Privacy notice

1. Intro

At Proximus we are committed to protecting the privacy of our customers and users. We recognize that the personal data you entrust to us is valuable and important to you, and we take our responsibility to safeguard your data very seriously.

In this privacy notice, we will provide you with detailed informfcontractation about the personal data we collect about you, what happens with your personal data if you use our services and apps and/or visit our different websites, for what purposes your personal data are used, and with whom your personal data are shared. You can also find out how you can control our use of your personal data. We will also explain your rights regarding your personal data, and how you can exercise these rights. To make the notice more readable, we have divided the different topics into chapters, which are easy to consult using the selection menu.

In addition to complying with relevant data protection laws and regulations, we are committed to upholding the highest ethical and moral standards in our handling of personal data. We believe that privacy is a fundamental human right, and that it is our duty to protect and respect your personal information.

2. Who are we?

The personal data we collect and use are stored in the files held by Proximus PLC under Belgian Public Law (Boulevard du Roi Albert II 27, 1030 Brussels).

3. Who is in scope of this Privacy Notice?

With this privacy notice, we want to inform any natural person (not legal persons nor companies) whose personal data we process in the context of the provision about how we process their personal data.

Hence, this privacy notice aims at informing the following categories of individuals, it being noted that the notice will be more relevant for certain categories of individuals than for others:

- Our customers, both residential and professional, and persons who have created a MyProximus account;
- Our ex-customers;
- Potential future customers (i.e. prospects);
- The customers of any subsidiary of the Proximus Group;
- The individuals using our services and products (e.g. family members of our customers, employees of our professional customers who use our services);
- The individuals using the service or product of another Belgian or foreign telecom operator that is currently using our network;
- The contact persons and representatives of our professional customers (e.g. employees of our professional customers);
- The contact persons of our residential customers and users of our products (e.g. relatives, guardians, judicial representatives that can legally represent these individuals);
- The contact persons of other third parties such as suppliers and partners that supply goods or services to us, indirect sales channels and subcontractors;
- Visitors of our offices, premises or shops;
- Visitors of our websites and users of our mobile applications;
- Participants in competitions, campaigns, surveys, webinars, events, etc.

As a Proximus customer, it may happen that you allow family members, friends, visitors and employees to use our products and services. An example is giving them access to your Wi-Fi. This will mean that we process some of their data, and this processing is therefore subject to this privacy notice. We have no relationship with them, and therefore cannot notify them of this. We count on you, as a customer, to take your responsibility and inform them about this.

4. What personal data do we collect and how long do we keep it?

This section provides an explanation of the categories of personal data that are processed by us and the data elements that fall under each of the categories of personal data. You can find more detailed information on what categories of personal data are used for the different purposes in sections 6 and 7 of this Privacy Notice.

4.1. Collected data (information you provide to us)

If you want to use our services and products, we need to collect some of your personal information. The personal data collected may vary depending on the situation in which they are collected. For example, we might collect your first and last name, address, login, email address, phone number, mobile phone number, date of birth, language or details of your identity document, which generally allow us to uniquely identify you. Depending on the reason why we are in contact, we might need additional information from you, such as specific preferences and requirements related to the service in question.

We may collect your personal information in a variety of ways. When visiting us in one of the Proximus points of sale or when browsing to the Proximus webshop, we can collect personal data from you via the electronic reading of your identity document or via the itsme app. Personal data can also be collected verbally in the Proximus points of sale, by phone via customer service, in writing via order forms, e-mail or text message, digitally via e-forms or when you chat with our chatbot or via our website, via MyProximus Web and MyProximus in the Proximus+ App and other Proximus apps or when you use social media to contact us.

From the moment you become a Proximus customer, each subsequent customer contact (e.g. when you place an order, participate in a survey, test or competition, call our customer service, register for a newsletter,…) comes with the collection and processing of personal data. Depending on the situation, Proximus will collect the following categories of personal data from you:

- **Identification and contact information**: Information allowing us to uniquely identify you and to contact you (first and last name, shipping/postal address, e-mail address, (mobile) telephone number, VAT number, pseudonym used online, easy switch ID, official identifier other than the national registry number,…);
- **National registry number**: The national registry number of a customer;
- **Profession information**: Information relating to your profession and your employer or the company you represent;
- **Personal characteristics**: Information relating to specific characteristics and/or attributes (age, sex, birth date, place of birth, nationality, language,…);
- **Family and household composition**: Data revealing a customer's family and/or household composition (number of children, marital status, number of housemates, dependant persons, name of partner,…);

- **IT and telecom product and service subscription information**: Information relating to the products or services that a person has subscribed to (customer install base, list of IT and telecom services to which a person has subscribed to, list of IT and telecom products that a person bought,…);
- **Financial data**: Information relating to a customer's financial 'credentials' (bank account number, credit card information,…);
- **Customer interactions**: Any records of customer's interaction with Proximus (website visits, shop visits, orders, content of shopping basket, servicing tickets…);
- **Survey specific information**: Information based on the questions asked in surveys (brand image questions, customer needs questions, consumer behaviour questions,…).

4.2. Obtained data (information we obtain from third parties)

We use personal data that is obtained from third parties, such as partners who provide us with identification and contact data of prospects. You can find more detailed information on how these data are used in sections 6 and 7 of this Privacy Notice.

- **Identification and contact information**: Information allowing us to uniquely identify you and to contact you (first and last name, shipping/postal address, e-mail address, (mobile) telephone number, VAT number, pseudonym used online, easy switch ID, official state-issued identifier other than the national registry number,…);
- **Personal characteristics**: Information relating to specific characteristics and/or attributes (age, sex, birth date, place of birth, nationality, language,…).
- **Product and service usage information**: Information concerning an end-user's usage of the products and services.

4.3. Observed or generated data (information we obtain through your use of our products and services)

We collect information when you use our products and services (fixed and mobile services, TV, ...) and websites or when you visit our premises.

- **Recordings of interactions with customer service** : The audio recording or text record of a customer's interaction with customer service (recording of customer service call, timestamp and duration of the conversation, a speech-to-text transcription, a saved chat conversation with a customer service agent,…);
- **Image and video records**: Images and videos of video surveillance cameras at the Proximus premises that are used for security purposes;
- **Internal identifiers**: Records that are used by Proximus to uniquely identify a customer or end-user (customer number, MyProximus credentials,…);
- **Technical identifiers**: Identifiers used in a technical context to relate a specific item of a customer (service ID, mobile number, IMEI number, device ID, ticket ID, case ID, quote ID, sales ID, IP address, box number,…);
- **Product and service subscription information**: Information on the products or services that a customer subscribed to (customer install base, list of services to which a customer has subscribed, list of products that a customer bought …);

- **Product and service usage information**: Information concerning an end-user's usage of the products and services (mobile data usage, call minutes, application usage, communication usage,...);
- **Hardware information**: Information on the devices used by a customer or end-user (type, brand and firmware information of hardware (decoder, modem, booster)) and of the devices that are connected to a Wi-Fi and/or mobile network (brand, type and IMEI number of a mobile device,…);
- **Billing information**: Information related to billing (past payments, outstanding amounts, invoice numbers,…);
- **Personal data generated in the context of transmitting electronic communications**: Information collected through the use of the mobile or fixed network by end users (call detail records (the originating phone number, the number you are trying to reach), TV logs, IMEI number of an end-user's device, date, time duration and location of a communication or internet connection,…)
- **Network location data**: Location data of an end-user's device collected through their use of the mobile network;
- **Consumption habits***:* Information relating to a customer's consumption habits (purchasing history, tv-viewing behaviour, web browsing behaviour);
- **TV viewing data:** Data generated by a customer's use of our Pickx (Proximus TV) services.

4.4. Derived data (information we derive from collected, obtained and observed or generated data)

In some cases, we use the collected, obtained and observed or generated data to make certain conclusions.

- **Segmentation information:** Information that is used in order to divide persons into different segments or groups (consumption habits, preferences, personal interests, product and service subscription information, bad payer information,…);
- **Preference profile**: A limited preference profile relating to the interests and preferences of a customer or end-user based on their participation in the Proximus reward program (Proximus For You) or their input in explicit surveys. In case you provided your consent to the use of tv viewing data and personal data generated in the context of electronic communications (certain websites or applications that you visit or use) for direct marketing purposes the preference profile can include this information as well;
- **Leisure and personal interests**: Information that provides an insight into the leisure activities or personal interests of a customer or end-user (membership to sports clubs, interest in fashion, subscription to an automobile magazine,…).

4.5. How long do we keep personal data?

The retention periods of the personal data we process depends on the purpose, you can find detailed information on the specific retention periods for the different purposes in sections 6 and 7 of this Privacy Notice.

5. Personal data sharing with third parties

We share your personal data with different categories of subcontractors, suppliers, partners, joint controllers, subsidiairies of the Proximus group, governmental entities or other third parties. When you use our products and services, we can share your personal data with third parties who collaborate with Proximus for the provision of products and services. We share your personal data with governmental entities when a legal obligation requires us to do so. In some cases, the sharing of personal data is based on your consent, or where adequate, our legitimate interest. In this section you can find an overview of the different categories of third parties with whom Proximus shares personal data.

5.1. Subcontractors, suppliers and partners

- Call centers for customer service and support purposes
- Partners or call centers who sell Proximus services in our name and on our behalf
- IT service providers
- Network and telecommunications service providers
- Suppliers of mobile devices
- Market research partners
- Courier services
- Installation technicians
- Billing service providers
- Payment service providers such as your bank or building society and collecting organisations
- TV service providers
- Recommendation engine providers
- Email service providers
- Marketing email providers
- Partners in the context of the loyalty program and competitions
- Debt-collection agencies and bailiffs
- Other telecom operators for the purpose of ensuring interconnection of electronic communication services
- Third party service providers for the purpose of direct carrier billing
- Law firms

Proximus can enlist the services of subcontractors located outside the European Economic Area. Proximus only works with subcontractors from countries that the European Commission deems can guarantee a suitable level of protection, or with subcontractors bound by the standard provisions approved by the European Commission.

In addition, your personal data may be shared outside the European Economic Area if this is required for the delivery of the service you wish to use, e.g. when you call a number in a country outside the European Economic Area or visit a website hosted by servers outside this area.

5.2. Joint controllers

We share your personal data with third parties who, together with Proximus, determine the purposes and means of processing of your personal data. Your personal data can be shared with the following third parties:

- Ads & Data for personalized targeted advertising (more detailed information can be found in section "7.2.3.2. Targeted advertising on web and in mobile applications (Ads&Data)".

5.3. Subsidiaries of the Proximus Group

We can share personal data of customers with other companies of the Proximus group in order to contact you by telephone with a view to informing you about their products and services that may be of interest to you.

Your personal data will be used as part of the legitimate interest of Proximus to allow other companies of the Group to process the data of Proximus customers in order to offer them the products/services best adapted to their needs. You can opt-out to the sharing of your personal data with other companies of the Proximus group via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy), by calling the Proximus customer service on 0800 55 800 or by sending an email to privacy@proximus.com .

5.4. Governmental entities

We have a legal obligation to share your personal data with certain governmental entities. The third parties with whom your personal data is shared in the context of a legal obligation are listed below and you can find more detailed information on data sharing in case of a legal obligation in section "6.3.3. Comply with legal dispositions". Your personal data is shared with the following third parties in the context of a legal obligation:

- Judicial authorities
- Intelligence and security services
- Judicial police officer of the Belgian Institute for Postal Services and Telecommunications
- Emergency services
- Judicial police officer of the Missing Persons Unit of the federal police
- Telecom Mediation Service
- (Deputy) Auditor of the FSMA
- Belgian Data Protection Authority
- Tax authorities

6. For what purposes (excluding marketing and sales purposes) do we use your personal data?

In this section you can find more information about the purposes (excluding marketing and sales purposes which can be found in section 7 of this Privacy notice) for which we process personal data. The purposes are divided in different categories. For each purpose there is a summary table containing the most important information such as what categories of personal data, the legal basis on which the

processing is based, the retention period of the personal data and where relevant the categories of third parties with whom the personal data is shared or information about how to exercise specific data subject rights in case it differs from the general ways to exercise data subjects rights that are explained in section 11 of this privacy notice. The summary table is followed by an explanation of the purpose.

6.1. General

6.1.1.Security purposes

6.1.1.1. Camera surveillance

Which categories of personal data will we use?

- **Observed or generated data**: Image and video records

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to protect our customers, visitors, employees, contractors, and property.

How long will we process this data for this purpose?

The camera surveillance image and video records are stored for a period of one month in accordance with the legally foreseen retention period unless the images contain proof of a crime or damage or help to identify a victim, witness or a suspect.

Who do we share this data with?

Camera surveillance images can be shared with judiciary and police forces based on a legal obligation in case of legal requests.

How can you request access?

If you would like to request access to the camera surveillance images on which you are captured please indicate the date, the location, and the time span during which you have been captured on the camera surveillance images and submit your request via privacy@proximus.com. For more information on the various ways to exercise your rights, you can consult section 11 below.

The premises of Proximus (including shops, buildings, sites…) are equipped with surveillance cameras as indicated by the camera surveillance pictogram at the entrance of the premises. The camera surveillance systems are used with the aim of preventing, establishing, or detecting crimes against persons or goods in accordance with the Belgian camera act. The camera surveillance images will not be used for any other purpose.

6.1.1.2. Visitor management

Which categories of personal data will we use?

- **Collected data**: Identification and Contact information

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to guarantee security and safety in our offices.

How long will we process this data for this purpose?

We will keep this data for a period of three years from the day of the visit.

With whom do we share this data?

Your data will be shared with the partner we rely upon for visitor management purposes.

In case of a planned visit to one of the Proximus offices, your name, contact and company details are collected and uploaded in a partner tool used for visitor management and access to the offices and the parking. This tool will furthermore generate a QR-code to enable your access to the Proximus offices on the day of your visit.

Upon arrival in the lobby, you can check in via one of the check-in tablets, where you are requested to scan the QR-code. This check-in will notify your host of your arrival, print your visitor badge and generate the guest wi-fi credentials. After your visit, you are requested to check out, again by scanning the QR-code on one of the tablets. Your data is kept for a period of three years from the day of the visit.

6.1.2. Recording of electronic communications for quality control purposes

Which categories of personal data will we use?

- **Collected data**: Identification and contact information
- **Observed or generated data:** Recordings of interactions with customer service

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to control the quality of the service of our call centres, as allowed by art. 10/1 of the Belgian Data Protection Act.

How long will we process this data for this purpose?

The conversations will be stored for a period of 1 month after the electronic communication has taken place.

With whom do we share this data?

This data is not shared with any third-parties. The recording can however take place in name of Proximus by one of its external call centres.

How can I object?

If you have a specific reason (motivated request), you can object to our use of your personal data for this purpose. Unless we have compelling grounds to continue using it, we will stop using it. For more information on the various ways to exercise your rights, you can consult section 11 below.

We are committed to offer you top-notch support and the ability to consult with one of our agents to solve any problem you might encounter while using our products and services. To achieve this level of quality of service however, we need to properly train our agents and provide feedback on their crucial work.

These recordings concern calls, but also for example, the chat conversations you might have with one of our agents.

These electronic communications are recorded and stored for one month. They are consulted only in the context of spot-checks and complaints regarding a specific call and are otherwise automatically deleted after a period of 1 month.

6.1.3.After-sales service, customer support and interactions with customer service

Which categories of personal data will Proximus use?

- **Collected data**: Identification and contact information, Personal characteristics, Financial data, Customer interactions, Copy of mandate or deed
- **Observed and generated data**: Internal identifiers, Technical identifiers, Product and service subscription information, Products and service usage information, Hardware information, Billing information, Personal data generated in the context of transmitting electronic communications, Consumption habits, Audio & Texting records

What justifies this processing activity?

The necessity of the processing for the performance of the contract (art. 6(1)(b) GDPR) as well as our legitimate interest (art. 6(1)(f) GDPR) to address your questions and/or requests in the most efficient way.

How long will we process this data for this purpose?

As long as you remain an Proximus customer. The data processed in the context of this purpose might be processed for a longer period in the context of other purposes, such as e.g., for legal archiving purposes.

The interactions with the digital assistant is processed for maximum 3 months after the closure of the conversation for documentation purposes to allow us to access your interaction history for more efficient management of requests in case of a recurring issue.

Regarding the retention period of recordings of electronic communications with our call centers, see section '6.1.2. Recording of electronic communications for quality control purposes'.

With whom do we share this data?

Depending on your request, your personal data will be shared with different types of recipients providing support, maintenance, general IT, and network-related services to Proximus.

