Data Processing Agreement (*version 14 August 2025*)

1 General

1.1 In the execution of the Contract, Telenet may receive, consult or otherwise process certain personal data at the request and on behalf of the Customer in its capacity as the Customer's processor. The Parties agree that Customer is the controller and Telenet is the processor of such personal data.

1.2 The Parties wish to comply with the applicable Data Protection Legislation, and to make arrangements by means of this Data Processing Agreement, which must be read together with the Annexes, with regard to the processing of personal data by Telenet on behalf of the Customer in the performance of the Contract.

2 Definitions

In addition to the terms already defined elsewhere in the Contract and the Data Protection Legislation, all capitalized words and expressions used, in the singular and plural, shall have the following meanings:

"Data Subject" an identified or identifiable natural person whose personal data is under the control of the Customer and is the subject of processing by Telenet in the context of the Contract;

"Annex" any annex to this Data Processing Agreement that forms an integral part of the Data Processing Agreement;

"Sub-processor" any third party used by the processor to process personal data on behalf of the controller;

"Data Processing Agreement" this data processing agreement between the Parties, including all Annexes, which forms an integral part of the Contract concluded between the Parties and as amended by the Parties from time to time;

"Confidential Information" as defined in the Contract;

"Data Protection Legislation" all Applicable Legislation as defined in the Contract in relation to the processing of personal data and privacy, including Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**General Data Protection Regulation**" or "**GDPR**""). The terms "personal data", "controller", "processor", "processing", "personal data breach", etc., have the meanings given to them in the Data Protection Legislation.

3 Obligations of the Parties

3.1 The Customer and Telenet shall comply with the Data Protection Legislation with regard to the processing of personal data in the context of the service.

3.2 The Customer is responsible for:

(i) compliance with all applicable obligations and duties of the controller;

(ii) the monitoring of rights exercised by Data Subjects;

(iii) providing the necessary legal basis for processing (including obtaining all necessary consents from the Data Subjects);

(iv) compliance with the applicable information obligations towards the Data Subjects.

4 Telenet obligations

4.1 Instructions

4.1.1 Telenet will only process the personal data in accordance with this Data Processing Agreement, according to the written instructions of the Customer, if it is reasonably necessary to provide the service in accordance with the Contract or as required by the mandatory Applicable Legislation and for the purposes as determined in the Annex to this Data Processing Agreement. The Parties agree that the Contract contains all the instructions of the Customer regarding the processing of the personal data. Additional or alternative instructions must be drawn up in writing and agreed in advance by both Parties.

4.1.2 Telenet will notify Customer as soon as possible if, in Telenet's opinion, an instruction from Customer infringes Data Protection Legislation.

4.1.3 Telenet is entitled to process the personal data without instructions from the Customer if it is obliged to process the personal data by a provision of Union or Member State law. In such a case, Telenet will notify the Customer of that legal requirement, unless such legal requirement prohibits this notification for important grounds of public interest.

4.2 Confidentiality

4.2.1 Telenet undertakes to safeguard the confidentiality of the personal data in accordance with the applicable Data Protection Legislation and to take all reasonable measures to ensure that:

(i) access to the personal data is limited to those employees who need to be able to consult the personal data and only to the extent necessary for the provision of services to the Client;

(ii) these employees are subject to appropriate obligations regarding the confidentiality and secrecy of the data, in accordance with the applicable Data Protection Legislation; and

(iii) these employees comply with this Data Processing Agreement and the Data Protection Legislation (hereinafter together the "**Data Protection Obligations**").

4.3 Third parties and Sub-processors

4.3.1 Telenet undertakes not to transfer or disclose personal data to third parties without the prior written consent of the Customer.

4.3.2 By entering into the Contract, the Customer authorizes Telenet to engage Sub-processors for the processing of personal data. When engaging Sub-processors, Telenet will:

(i) enter into a written agreement with each Sub-processor containing obligations in relation to the processing of the personal data that are equivalent to, and no less stringent than, the Data Protection Obligations; and

(ii) remain liable to the Customer for any breach of the Data Protection Obligations by a Sub-processor.

