

PERSONAL DATA PROCESSING AGREEMENT

Between

Proximus PLC under Belgian Public Law,
Boulevard du Roi Albert II / Koning Albert II-laan, 27
1030 Brussels
VAT BE 0202.239.951, Brussels Register of Legal Entities,
hereby represented by Karl Cuveele, Director Group Procurement

hereinafter referred to as “**Proximus**”,

And

Name:
Registered office:
Postal code & City:
Country:
Trade register number
VAT number:
hereby represented by

hereinafter referred to as “**the Supplier**”,

The following has been agreed:

The Parties have concluded an agreement nr 46 XXXXXXXX for the delivery of certain products and/or services (hereafter referred to as the “Services”). The agreement and all schedules, exhibits, subordinate agreements, work orders, purchase orders, amendments and any other subsequent documents incorporated therein are collectively referred to as “the Agreement”.

The present Personal Data Processing Agreement, including the GDPR-Annex, shall become an integral part of the Agreement and replaces any existing data protection provisions in the Agreement. In the event of any conflict between the terms of the Agreement and this Personal Data Processing Agreement, the provisions of this Personal Data Processing Agreement shall prevail.

ARTICLE 1 – PERSONAL DATA PROCESSING

1.1. The terms used in this Personal Data Processing Agreement shall bear their respective meaning given in the EU Regulation 2016/679 of April 27th 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, hereinafter called the “GDPR”.

The purpose of this Personal Data Processing Agreement is to ensure the compliance with GDPR and any other applicable personal data protection legislation, hereinafter referred to as the “Data Protection Law”.

This Personal Data Processing Agreement shall apply should Proximus directly or indirectly, e.g. through the Proximus employees or Proximus customers or end-users of customers, provide or make available personal data to the Supplier in connection with his delivery of Services, without limiting any confidentiality provisions already agreed upon between Proximus and the Supplier

With regard to these personal data, the Supplier will in principle act as data processor and Proximus will act as data controller.

1.2. Subject-matter, duration, nature and purpose of the processing, the type of personal data, categories of data subjects and the obligations and rights of Proximus

The personal data will be processed in order to provide Proximus with the Services as described in the

Agreement.

The processing consists of all data processing activities that are performed following the instructions of Proximus and that are necessary to deliver the Services to Proximus.

The categories of data to be processed by the Supplier will be limited to the personal data that are necessary to deliver the Services to Proximus and will be described in the GDPR-Annex to this Personal Data Processing Agreement.

The Supplier will promptly notify Proximus in writing in the event it establishes that personal data are communicated by or on behalf of Proximus to the Supplier which the Supplier should reasonably not receive in the framework of delivering the Services to Proximus.

The personal data can relate to Proximus employees, Proximus customers, end-users of Proximus customers, Proximus prospects or other categories as described in the Agreement.

The duration of the processing is limited to the duration the Agreement. The obligations of the Supplier with regard to the data processing shall in any case continue until the personal data have been properly deleted or have been returned on demand of Proximus.

With regard to the personal data Proximus shall have the rights and obligations of a data controller as set out in the GDPR and Data Protection Law, in the Agreement and in this Personal Data Processing Agreement.

The personal data shall remain at all times the property of Proximus.

1.3. Rights and obligations of the Supplier

The Supplier provides at all times during the performance of this Agreement sufficient guarantees for his compliance with the requirements of the GDPR and Data Protection Law.

The Supplier shall not process any personal data for purposes other than which are strictly necessary for the performance of his obligations under the Agreement in accordance with Proximus's documented instructions given in the Agreement or by any other means during the performance of the Agreement, except if he's required to do so by EU or EU Member State law to which the Supplier is subject. In the latter case the Supplier shall inform Proximus of that legal requirement before the start of any processing related thereto, unless that law prohibits such information being provided on important grounds of public interest.

The Supplier shall treat the personal data as strictly confidential in accordance with the terms of the provisions on confidentiality in the Agreement or in any other applicable contract between Proximus and the Supplier and ensures that all representatives, authorised to process the personal data in accordance with the provisions of the Agreement and this Personal Data Processing Agreement:

- (a) are informed of the confidential nature of personal data:
- (b) have received appropriate training in relation to data protection legislation:
- (c) are subject to user authentication and log-on processes when accessing the personal data and:
- (d) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality no less strict than as described in the Agreement and in the present Personal Data Processing Agreement.

The Supplier shall restrict access to personal data to his representatives who require such data to perform the tasks allotted to them by the Supplier in the performance of the Supplier's obligations under the Agreement and will allow access to personal data for such representatives on a strict "need-to-know" basis (excluding all access to personal data which are not strictly necessary for that representative to perform its part of the Services).

The Supplier shall take appropriate technical and organisational measures:

- to assist Proximus in the fulfilment of its obligations to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR, such as their right of access, their right to rectification, erasure, restriction of processing of their right to data portability, to object to processing of their data or any other request, complaint or communication relating to Proximus's obligations under the GDPR;
- to inform Proximus immediately upon becoming aware of such requests received directly from data subjects;

- to provide all data, requested by Proximus, within the timescale specified by Proximus and:
- where applicable, provide such assistance to enable Proximus to comply with the relevant request within the timescales.

