless Controller has explicitly given written permission, notwithstanding deviating legal requirements.
5.4. Processor will inform Controller without undue delay, as soon as he has taken note of unjust Processing of Personal Data or breaches to security measures as mentioned in paragraph 1 and 2.
5.5. Processor aids Controller in meeting obligations pursuant to articles 32 up to and including 36 of the Regulation.

Article D6 Confidentiality Personnel of Processor

6.1. Personal Data is confidential as meant in article 13.1 of the TinQwise General Terms and Conditions.

6.2. Processor proves on request of Controller that his Personnel commits to confidentiality as meant in article 13.2 of the TinQwise General Terms and Conditions.

Article D7 Subprocessor

7.1. When Processor, considering article 8 of the TinQwise General Terms and Conditions, hires another processor to undertake processing activities on behalf of the Controller, this processor will at least adhere to the same obligations as mentioned in this Processing Agreement.
7.2. The Subprocessors mentioned in Appendix 2 can possibly process Personal Data outside the EEA and Controller agrees to this. Controller knows named Subprocessors work according to their Standard Contractual Clauses-agreement, as to allow work outside the EEA.
7.3. Controller is allowed to replace a Subprocessor, if it meets provisions as meant in articles D7.1 and D7.2.

Article D8 Assistance due to rights Subject

Processor assists Controller in fulfilling his duty to answer requests of Subject to exercise his rights as mentioned in chapter III of the Regulation.

Article D9 Violation related to Personal Data

9.1. Processor informs Controller without undue delay, as soon as he has taken note of a Personal Data Breach, in accordance with the procedure as mentioned in Appendix 4.
9.2. Processor also informs Controller about progress of concerning Personal Data Breach after notification based on paragraph one.
9.3. Parties bear their own cost related to notification to competent regulatory authorities and Subject.

Article D10 Return or deletion of Personal Data

10.1. After termination of the Agreement, Processor ensures the return to the Controller or deletion of Personal Data, according to Controller's choice. Processor deletes copies, save deviating legal regulations.
10.2. Personal Data are removed from operational systems in due time by Controller.

Article D11 Information obligation and audit

11.1. Processor provides all information needed to prove that obligations in this Processing Agreement are and will be met.
11.2. Processor cooperates with audits, in any way needed, for which costs are borne by Controller.

Appendix 1 – The Processing of Personal Data

The overview below shows which regular Personal Data is kept in TinQwise LXP.

✓	Name		~~Date of birth~~	✓	User name
	~~Address~~		~~Gender~~		~~Employee identification number~~
	~~Zipcode~~		~~Telephone number~~		~~Netwerk path~~
	~~Place~~	✓	Email address	✓	Login-/logout time (session)
✓	IP-address	✓	Random ID	✓	Page views
✓	Country		~~Business line~~	✓	Recommendations
✓	Function/Role	✓	Business unit	✓	Finished Modules
	~~Starting date employee~~	✓	Password	✓	Language of preference
✓	~~Profile photo~~				

TinQwise does not process Sensitive Personal Data. Changes to the listed definition of Personal Data processed are documented and agreed in the Order confirmation between Controller and Processor.

Especially for the Intercom Service application within TinQwise LXP, the following records (only of Administrators) are kept:

✓	User name	✓	User ID		
✓	First name	✓	IP Address		
✓	Last name	✓	Page views		

Please note:

- The data (relating to Article D5) is hosted in the USA and Canada.
- The use of Intercom as Subprocessor is only applicable if Controller chooses to use this application. Subprocessor handles Personal Data from Administrators only. In this service application, videos and other aids are available in which the use of TinQwise LXP as an Administrator is explained. It is also possible to ask questions directly to the TinQwise Service Desk. This option only applies to Administrators.

Appendix 2 – List of Subprocessors

1. **TinQwise India Learning and Development Private Limited –** provides learning specialists, implementation specialists, and technical support to TinQwise, which may involve access to TinQwise systems.
2. **Amazon Web Services Europe (AWS EMEA SARL)** – with datacentres in Dublin (Ireland) and Frankfurt (Germany) - is hosting the Software and data (*aws.amazon.com/legal/aws-emea/*).
3. **Intercom R&D Unlimited Company** – is providing an integrated service, support and communication platform for Administrators (*www.intercom.com*).
4. **Hallo, Amersfoort** – is providing ICT and workplace services to TinQwise including office automation (https://hallo.eu)
5. **HubSpot** – is providing CRM data for TinQwise including the contact persons en contact data of Controller. Please refer to https://legal.hubspot.com/dpa and the specific Chapter 7. “Additional Provisions for European Data”.
6. **Microsoft Corporation** – is providing document data storage for TinQwise including also documents we get from Controller Please refer to https://privacy.microsoft.com/nl-nl/privacystatement.