Additionally, depending on the channel used to address your question or problem to Proximus, some of your personal data might also be shared with the third party acting on behalf of the customer (e.g., Telecommunciations Mediation Service, Testaankoop / Testachats).

Proximus is committed to offer you the best customer experience both via the various customer service channels (phone, chat, contact form or FAQs on the Proximus website) that we put at your disposal and via indirect channels you may reach out to in case of a question or issue (e.g., third party representing you).

Contacting customer service in case of question or issue

Given the different questions you can address to our customer service and depending on the channel used to get in touch with this service, we may process different sets of personal data from you, and we may share your data with different internal or external parties.

Below we describe the different steps that when you are in touch with the customer service:

1. Smart routing in some of our customer service channels

For us to help our customers as quickly and efficiently as possible, processes were set up to correctly identify you and to analyse your question or issue. These processes were built into the following channels:

- *By phone or by chat – Automated interactions with AI bot*

  When you contact our customer service via call or chat, you will first meet a digital assistant that will offer to assist you. Proximus wants to improve its interactions with its customers through different means, aiming to reduce as much as possible the waiting time when you try to reach our services.

  When you reach out to our customer service, you will be put in contact with an AI that will offer to assist you and will try to identify the reason why you reach out to us to assist you in the most efficient way. The AI will take different actions, depending on the following:

  - If the AI can **correctly identify** the reason for your call/message, and it **is able to assist** you without the intervention of an agent, then it will offer you the information it believes you need or the solution you might have requested.
  - If the AI can **correctly identify** the reason for your call/message, and it **is not able to assist** you without the intervention of an agent, then it will put you directly in contact with the right agent that will attempt to assist you with your request.
  - If the AI is **not able to correctly identify** the reason for your call/message, then it will put you directly in contact with an agent that will attempt to assist you with your request.

  Please note that you are always offered the possibility to be put in contact with an agent.

  Although the aim of the AI is to filter of the requests received by our customer service and to put you in contact with the right agent, some small decisions might be taken automatically (cancellation of an invoice for instance). However, such actions could require additional identification from you in order to prevent usurpation of your identity before taking any actions that could impact you.

- *By phone – Interactive Voice Response ('**IVR**')*

  Proximus relies on IVR for effective call routing. This technology uses the personal data you provide (i.e., phone number or line number and customer number) to verify your identity and to either route you immediately to the best fit agent, depending on the type of question or problem you selected in the selection menu, or to directly reply to your question (in case an intervention by an agent is not required).

- *Via the contact form on the Proximus website*

You may also use a contact form to address Proximus with your question or issue. Proximus may request certain personal data (i.e., phone number or line number, customer number, email address and the personal data you potentially provide to us in the free text field or in the attachment to the contact form) to identify you and immediately direct your question or issue to the appropriate agent.

- *Via the FAQs on the Proximus website*
  The Proximus website contains a section with FAQs, which guide you through some questions to determine the potential answer to your inquiry or resolution of your issue. Each time you indicate that a proposed step in the guided FAQ did not suffice as an answer to your question or did not resolve your issue, further questions are asked, or other guidance is given. At the end of a guided FAQ flow, you can indicate that you want to get in touch with our customer service channels to help you. The information on your questions and the steps taken in the guided FAQ flow are captured and used to immediately direct your question to the appropriate agent.

2. Identification and authentication by a customer service agent

Depending on the result of the checks in the smart routing of your chosen communication channel and depending on the nature of your question or issue, the agent may, through question and answer, process some additional personal data (e.g., IBAN number, a mandate or a copy of your identity document). In this way, the agent can verify that you are the customer account holder or that you are mandated on behalf of the customer account holder to contact Proximus.

3. Handling your question or issue

After the customer service agent has been able to identify you sufficiently, he will proceed to handle your question or issue.

Depending on the reason why you contact Proximus, the customer service agent will request or consult certain personal data related to you (e.g., the technical identifier or information relating to the performance of the product for which you are calling) and pass on certain information to other teams offering assistance, maintenance or general IT- and network-related services to Proximus.

4. Feedback to the third party (only applicable when you contact Proximus through a third party acting on your behalf)

If your question or problem is submitted to Proximus via a third party, we will also report back to this third party about the handling of the question and/or the resolution of the issue. Personal data essential for the response to the third party may thereby be shared with this third party.

Customer interactions initiated by Proximus

Next to the situations where you reach out to Proximus, Proximus might also reach out to you (e.g., to schedule an appointment for installation of your equipment and to remind you of an appointment you made). This requires the processing of your personal data (i.e., name, mobile phone number, language information relating to your appointment and your actions re. the appointment communication).

6.2. When you're becoming a customer

6.2.1. Contract commencement purposes

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Personal characteristics, Family and household composition, Financial data, Customer interactions, National registry number.
- **Observed or generated data**: Internal identifiers, Technical identifiers.

What justifies this processing activity?

The necessity of the processing in order to take steps at the request of the data subject prior to entering into a contract (art. 6(1)(b) GDPR) and the necessity of the processing to comply with a legal obligation (art. 6(1)(c) GDPR) namely the legal obligation of Proximus to carry out an identity check as provided for under article 127, §3 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

We will retain the personal data collected for this purpose for as long as you remain an Proximus customer. The personal data processed in the context of the provision of our services might be processed for a longer period of time in the context of other purposes, such as e.g., for legal archiving purposes.

In case we need to identify you by reading or taking a copy of your (Belgian or foreign) identity card or document, your identification document will no longer be kept than necessary for the validation of it. After the validation process, your identity document is deleted. The retrieved identification data can be stored at a maximum up to 10 years after you have ceased to be a Proximus customer.

With whom do we share this data?

For this purpose, your personal data may be processed by our indirect physical sales channels, for example in case you purchase one of our products or services via a non-Proximus branded shop. In addition, your personal data will be shared with service providers acting on our behalf to provide services such as processing the documentation used for the on-boarding of new customers. Lastly, we may have to share your personal data with official authorities in the context of our legal obligations.

When you become a Proximus customer and conclude a contract with us, we will collect and process personal data about you. We will ask you for some personal data, such as your name, address, telephone number, e-mail address, for the management of our contractual relationship.

To comply with our legal obligations, we also read or take a copy of your Belgian identity card, which includes your national registry number, or your foreign identity document (such as your foreign identity card or passport). Please refer to section "6.3.3. Comply with legal dispositions" for more information about how we store personal data and share them with official authorities in the context of our legal obligations. If you have more questions about our online verification of your identity, please consult this page of our website.

We also assign information to you, such as a customer number, login data, phone number, box number or other technical identifiers linked to the services and products we will provide you.

In case you move from another operator to Proximus and opt for "Easy Switch" to facilitate the switch of operators, we will ask you to provide an Easy Switch ID and your customer number and will take care of the cancellation and the transfer. We will obtain the other necessary information to conclude the contract with Proximus from your previous operator.

6.2.2. Assessment of new orders

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, personal characteristics, IT and telecom product and service subscription information, customer interactions.- **Obtained data**: Personal characteristics.

- **Observed or generated data**: Internal identifiers, product and service subscription information, billing information.

- **Derived data**: Family and household composition, segmentation information.

What justifies this processing activity?

The necessity of the processing in order to take steps at the request of the data subject prior to entering into a contract (art. 6(1)(b) GDPR) as well as our legitimate interest (art. 6(1)(f) GDPR) in assessing new orders to mitigate risks of non-payments and non-compliance with the contracts and to protect our financial interests.

How long will we process this data for this purpose?

Information concerning the non-payments of a former customer is deleted when the debt is time-barred (namely 5 years after the issue of the last unpaid invoice) or when the former customer has settled all his/her debts with us.

Information linked to the other types of assessments performed (see detail below) is kept until our competent services reevaluate whether the triggering factor of the assessment is still relevant, which is done at regular intervals or at least when a new order is triggered for manual review.

With whom do we share this data?

The information related to the outcome of the assessment of your new order may be processed by our indirect physical sales channels, for example in case you purchase one of our products or services via a non-Proximus branded shop.

We do not share any other personal data with third parties in the context of this processing activity.

How can I object?

In the case where the processing of your personal data is based on our legitimate interest, if you have a specific reason (motivated request), you can object to our use of your personal data for this purpose. Unless we have compelling grounds to continue using it, we will stop

using it. For more information on the various ways to exercise your rights, you can consult section 11 below.

We, like any business, must protect ourselves against the risk of non-performance by new or existing customers of their obligations. The key obligation of the customers is payment of their products and services. In this context, we need to assess the risk of non-payment when dealing with new orders from new or existing customers.

When you order a new product or service from us, we can assess the risk of non-compliance with your payment obligation based on various factors such as possible debts towards Proximus. Here are the typical steps involved in assessing a new order.

When new or existing customers submit a new order, we will collect relevant customer information from them and verify their identity, as explained in section 6.2.1. "Contract commencement purposes" above. Based on this information and other information available to us based on past activities of these customers (such as history of non-payments), we will assess the new order. The result of this assessment can be that the new order is validated without any further review, that the new order is flagged for review (*for example, when the identification of the new customer has not been completed, when the order is linked to a specific postal address which has been marked as presenting a high risk of non-payment or non-compliance with the contract, when the customer has been placed under guardianship by a competent judge or when we have otherwise registered a flag on the customer profile to submit any order to a manual check before validation*), or that the new order is blocked (*for example, when the person concerned is a former customer and shows a history of fraudulent activities or non-payments which lead to the termination of his/her services and which have not been paid off since*).

In case the order is flagged for review, it will go through a manual case-by-case analysis by our competent services to detect factors whose combination would indicate a risk of non-payment or non-compliance on the part of the customer. Based on the results of the manual review of the order, we can take the decision of validating, refusing, or submitting the order to specific conditions (such as a prepayment) to mitigate the risk associated with the order.

As far as our professional customers are concerned, we may acquire some data from third parties and process such data in order to know the companies with whom we might enter into business and ensure that these companies are financially sound. Please refer to section 7.1.1.3. "Acquisition of data relating to potential and existing professional customers" for more information about how we collect and process such data.

6.2.3. Social tariff

Which categories of personal data will we use?

- **Collected data:** National registry number;
- **Observed or generated data:** Product and service subscription information, Internal identifiers.

What justifies this processing activity?

This processing activity is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations foreseen in article 74 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

The national registry number will be processed for this purpose during eligibility check, determining whether the consumer is eligible to benefit from the social tariff. The other personal data will be processed as long as you remain a Proximus customer benefiting from the social tariff.

With whom do we share this data?

The Federal Public Service Economy who is responsible for performing the check to verify an applicant's eligibility for the social tariff

Article 74 of the Belgian Electronic Communications Act imposes an obligation on Proximus as an operator to offer specific telecommunications services at a reduced price for eligible consumers, which is known as the social tariff. Consumers can request Proximus to benefit from the social tariff, upon which Proximus needs to check their eligibility. The Federal Public Service Economy is responsible for the check and provides a dedicated portal for operators to submit consumers' national registry number for verification.

Once the national registry number is submitted to the portal, it will indicate whether the applicant is eligible or not for the social tariff. If the check results in a negative outcome, indicating the applicant's ineligibility, the result of the check will be accompanied by a document containing a list of contact points for any questions relating to the reason for refusal, which Proximus will provide to the applicant. However, Proximus does not receive any information regarding the specific reason for refusal by the Federal Public Service Economy.

For consumers who have submitted a request to benefit from the previous social tariff regime before 1/3/2024, the Federal Public Service Economy will notify Proximus when they are no longer eligible for the social tariff. When this occurs, Proximus is legally obliged to terminate the social tariff for these consumers.

6.3. When you are a customer or user

6.3.1. Delivery of requested products and services

6.3.1.1. Provision of our products and services

Which categories of personal data will we use?

- **Collected data**: Identification and Contact Information
- **Observed or generated data**: Product and service subscription information, Personal data generated in the context of transmitting electronic communications, Network location data, Technical identifiers, Product and service usage information.

What justifies this processing activity?

This processing is necessary for the performance of the contract to which you are a party (art. 6(1)(b) GDPR). Regarding personal data which would fall within the scope of ePrivacy legislation, their processing is allowed under article 122, 123 and 125 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

As long as you remain an Proximus customer. The data processed in the context of this purpose might be processed for a longer period of time in the context of other purposes, such as e.g., for legal archiving purposes.

With whom do we share this data?

Depending on the actual services you will use, your personal data will be shared with different types of recipients providing support, maintenance, and general IT and network-related services to Proximus.

Unsurprisingly, we will need to process your personal data to provide you with the services you pay for, for the purpose of enabling their proper functioning:

- If you are using voice-to-voice or SMS services (be it mobile or fixed), we will need to process data to make sure that a connection is established between the proper caller and callee and that the telephony and SMS traffic is properly routed across its network.

- In the context of the provision of internet access services, we will need to process technical data on your usage that is needed to transport internet traffic over our network and displaying the content you expect while accessing the internet.

- Finally, if you use Pickx (Proximus TV) services, we will process technical data about your usage. We require this data to be able to provide our Pickx services to you, to deliver on-demand items (i.e., VOD), to schedule your recordings and keep them available for you.

Important note: As a matter of principle, in the context of the provision of its services, we do **NOT** access the content of your electronic communications. We will process the metadata necessary to ensure the functioning of our services and the correct transmission of an electronic communication (such as e.g., the delivery of an SMS to the correct recipient), but our network will serve only as a mere conduit for the content of the communications itself.

Access to the content of communications is rigorously regulated and is only allowed under specific circumstances exhaustively enumerated under specific articles of the Belgian Electronic Communications Act.

6.3.1.2. Interconnection with other telecom operators

Which categories of personal data will we use?

- **Observed or generated data**: Personal data generated in the context of transmitting electronic communications

What justifies this processing activity?

This processing is necessary for the performance of the contract to which you are a party (art. 6(1)(b) GDPR). This processing of traffic data is allowed by art. 122 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

As long as it is necessary for the transmission of the communication. Traffic data relating to interconnection will also be stored for billing purposes (see section "6.3.2.1. Billing and accounting").

With whom do we share this data?

We will need to both receive and share data with the other telecom operators involved in that specific electronic communications, for the purpose of ensuring interconnection of electronic communications services.

While it might not directly ring any bells, interconnection is a key activity enabling your seamless day-to-day use of electronic communication services. In simple terms, interconnection is what enables you – a Proximus customer – to make use of your mobile data or to reach another person (be it by phone or SMS) using the services of another operator, located on another electronic communications network, in or outside Belgium.

All telecom operators have a legal obligation to enable access to their network and to negotiate interconnection agreements with the operators of other networks, based on the European Electronic Communications Code as well as the Belgian Electronic Communications Act. These other operators might include national operators (e.g., Telenet or Orange), operators in foreign countries (e.g., Deutsche Telekom, Vodafone), and international carriers (e.g., BICS).

Without interconnection agreements and the necessary processing of personal data these activities involve, global communication as we know it today would not be possible.

In the context of interconnection services, your phone number and usage information might be exchanged with other interconnection partners to ensure routing of the communication as well as for billing purposes, reconciliation and payment settlement purposes, dispute management purposes.

6.3.2. Customer management

6.3.2.1. Billing and accounting

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Personal characteristics, Financial data.
- **Observed or generated data**: Internal identifiers, Technical identifiers, Product and service subscription information, Product and service usage information, Billing information, Personal data generated in the context of transmitting electronic communications.

What justifies this processing activity?

This processing is necessary for the performance of the contract to which you are a party (art. 6(1)(b) GDPR) or our legitimate interest (art. 6(1)(f) GDPR) to process personal data to accurately bill and invoice for the services we provide to end-users of our professional customers . The processing of your traffic data for this purpose is allowed by art. 122, §2 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

We will keep billing-related data for the duration of the contract with you and for an additional 7 years thereafter to comply with our legal obligations related to tax and accounting.

With whom do we share this data?

We will share your personal data with service providers acting on Proximus' behalf to provide billing-related services such as the management of our legal archive for documents such as invoices. In addition, some of your personal data will be shared with the company that employs you or other business relations of yours in case your employer pays all or part of your bill. If you choose to pay your bills by means of direct debit, some of your personal data will be shared with payment service providers such as your bank or building society and collecting organisations so that your direct debit instruction is completed.

Billing is a part of the majority of services we offer to you. For this purpose, we use data related to your contract and your consumption to calculate and generate invoices, generally on a monthly basis. This also implies the application of the appropriate taxes and credits.