The Supplier, at its own cost, and taking into account the nature of processing and the information available to him, assists Proximus in ensuring compliance with the obligations related to:

- the security of the processing under any applicable laws;
- the data breach notification obligations towards the supervisory authorities and towards the data subject;
- and the carrying out of any data protection impact assessments and prior consultations with supervisory authorities Proximus is obliged to perform.

1.4. Security of processing

The Supplier shall implement appropriate technical and organisational measures to protect the personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed and to ensure a level of security appropriate to the risk, including among other things as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Supplier shall take steps to ensure that any natural person acting under the authority of the Supplier who has access to personal data does not process them except on instructions from Proximus, unless he or she is required to do so by Union or Member State law.

The Supplier shall respect and apply the measures described in the specific provisions on security in the Agreement.

1.5. The end of data processing

As soon as it is no longer required for the performance of the Supplier's obligations under the Agreement and at the latest at the end of the Agreement, the Supplier shall properly delete or, if requested by Proximus at the end of the performance, return to Proximus, all personal data he has been processing in the performance of in the Agreement and any copy of it, unless EU or EU Member State law requires storage of the personal data.

Immediately after the proper deletion of the personal data (meaning that such personal data cannot be recovered or reconstructed), the Supplier shall give a written confirmation of such data deletion to Proximus.

If the Supplier cannot destroy or delete all personal data because of technical reasons, the Supplier will immediately inform Proximus thereof and will take all necessary steps to:

- (i) come the closest possible to a complete and permanent deletion of the personal data and to fully and effectively anonymize the remaining data;
- (ii) and make the remaining personal data which is not deleted or effectively anonymized unavailable for further processing.

1.6. Engaging a sub-processor (i.e. GDPR's "another processor")

The Supplier shall not engage a sub-processor without prior specific written authorisation of Proximus. Proximus does not give general written authorizations.

The Supplier shall inform Proximus at least 1 month in advance and by means of a written communication about his intention to engage a sub-processor, including his identity, the location where the personal data will be

processed by such sub-processor, the concerned data processing activities.

The Supplier shall carry out adequate due diligences on such sub-processor to ensure that it is capable of providing the level of protection for the personal data as is required by this Personal Data Processing Agreement, and provide evidence of such due diligence to Proximus.

Where the Supplier engages a sub-processor for carrying out specific processing activities on behalf of Proximus, the same data protection obligations as set out in this Personal Data Processing Agreement between Proximus and the Supplier shall be imposed on that sub-processor by way of a contract.

Where the sub-processor fails to fulfil its data protection obligations, the Supplier shall remain fully liable to Proximus for the performance of the sub-processor's obligations.

1.7. Transfer of personal data outside the European Economic Area

The Supplier or its sub-processor shall not transfer the personal data outside the European Economic Area and shall prevent the personal data from being accessed from a country which does not belong to the European Economic Area, except for countries which do ensure an adequate level of data protection according to an adequacy decision of the European Commission which Supplier will inform Proximus about.

The Supplier will exceptionally be allowed to bring the personal data outside the European Economic Area, under the following two cumulative conditions:

1. The prior specific written authorization of Proximus;
2. Appropriate safeguards in conformity with the GDPR are in place, such as e.g.:
 - the signing of the Standard Contractual Clauses of the European Commission for the transfer of personal data to processors established in third countries (2010/87/EU),
 - or, Approved Binding Corporate Rules,
 - or, adherence to an approved code of conduct, ...

In case of transfer of the personal data to the Supplier's sub-processor established outside the EEA, the Standard Contractual Clauses of the European Commission (2010/87/EU) will be executed between Proximus and the sub-processor. It is the responsibility of the Supplier to take the necessary steps to facilitate the signature of the Standard Contractual Clauses of the European Commission between Proximus and the sub-processor.

The transfer outside the EEA shall immediately cease to take place from the moment such adequacy decision from the European Commission or such safeguards are no longer valid or its conditions to apply are no longer fulfilled.

1.8. Personal data breach

Immediately after the detection of a personal data breach, or circumstances that are likely to give rise to a personal data breach, in the framework of the Services supplied to Proximus by the Supplier, the Supplier shall inform Proximus about the (likely) breach. Supplier will do so in a timescale and in a manner which allows Proximus to meet any obligations to report a personal data breach under the GDPR and Data Protection Law.

Hereto, the Supplier shall send an email flagged as "highly important and immediate follow up" to the Proximus Computer Security Incident Response Team at the address: csirt@Proximus.com.

This email shall at least include the following information: summary, circumstances and nature of the incident, content and number of the personal data (records) concerned, categories and number of individuals concerned, potential consequences, measures taken or proposed to be taken to mitigate the effects of the breach, date and time of the incident and of the detection of the incident and the contact details of the data protection officer or other relevant contact from whom more information may be obtained. The Supplier shall immediately respond to any supplementary question from Proximus regarding the incident and shall take all reasonable measures required by Proximus to address the personal data breach and to mitigate its possible adverse effects. Without prejudice to the foregoing, the Supplier shall in each event co-operate with Proximus and take such reasonable commercial steps as are directed by Proximus to assist in the investigation, mitigation and remediation of a personal data breach.