Appendix 3 – Appropriate technical and organizational measures

Protection measures

a. TinQwise will take appropriate technical and organizational measures to protect Personal Data from loss or any form of unlawful processing. These measures guarantee an appropriate security level for the Personal Data which is processed.

b. TinQwise applies the OWASP principles of 'security by design' and follows OWASP standards in all its coding methods (https://owasp.org/).

c. TinQwise takes at least the following measures:

I. encryption of digital files containing Personal Data;

II. secure network connections through a Transport Layer Security (TLS1.2) technology or comparable technology which provides at least the same level of security;

III. firewalls to block inbound traffic across other ports than HTTP and HTTPS. Blacklisting of IP addresses with failed log-in attempts;

IV. TinQwise hosts the application in ISO27001 and SOC2 compliant data centres;

V. providing access to TinQwise employees and others involved, only on an individual account basis and using two factor authentication measures.

Policies

The following policies are available upon request:

Policy / Document	Beschrijving
000 Roles & Definitions	All general roles and definitions used in TinQwise Policy set
001.1 Corporate Social Responsibility	Our view and approach on what corporate social responsibility means for TinQwise.
002.1 ISRMS Governance	An overview of our information security risk management system.
003.1 Security Incident Management	Outline of the information security requirements and incident management. Rules and requirements to mitigate risks related to information security incidents.
003.2 Data Privacy	Our approach to data privacy in TinQwise LXP, how we handle customer data and make sure it's secure.
003.3 Secure Development	Defines internal rules for secure development of our software and systems.
003.4 Change Management	Procedures around minimizing negative impact on services and users in case of changes.
004.1 Access Control	Requirements and policies around access to customer information, platform and systems.
004.2 Asset Management	Procedures around our software and hardware assets like laptops and servers.
004.3 Operational Resilience & Disaster Recovery	Policy and procedures to provide continuous service through people, processes, and technology.
005.1 Data Segregation & Retention	Detailed description of how we implement segregation and retention of data.

Appendix 4 – Procedures in case of Personal Data breaches

This appendix specifies the steps on how the Processor will deal with Personal Data Breaches and how it will inform involved persons and organizations, including the Controller.

Procedure Personal Data Breaches

Steps	Activity	Person responsible
1. A (possible) Personal Data Breach is discovered	• Immediately report (possible) data breach by informing the Data Protection Officer;	Employee who does discovery
2. Create a file	• Create a file and state the time of discovery, the time of informing the Data Protection Officer and the employee who did the discovery;	Data Protection Officer
3. Fight the Personal Data Breach	• Stop the data breach if possible; • Take measures to minimize the data breach and consequent damages; • Record the actions of the measures taken in the file;	Team lead (of the team in which the Personal Data Breach took place)
4. Assess the Personal Data Breach	• Assess whether Personal Data has been lost or could be used unlawfully; • Determine who or which department within the organisation is involved; • Determine whether a Processor was involved in the incident. If so, he needs to be involved in the process; • Record the actions of the measures taken in the file;	Team lead (of the team in which the Personal Data Breach took place) + Data Protection Officer
5. Determine impact of the Personal Data Breach	• Determine the Controller / Clients who may have been affected by the Personal Data Breach; • Assess the type of information leaked, e.g. health information, passwords, information about the financial situation or information which could lead to stigmatisation/abuse; • Assess the extent of the leaked data; • Assess the impact the leak can have on people involved (the Involved); • Determine the possible negative impact; • Record the actions of the measures taken in the file;	Team lead (of the team in which the Personal Data Breach took place) + Data Protection Officer
6. Determine approach for informing and recovery	• Determine the Processor(s) approach/informing; • Prepare the AP's approach/informing; • Prepare the Involved approach/informing; • Prepare the Involved actions and follow-up; • Determine actions in interest of TinQwise; • Determine actions for improvement security • Record the actions of the measures taken in the file;	Data Protection Officer
7. Report to the Processor(s) involved	• If it is decided to inform one or more Controllers, this must generally be done within 48 hours; • Check for each Data Controller involved whether there are specific agreements regarding the obligation to report, time and information; • Make the written report to the Contact Person of the Processor or the person who is specifically registered as a contact person in the event of a Personal Data Breach;	Data Protection Officer

Steps	Activity	Person responsible
8. Report to Autoriteit Persoonsgegevens (AP)	• Reports to AP are always made by/in consultation with the Controller concerned; • If it is decided that AP needs to be informed, this needs to be done within 72 hours; • Report on website of Dutch Data Protection Authority; • The Report form Data Breaches (Meldformulier Datalekken) can be used in advance;	Controller(s) + Data Protection Officer
9. Inform Involved	• Reports to Involved, which do not concern Personnel of the Service Provider, are always made by/in consultation with the Controller concerned; • Reporting through (for example) a letter; • Inform what happened, what personal data is involved and what possible consequences the data breach can have; • Inform about the actions taken by TinQwise and the actions that can be taken by the Involved themselves, to prevent damages;	Controller(s) + Data Protection Officer
10. Carry out repair work	• Recover the data breach • Improve security • Provide follow-up to people Controllers and Involved;	Team lead (of the team in which the Personal Data Breach took place) + Data Protection Officer
11. Optimize the process of security and data breaches	• Register, evaluate and improve security and process concerning Personal Data Breaches	Data Protection Officer