We will also use your contact details to send you billing documents and ensure that the invoice is appropriately delivered to our customers. Depending on your preferences, your invoice will be sent to you:

- on paper via the post;
- online, via SMS or email; or
- on your MyProximus account, via the Proximus+ App and on myproximus.be.

If you choose to pay your bills by means of direct debit, you authorize your bank to pay your Proximus bill automatically. This is done on the due date, which is mentioned on your bill or payment statement.

In case you use the possibility to pay for products/services offered by third parties via a statement in your Proximus invoice, we and this third party will share billing-related personal data about you, as further explained in section "6.3.2.3. Third-Party Services or Direct Carrier Billing".

6.3.2.2. Collection process

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Personal characteristics, Financial data, Customer interactions.
- **Observed or generated data**: Internal identifiers, Product and service subscription information, Billing information.
- **Derived data:** Segmentation information.

What justifies this processing activity?

This processing is necessary for the performance of the contract to which you are a party (art. 6(1)(b) GDPR).

How long will we process this data for this purpose?

We will keep billing-related data for the duration of the contract with you and for an additional 7 years thereafter to comply with our legal obligations related to tax and accounting.

With whom do we share this data?

Debt-collection agencies and bailiffs.

In case a customer does not pay invoices or fees in a timely manner, we may be obliged to take actions in order to collect the unpaid amounts.

In view of collecting unpaid invoices or fees from our customers, we may process your personal data in order to take different types of actions, where appropriate, such as:

- Classify the concerned person depending on the type of customer (e.g. residential or business customer), the communications with the customer in the context of collection (timing and means of communications like call or SMS), the collection actions towards the customer (payment promise and instalment plan) and the reason for the delay or absence of payment (e.g. bankruptcy, passing) in order to define the appropriate collection steps;
- Inform the customer about the unpaid amount;
- Temporarily cut off the customer's access to our services (telephone, TV and internet);
- Flag the customer as a 'bad payer'; or
- Make use of the services of a debt-collection agency or a bailiff.

6.3.2.3. Third-Party Services or Direct Carrier Billing

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Financial data.
- **Obtained data:** Product and service subscription information.
- **Observed or generated data**: Internal identifiers, Technical identifiers, Product and service usage information, Billing information.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to offer direct carrier billing payment services for third-party services to our partners and provide a safer means of payment for our customers online.

How long will we process this data for this purpose?

For the purpose of offering direct carrier billing payment services, we will keep your personal data for 2.5 years after their creation. This is without prejudice of the retention period of billing-related data in order to comply with our legal obligations related to tax and accounting.

With whom do we share this data?

Third-party service providers (usually online merchant who offer digital content) from which you purchased services to be paid by means of direct carrier billing.

How can I object?

Any subscription paid via direct carrier billing can be stopped by replying STOP (in capitals) to the third-party service provider's mobile number or by contacting the contact number of the third-party service provider. For more information on alternative ways to exercise your rights, you can consult section 11 below.

We offer our customers the possibility to pay for products/services offered by third parties ("third-party services") via direct carrier billing. When you want to buy a digital service for instance, the provider of the service will offer you different means of payment. One of them is called "direct carrier billing". It means the amount of the third-party service will be mentioned in a statement attached to your mobile telecom operator's invoice.

If you wish to resort to this means of payment, we will share personal data about you with the service provider. The provider will mainly transfer us information about the third-party service purchased. If required, we will use and transfer your phone number to allow your identification by the provider and confirm whether the transaction can go through or not (e.g. if you decided on a limited maximum amount lower than the price of the service, the transaction will not go through).

For these categories of information, we are acting as a controller and are transferring your personal data based on our legitimate interest to offer direct carrier billing payment services for third-party services to our partner and provide a safer means of payment for our customers online.

When the transaction is confirmed, the service will be mentioned in a statement attached to your telecom invoice and the amount will be collected by us and transferred to the third-party service provider. In this situation, the service provider is controller of the data related to the purchase of the third-party service and we are acting on the service provider's behalf as its processor.

6.3.2.4. Verification services to 3rd Parties

Which categories of personal data will Proximus use?

Proximus acting as a sub-processor:

- **Obtained data**: Identification and contact information (collected by Digital Service Providers and shared with Proximus via Telesign).

Proximus acting as a controller:

- **Collected data**: Identification and contact information, Subscription information.

What justifies this processing activity?

Proximus and Digital Service Providers both have legitimate interests (art. 6(1)(f) GDPR) that justify this processing activity. Proximus aims to generate revenue and assist Digital Service Providers in combating fraud through telecommunication services. Meanwhile, Digital Service Providers seek to prevent fraud on their platforms and streamline the identification process for individuals seeking registration.

How long will Proximus keep this data?

The match results and risk levels are deleted after 90 days.

Who do we share this data with?

The match results are shared with our subsidiary, Telesign, who is acting as processor for the Digital Service Providers. No other data is shared by Proximus.

How can I object?

If you have a specific reason (motivated request), you can object to our use of your personal data for this purpose. Unless we have compelling grounds to continue using it, we will stop using it. For more information on alternative ways to exercise your rights, you can consult section 11 below.

We can process your personal data for the provision of verification services to third parties (Digital Service Providers), including subsidiaries of the Proximus Group, to allow them, in the context of preventing and combating fraud, to check whether the data they possess corresponds with the data in our customer database, **but without disclosing your name or other customer data to the third party**. It allows them to evaluate the validity of data a unique customer provides during the registration process and as such helps them to detect the creation of fake accounts.

It is important to emphasise that in this process, we never share your name with these Digital Service Providers – only the match results as well as a risk level are communicated to Telesign.

6.3.2.5. Dispute management

Which categories of personal data will we use?

The categories of personal data we will use for dispute management purposes, will depend on the nature of the dispute. In general, we will process the data necessary to uniquely identify you (identification and contact information). Depending on the nature of the dispute, other personal data might also be processed (e.g., in case of a billing dispute, billing and payment information will be processed.

What justifies this processing activity?

This processing is necess for the performance of the contract to which you are a party (art. 6(1)(b) GDPR) in case of a dispute related to you as a customer or our legitimate interest (art. 6(1)(f) GDPR) to resolve disputes in case of a dispute when you are not a Proximus customer.

How long will we process this data for this purpose?

Your personal data will be kept for ten years after the dispute has come to an end for evidentiary purposes (e.g. if your name appears in a document that serves as evidence in a dispute between you and us, this personal data will be kept for ten years because the evidence document will be kept as long).

In order to manage potential future data protection related disputes, a trace of your consent (e.g. consent collected for targeted advertising purposes) will be stored for the duration of the consent + 5 years, which is the prescription period for any actions before the Belgian Data Protection Authority.

With whom do we share this data?

The people with whom your personal data in the context of dispute management is shared, will also depend on the nature of the dispute. Your personal data might for example be shared with a law firm in case the dispute is taken to court.

In the context of a dispute, we will process some of your personal data. First, we will process the personal data linked to your customer account, in order to uniquely identify you and to contact you in the context of the dispute. Depending on the nature of the dispute, we might also process other personal data (e.g., billing information, payment information, information about your products and services) and share your personal data with other partners (e.g., law firm, debt collection agency,…).

For more information about your data subject rights you can consult section 11 below.

6.3.2.6. Market research

Which categories of personal data will We use?

- **Collected data:** Identification and contact information, Personal characteristics, IT and telecom product and service subscription information, Survey specific information.
- **Obtained data:** Identification and contact information.
- **Observed or generated data:** Product and service usage information, Product and service subscription information, Billing information, Hardware information.
- **Derived data:** Segmentation information.

What justifies this processing activity?

Sending out the invitations to participate to market surveys: our legitimate interest (art. 6(1)(f) GDPR) to perform market research.

The processing in the context of the participation to market surveys: your consent (art. 6(1)(a) GDPR) to participate to market surveys.

How long will we process this data for this purpose?

The contact and identification information used to send out invitations are retained for a maximum of 5 years after the end of your contract with Proximus.

The personal data processed in the context of market research and surveys is retained for a maximum of 3 years after the date of the survey.

Who do we share this data with?

We share and receive personal data in the context of market research with/from different research partners.

Some of our research partners perform market surveys, orientated towards data subjects in our customer and user database, on our behalf. These market surveys are sent out through different communication channels (SMS, email and pop-ups on the website and in Proximus applications) or are conducted through interviews (face to face interviews, interviews via digital means or phone interviews);

Other research partners of ours are only involved in the recruitment of participants that match the target profile for specific market surveys; and

Our research partners can also provide us with results of market surveys oriented towards data subjects within their own database.

How can I object?

If you don't want to receive invitations to participate to market research surveys, you can opt-out for market research through the privacy preferences in your 'My Proximus' environment via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) or submit a request through the webform or via privacy@proximus.com .

For more information on alternative ways to exercise your rights, you can consult section 11 below.

How can I withdraw my consent?

You can always withdraw your consent, at any time, by contacting privacy@proximus.com.

For more information on alternative ways to exercise your rights, you can consult section 11 below.

We do market research with the aim of testing and improving (new) products and services, which consists of performing market surveys on the following concepts:

- **Brand image and communication testing**: before launching a large communication campaign, we perform a pre-test of the campaign to ensure that the message is well understood and clear, and that the campaign will generate impact. After the media campaign went live, we test among a representative sample of the target group if the communication campaign had impact (seen, know which brand, liking, message take out…).
- **Concept testing**: before launching a new service or product, it is tested among consumers to be sure it is relevant for them and there is a market potential for us.
- **Understanding of customer needs and behaviors**: to better understand consumers and the new trends, we perform market research to unveil their needs and how they are behaving.
- **Market penetration of products and services and benchmarks with regards to the competition:** measure the penetration of products and services and define their clientship in order to have a good view on our position vs competitors.
- **Satisfaction and loyalty:** surveys to measure the satisfaction level of our customers or of the customers of competitors with regards to different products or services.

We sometimes also cooperate with research partners:

- Some of our research partners perform market surveys, orientated towards data subjects in our customer and user database, on our behalf. These market surveys are sent out through different communication channels (SMS, email and pop-ups on the website and in Proximus applications) or are conducted through interviews (face to face interviews, interviews via digital means or phone interviews);
- Other research partners of ours are only involved in the recruitment of participants that match the target profile for specific market surveys; and
- Our research partners can also provide us with results of market surveys oriented towards data subjects within their own database.

6.3.3. Comply with legal dispositions

6.3.3.1. Legal obligation to store and to share traffic data and other location data other than traffic data (art. 121/8, 122, art. 123 and art. 127/1, §2 Belgian Electronic Communications Act)

Which categories of personal data will we use?

- **Observed or generated data:** Personal data in the context of electronic telecommunications.

What justifies this processing activity?

This processing activity is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations foreseen in art. 121/8, 122, art. 123 and art. 127/1, §2 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

The Belgian Electronic Communications Acts foresees in different retention periods, depending on the types of data that are stored:

- **Identifiers of both the source and the destination of the communication, exact date and time of the beginning and the end of the communication and location of the terminal equipment of the communicating parties at the beginning and at the end of the communication and other location data:** 4 months from the date of the communication and – in case of specifically identified fraud or specifically identified malicious use of the network – for as long as needed to analyse and mitigate this fraud or malicious use.
- **Phone number at the source of the incoming communication, IP address, timestamp and gate used for sending the incoming communication and exact date and time of beginning and end of the communication:** 12 months from the date of the communication and – in case of specific malicious use of the network – for the period needed to process this malicious use of the network.

With whom do we share this data?

- Internally, your traffic data and other location data can only be processed by Proximus collaborators in charge of managing telecommunications traffic, combating fraud or malicious use of the network, complying with legal obligations or by members of the Coordination Cell (each service has only access to the strict necessary).
- The following official authorities might be informed of (parts of) your traffic data and other location data in the context of their respective competences: (1) Belgian Institute for Postal Services and Telecommunications ("**BIPT**"), (2) Telecom Mediation Service, (3) Belgian Competition Authority, (4) Judicial authorities or the Council of State.
- Your location data can be shared with the management centers of emergency services offering on-site aid in case of an emergency communication.

- The following official authorities might request access to your traffic data and other location data, under specific circumstances prescribed by law: (1) Intelligence agencies and security services, (2) Authorities competent for the prevention of serious threats to public security, (3) Authorities responsible for safeguarding vital interests, (4) Authorities competent for investigating security breaches, (5) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of an infringement committed online or through an electronic communications network or service, (6) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of a serious crime, (7) Administrative authorities responsible for safeguarding an important economic or financial interest of the EU or Belgium, (8) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of a criminal offence, (9) the BIPT, (10) Authorities legally authorised to re-use data for purposes of scientific or historical research or for statistical purposes.

To comply with its legal obligation to take appropriate, proportionate, preventive and curative measures to detect fraud and malicious use of its network and services and to enable centres of emergence services offering on site aid to treat an incoming emergency communication, Proximus stores traffic data and other location data. Proximus has a legal obligation to store traffic data and other location data in order to:

- detect fraud or malicious use of the network or the service and to both identify the source and the identity of the perpetrator; and
- enable management centres of emergency services offering on site aid to treat an incoming emergency communication.

The Belgian Electronic Communications Act imposes on Proximus not only (in most cases) which personal data it must store and for how long, but also who within the company may process the data and to which other official authorities the data could be transmitted, when requested and under specific circumstances.

6.3.3.2. Processing of data based on art. 125 Belgian Electronic Communications Act

Which categories of personal data will we use?

- **Observed or generated data:** Personal data in the context of electronic telecommunications, Technical identifiers, Location data of an end-user's terminal equipment, Volume usage information

What justifies this processing activity?

In the case Proximus processes your personal data to offer you a service aiming at preventing the reception of unsolicited electronic communications, when this processing is not justified by Proximus' legal obligation or legitimate interest to prevent fraud: your consent (art. 6(1)(a) GDPR).

Processing of your personal data in the context of a request of the BIPT on demand of the the judicial police officer of the Missing Persons Unit of the federal police: protection of a vital interest (art. 6(1)(d) GDPR).

In the context of the processing of personal data to enable the intervention of aid- and emergency services: our legitimate interest (article 6(1)(f) GDPR).

Processing of personal data for the prevention of fraud committed by means of messages using telephone numbers, such as SMS or MMS messages, as authorized by article 125, §1, 7° of the Belgian Electronic Communications Act: our legitimate interest (article 6(1)(f) GDPR).

Processing of personal data in the context of the collaboration obligation towards authorities: our legitimate interest (article 6(1)(f) GDPR).

For what purposes will your personal data be processed?

- To enable intervention of aid and emergency services;
- When the BIPT processes this data in the context of its general supervision and control mission or by order of the investigating judge, public prosecutor or on request of the department head of the state intelligence and security services, the judicial police officer of the Missing Persons Unit of the federal police;
- When the Telecom Mediation Service processes this data in the context of his legal investigative tasks;
- When officials authorised by the Minister of Economy in the context of their legal investigative competences process this data;
- To offer end users services consisting of preventing the reception of unsollicited electronic communications; and
- When operators process this data with the sole purpose of combating fraud committed through messages using telephone numbers. This includes the anti-smishing platform set up by Proximus in the scope of its Cyber Security Program (see our specific privacy notice related to network fraud prevention for further information about how we process personal data in the context of our actions to combat fraudulent messages over mobile text messages (SMS/MMS)).

With whom do we share this data?

- Internally, your data can only be processed by Proximus collaborators in charge of managing telecommunications traffic, combating fraud or malicious use of the network, complying with legal obligations or by members of the Coordination Cell (each service has only access to the strict necessary). The following official authorities might request access to your personal data in the context of electronic telecommunications, under specific circumstances prescribed by law: (1) the BIPT, (2) the Telecom Mediation Service or (3) Officials authorized by the Minister of Economy, (4) Belgian Competition Authority and (5) Judicial authorities of the Council of State. Within the scope of their competence, they can be informed of relevant traffic and billing data with a view to settling disputes, including interconnection and billing disputes.

Article 124 of the Belgian Electronic Communications Act provides for the principle of telecommunications secrecy. This means that, in principle, no one may learn about any information related to the electronic communication (its content, the identity of persons concerned, or

information related to the communication) without the consent of all persons, directly or indirectly, concerned by the communication.