4.3.3 The Customer also authorizes Telenet to engage additional or other Sub-processors at any time. Telenet will inform Customer of such engagement. The Customer accepts and acknowledges that it will have the right to object to the engagement within 30 days of such notification by terminating the Contract, but only on condition that:

(i) the objection is based on an objective, compelling and substantiated justification as to why the new Sub-processor is unable to comply with its obligations under the Contract and the Data Protection Legislation; and

(ii) Telenet cannot reasonably refute or remedy the objection.

4.3.4 Customer understands and acknowledges that all information relating to the Sub-processors appointed by Telenet is considered Confidential Information.

4.4 International transfers

Customer authorizes Telenet to process the personal data in a third country outside the European Economic Area that is not recognized by the European Commission as ensuring an adequate level of protection in accordance with Article 45 of the GDPR, provided that appropriate safeguards are provided in accordance with the Data Protection Legislation (such as, for example, the signing of the standard contractual clauses for the transfer of personal data to third countries established in third countries, approved binding corporate rules, or adherence to an approved code of conduct).

4.5 Technical and organizational measures

Telenet implements appropriate technical and organizational measures to ensure, in accordance with the applicable Data Protection Legislation, a level of protection appropriate to the risk of the processing of the personal data (including the risk of accidental or unauthorized access, alteration, destruction, damage, corruption or loss, and any other unauthorized or unlawful processing or communication). Technical and organizational measures are only taken to the extent and to the degree that they directly or indirectly contribute to the protection of personal data. Since all technical and organizational measures are subject to technical progress and development, Telenet has the right to take other appropriate measures at any time. An overview of the technical and organizational measures taken for the processing of personal data on Telenet's systems and networks for the benefit of the Customer is set out in Article 11 of this Data Processing Agreement.

4.6 Personal data breach

Telenet will notify Customer as soon as possible if it becomes aware of a personal data breach relating to personal data processed by Telenet on behalf of Customer on Telenet's systems and networks and shall provide the Customer with information about the personal data breach as soon as possible, taking into account the nature of the processing and the information available to Telenet. If the personal data breach is due to an act or omission by Telenet, Telenet will take all reasonable measures to recover, reassemble and/or reconstruct any personal data lost, damaged, destroyed, altered or compromised as a result of the personal data breach within a reasonable period of time.

4.7 Support

4.7.1 Telenet shall provide the Customer with such assistance and/or cooperation as the Customer may reasonably request in order to comply with its obligations under the Data Protection Legislation (with regard to the personal data that Telenet processes on behalf of Customer in the context of the Contract), including:

(i) providing information, at the Customer’s request, about the technical and organizational measures taken by Telenet to protect the personal data;

(ii) if and to the extent permitted by law, informing the Customer of any request for access to the personal data that may be made by any supervisory authority, court or other body in a competent jurisdiction. For the avoidance of doubt and to the extent permitted by law, Telenet shall not communicate or disclose any personal data upon receipt of such a request without first consulting the Customer;

(iii) informing the Customer of requests from Data Subjects exercising their rights as Data Subjects under Data Protection Legislation and, where applicable, provide the necessary assistance in the execution of such requests;

(iv) cooperate with the data protection impact assessment that the Customer is required by law to carry out in relation to the processing activity performed under the Contract and the obligation to consult the competent supervisory authority prior to the processing if a data protection impact assessment indicates that the processing would pose a high risk if the Customer does not take measures to mitigate that risk;

(v) notifying personal data breaches resulting from the processing of personal data by Telenet on behalf of the Customer to the supervisory authority in accordance with Article 33 of the GDPR and, if applicable, the communication to the Data Subject in accordance with Article 34 of the GDPR.