1.9. Audit, Compliance, Complaint and Supervisory Authority Cooperation and appointed Representative

The Supplier shall allow for and shall contribute to audits and inspections conducted by Proximus or an auditor mandated by Proximus. Proximus or an auditor mandated by Proximus may, subject to reasonable prior notice, enter the rooms or locations where the personal data is processed by the Supplier and inspect, audit and copy any relevant records, processes and systems to verify compliance with GDPR, Data Protection Law and this Personal Data Processing Agreement.

The Supplier shall fully cooperate and make available to Proximus on its demand all information that is necessary to demonstrate compliance with the GDPR and Data Protection Law obligations and obligations under this Personal Data Processing Agreement.

The Supplier shall immediately notify Proximus if any complaint, allegation or request relating to the Supplier's processing of the personal data impacts Supplier's processing activities. The Supplier shall provide all such cooperation and assistance as Proximus may reasonably require in relation to any such complaint, allegation or request.

The Supplier shall co-operate with the competent supervisory authority.

If the Supplier is not situated in the European Economic Area, the Supplier shall appoint his GDPR representative in Belgium and shall provide Proximus with his GDPR representative's contact details in the GDPR-Annex to this Agreement.

1.10. Liability and personal data processing

The Supplier acknowledges that the obligations of this Personal Data Processing Agreement are essential and that any violation thereof will seriously harm Proximus. The Supplier shall have full and sole liability for all damages resulting from a failure on its part or that of his sub-processor to comply with the provisions of this Personal Data Processing Agreement and Supplier shall indemnify and hold harmless Proximus against all expenses, losses, costs and damages arising therefrom. Should any person to whom personal data relates lodge a claim for compensation against Proximus and such claim is due to the Supplier's failure to comply with the provisions of this Personal Data Processing Agreement, the Supplier shall assist and intervene in Proximus's defence upon Proximus's request and shall indemnify and hold harmless Proximus from and against all expenses, losses, costs and damages.

Done at [redacted] on [redacted] in duplicate, each Party acknowledging having received its original copy.

For Proximus,

Name Karl Cuveele
Title Director Group Procurement
Date
Signature

For the Supplier,

Name [redacted]
Title: [redacted]
Date: [redacted]
Signature

GDPR-ANNEX: GDPR SPECIFICATIONS OF DATA PROCESSING

Instructions for the person who completes this GDPR Annex.

The components in YELLOW HIGHLIGHT ARE ONLY EXAMPLES and must be replaced with the actual data that corresponds to the reality. By actual data is meant: the actual names, address, date, numbers, references, specifications, ...

A.1 Document that describes the Services

Agreement nr 46 XXXXXXXXXXXX

A.2 Subject-matter of the processing

(marketing, profiling, insurance, IT systems management, connection of smartphone or 4G network, payroll, organisation of training, processing traffic fines, ...)

A.3 Nature and purpose of the processing

(data inventory, data processing in a cloud environment, maintenance and updating of IT data systems, merging of data, anonymize, in SAP, ...)

(e-mailing, salary calculations, contract management, technical database, software testing, ...)

A.4 The type of personal data

(Describe here which categories of personal data will be processed by the supplier.

Here are some EXAMPLE categories:

identification data, contact details, financial data, metadata for communication services, authentication data, product and service data, technical identification data, special categories of data, ...)

A.5 Categories of data subjects

(business contacts, customers, employees, private individuals, children, adults, retirees, people with disabilities, ...)

A.6 Supplier's contacts for processing personal data

Name and contact details:

- those of the supplier responsible for GDPR
- the Data Protection Officer (DPO) of the supplier
- the supplier's contact for the supervisory authority

If the supplier is established outside the European Union:

- name and contact details of the representative of the supplier within the EU;

A.7 Physical location of the processing by the supplier

(which data in which country through which data streams, where is the data physically stored and from where is the data accessible, inside or outside EU; which jurisdictions are involved; ...)

A.8 Identity of the Supplier's sub-processor (i.e. GDPR's "another processor")

If not applicable, please state "not applicable"

For each sub-processor: the supplier must request a prior written specific permission from Proximus.

Name, address and company code of the sub-processor:

Name and contact details of:

- those of the sub-processor responsible for GDPR
- the Data Protection Officer (DPO) of the sub-processor
- the sub-processor's contact for the supervisory authority

If the sub-processor is located outside the European Union:

- Name and contact details of the sub-processor's Representative within the EU:

A.9 Physical location and specifications of the sub-processor's processing

If not applicable, please state "not applicable"

(which data in which country through which data streams; where is the data physically stored and from where is the data accessible, within or outside EU; which jurisdictions are involved; ...)

(what exact part of the processing will be done by the sub-processor, detailed specifications of this part, ...)