In some circumstances however, the principle of telecommunications secrecy can be overruled, namely:

- in the specific circumstances as described in articles 122 and 123 of the Belgian Electronic Communications Act (more detailed information can be found in section "6.3.3.1. Legal obligation to store and to share traffic data and other location data other than traffic data (art. 121/8, 122, art. 123 and art. 127/1, §2 Belgian Electronic Communications Act)");
- when allowed or imposed by means of law;
- to ensure the security and good functioning of the electronic communications networks and services, and in particular to detect and analyse a potential or actual attack on that security, including to identify the origin of that attack (more detailed information can be found in section "6.3.6.2. Network and information security");
- when it concerns actions to monitor and verify the good functioning of the network and to ensure the optimal performance of the electronic communications service (more detailed information can be found in section "6.3.6.3. Network management");
- to enable the intervention of aid and emergency services;
- when it concerns actions to combat fraud committed through messages using telephone numbers (e.g. smishing and spoofing) (see our specific privacy notice related to network fraud prevention for further information about how we process personal data in the context of our actions to combat fraudulent messages over mobile text messages (SMS/MMS)); and
- when actions are taken by certain official authorities, as determined by law.

6.3.3.3. Legal obligation to store and to share personal data processed or generated in the context of the offering of networks or services to end users (art. 126 and art. 127/1, §3 Belgian Electronic Communications Act)

Which categories of personal data will we use?

- **Collected data:** Identification and contact information, National registry number or official external identifier other than the national registry number.
- **Observed or generated data:** Personal data in the context of electronic telecommunications, Location data of an end-user's terminal equipment, Product and service subscription information, Technical identifiers.

What justifies this processing activity?

This processing activity is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations foreseen in art. 126 and art. 127/1, §3 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

- As a principle, we will store your personal data for this purpose as long as the electronic communications service is used + 12 months after the end of the service.

- Some personal data that is related to a specific session (e.g., IP address at the source of the connection and identifiers of the terminal equipment of the end user like IMEI, PEI and MAC) will only be stored during the session + 12 months after the end of the session.

With whom do we share this data?

The following official authorities might request access to your personal data, under specific circumstances prescribed by law: (1) Intelligence agencies and security services, (2) Authorities competent for the prevention of serious threats to public security, (3) Authorities responsible for safeguarding vital interests, (4) Authorities competent for investigating security breaches, (5) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of an infringement committed online or through an electronic communications network or service, (6) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of a serious crime, (7) Administrative authorities responsible for safeguarding an important economic or financial interest of the EU or Belgium or (8) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of a criminal offence.

Proximus has a legal obligation to store certain data, defined by law, when this data is processed or generated in the context of the provisioning of electronic communication networks or electronic communication services. These data include data identifying the end user of the network or service (e.g. first name and last name, national registry number,…), data identifying the date, time and location of the activation of the service (e.g. date and time of the activation of the service, physical address of the point of sales where the service was activated,…) as well as data identifying the subscription and the terminal equipment (e.g. IMSI, IMEI, MAC,…).

Proximus stores this data for the period prescribed by law and during this retention period, it is possible for some official authorities to request access to (some of) this data, under the conditions prescribed by law.

6.3.3.4. Legal obligation to store and to share personal data for the purpose of safeguarding national security, combating serious crime, preventing serious threats to public security, and protecting the vital interests of a natural person in certain geographical areas determined by law (art. 126/1 to art. 126/3 and art. 127/1, §4 Belgian Electronic Communications Act)

Which categories of personal data will we use?

- **Collected data:** Identification and contact information, National registry number or official external identifier other than the national registry number.
- **Observed or generated data:** Personal data in the context of electronic telecommunications, Location data of an end-user's terminal equipment, Product and service subscription information, Technical identifiers.

It is important to note that the categories of personal data described above, will **only** be stored **for certain geographical areas determined by law**:

- Judicial districts that meet established criteria regarding the number of offences committed;
- Police districts that meet established criteria regarding the number of offences committed and are part of a judicial district that, in turn, does not meet established criteria regarding the number of offences committed;
- Zones with a threat level '3';
- Areas particularly exposed to threats against national security or for the commission of serious crime (e.g., harbors, railway stations, airports, prisons, nuclear sites…);
- Zones where there is a potential serious threat to the vital interests of the country or the essential needs of the population (e.g., highways, town halls, the royal palace, hospitals, the National Bank of Belgium…); and
- Zones where there is a potentially serious threat to the interests of international institutions established on the national territory (e.g., embassies, EU and EEA buildings, buildings of NATO and UN…).

What justifies this processing activity?

This processing activity is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations foreseen in art. 126/1 to art. 126/3 and art. 127/1, §4 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

- Most of the time, we will store your personal data for this purpose for a period of 12 months from the date of the communication.
- Data relating to the date and time of connection of the terminal equipment with the network due to the fact that this equipment is started up and data relating to the date and time of disconnection of the terminal equipment with the network due to the fact that this equipment is shut down, will be stored for a period of 6 months after it has been generated.
- In specific cases determined by law, a different retention period applies (from 6 months from the date of the communication to 9 months from the date of the communication).

With whom do we share this data?

The following official authorities might request access to your personal data, under specific circumstances prescribed by law: (1) Intelligence agencies and security services, (2) Authorities competent for the prevention of serious threats to public security, (3) Authorities responsible for safeguarding vital interests or (4) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of a serious crime.

Certain data - either collected, processed, or generated in the context of the telecommunications networks and services provided by Proximus - may be of great importance in safeguarding national security, combating serious crime, preventing serious threats to public security and protecting the vital interests of natural persons.

Therefore, Proximus is legally obliged to store certain personal data allowing for the identification of end users, of their terminal equipment and of the use of the network or service by these end users and to make this data available to certain official authorities for the abovementioned purposes.

The legal storage obligation, however, is subject to criteria determining certain geographical areas.

6.3.3.5. Legal obligation to store and to share personal data for the purpose of direct or indirect identification of subscribers of an electronic communications payment service (art. 127 and art. 127/1, §3 Belgian Electronic Communications Act)

Which categories of personal data will we use?

- **Collected data:** Identification and contact information, National registry number, Official external identifier other than the national registry number, Personal characteristics.
- **Observed or generated data:** Personal data in the context of electronic telecommunications, Location data of an end-user's terminal equipment, Product and service subscription information, Technical identifiers, Financial and billing information.

What justifies this processing activity?

This processing activity is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations foreseen in art. 127 and art. 127/1, §3 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

We will store your personal data from the date of the activation of the service until 12 months after the termination of the service.

With whom do we share this data?

The following official authorities might request access to your personal data, under specific circumstances prescribed by law: (1) Intelligence agencies and security services, (2) Authorities competent for the prevention of serious threats to public security, (3) Authorities responsible for safeguarding vital interests, (4) Authorities competent for investigating security breaches, (5) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of an infringement committed online or through an electronic communications network or service, (6) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of a serious crime, (7) Administrative authorities responsible for safeguarding an important economic or financial interest of the EU or Belgium or (8) Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of a criminal offence.

Proximus has a legal obligation to store certain personal data allowing the identification of the subscribers of an electronic communications payment service, so that the official authorities that are entitled to request access to certain data can identify the subscriber.

Proximus is legally obliged to store these data throughout the entire duration of the activation of the service and for 12 months after the termination of the service.

6.3.3.6. Location sharing trough AML with Belgian emergency centers

Which categories of personal data will we use?

- **Collected data**: Identification and Contact information.
- **Observed data**: Location data (collected through the use of the mobile network by you).

What justifies this processing activity?

This processing activity is necessary to comply with a legal obligation (art. 6(1)(c) GDPR), namely the obligations foreseen in art. 107 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

We process and disclose this data to the emergency services as long as you have a subscription with Proximus.

With whom do we share this data?

Your location data is shared with Belgian emergency centers (medical emergency service, fire department, police station,…).

Proximus is required by law to disclose your identification and contact information and location data to the emergency services when you place an emergency call. During an emergency call, every phone supporting Advanced Mobile Location (AML) can transmit the most accurate position possible to the emergency centers. The location information is only sent to the emergency centers when you call 112 or 101 (or the old number, 100, which is no longer promoted). The transmission of location data complies with Belgian law and is only used for efficiently locating an incident.

In addition to this location data, we also provide them with the following information: your phone number, your name, first name (and, if available, the initial or initials of your first name), or the name of the company, body or firm, an indication of whether your number is used for fixed or mobile service (nomadic use is also indicated if we have this information) and your geographical coordinates. For fixed electronic services, these include the street name, house number, box number, postcode and municipality where the service is installed. For mobile services, they include the street name, house number, box number, postcode and municipality where you are established.

6.3.3.7. Access of emergency services to the Central Number Database (CNDB)

Which categories of personal data will we use?

- **Collected data**: Identification and contact information
- **Observed or generated data**: Product and service subscription information

What justifies this processing activity?

This processing activity is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations foreseen in article 106/2 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

Your personal data is processed by the Central Number Database as long as you are a subscriber with Proximus. Upon termination of the subscription, the Central Number Database permanently deletes the personal data, provided you do not become a customer of another operator.

With whom do we share this data?

Your data will be shared with the emergency services as defined in article 107, §1, a. of the Belgian Electronic Communications Act, namely the medical emergency service, the fire fighter services, the police services and the civil protection, via the Central Number Database.

To comply with its legal obligation, Proximus has a legal obligation to give access to the Central Number Database, a database established together with other Belgian operators providing public telephony services, to emergency centers. The Central Number Database centralizes subscriber data of all operators. The types of subscriber data centralized in the Central Number Database is stipulated by law and entails i) the phone number, ii) the first name and last name and the initials, if any, iii) the street, house number, box number, postal code and city of installation of the product (in case of a fixed product) or where the subscriber resides (in case of a mobile product), iv) the type of phone product (i.e. mobile phone number or fixed line number) and v) the name of the operator (article 106/2, §3 Belgian Electronic Communications Act).

Management centers of emergency services offering on-site aid in case of an emergency communication are connected to the Central Number Database, so they have immediate access to the subscriber data belonging to the caller in case of an emergency call. Based on this information, the management center can quickly identify and locate the caller. For more information about the sharing of location data with Belgian emergence centers, see the section “6.3.3.6. Location sharing through AML with Belgian emergency centers”.

6.3.4. Directory management

Which categories of personal data will we use?

- **Collected data:** Identification and contact information, profession information.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to appear in public telephone directories and directory assistance services.

If you consent to this publication, Proximus might have to further share your data, as it is necessary to comply with a legal obligation (art. 6(1)(c) GDPR), namely the obligations foreseen in art. 45 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

We make your data available to the people who draw up and distribute the telephone directory or offer a directory assistance service via the Central Number Database as long as

you have not changed your preferences in this regard and/or withdrawn your consent for the inclusion of your business activity.

With whom do we share this data?

Any company which would draw up and distribute a telephone directory or offer a directory assistance service. This sharing takes places via the Central Number Database (CNDB).

How can I withdraw my consent?

You can always withdraw your consent, at any time, either by email to gids@proximus.com or annuaire@proximus.com. You can also withdraw your consent by using the webform on the Proximus website or by adjusting your privacy settings in MyProximus Web or MyProximus in the Proximus+ App.

For more information on the various ways to exercise your rights, you can consult section 11 below.

By default, your contact information is not included in directory services or telephone directory. If you wish to have your contact information published free of charge in directory services or telephone directory, we invite you to modify your preferences in MyProximus. You may also, if you are a natural person, consent to the inclusion of your professional activity in telephone directories or directory enquiry services in MyProximus.

If you have expressed the wish to have your contact information published in directory services or telephone directory, we are required by law to make them available to the people who draw up and distribute the telephone directory or offer a directory assistance service via the Central Number Database.

In this case, we provide them with the following information: your phone number, your name, first name (and, if available, the initial or initials of your first name) or the name of the company, body or firm and your address. For fixed electronic communications services, these include the street name, house number, box number, postcode and municipality where the service is installed. For mobile services, they include the street name, house number, box number, postcode and municipality where you are established. If you are a natural person, and provided we have your consent to do so, we may also disclose to them your professional activity for inclusion in telephone directories or directory enquiry services. You have the right to access and rectify your data at any time via MyProximus.

Note that some directories are likely to offer reverse search features (other than a search based on your name or location): search by phone number, by keyword, by professional activity, etc. Please consult the providers of directory and directory enquiry services for more information on this subject.

We make your data available to the people who draw up and distribute the telephone directory or offer a directory assistance service via the Central Number Database as long as you have not changed your preferences in this regard and/or withdrawn your consent for the inclusion of your business activity. You can change your preferences and/or withdraw your consent for the inclusion of your professional activity in telephone directories or directory enquiry services at any time via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy).

6.3.5. Sale of anonymized reports (aka location analytics)

Which categories of personal data will we use?

- **Observed or generated data**: The network location data used for the analytics reports have been aggregated, anonymized and extrapolated. No personal data or data on individuals are used in the context of the analytics reports.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to anonymize the network location data as foreseen by article 123 of the Act of 13 June 2005 on electronic communications which allows for the processing of electronic communication data (including location data) that have been anonymized.

How long will we process this data for this purpose?

As the network location data have been anonymized, they are out of scope of the GDPR and the obligation to have a determined retention period does not apply.

With whom do we share this data?

The anonymized, aggregated, and extrapolated location analytics reports are part of the analytics solutions and are shared with customers of the Proximus MyAnalytics platform. We do not share individual location data.

How can I object?

You can object to the processing of network location data for the creation anonymized analytics reports in the My Proximus environment where you have the possibility to submit such a request. You can find this under my account/my privacy/mobile data network. For more information on alternative ways to exercise your rights, you can consult section 11 below.

The network location data is aggregated, anonymized and extrapolated to create an analytics report. No individual personal data or personal preferences are collected, shared or resold in any way.

We are active in the analytics market and offers solutions revolving around anonymised location reports based on the network location data of devices on the Proximus mobile network. Every activity of a mobile phone on the Proximus mobile telecommunications network generates network location data. This location information makes it possible to determine the antenna tower through which a mobile phone is connected to the Proximus mobile network. When a phone is off or in airplane mode, no network location information is received. Unlike e.g. GPS data, this is not accurate location data and therefore it can never be deduced where exactly a cell phone is located within the coverage area. For example, it cannot be deduced from this data whether a particular person has been to a particular restaurant, or shop, bakery, …. The network location data are aggregated, anonymized, and extrapolated before creating the analytics reports. The mobile location data are processed to create anonymous, aggregated reports to report on visitor numbers, the origin of visitors and/or the flow of persons in a certain area or during a certain period. In order to ensure the anonymity of the analytics

reports, a threshold of 30 persons is used. Consequently, an analytics report can only be created if there are at least 30 persons in an area.

Local authorities, event organisers or entrepreneurs are interested in such reports in order to obtain information, for example, about the number of visitors at a particular location.

6.3.6. Fraud prevention and network security

6.3.6.1. Detection and prevention of telecommunications fraud

Which categories of personal data will Proximus use?

- **Collected data**: Identification and contact information, IT and telecom product and service subscription information, Customer interactions.

- **Observed or generated data**: Internal identifiers, Technical identifiers, Product and service usage information, Hardware information, Billing information, Personal data in the context of electronic communications, Network location data, Consumption habits.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to ensure the security and integrity of our telecommunications network and services, to protect our reputation and financial interests, as well as protecting our customers. Regarding personal data which are traffic data, their processing for this purpose is allowed under articles 122, §4, paragraph 2, and 125, §1, 7°, of the Belgian Electronic Communications Act.

The necessity of the processing for the performance of the contract to which you are a party (art. 6(1)(b) GDPR). Regarding personal data which are traffic data, their processing for this purpose is allowed under article 125, §2, of the Belgian Electronic Communications Act.

This processing of some of the traffic data used for this purpose is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations to prevent fraudulent activities foreseen in articles 121/8 and 122, §4, paragraph 1, of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

We retain your personal data for as long as necessary to detect, investigate and stop cases of telecommunications fraud, and to comply with our legal obligation to retain certain traffic data, as explained in section 6.3.3.1. “Legal obligations to store and to share traffic data and other location data other than traffic data (art. 121/8, 122, art. 123 and art. 127/1, §2 Belgian Electronic Communications Act)”.

With whom do we share this data?

For this purpose, your personal data will be processed by our internal departments involved in fraud detection and prevention.

Besides, third-party service providers who support us in monitoring and analyzing the network traffic may also process your personal data.

To investigate suspicious activities spanning across multiple networks or countries, we may collaborate and share limited personal data with another Belgian or foreign telecom operator.

If there's a confirmed case of smishing, we might share specific details related to confirmed cases of smishing (such as detected malicious domains) to Centre for Cyber Security Belgium (CCB).

Lastly, we may have to share your personal data with official authorities in the context of our legal obligations. Please refer to section "6.3.3. Comply with legal dispositions" for more information.

How can I object?