4.7.2 If Telenet, in its capacity as processor, receives a request from a Data Subject regarding the processing of personal data in the context of the Contract to the Customer, it shall in no case respond to this request of the Data Subject and shall forward this request to the Customer without delay.

4.7.3 Telenet reserves the right to charge the Customer for all reasonable costs related to its obligations to provide such assistance and/or cooperation.

4.8 Audit

4.8.1 The Customer has the right to reasonably verify whether Telenet complies with this Data Processing Agreement. During the term of the Data Processing Agreement, Telenet shall provide the Customer with all information necessary to demonstrate compliance with the obligations of the Data Processing Agreement and the obligations arising directly from the applicable Data Protection Legislation.

4.8.2 Telenet shall agree to and cooperate with reasonable requests for audits to be carried out by an accredited independent auditor appointed by the Customer and who does not engage in competitive activity, at the Customer's expense, upon a prior written request from the Customer with thirty (30) calendar days' prior notice. The Parties agree to limit the number and scope of the audits to what is necessary to verify Telenet's compliance with the Data Processing Agreement, with a maximum of once per calendar year.

4.8.3 Telenet shall provide all reasonable support and assistance during the audit. Customer shall provide Telenet with a copy of the draft audit report and shall allow Telenet to comment and propose changes before the final version of the audit report is drawn up. The Parties agree that any audit report is confidential and may not be published or otherwise shared with third parties.

4.9 Deletion

Upon termination of the Contract, Telenet shall, without undue delay, cease any use of the underlying personal data processed on behalf of the Customer and – unless the law requires the continued retention of the personal data – destroy or anonymize the personal data and the copies it holds thereof.

5 Liability

Without prejudice to the liability exclusions and limitations of the Contract, Telenet can only be held liable for the damage caused by the processing of personal data as a result of the non-compliance with this Data Processing Agreement, if Telenet failed to comply with the Customer's lawful instructions or for a breach of the obligations of the Data Protection Legislation specifically aimed at processors. However, Telenet shall not be liable to the Customer if and to the extent that the Customer is directly or indirectly liable for the damage (e.g. if the damage is the result of the Customer's failure to comply with any of its obligations or responsibilities under the Contract or the non-compliance with applicable law). In this regard, the Customer indemnifies Telenet against claims from third parties.

6 Duration and termination

6.1 This Data Processing Agreement shall apply upon its acceptance by both Parties and shall remain in force after the expiry or termination of the Contract, as long as Telenet has access to the personal data that are the subject of this Data Processing Agreement.

6.2 This Data Processing Agreement may only be terminated during the duration of the processing of personal data by Telenet after mutual agreement between the Parties.

7 Entire agreement

This Data Processing Agreement replaces all other written or oral negotiations, agreements, understandings or representations between the Parties with regard to privacy and the protection of the personal data processed by Telenet under the Contract on behalf of the Customer.

8 Amendments

This Data Processing Agreement may only be supplemented, amended or modified by mutual agreement of the Parties. No addition, amendment or modification of this Data Processing Agreement shall be binding unless it is in writing and signed by both Parties.

9 Applicable law and competent court

9.1 This Data Processing Agreement and all (extra)contractual obligations arising from or related to it are governed by and interpreted in accordance with Belgian law.

9.2 Any dispute relating to the conclusion, validity, interpretation and/or performance of this Data Processing Agreement or of subsequent contractual arrangements or obligations arising from it, as well as any other dispute relating to or in connection with this Data Processing Agreement, shall be subject to the exclusive jurisdiction of the courts and tribunals of Antwerp (Mechelen division).

10 Translation

In the event of any doubt or discrepancy between the different language versions, the Dutch-language version of the Data Processing Agreement shall prevail.

11 Overview of technical and organizational measures

11.1 Preliminary

Telenet shall implement the measures described in this article, provided that the measures directly or indirectly contribute or can contribute to the protection of the personal data that Telenet processes in the context of the provision of services to the Customer.

The technical and organizational measures apply to the processing of personal data on behalf of the Customer on Telenet's systems and networks and/or in Telenet's premises/buildings.

The technical and organizational measures are subject to technical progress and development. In this respect, Telenet is permitted to implement alternative adequate measures, provided that the level of security of such measures is not less than the measures set out in this article.

The Customer may at any time, at its own expense, demand changes to the technical and operational measures described in this Article, if such changes are necessary in its opinion to comply with the legal requirements with regard to data protection and related security issues in relation to the service provided by Telenet under the Contract. Any such changes require the mutual agreement of the Parties.

11.2 Description of the technical and organizational measures

A. Physical access control to branches/buildings

Telenet shall take the following physical access control measures, insofar personal data are processed in Telenet's premises/buildings:

1. Restriction of access rights to office buildings, data centers and server rooms to the minimum necessary based on a prior security screening of all employees who (want to) gain access to the data centers. Access by external people is requested in advance subject to justification.
2. Effective control of access rights through an adequate locking system (e.g. security key with documented key management, electronic locking systems with documented management of authorization).
3. Comprehensive and fully documented processes for attainment, change and withdrawal of access authorization.
4. Regular and documented review of access authorizations granted to date.
5. Measures for the prevention and detection of unauthorized access and access attempts (e.g. regular review of burglary protection of the doors, gates and windows, alarm systems, video surveillance, security guards and security patrol).
6. Written regulations for employees and visitors on how to deal with technical access security measures.
7. Offering training to employees on a regular basis about physical access security of Telenet premises/buildings.

B. Logical access control to systems

Telenet shall take the following measures to control access to systems and networks in which personal data is processed on behalf of the Customer or via which admission to personal data of the Customer is possible, insofar as this personal data is processed on Telenet's systems and networks:

1. Restriction of admission rights to IT systems and (non-)public networks to the minimum necessary.
2. Effective control of authentication, authorization, and accounting through personalized and unique user identifications and secure authentication processes.
3. When using passwords for authentication, regulation shall be adopted to ensure the quality of passwords in terms of length, complexity and change frequency. Technical testing methods shall be implemented to ensure password quality.
4. When using asymmetric key methods (e.g. certificates, private-public-key methods) for authentication, it shall be ensured that secret (private) keys are always protected with a password (passphrase). The requirements set in accordance with paragraph 3 are to be observed.
5. On a regular basis, full reviews of all accounts and, if an account does not need to have certain access on a regular basis, the rights to it shall be revoked.
6. Regular and documented review of the logical access privileges granted to date.
7. Appropriate measures shall be taken to secure the network infrastructure (e.g. network port security IEEE 802.1X, intrusion detection systems, use of 2-factor authentication for remote access, separation of networks, content filtering, encrypted network protocols, etc.).
8. Written regulations and training on a regular basis for employees in dealing with the above security measures and safe use of passwords.
9. Ensuring the installation of critical or important security updates/patches within a reasonable timeframe, depending on the criticality, risk, and testing requirements:

a. in controller operating systems;

b. in server operating systems, which are accessible via public networks (e.g. web servers);

c. in application programs;

d. in security infrastructure (virus scanners, firewalls, IDS systems, content filters, routers, etc.); as well as

e. in server operating systems of internal servers.

C. Data access control

Telenet shall take the following measures for access control, insofar as Telenet itself is responsible for the access authorization of the personal data that is processed on behalf of the Customer:

1. Restriction of access authorization to personal data to the bare minimum required.
2. Effective control of access authorization through an adequate rights and roles concept.
3. A comprehensive and fully documented process for authorizing access, changing, copying and deleting personal data shall be in place.
4. Reasonable measures for the protection of terminal equipment, servers and other infrastructure elements against unauthorized access (e.g. multi-level virus protection concept, content filtering, application firewall, intrusion detection systems, desktop firewalls, system hardening, content encryption).
5. Technical security measures for export and import interfaces (hardware and application related).