In the case where the processing of your personal data is based on our legitimate interest, if you have a specific reason (motivated request), you can object to our use of your personal data for this purpose. Unless we have compelling grounds to continue using it, we will stop using it. For more information on the various ways to exercise your rights, you can consult section 11 below.

As an electronic communications provider, '**telecommunications fraud**' is a big concern for us. This notion covers practices where fraudsters abuse our telecommunications products and services to try to illicitly acquire money or other advantage from us or from our customers.

To defend ourselves and our customers, we adopt a multidimensional approach to detect and prevent telecommunications fraud.

To detect anomalies or unusual activities that may indicate fraud, we analyze information generated in the context of the use of our telecommunications products and services. This can be done by:

- setting up rules to detect known types of fraud (such as 'PBX hacking', where fraudsters gain unauthorized access to a company's 'Private Branch Exchange' system, allowing them to make long-distance or international calls billed to the compromised company, or 'International Revenue Share Fraud' where attackers artificially inflate traffic to international premium-rate numbers causing significant financial losses);
- comparing the current usage of our products and services against historical data to detect deviations (for example, if one of our customers suddenly starts making an unusually high number of international calls, it could be a sign of fraudulent activity);
- monitoring SIM cards activity, for example by detecting frequent changes of SIM cards in a device which can indicate SIM swapping attacks; or
- monitoring technical identifiers (such as IP addresses or device identifiers) to detect fraud at the level of the device or unauthorized access to customer accounts.

When suspicious activities are detected, we need to take actions to protect us and our customers. Depending on the type of alert, we may take an automated response to temporarily suspend the affected product or service until our internal departments in charge of fraud detection and prevention verify the alert. In other cases, the suspicious activity will first be investigated by the concerned department who will then define the necessary measures to stop it.

It is also possible that we alert our customers about suspicious activities on their account so that they can take protective actions.

Likewise, we also define usage thresholds for activities like call duration, number of SMS sent, or data usage, triggering alerts to our customer when the threshold has been exceeded. This allows us to

detect suspicious, unusual usage and violations of our General Conditions and prevent you from getting an unpleasant surprise when you see the amount of your next invoice.

We may also have to report fraudulent activities to competent authorities and collaborate with them to investigate such cases. Please refer to section "6.3.3. Comply with legal dispositions" for more information about how we store personal data and share them with official authorities in the context of our legal obligations.

Please refer to our specific privacy notice related to network fraud prevention for further information about how we process personal data in the context of our actions to combat fraudulent messages over mobile text messages (SMS/MMS).

6.3.6.2. Network and information security

Which categories of personal data will we use?

- **Observed or generated data**: Personal data generated in the context of transmitting electronic communications.

What justifies this processing activity?

This processing is necessary for the performance of the contract (article 6(1)(b) GDPR). The processing of personal data in the context of this purpose that extends beyond what is strictly necessary for the performance of the contract is based on our legitimate interest (article 6(1)(f) GDPR) to manage the risks relating to the security of our networks and services as foreseen by article 107/2 §1 of the Belgian Electronic Communications Act. The processing of traffic data for this purpose is allowed by Article 122 §4/1 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

The personal data processed in the context of network and information security can be retained for a period of 12 months in accordance with article 122 §4/1 of the Belgian Electronic Communications Act except in cases of a potential or actual attack on the network where the personal data can be retained for as long as necessary to handle the attack.

With whom do we share this data?

We may share the data with competent governmental authorities in accordance with article 122 §4/1 of the Belgian Electronic Communications Act.

How can I object?

In the case where the processing of your personal data is based on our legitimate interest, if you have a specific reason (motivated request), you can object to our use of your personal data for this purpose. Unless we have compelling grounds to continue using it, we will stop using it. For more information on the various ways to exercise your rights, you can consult section 11 below.

6.3.6.3. Proximus is committed to guarantee the uninterrupted availability of our services. An important aspect in this commitment is the safeguarding of our networks through a range of different security measures against any potential threats that could cause service disruptions. Furthermore, these security measures also aim to protect the (personal) data of our customers that pass through our networks, ensuring it remains secure against any threats. Under the provisions of article 122 §4/1 of the Belgian Electronic Communications Act, traffic data may be processed for the purpose and in particular to identify the origin of an attack on the network. Network management

Which categories of personal data will we use?

- **Observed or generated data**: Personal data generated in the context of transmitting electronic communications, Network location data.

What justifies this processing activity?

This processing is necessary for the performance of the contract to which you are a party (art. 6(1)(b) GDPR). This processing of traffic data is allowed by Article 125 §1. 2° of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

The personal data processed in the context of this purpose will be retained for as long as necessary for the transmission of the communication.

With whom do we share this data?

We may share the data with companies that assist us in the context of network management and network provisioning.

Proximus is committed to ensuring the optimal performance of our telecommunication networks and services. To this end, we analyse information relating to the use of the telecommunication networks with the aim of resolving and/or preventing network issues.

Through this analysis, we can identify when an outage occurs in our mobile network, when our fixed network is overloaded or threatens to become congested, or when the quality of certain connections is not optimal. By studying and analyzing network usage, we can respond quickly to prevent these situations and perform effective network management.

You can find more information on the management of fixed and mobile internet traffic on our network through this link.

6.4. When you have ceased to be a customer or user

6.4.1. Archiving purposes

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Customer Interactions, Financial data; Billing information.
- **Observed or generated data:** History of product and service subscription information

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to defend our rights in case of contractual liability claims.

How long will we process this data for this purpose?

10 years after the end of the contractual relationship with Proximus (as foreseen in art. 2262bis of the Belgian Civil Code).

With whom do we share this data?

This data is not shared with any third-parties.

Sometimes a conflict might arise between us and, for example, one of our (ex-) customers. While we strive to resolve most such disagreements before further escalation, regrettably this cannot always be avoided. For this reason, we need to keep an archive of different categories of personal data relating to your contractual relationship in order to potentially defend our rights and interests in case of legal steps being undertaken.

7. For what marketing and sales purposes do we use your personal data?

In this section you can find more information about the marketing and sales purposes for which we process personal data. The purposes are divided in different categories. For each purpose there is a summary table containing the most important information such as what categories of personal data, the legal basis on which the processing is based, the retention period of the personal data and where relevant the categories of third parties with whom the personal data is shared or information about how to exercise specific data subject rights in case it differs from the general ways to exercise data subjects rights that are explained in section 11 of this privacy notice. The summary table is followed by an explanation of the purpose.

7.1. When you're not a customer yet

7.1.1. Collection of contact data

7.1.1.1. Direct collection of contact data via events, …

Which categories of personal data will we use?

- **Collected data**: Identification and contact information.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to collect your data when you are attending an event for a specific purpose (e.g. to manage your subscription to a certain event, to participate to a contest or a game, to keep you informed on (a specific) product(s) or service(s),…).

How long will we process this data for this purpose?

Your contact data will be stored and processed for this purpose for 3 years after you have given your consent.

A proof of your consent will be stored for the duration of the consent (3 years) + 5 years, which is the prescription period for any actions before the Belgian Data Protection Authority.

With whom do we share this data?

Depending on the purpose for which your contact details were collected, your data may be shared with call centers working on our behalf (in the context of telemarketing campaigns), subsidiaries of the Proximus Group or other partners.

How can I withdraw my consent?

You can always withdraw your consent, at any time, to the processing of your contact details, collected via an event, by addressing your request to Proximus DPO at the e-mail address privacy@proximus.com. For more information on the various ways to exercise your rights, you can consult section 11 below.

We regularly organize events or attend to events to present and promote new or existing products and services.

If we organize an event for which advance registration is required, certain contact data will be requested from you at the time of registration. This information will be used to contact you in the run-up to and possibly also after the event. If you have agreed to this, the data can also be used to keep you informed about certain products and services.

When you attend an event organized by us or where we are present, you may also voluntarily leave your contact data, for example in order to be kept informed of a product or service that interests you or similar products and services, or because you are taking part in a contest.

The collection and further processing of your contact data will be based on your consent.

Depending on the purpose for which your contact data is collected, the retention period and any parties with whom your contact data is shared will also vary. You will be informed of the specific retention period and the specific partners with whom your personal data will be shared prior to the collection of your contact data.

It is always possible to withdraw your consent for the processing of your contact data. If there is a specific e-mail address to which your request can be sent, you will be informed about this prior to the collection of your contact data. In all other cases, you can send your request to privacy@proximus.com. Please refer to section 11 below for more information about your right to object.

7.1.1.2. Acquisition of prospect data relating to potential residential customers

Which categories of personal data will we use?

- **Obtained data**: Identification and Contact information, Personal characteristics, Segmentation information.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR), acquired via the third parties involved in the collection of your personal data.

How long will we process this data for this purpose?

In practice, these third parties deliver monthly databases which we use only in the context of one campaign – we do not import this data into our own systems for further reuse.

The telecommunications sector is competitive, and customers are more and more open to changing operators to get a better deal. For that reason, we strive to broaden our spectrum of new potential customers on a regular basis.

On top of our actions to collect data of potential customers via our own actions and events, we also acquire some data for these purposes from third parties. In practice, we call upon the services of a few such third parties:

- TheWave (formerly known as Gowie)
- EDM (part of The Data Agency)
- Fiberklaar and Unifiber (Proximus joint ventures deploying fiber and organizing prospecting actions in this domain)
- bpost

In practice, these third parties deliver monthly databases which are only used in the context of one campaign – we do not import this data into our own systems for further reuse.

How is this data collected? These third parties might have their own sources (which are subject to the same stringent rules on consent collection) or organize contests and events of their own, through which your consent might be collected.

For more information on the actual marketing activities based on the data acquired, among others, from third parties, see the section "7.1.2. Proximus-led commercial prospection" below.

7.1.1.3. Acquisition of data relating to potential and existing professional customers

Which categories of personal data will we use?

- **Obtained data**: Identification and contact information (e.g. list of company directors, shareholders, authorized representatives and contact persons, their first name, last name, business address, fixed and mobile phone number, email address, website), Personal characteristics, Profession information.

What justifies this processing activity?

Personal data about professional customers and prospects acquired from third parties may be processed by us for different purposes (see below). The lawful bases for such processing are detailed in the relevant sections of this privacy notice but can be summarized as follows:

- Our legitimate interest (art. 6(1)(f) GDPR) to ensure that we do business in a safe way by better understanding the companies with which we are or may be entering into business; and to promote our brand, as well as relevant products and services, to existing customers.

- Your consent (art. 6(1)(a) GDPR), acquired by the third parties involved in the collection of your personal data or directly by us.

How long will we process this data for this purpose?

The retention periods of the personal data acquired from third parties depends on the purposes for which we process it (see below). The respective retention periods are detailed in the relevant sections of this privacy notice.

How can I object?

You can always object (without motivation) to the use of your personal data for direct marketing purposes, including profiling to the extent that it is related to such direct marketing. If you have a specific reason (motivated request), you can object to our use of your personal data for the other purposes described below. Unless we have compelling grounds to continue using it, we will stop using it. For more information on the various ways to exercise your rights, you can consult section 11 below.

To strive in the telecommunications and IT industry, we must ensure that we carry out business in a safe and efficient way. This is why we collect and process data in order to know the companies we are in business with or might enter into business with, ensure that these companies are financially sound, and spread awareness around our products, services, offers and promotions by contacting them directly.

If you are the director, shareholder, authorized representative or contact person of an existing or potential professional customer of ours, we may process personal data about you such as your name, business address, phone number, email address, title and function, language, date of birth, etc.

If you represent a one-person company or exercise a liberal profession, we may process company information such as financial information, segmentation information, business information, product and service subscription information which qualify as personal data and fall within the scope of the GDPR.

We acquire some of this data from third parties, including:

- Graydon/creditsafe
- Inoopa
- Smart Profile
- Trends Business Information
- Unizo

We acquire from these third parties and use the data about existing and potential professional customers and their representatives for various purposes:

- Collect additional information about professional customers in order to match it with the existing data in our database and ensure this data remains accurate and up to date (e.g. that companies' details and contact information are up to date, that closed or merged legal entities are removed, etc.).
- Categorize companies in order to obtain insights about their financial situation (e.g. their creditworthiness, solvability, liquidity, suggested credit-limit) or about their potential interests in IT and Telco products.
- Screen companies financially to ensure that we do business with companies which are financially solid and not likely to go bankrupt, have delays in payments, etc.
- Manage credits and take informed decision about granting a credit and defining the credit-limit in light of the financial situation of the company.
- Contact the company's representative or contact person by e-mail or by phone to promote our products, services, offers and promotions that may be of interest to the company. The way we process personal data for direct marketing towards existing customers is further detailed in section "7.2.2. Promotion of our products and services" and towards prospect

customers in sections "7.1.2. Proximus-led commercial prospection" and "7.1.3. Commercial prospection led by indirect sales partners".

Depending on the circumstance, the third party may collect the information directly from the concerned persons via surveys, events or phone calls. In addition, these third parties have their own sources which include official and/or public sources (such as the Crossroads Bank for Enterprises, Belgian Gazette, Chamber of Commerce, National Social Security Office and the Belgian National Bank) or private sources (such as the third party's partners or customers).

7.1.2. Proximus-led commercial prospection

Which categories of personal data will we use?

- **Collected or obtained data**: Identification and contact information.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to be kept informed about Proximus' offers and promotions.

How long will we process this data for this purpose?

Your contact data will be stored and processed for this purpose for 3 years after you have given your consent.

A proof of your consent will be stored for the duration of the consent (3 years) + 5 years, which is the prescription period for any actions before the Belgian Data Protection Authority.

With whom do we share this data?

Proximus' controlled call centers and companies involved in the printing and distribution of promotional flyers, acting as processors (in the context of these campaigns).

How can I withdraw my consent?

Changed your mind after giving your consent? Please use the unsubscribe link in our e-mails, reply STOP if you receive a text message, or contact the Proximus DPO at the e-mail address privacy@proximus.com if you no longer wish to be called, contacted via digital channels, or receive postal mail from us. For more information on alternative ways to exercise your rights, you can consult section 11 below.

Like any other commercial company, we have a vested interest in promoting our products and services, brand, image, and promotions to potential customers who clearly expressed an interest in receiving such communications. To achieve these goals, we will process personal data of prospects who have given their consent to spread awareness around these offers and promotions by contacting them directly, be it by phone, postal mail or e-mail.

We might directly acquire your data and consent (e.g., via consent collection campaigns during music festivals) or we might acquire these data via a third-party (see section "7.1.1.2. Acquisition of prospect data relating to potential residential customers" above).

We are committed to only contacting you at reasonable intervals. For example, telemarketing campaigns which we control will only include a potential residential customer in one campaign per semester, while a potential SME customer might be included on a quarterly basis.

7.1.3. Commercial prospection led by indirect sales partners

On top of our own commercial prospection activities, we also call upon the services of companies specialized in sales to their own audiences, via different channels. These companies apply their own expertise and use their own databases to make sales for multiple different customers across different sectors.

The following companies are authorized to sell our products and services, among the products of their other customers:

- U-Smile
- NEO Group
- Onlyoo

The following companies are also authorized to sell selling our products and services (among the products of their other customers) specifically on their own website on the internet:

- Astel
- DPG Media
- E-contract
- Mijn verhuis
- Mobiel Werkt
- Smooved
- Wikipower

A few important notes:

- These indirect sales partners act – for their prospecting activities – as **separate controllers**.

- The sales representatives from these companies must respect a basic set of rules set out in the "Proximus Indirect Sales Charter", but are otherwise acting in total freedom in the context of these prospecting activities – we have no control over their sales campaigns, whom they target, …

- In any contact, these sales representatives must present themselves as working for one of these indirect sales partners, and **NOT for Proximus**.

- These companies use their own databases, for the benefit of multiple different clients – Proximus does not deliver any personal data to these indirect sales partners.

- Have you been contacted by one of these indirect sales partners and want to exercise your data subject rights? You can contact the specific partner directly.

7.1.4. Proximus Newsletters

Which categories of personal data will we use?

- **Collected data***:* Identification and contact information, Personal characteristics.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to use your data for the newsletter when you subscribe to the newsletter as a prospect.

How long will we process this data for this purpose?

Your data will be processed for 3 years as from the date of the consent.

With whom do we share this data?

Our marketing email providers.

How can I object?

If you want us to stop sending you newsletters, you can do so by using the unsubscribe link in Proximus e-mails. For more information on alternative ways to exercise your rights, you can consult section 11 below.

We have a strong interest in promoting our products, services, and promotions to existing customers and prospects who subscribed to the newsletter. We therefore process your identification and contact data to send out newsletter emails, which contain more information on those products, services, and promotions.

Your personal data is shared with our marketing email providers. These mail service providers take care of sending out the newsletters.

7.2. When you are a customer or user

7.2.1. Creation and enrichment of customer profile

7.2.1.1. Basic segmentation of our customers for direct marketing purposes

Which categories of personal data will we use?

- **Collected (or obtained) data**: Identification and contact information, Personal characteristics, Family and household composition, Customer interactions.
- **Observed or generated data**: Product and service subscription information.
- **Derived data**: Segmentation information, Leisure and personal interests.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to further promote our brand, as well as relevant products and services, to existing customers.

How long will we process this data for this purpose?

For five years after the end of your contractual relationship with Proximus.

How can I object?

You can always object (without motivation) to the use of your personal data for marketing profiling purposes, as well as restrict the channels via which you wish to be contacted, via MyProximus Web and/or MyProximus in the Proximus+ App and opting out from “Marketing

offers and personalized content". For more information on alternative ways to exercise your rights, you can consult section 11 below.

When it comes to direct marketing practices, a company has generally two choices. The first one is to "carpet bomb" its whole eligible customer base, meaning to target everyone with the same marketing message. This is costly and counterproductive for the company, given the limited relevance of such a single common message for most of the target audience, but can also be frustrating for the recipients who might feel spammed with entirely irrelevant offers and promotions.

The second approach is to limit the target audience to the persons to whom your message might actually appeal. This involves having an idea of what might appeal to a specific customer. This in turn requires processing of personal data, such as the products already owned by a customer or the area they live in, to only address the customers to whom a specific offer or promotion might apply. This approach allows to limit the target audience to the customers who are eligible for - and might at least potentially be interested in - a specific offer or promotion. Unsurprisingly, this is our preferred approach.

In practice, we use different types of personal data when preparing a target audience for a specific marketing campaign.

On a more general level, each Proximus customer belongs in one specific market segment. To illustrate this concept, imagine a person subscribing for a family-oriented Flex pack, with multiple mobile phones for their family members. Such a customer will belong to the 'Residential (as opposed to professional) – Family' segment. A single customer can only fit in one unique market segment of this type.

While that level of segmentation provides a first way of excluding some customers to whom a specific campaign would be irrelevant, it is not sufficient to achieve a satisfactory level of relevance for each campaign.

When preparing a campaign, we will thus also consider the information already being processed on our customers. Do you already own a mobile phone subscription with us? You will be excluded from any campaign promoting mobile subscriptions to customers with only a TV or internet line. Have you recently acquired an expensive phone in a joint offer with a Proximus subscription? You will be more likely to be included in a campaign promoting phone insurance. This allows for campaigns which are much more relevant than simply based on a customer's macrosegment.

Finally, the highest level of campaign personalisation involves the actual preferences of the customers. The determination of preferences mostly happens with your consent (see section *"7.2.1.2. Consent-based segmentation of our customers for direct marketing purposes"*); however, it is possible that we build a limited preference profile based on your participation in the Proximus reward program (Proximus For You) or based on your input in explicit surveys.

What are those preferences? Based on the data sources mentioned above, we will slowly build a good idea of your interests. These interests and preferences will be represented in a score from 1 to 10 assigned to your customer profile for different types of dimensions. Did you mention in a specific survey that you attended multiple festivals in recent years? Your 'music lover' score might increase. Did you participate in multiple gaming-related contests in the context of the "Proximus For You" reward program? Similarly, your 'gaming lover' score might also be impacted by this information.

Important note: The vast majority of this preference scoring takes place only with your consent, as the main data used to derive your preferences is your usage of our products and services, as well as

the type of websites or applications you use (see section "7.2.1.2 Consent-based segmentation of our customers for direct marketing purposes").

You can always object to the use of your personal data for marketing profiling purposes, as well as restrict the channels via which you wish to be contacted, via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) and opting out from "*Marketing offers and personalized content*". For more information on alternative ways to exercise your rights, you can consult section 11 below.

7.2.1.2. Consent-based segmentation of our customers for direct marketing purposes

Which categories of personal data will we use?

- **Observed or generated data**: Personal data generated in the context of transmitting electronic communications, TV viewing data.
- **Derived data:** Leisure and personal interests, Preference profile.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to the use of these types of data for the further personalization of our offers and promotions.

How long will we process this data for this purpose?

For five years after the end of your contractual relationship with Proximus.

How can I withdraw my consent?

You can always withdraw your consent, at any time, to the use of your personal data for marketing purposes, as well as restrict the channels via which you wish to be contacted, via MyProximus Web and/or MyProximus in the Proximus+ App. For more information on alternative ways to exercise your rights, you can consult section 11 below.

With your consent, we can go a step further in the customization of our offers and promotions, by enriching your preference profile. For more basic information on how we prepare customer preference profiles for the purposes of building target audiences for marketing campaigns, see section "7.2.1.1. Basic segmentation of our customers for direct marketing purposes" above.

With your consent, we can adapt our offers and your preference profile on the basis of:

- **Certain websites or applications that you visit or use**. We are able to identify the names of these websites or applications based on an analysis of your landline and/or mobile internet traffic as long as you have a Proximus mobile subscription and/or a Proximus internet connection. This allows us to more accurately identify your areas of interest, activities and buying habits. This operation is based exclusively on a limited list of websites and applications. Websites and applications of a sexual, religious or political nature, for example, are excluded. The sole purpose of this operation is to refine the products and services that we offer you. For example, if you regularly visit the Jupiler Pro League website, this information can help us refine our commercial proposals. You might therefore be more interested in our sports

package than in our series package. Under no circumstances do we collect the details of the pages visited/applications used. For example, if you are listening to music via Spotify, we will not be able to identify the artist you are listening to.

- **Data on the usage of your Proximus services (TV, mobile and landline telephony, and/or internet).** When you make a call, we generate data such as the duration of your calls, the start and end time, the numbers called, the date, etc. For example, if you make a large number of international calls, this information can help us refine our commercial proposals. Accordingly, we may offer you an "international call" option the next time the company contacts you. We can also identify the types of programs you watch, record or rent via our TV Proximus service (Pickx) to identify your areas of interest. Similarly, we can identify the model of phone you use to connect to our mobile network or the type of device connected to your modem (printer, game console, mobile phone, etc.), as well as the status of your WiFi connection. For example, if we detect that you have a game console, we can provide you with a technical solution that enables you to improve your gaming experience.

Important note: If there are several users (family members, co-tenants, etc.) sharing a single Proximus subscription (internet connection, TV, etc.), the data on all these users will be combined. This will also be the case if you are the holder of several mobile subscriptions, unless the end users have identified themselves by creating a MyProximus account. When, as the customer, you give your consent to these processing activities, you should therefore also inform the other users of your choice.

You can always withdraw your consent to the use these personal data for marketing profiling purposes via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) and opting out from one or more sources of data under "*Tailor-made Proximus offers*". For more information on alternative ways to exercise your rights, you can consult section 11 below.

7.2.1.3. Consumption profiling for the calculation of the most advantageous tariff plan

Which categories of personal data will we use?

- **Observed or generated data**: Billing information, Product and service subscription information, Product and service usage information, Consumption habits.

What justifies this processing activity?

This processing activity is necessary for compliance with a legal obligation of Proximus (art. 6(1)(c) GDPR), namely the obligations foreseen in arts. 109 and 110/1 of the Belgian Electronic Communications Act.

How long will we process this data for this purpose?

This most advantageous tariff plan is calculated on the basis of your consumption profile for the last year. Only data from the last calendar year is relevant for this purpose.

Belgian telecommunications operators have an obligation to indicate, at least once a year and on a durable medium, which tariff plan would be most advantageous to the users based on their consumption profile. In addition, the users may require the operator – at any time - to indicate which tariff plan is the most advantageous for them. The operator must answer within two weeks at the latest.

In order to be able to provide you this information within that short timeframe, we need to continually establish your consumption profile for the last calendar year.

Keep in mind that since this is necessary for Proximus' compliance with a legal obligation, there is no possibility to object to this processing activity!

7.2.1.4. Market insights analysis

Which categories of personal data will we use?

- **Collected data:** Identification and contact information, Personal characteristics, Family and household composition.
- **Observed or generated data**: Product and service subscription information, Customer interactions.
- **Derived data:** Leisure and personal interests, Preference profile.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to extract current market insights, based on the data already processed for other purposes, and to monetize these insights without having impact on the privacy of the concerned data subjects.

How long will we process this data for this purpose?

Once the data is anonymised, the output will be stored indefinitely. The actual personal data will be processed in line with the segmentation purposes.

As most companies, we have an interest to build our market intelligence by analysing the data we store on our customers and extract statistical insights into e.g., the geographical spread of customers with a specific product, the proportion of customers with a specific preference profile in a certain age range, …

How will we do this? It will of course depend on the exact scenario, but you can imagine the following example: we would like to determine the proportion of "football lovers" in a given municipality. In such a case, we would select customers living in that specific municipality which, first of all, have any sort of preference profile, and then count specifically how many of these preference profiles reflect an interest in football. The final output of this exercise would be a simple statistical report on the proportion of customers with a football preference compared to the entire customer base for that specific municipality.

These anonymous reports could then feed our general market intelligence, leading to potentially more effective advertising and marketing campaigns, but could also potentially be sold to other companies, without affecting the privacy of our customers.

7.2.2. Promotion of our products and services

7.2.2.1. Promotion of our products and services via telephone and e-mail campaigns

Which categories of personal data will we use?

- **Collected data**: Identification and contact information.
- **Derived and inferred data**: Product and service subscription information, Leisure and personal interests, Preference profile.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to further promote our brand, as well as relevant products and services, to existing customers.

How long will we process this data for this purpose?

For five years after the end of your contractual relationship with Proximus.

With whom do we share this data?

Call centres working on our behalf, acting as processors (in the context of telemarketing campaigns).

How can I object?

If you want us to stop contacting you for marketing purposes, please use the unsubscribe link in our e-mails, reply STOP if you receive a text message from us, or contact the Proximus DPO at the e-mail address privacy@proximus.com if you no longer wish to be called by us, be contacted via digital channels or receive postal mail from us. You can also object to the use of your personal data for marketing purposes, as well as restrict the channels via which you wish to be contacted, via MyProximus Web and/or MyProximus in the Proximus+ App. For more information on alternative ways to exercise your rights, you can consult section 11 below.

Like any other commercial company, we have a vested interest in promoting our products and services, brand, image, and potential offers to existing customers. To achieve these goals, we will process customer's personal data to spread awareness around these offers and promotions by contacting them directly, be it by phone or per e-mail.

In practice, these activities take place in two stages:

- First, a list of customers to be contacted in the context of a specific campaign is prepared. Whether you are included in a campaign will depend on the goal of the campaign (what product or service we are promoting) and your preference profile, if there exists one (to determine whether you would be interested in the product or service being promoted, or whether you qualify for a specific action). In some cases, we might launch general campaigns which will target all customers indiscriminately.

- Once the target list has been prepared and you have been included as a potential target, we will process your identification and contact information (relevant to the communication channel used for this specific campaign, e.g., your e-mail address for an e-mail campaign) to deliver the marketing message.

We are committed to only contacting you at reasonable intervals, with different intervals per channel of communication.

It goes without saying that you – the customer – remain in absolute control of your preferences when it comes to Proximus' marketing outreach. You can always object to the use of your personal data for marketing purposes, as well as restrict the channels via which you wish to be contacted, via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) and opting out from "*Marketing offers and personalized content*". For more information on alternative ways to exercise your rights, you can consult section 11 below.

7.2.2.2. Promotion of our products and services online (e.g. on social media)

Which categories of personal data will we use?

- **Collected data**: Personal characteristics.
- **Derived and inferred data**: Leisure and personal interests, Preference profile.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to further promote our brand, as well as relevant products and services, to existing customers.

How long will we process this data for this purpose?

Your personal data will be stored and processed for this purpose as long as you are a Proximus customer, plus 5 years after the end of your contractual relationship with Proximus.

With whom do we share this data?

We do not share your personal data with the social media platform but determine a specific target audience and ask the platform to show a specific advertisement to this target audience.

How can I object?

You can change your settings for advertising via MyProximus Web and/or MyProximus in the Proximus+ App or via www.youronlinechoices.com, or contact the Proximus DPO at the e-mail address privacy@proximus.com. For more information on alternative ways to exercise your rights, you can consult section 11 below.

We can display advertisements about our products and services on social media platforms.

If you have a Facebook, Instagram, Twitter, LinkedIn or Google account, we can display advertisements on these social media platforms about products, services and promotions that might interest you. To this end, we determine a specific target audience by using a number of parameters such as age, gender, interests, and share this target with the provider of a social media platform and ask the provider to show a specific advertisement to this target audience. For example, we may ask a social media platform to show a Proximus advertisement to men between 20 and 25 years with an interest in football. It is important to note that we do not share your personal data with the provider of the social media platform.

If you don't want such online advertisement, you can always object to the use of your personal data for marketing purposes or restrict the channels via which you receive information about our products and services, via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) . You can also change your preference concerning such online advertising via the website www.youronlinechoices.com. For more information about your data subject rights you can consult section 11 below.

If you visit our Facebook page, Facebook can collect personal data about you and link it with other personal data Facebook has collected about you elsewhere. Facebook can use this data to provide us anonymous statistics about the people who visit our Facebook page. For more information and to exercise your privacy rights concerning the data collected by Facebook, please consult Facebook's privacy notice.

Lastly, we also use advertising cookies and trackers on our websites and mobile applications to collect information about your browsing habits on our websites and applications and show you ads on other websites for products and services you may be interested in. Such processing is carried out based on your consent. If you want more information about our use of advertising cookies and how to adapt your preferences or withdraw your consent, please consult our cookie policy.

7.2.2.3. Promotion of our products and services on Pickx (Proximus TV)

Which categories of personal data will we use?

- **Collected data**: Identification and Contact information, Personal characteristics
- **Observed or generated data**: Technical identifiers, Subscription information
- **Derived data**: Consumption habits, Leisure and personal interests, Preference profile.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to further promote our brand, as well as relevant products and services, to existing customers.

How long will we process this data for this purpose?

Identification and contact information and personal characteristics will be processed for as long as you are a Proximus customer.

Other data processed in the context of this purpose is stored for 2 years as of the collection of the data.

With whom do we share this data?

Partners helping us to deliver Pickx services and ThinkAnalytics, the partner who provides us with the recommendation engine in the context of movie or TV program recommendations.

How can I object?

You can always object (without a motivation) to the use of your personal data for this purpose yourself via the options menu on your TV screen or via MyProximus Web or MyProximus in the Proximus+ App (see section 11 below). For more information on alternative ways to exercise your rights, you can consult section 11 below.

Like any other commercial company, we have a vested interest in promoting its products and services, brand, image, and potential offers to existing customers. To achieve these goals, we will process customer's personal data to provide you with personalized recommendations relating to Pickx services (including movie or TV program recommendations) and other Proximus products and services.

It goes without saying that you – the customer – remain in absolute control of your preferences when it comes to our marketing outreach. You can always object (without a motivation) to the use of your personal data for this purpose yourself via the options menu on your TV screen or via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) . For more information on alternative ways to exercise your rights, you can consult section 11 below.

7.2.2.4. Proximus Newsletters

Which categories of personal data will we use?

- **Collected data***:* Identification and contact information, Personal characteristics.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to further promote the brand, as well as relevant products, services and promotions, to existing customers;

How long will we process this data for this purpose?

Your data will be processed for as long as you are a Proximus customer + 5 years after a person has ceased to be a Proximus customer.

With whom do we share this data?

Our marketing email providers.

How can I object?

If you want us to stop sending you newsletters, you can do so by using the unsubscribe link in Proximus e-mails. You can always object (without a motivation) to the processing of your personal data for the purpose of sending out newsletters in MyProximus Web or MyProximus in the Proximus+ App where you have the possibility to submit such a request. For more information on alternative ways to exercise your rights, you can consult section 11 below.

We have a strong interest in promoting our products, services, and promotions to existing customers and prospects who subscribed to the newsletter. We therefore process your identification and contact

data to send out newsletter emails, which contain more information on those products, services, and promotions.

Your personal data is shared with our marketing email providers. These mail service providers take care of sending out the newsletters.

7.2.2.5. Proximus For You – the Proximus Loyalty Program

Note: This processing activity is not applicable to customers of the Scarlet brand.

Which categories of personal data will we use?