Telenet shall have the following obligations to cooperate with the access control, unless Telenet is managing the access authorizations to personal data:

1. A comprehensive process for application, change and withdrawal of access authorizations in its area of responsibility.
2. Regular and documented review of the assigned access authorizations assigned to date, as far as is possible.
3. Immediate notification to the Customer if the existing access authorization are no longer required.

D. Data flow control

Telenet shall take the following measures for transmission control, insofar personal data are received, transferred or transported by Telenet on behalf of the Customer:

1. Appropriate measures to secure the network infrastructure (e.g. network port security IEEE 802.1X, intrusion detection systems, use of 2-factor authentication for remote access, separation of networks, content filtering, encrypted network protocols, etc.).
2. Data media encryption.
3. Use of encrypted communication protocols (such as TLS-based protocols).
4. Inspection mechanisms to identify remote terminals during transmissions.
5. Checksums adjusted with received personal data.
6. Written regulations and mandatory annual training for employees for the handling and security of mobile devices and data carriers.

E. Data entry control

In order to be able to subsequently check and verify whether and by whom the personal data can be accessed, modified or deleted from the data processing systems, Telenet shall take the following measures to control entry into its systems that serve the processing of personal data on behalf of the Customer or enable or provide access to such systems, insofar as Telenet is responsible for data entry:

1. Creation and revision-secure storage of process protocols.
2. Securing backup log files against tampering.

F. Data processing control

In order to ensure that the personal data can only be processed in accordance with the provisions of this Data Processing Agreement, Telenet shall foresee processes and documentation for:

1. Selection of Sub-processors under Data Protection Legislation and technical aspects.
2. Ensuring prescribed statutory preliminary inspection of Sub-processors in accordance with provisions of the Applicable Legislation.
3. Ensuring the timely instruction of the operational Data Protection Officers when introducing new or amending existing procedures for the processing of personal data.

4. Obligations of any person entrusted with the processing of personal data to maintain data secrecy pursuant to applicable law provisions.

5. Ensuring the familiarization of the people entrusted with the processing of the personal data with the Data Protection Legislation and the specific instructions of the Customer.

6. Maintaining the recognition of the operational Data Protection Officer.

7. Ensuring the immediate notification of the Customer in the event of an unlawful acquisition of knowledge of personal data or other protected information.

G. Availability control

In order to ensure that all personal data is protected against accidental destruction or loss, Telenet shall implement the following measures to control availability, provided that the processing of the personal data is required to maintain productive services for the Customer:

1. Operation and regular maintenance of fire alarm systems in server rooms, data centers and critical infrastructure spaces.

2. Creating regular backups and ensuring a robust and resilient disaster recovery capability is implemented.

3. Regularly review and testing of backup integrity.

4. Processes and documentation for the recovery of systems and data.

5. Storage, processing and destruction of hard copy personal data in accordance with security good practice.

H. Appropriation control

In order to ensure that personal data collected for different purposes can be processed separately, Telenet shall take the following measures for the separation of personal data for the benefit of the Customer:

1. Logical and/or physical separation of test, development and production systems.

2. Controller-level separation within processing systems and at interfaces.

3. Ensuring continued identifiability of personal data.

I. Retention and deletion of data

In order for the personal data to be retained only for as long as required and deleted when its processing fulfilment is complete, Telenet shall take the following measures to ensure the deletion of personal data, provided that these personal data are processed for the benefit of the Customer:

1. Ensure that the personal data can always be deleted or anonymized at the request of the Customer.

2. Processes, tools and documentation for secure deletion in such a way that recovery of the personal data is not possible using current state-of-the-art technology.

3. Guidelines for employees on how and when to delete personal data.

Annex(es): Specific details of the processing of personal data

To be consulted on the web pages of the relevant products and services.