- **Collected data:** Identification and contact information.
- **Derived data:** Leisure and personal interests.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to organize a loyalty program offering advantages and surprises to members.

How long will we process this data for this purpose?

The personal data processed in this context will be retained for a period of 2 years after your participation to a contest or deal.

With whom do we share this data?

The contact and identification information can be shared with partners that collaborate with us in the context of the Proximus For You Program to provide the deals, gifts and events to members.

How can I object?

You can always object (without a motivation) to receiving communications in the context of the Proximus For You Loyalty program yourself in the privacy settings via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy). For more information on alternative ways to exercise your rights, you can consult section 11 below.

Proximus For You is our loyalty program offering members numerous exclusive advantages and surprises. The Proximus For You experiences give members the chance to win unforgettable experiences through fun and original contests. The Proximus For You deals grant members the opportunity to benefit from exceptional discounts with our partners, to receive surprises and gifts and have access to exclusive Proximus events. The surprises and gifts can be personalized based on a member's areas of interest through the list of contests, deals and events a member showed interest in. These areas of interest are also used for the purpose of consent-based profiling of Proximus customers for direct marketing purposes in case you have provided your consent to this purpose. You can consult the section on that purpose for more information on the processing of personal data in the context of consent-based profiling of Proximus customers for direct marketing purposes.

In the context of the Proximus For You loyalty program we can send members email and SMS communications as well as push notifications.

7.2.3. Other uses of your customer profile

7.2.3.1. Personalised advertising on TV

Note: This processing activity is not applicable to customers of the Scarlet brand.

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Personal characteristics, Customer interactions.
- **Observed or generated data**: Consumption habits.
- **Derived data**: Segmentation information.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to collect personal data and use it for personalized advertising on the Pickx service.

How long will we process this data for this purpose?

Identification and contact information and personal characteristics will be processed for as long as you are a Proximus customer.

Data related to your consumption habits and segmentation information will be stored for 1 year upon collection of the data.

Data related to your interactions as a customer with Proximus will be kept for 2 years upon the date of the interaction.

How can I withdraw my consent?

You can always withdraw your consent, at any time, by adjusting your privacy settings in MyProximus Web or MyProximus in the Proximus+ App. For more information on alternative ways to exercise your rights, you can consult section 11 below.

By obtaining your consent, we offer you the opportunity to benefit from customized advertising on our TV services, here referred to as Pickx. These ads mainly relate to products and services of third-party companies.

With your consent, we have the possibility to further customize the advertisements on Pickx. This customization is done on the basis of different data groups:

- Administrative data which you have provided to us (language, age, postal code, Proximus services used, etc.).
- We collect information on the use you make of Pickx. These elements consist of information on your use of the Pickx service via your decoder, the Pickx application and its TV service on the Web. This information includes TV programs, films and series that you watch, record or rent (sports, cooking, news, children's programs, etc.) and the actions you perform from your remote control.
- Please note that the analysis of all the programs consulted via the Pickx platform never concerns sexual, religious, or political content.

- Data which we have purchased from external firms, such as statistical data on the neighborhood in which you live, whether the homes have gardens, the type of household you have, etc.

If there are several users (family members, co-tenants, etc.) sharing the same Pickx subscription, the areas of interest identified will only apply to the subscriber's personal profile. This is because the technology is not capable of detecting who is watching a specific type of program. For example, if a member of your family regularly watches Jupiler Pro League matches, football will be added as an area of interest to your profile.

When you give us your consent, you should therefore also inform the other users of your choice.

And what if I change my mind? No problem. You can change your consent at any time via the "privacy" settings of MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) . For more information on alternative ways to exercise your rights, you can consult section 11 below.

7.2.3.2. Targeted advertising on web and in mobile applications (Ads & Data)

Note: This processing activity is not applicable to customers of the Scarlet brand.

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Personal characteristics, Customer interactions.
- **Observed or generated data**: Consumption habits.
- **Derived data**: Segmentation information.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to collect personal data and transmit them to Ads & Data to automatically display targeted ads on websites and applications in the Ads & Data portfolio.

How long will we process this data for this purpose?

Your identification and contact information and personal characteristics will be processed for as long as you are a Proximus customer.

Data related to your consumption habits and segmentation information will be stored for 1 year upon collection of the data.

Data related to your interactions as a customer with Proximus will be kept for 2 years upon the date of the interaction.

With whom does we share this data?

Ads & Data, as a joint controller.

How can I withdraw my consent?

You can always withdraw your consent, at any time, in the following ways: i) by adjusting your cookie settings so that we no longer collect data related to your use of our websites and mobile applications through the Proximus website or the Proximus app; or ii) by adjusting your privacy settings in MyProximus Web or MyProximus in the Proximus+ App. For more information on alternative ways to exercise your rights, you can consult section 11 below.

Proximus and Ads & Data (Harensesteenweg 226, 1800, Vilvoorde, Belgium, KBO: 0809.309.701) process your personal data as joint controllers for purposes of targeted advertising on websites and applications in the Ads & Data portfolio. Ads & Data, an organisation ensuring the collaboration between Belgian providers of advertising space, builds up target groups for advertisements and show personalised advertisements on digital media and television, together with Proximus.

The categories of personal data that Proximus and Ads & Data collect and use, subject to your consent, are:

- Personal data you have shared directly with us, such as name, e-mail address, age, gender, postal code.
- Data collected during your visit to and use of our websites and mobile applications such as unique identifiers (e.g. your IP address), the URL of the pages visited, click behaviour with regard to viewed articles or advertisements.
- Derived data: these are interests that we derive from data at its disposal such as age, gender, postal code, Proximus products and services, ... and possibly your viewing behaviour, characteristics based on statistical and public data. Based on this information, we can for instance deduce that you are a “cooking enthusiast”.

This collaboration means, among other things, that, subject to your consent, we will collect these personal data and transmit them to Ads & Data in an encrypted form. This encryption means that Ads & Data will not be able to identify you directly. Ads & Data then uses this information to build your advertising profile (e.g. sports fan, male, age group, ...). Ads & Data uses this to automatically display, with the help of service providers, targeted ads on websites and applications in the Ads & Data portfolio.
In concrete terms, this means that Proximus and Ads & Data process your personal data for the following purposes and on the basis of the following legal grounds:

- To create personalized online advertising profiles, based on your consent;
- To select personalized advertisements, based on your consent;
- To measure the performance of advertisements, based on your consent.

For these purposes, we will communicate your personal data to Ads & Data in its capacity as joint controller, who will process them into an advertising profile.

You may withdraw your consent for the aforementioned purposes at any time, firstly by adjusting your cookie settings so that we no longer collect data related to your use of our websites and mobile applications either through the Proximus website or the Proximus app, and secondly by adjusting your privacy settings in MyProximus Web or MyProximus in the Proximus+ App. It may also be useful to check whether you have accepted advertising cookies from third parties on other sites or applications on which you surf and on which Ads & Data broadcasts targeted advertisements, a list of these partners can be found on the Ads & Data website.

Ads & Data will share your advertising profile with:

- Processors that process data on our behalf (e.g. IT companies);
- Advertisers who want to use Ads & Data's services to display advertising on our websites and applications.

Ads & Data also shares an identification number from your browser with platforms that provide support services for selecting and displaying targeted advertisements.

Some recipients may be located in countries outside the European Economic Area (EEA). If your encrypted data is transferred to them, this will be covered by appropriate safeguards, such as European Standard Contractual Clauses, to continue to ensure an adequate level of protection.

Ads & Data will constantly update your personal data and keep it for a maximum of 13 months.

As a data subject, you have several rights. These are explained in section 11 below. Both Proximus and Ads & Data allow you to exercise certain rights in accordance with the legal requirements. The Proximus Data Protection Officer acts as a central contact, among other things because Ads & Data has no data to directly identify you (e.g. name or e-mail address) and will therefore not be able to respond to your request.
You can always withdraw your consent, at any time, in the following ways: i) by adjusting your cookie settings so that we no longer collect data related to your use of our websites and mobile applications through the Proximus website or the Proximus app; or ii) by adjusting your privacy settings in MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) .

7.2.3.3. Targeted advertising on web and in mobile applications

Note: This processing activity is not applicable to customers of the Scarlet brand.

Which categories of personal data will we use?

- **Collected data**: Identification and contact information, Personal characteristics, Customer interactions.
- **Obtained data**: Data collected by third parties for which you gave your prior consent, statistical and public data obtained from external sources (e.g., data on the neighbourhood where you live you have given your prior consent to the partner, cadastral data of your home taken from the cadastral plan made publicly available by the Federal Ministry of Finance).
- **Observed or generated data**: Consumption habits.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to collect and use your data for the purposes of targeted advertising on web.

How long will we process this data for this purpose?

Identification and contact information and personal characteristics will be processed for as long as you are a Proximus customer.

Data related to your consumption habits will be stored for 1 year upon collection of the data.

Data related to your interactions as a customer with Proximus will be kept for 2 years upon the date of the interaction.

Data collected by third parties is only processed by Proximus for the execution of a specific campaign.

With whom do we share this data?

We share your personal data with our DPM (= data management platform) and with other websites and mobile applications that host ad banners.

How can I withdraw my consent?

You can always withdraw your consent, at any time, in the following ways: i) by adjusting your cookie settings so that we no longer collect data related to your use of our websites and mobile applications through the Proximus website or the Proximus app; or ii) by adjusting your privacy settings in MyProximus Web or MyProximus in the Proximus+ App. For more information on alternative ways to exercise your rights, you can consult section 11 below.

Proximus, acting as an advertising agency (not as a telecommunications operator), has the possibility of presenting you with advertisements relating to its products and services or to those of other advertisers, on Proximus websites and applications or on third party owned websites and applications.

An advertising agency is tasked with buying and selling online media space for advertisers, i.e. brands or companies wishing to promote their products and services through a campaign on the internet or in a mobile application. In effect, the Proximus advertising agency acts as an intermediary between advertisers or other parties and those third-party website and application owners who sell advertising space, for example in the form of static banners and videos.
When you view websites and applications that show advertisements, by accepting their advertising cookies you are already consenting to a certain amount of advertising personalization based on your preferred language for instance. By granting us your consent, we can present you with more targeted and relevant advertising.

<u>Web profile</u>

We'll be able to choose advertisements that best match your web profile which is determined from the data that we hold about you.
For example, if we notice that you often watch football on television, we may infer that football is one of your interests and as a result, football related ads will more likely be shown.

The data we use to build your web profile are as follows:

- Administrative data that you have shared with us (language, age, postal code, type of customer, etc);

- Information about Proximus products that you purchased and/or Proximus services that you use(d);
- Information relating to billing;
- The types of programmes you watch (sports, news, cookery, children's programmes, etc) when you have a subscription to Pickx;
- The types of competitions you participate in on Pickx and data collected through our Proximus For You loyalty program;
- Data collected from the Family Life application if you happen to use this Proximus service.
- Ads that you have already viewed if you have a Proximus TV subscription and you already benefit from personalized ads on TV – this is used to create consistency between the different media on which you view ads;
- Data that we have derived from the information above (e.g., if you have just bought a state-of-the-art smartphone from Proximus, we may conclude that you are a fan of new technology);
- Data we receive from our partners and for which you have given your prior consent to the partner. Please find the list of our partners here;
- Statistical and public data that we have obtained from external sources such as data on the neighbourhood where you live. Please find the list of our external sources here;
- Cadastral data of your home taken from the cadastral plan made publicly available by the Federal Ministry of Finance (e.g. used to determine whether you have a garden);
- The following data collected through third-party advertising cookies will also be added to your web profile:
    - Ads you have already viewed on websites and applications;
    - Your interactions with those websites and applications;
    - Pages visited on those websites and in those applications. For example, if you browse a website selling sporting goods or have clicked on an advertisement that we have shown you in connection with sporting goods, this will allow us to identify an interest and add it to your profile.
    - Data related to advertising cookies which you have accepted (browsing, language, location, etc).

Your web profile allows us to replace certain banner ads or video ads with ones that are more relevant to you. You will not receive more advertising than you do currently.

List of advertisers

We also have the possibility of sending you advertisements based on lists of users selected by the advertisers. This list may be refined by us at the advertiser's request using segmentation criteria proposed by us.

For example, an advertiser could ask us to refine a list of users to select only those believed to have an interest in football (as determined by their web profile above) and to exclude those who do not.

Making the link between your viewing of websites and applications on which we run ads and data we have about you will only be made if you give us your consent and:

- You have authenticated yourself at least once on one of the Proximus websites or applications (Pickx, MyProximus, Proximus.be, etc).
- You have accepted advertising cookies from third parties on the Proximus websites or applications (see the cookie management policy on our website).

- You have accepted advertising cookies from third parties on the website or application which you are using and on which we feature advertising.

You can withdraw your consent at any time via the privacy settings of MyProximus. If you wish to withdraw your consent, go to your MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy). For more information on your data subject rights, you can consult section 11 below.

7.2.3.4. Targeted advertising through TV channels

Note: This processing activity is not applicable to customers of the Scarlet brand.

Which categories of personal data will Proximus use?

- **Collected data**: Identification and contact information, Personal characteristics, Customer interactions.
- **Observed or generated data**: Consumption habits.
- **Derived data**: Segmentation information.

What justifies this processing activity?

Your consent (art. 6(1)(a) GDPR) to collect personal data and use it for personalized advertising on the Pickx service, with the direct participation of the sales houses of the TV channels and the advertising platforms broadcasting targeted ads.

How long will we process this data for this purpose?

Identification and contact information and personal characteristics will be processed for as long as you are a Proximus customer.

Data related to your consumption habits and segmentation information will be stored for 1 year upon collection of the data.

Data related to your interactions as a customer with Proximus will be kept for 2 years upon the date of the interaction.

With whom do we share this data?

Your personal data is shared, after pseudonymisation, with DPG Media and Ads&Data, who operate as joint controllers together with Proximus.

How can I withdraw my consent?

You can always withdraw your consent, at any time, by adjusting your privacy settings in MyProximus Web or MyProximus in the Proximus+ App. For more information on alternative ways to exercise your rights, you can consult section 11 below.

Note: Contrarily to the processing activity described in section 7.2.3.1 "Targeted advertising on TV", pseudonymsed data will be shared with the other joint controllers involved in this activity, as described

in the text below. This also allows for the personalization of unskippable advertising present on some TV channels.

What is the purpose of this processing activity?

If you give your consent, you allow the advertising sales houses of our partner broadcasters (www.proximus.be/tvregies) to select and distribute the personalized ads you see on the Pickx service (on your decoder, Pickx app and Pickx website) based on your customer profile and to measure their performance.

This means that you will see the same ads less often and also fewer ads that are inconsistent with your needs and focus of interest.

The joint controllers of your personal data are Proximus, the sales houses of the TV channels and the advertising platforms broadcasting the targeted ads. You can find the list of the sales houses of the concerned partner channels and advertising platforms here (www.proximus.be/tvregies).

As a data controller, we must comply with a number of obligations, such as safeguarding your rights, reporting security breaches, etc. As data processing co-controllers, we have established and assigned these obligations in an agreement that clearly describes the roles and responsibilities of each of the parties in carrying out the obligations imposed by the General Data Protection Regulation.

Contrarily to the processing activity described in section 7.2.3.1 “Targeted advertising on TV”, pseudonymsed data will be shared with the other joint controllers involved in this activity.

How do the TV broadcasters adjust the TV ads on the Pickx service and how do they measure their results?

Through their advertising platforms, the advertising sales houses of the concerned TV channels decide which commercials are shown to which subscribers based on their customer profile(s).

For this purpose, we share the following information with the advertising platforms of the sales houses of the respective TV stations:

- an encrypted identification code,
- technical information regarding the type of software or device used,
- as well as your customer profile(s) (for example young family, often watching cooking programs)

This allows the sales houses of the concerned TV stations to expose the commercials to the best suited public based on the segment data and in particular:

- to estimate in advance the broadcasting costs of the advertising spots according to the chosen target audience, channel and broadcasting time slots
- to make a report on the results of the targeted TV ad campaign after broadcasting

Subsequently, the sales house of the concerned TV channel communicates the aggregated results of the advertising campaign to the advertiser to inform him about the exposed audience and the volumes of ads seen.

This method also allows sales houses to limit the number of exposures to a particular advertisement on customer level.

How is your customer profile made?

Your customer profile is based on:

- the type of programs you watch on our TV services (sports, news, cooking, children's programs...)
- the ads you have already watched if you have a TV subscription and if you already use the personalized advertising service. This ensures more consistency between the media on which you view the ads.
- the types of contests you participate in on Pickx and the data collected by our Enjoy! loyalty program
- data about the composition of your family, collected in the Proximus+ app, if you use this application.
- administrative data you have communicated to us (language, age, postal code, type of customer, etc.), Proximus products purchased, Proximus services used, information about your billing, etc. and other data we have derived from this information.
- user data that we receive from partners and for which you have given prior consent to the partner. We have the possibility of showing advertisements based on selected user lists and communicate the list of subscribers who have viewed the advertising campaign. A list of our partners can be found here
- statistical and public data obtained by Proximus from external sources, such as statistical data about the area where you live. A list of our external sources can be found here
- cadastral data about your home, taken from the cadastral map published by the Federal Government Service Finance. This map is used, for example, to determine whether or not you have a garden.

What if you change your mind?

No problem. You can change your consent at any time via the privacy settings in the MyProximus section of the Proximus+ app or on Pickx TV.

7.3. When you have ceased to be a customer or user

7.3.1. Ex-customer consent acquisition campaigns

Which categories of personal data will we use?

- **Collected or obtained data**: Identification and contact information.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to promote our brand, as well as relevant products and services, by inquiring whether an ex-customer would be interested to get offers and promotions beyond the usual retention period.

How long will we process this data for this purpose?

As this is a further purpose to the initial purpose of direct marketing towards ex-customers, the retention period will be identical; 5 years after the end of your contractual relationship with Proximus.

With whom do we share this data?

Call centers working on our behalf, acting as processors (in the context of these campaigns).

How can I withdraw my consent?

Please use the unsubscribe link in Proximus e-mails, reply STOP if you receive a text message, or contact the Proximus DPO at the e-mail address privacy@proximus.com if you no longer wish to be called, contacted via digital channels, or receive postal mail from Proximus. You can also object to the use of your personal data for marketing purposes, as well as restrict the channels via which you wish to be contacted, via MyProximus Web and/or MyProximus in the Proximus+ App. For more information on alternative ways to exercise your rights, you can consult section 11 below.

As an ex-customer, you might be interested in being informed of the different offers and promotions relating to our products beyond the standard retention period of five years. For that reason, towards the end of the five-year retention period for the purpose of direct marketing towards ex-customers, during one of the standard marketing calls, one of our call center agents will ask you whether you would be interested in getting further offers and promotions, for another period of 3 years.

Not interested? Don't feel pressured! You can always refuse, and our call center agents are not in any way incentivized for the collection of such consents.

Changed your mind after giving your consent? Please use the unsubscribe link in our e-mails, reply STOP if you receive a text message, or contact the Proximus DPO at the e-mail address privacy@proximus.com if you no longer wish to be called, contacted via digital channels, or receive postal mail from Proximus.

7.3.2. Ex-customer 'win-back' actions

Which categories of personal data will we use?

- **Collected data**: Identification and Contact information.
- **Derived and inferred data**: Leisure and personal interests ('*preference profile*' – for more information, see sections below).

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to further promote our brand, as well as relevant products and services, to existing customers.

How long will we process this data for this purpose?

We will process your data as an ex-customer for 5 years after the end of your contractual relationship with Proximus.

With whom do we share this data?

Call centres working on our behalf, acting as processors (in the context of telemarketing campaigns).

How can I object?

If you want us to stop contacting you for marketing purposes, please use the unsubscribe link in our e-mails, reply STOP if you receive a text message from us, or contact the Proximus DPO at the e-mail address privacy@proximus.com if you no longer wish to be called by us, be

contacted via digital channels or receive postal mail from us. For more information on alternative ways to exercise your rights, you can consult section 11 below.

Just as for our customers, we have a vested interest in promoting our products and services, brand, image, and potential offers to ex-customers, in an attempt to win them back. To achieve these goals, we will process ex-customers' personal data to spread awareness around these offers and promotions by contacting them directly, be it by phone or per e-mail.

In practice, these activities take place in two stages:

- First, a list of ex-customers to be contacted in the context of a specific campaign is prepared. Whether you are included in a campaign will depend on the goal of the campaign (what product or service we are promoting) and your preference profile, if there exists one (to determine whether you would be interested in the product or service being promoted, or whether you qualify for a specific action). In some cases, we might launch general campaigns which will target all customers indiscriminately.

- Once the target list has been prepared and you have been included as a potential target, we will process your identification and contact information (relevant to the communication channel used for this specific campaign, e.g., your e-mail address for an e-mail campaign) to deliver the marketing message.

We are committed to only contacting you at reasonable intervals, with different intervals per channel of communication.

It goes without saying that you remain in absolute control of your preferences when it comes to Proximus' marketing outreach. If you want us to stop contacting you for marketing purposes, please use the unsubscribe link in our e-mails, reply STOP if you receive a text message from us, or contact the Proximus DPO at the e-mail address privacy@proximus.com if you no longer wish to be called by us, be contacted via digital channels or receive postal mail from us.

8. How do we protect your personal data?

The databases containing your personal data are secured. Updates guarantee a high level of protection.

We take technical and organizational measures to protect the databases in which your data are stored against unauthorized access/use, theft or loss. Our security measures are regularly evaluated and updated to ensure that we can continue to provide a high protection level.

Here you will find a general overview of the technical and organizational measures taken by us.

9. Information about specific products and services

9.1. Services for professional customers in which Proximus is acting as a data processor

Proximus acts as a data processor whenever it processes personal data on behalf of the customer.

This is for instance the case for personal data that:

- the customer stores in Proximus' data centers or cloud (e.g. Private or public cloud services, IT Security services, Contact center services, Workplace services, Internet of Things patforms and many other cloud based services);

- the customer enters in a tool made available by Proximus (e.g. Invoice Insights, Mobile Device Management);
- the customer has entrusted to Proximus for configuring the service;
- are processed by Proximus for providing assistance to the customer.

Other data processors or "sub-processors"

When Proximus acts as a data processor for the personal data of the customer or its end users, it can be assisted by sub-processors. Proximus remains liable to the customer for the protection of the personal data of the customer's end users. The Proximus subcontractor list covers the subcontractors for the products and services provided to our professional customers for which Proximus acts as a data processor. Proximus will keep the list up-to-date.

The list of subcontractors can be consulted here.

9.2. Personal data in MyProximus

The information relating to the processing of personal data in the context of MyProximus can be found in the privacy notice for MyProximus.

9.3. Family life

Proximus requires that the user creates a MyProximus account prior to accessing this service. The data collected during the creation of the account is necessary in order to give access to the service. The "Family life" profile includes the following mandatory pieces of information: the surname, first name and email address. The user has the possibility of completing his profile by adding other optional data (photos, videos, telephone number, gender, birthday, etc.).

The data that the user provides via the various shared tools of Family life will only be used in the context of this provided service. Only members of the circle can see the information and content that the User shares. In addition to the shared information the user also has the possibility of creating private events in the "Calendar" tool and private tasks in the "TO DO list" tool. These private events will only be visible to the user and, if he/she wishes, by a limited number of members of the circle that he/she explicitly selects.

The user also has the possibility of sharing his location data to other members of the circle in real time or in specific locations. Users can limit the sharing of theirposition either in time, or to specific places and/or to certain members of the circle. To use features such as these, the uUser must enable location services by turning on the “Location” function in the application before it can use his location data. Location data is processed for the sole purpose of providing the user with the requested location services, i.e. to allow other members of the circle to locate him. Location data is not shared with third parties. Location data is kept as long as the “Locate” function is enabled in the application. The user can disable location services at any time by turning off the “Locate” function in the application.

The username linked to a user is associated to every post he/she creates. A user (administrator or otherwise) can delete any post (message, photo, event, task, contact, ...) that he/she has posted. In the event that the posts are not explicitly removed prior a user leaving a circle or terminating the service, the username linked to the user will be removed from all posts they may have created. The user retains the possibility of deleting posts prior to leaving a circle or terminating the service.

Unless otherwise specified, user data is managed and processed as long as the user account remains active. In the event that the user decides to terminate this service, notably in the event of account termination, his "Family life" user profile will be removed from the date of deactivation. The removal

of the "Family life" user profile is independent of his/her MyProximus account, which shall remain active, as it allows access to other services.

9.4. Data processing when you use Pickx (TV) through your decoder, the Pickx app or through the Pickx website

The personal data generated when you use Pickx or data that you provide yourself in the context of Pickx are processed and included in our databases. We may process this data to provide you with the Pickx service, to improve our services, to conduct market studies, to produce statistical reports, to create user profiles and to bring personalised or non-personalised recommendations.

The Pickx decoder is equipped with software which registers and stores the operations performed with the decoder. The Proximus Pickx app and website contain similar functions.

All this data can be processed to:

- allow the successful implementation of the contract;
- correctly deliver the Pickx services and solve technical problems;
- provide you with personalized recommendations relating to Pickx services and other Proximus services;
- allow customer management;
- conduct market surveys and create user profiles;
- generate statistical reports on viewing behavior for internal purposes and for reporting to TV channels and the media regulator;
- adapt advertising on Pickx to your profile;
- detect fraud, e.g. breaches of intellectual property rights;
- conduct (personalized) information or promotional campaigns related to Proximus Group products and services by any means, including by post and/or e-mail.

If you prefer not to receive any information about our products, services or promotions via your TV screen, or don't want the advertising on Pickx to be adapted to your profile or to receive any personalized recommendations relating to the Pickx services, you can find out how to indicate your preferences in the section 11.

In some cases, Proximus may disclose the collected data:

- to partners that help us deliver the Pickx services;
- if such disclosure is necessary for delivering a Pickx service;
- if you have consented to such disclosure.

Using the Pickx app in another EU Member State

You can use the Pickx app when you are temporarily in an EU Member State other than Belgium, according to the European Regulation on portability, only if you are a resident of an EU Member State. Proximus therefore verifies your Member State of residence when you conclude the TV app contract and during the performance of the contract. Within the limits of the European Regulation on portability, Proximus decides which verification methods it will use. The processing of personal data for this verification is limited to what is considered proportional. The personal data will not be kept longer than is required for the verification.

9.5. Doktr

The information relating to the processing of personal data in the context of Doktr can be found in the Privacy Policy of Doktr.

9.6. Banx

The information relating to the processing of personal data in the context of Banx can be found in the Privacy Policy of Banx.

10. What are cookies (and related technologies) and how are they used?

Cookies allow us to recognize you as a visitor on our websites, so that we can provide you with personalized information.

You can consult our cookie policy via the hyperlink "Cookie policy" at the bottom of the homepage of our websites.

When you log in to MyProximus, we place a cookie in your browser. This way, we can recognize you as a visitor on our website and adapt the content of our websites to your personal situation, even if you don't log in to MyProximus on your next visit.

If you don't want to receive any personalized messages when you visit our website www.proximus.be , follow these instructions:

•Click "I am not… (your name)" on the page where you log in to MyProximus;

•Then, click the Proximus logo at the top left; you will then arrive on the non-personalized version of the website.

For the relevant cookie policy: consult the website (not all websites have all types of cookies).

If you accepted cookies for targeted advertising by Proximus and third parties on our websites, We can give our trusted partners access to such cookie information via its Data Management Platform. The list of partners with whom we share cookie information is available via the cookie manager on Proximus' websites.

11. What are my privacy rights and how can I exercise them?

You have the right to inspect, correct and delete your personal data. You can also object to the use or processing thereof. You can withdraw your consent and change your choice. Finally, you can register to be included on the Do Not Call Me list. If you are a Proximus (ex)customer, in most cases you can indicate your privacy preferences via MyProximus (Web and in the Proximus+ App) or via our customer service. If you are not a customer, you can always call our customer service to submit a request to exercice your privacy rights.

To ensure that the request is made by the right person, we ask you to provide certain information to confirm your identity and to avoid anyone else exercising your rights. If this information is not sufficient to confirm your identity, we may ask for additional information to allow us to uniquely identify you or ask you to send us a copy of the front side of your identity card (you may redact all information on your identity card that is not relevant to confirm your identity).

We have one month to respond to your request. This term starts running as soon as we have all the information we need to meet your request.

The term of one month may be extended by a maximum of 2 months, depending on the number and complexity of the requests. We will keep you informed of any delay in our response within the initial term.

We strive to adapt our systems and databases as quickly as possible. But, in practice, it may take some time to implement your choice.

If you are not satisfied with our answer, please let us know at the Proximus Data Protection Office, either by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

You can submit a complaint to the Data Protection Authority

If you are not satisfied with the answer you receive from Proximus, or you do not agree with our opinion, you can contact the Data Protection Authority and submit a complaint. More information: see https://www.dataprotectionauthority.be/contact-us.

11.1. You can access your personal data

You have the right to request access to your personal data. We will then provide you with an overview of the personal data we process on you. We will also give you additional information on, for example, why these personal data are processed, the origin of the data, the types of third parties with whom we share your personal data, etc.

Proximus (ex)customer:

Contact the Proximus Data Protection Office by e-mail: privacy@proximus.com, via this web form or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

Not a Proximus (ex)customer:

Contact the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

11.2. You can have your personal data corrected

If you notice that certain data that we have about you are no longer correct, you can have them changed. For this, contact our customer service.

Some personal data, such as contact details, are available in the MyProximus environment and you can change them there yourself via MyProximus Web (click on your name or avatar in the top right corner > My account > Edit profile) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Personal data). If that doesn't work, contact the Proximus customer service on 0800 55 800 or via chat.

11.3. You can have your personal data deleted

In certain cases (e.g. when you don't have any Proximus products or services anymore and you would like to have your contact data deleted), you can ask for your personal data to be deleted.

We are unable to delete certain personal data (e.g. billing data) because it is required by law to keep those data.

Contact the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

11.4. Removal of data from the telephone directory and the 1207/1307 database

If you don't want to have your contact information published in directory services or the telephone directory, you can adapt this preference yourself via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy). If that doesn't work, you can submit your request via this webform, by e-mail: annuaire@1307.be or by post: Service Annuaire, Boulevard Roi Albert II 27, B-1000 Brussels.

11.5. You can object to the use of certain personal data

You can always object (without a motivation) to the use of your personal data for marketing purposes.

Proximus (ex)customer

You can adapt the channels and preferences regarding communications for marketing purposes via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) . If that doesn't work, contact the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

You can also follow the instructions in the e-mails and texts you receive from us to stop receiving such commercial messages in the future.

If you want to completely object to the use of your personal data for marketing purposes, you can also register this in MyProximus, submit your request via this webform or contact the Proximus customer service on 0800 55 800 or via chat.

Not a Proximus (ex)customer

You can object to the use of your personal data for marketing purposes by contacting the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

The self-employed and SMEs can inform us about their privacy preference via the toll-free number 0800 55 500.

Medium-sized and larger companies as well as public institutions can call the toll-free number 0800 55 200.

Objection to the use of mobile network location data for anonymous reporting

You can object to the use of mobile network location data for anonymous reporting via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy > Network mobile data) and/or MyProximus in the Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy > Network mobile data). If that doesn't work, contact the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

If you have a specific reason (motivated request), you can object to us using your personal data for purposes other than those required for the performance of an agreement or for complying with a legal obligation (e.g. fraud prevention). In case of a justified request, we will stop using your personal data unless we have compelling grounds to continue using it.

You can submit a request to object to the processing of your personal data for a specific purpose by contacting the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

11.6. You can withdraw a consent previously given

Whenever you give us explicit consent to process personal data for specific purposes (e.g. personalized TV advertisements, personalized advertisements on web and in mobile applications…), you can withdraw the consent previously given at any time. You can do this via MyProximus Web (click on your name or avatar in the top right corner > My account > Alerts and Privacy) and/or MyProximus in the

Proximus+ App (click on the settings icon in the top right corner > Manage your account > Alerts and privacy) .

If that doesn't work or if you have another request or question regarding the withdrawal of consent, you can the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

11.7. You can sometimes object to the fully automated processing of your personal data

If we process your personal data in a fully automated way (without human intervention), you can object to this.

You can submit a request to object to the fully automated processing of your personal data by contacting the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

11.8. You can ask to transfer your personal data

You can transfer personal data that you provided to us (e.g. contact details) to yourself or a third party.

You can submit a request for the transfer of your personal data by contacting the Proximus Data Protection Office by e-mail: privacy@proximus.com or by post: Boulevard du Roi Albert II 27, 1030 Brussels.

11.9. You can register to be included on the Do Not Call Me list

If you no longer wish to receive any commercial calls from any company or organization on your landline or mobile, you can register to have your name put on the "Do Not Call Me" list. You can do this by calling the number 02 882 19 75.

All companies and organizations that make offers by telephone or mobile phone are required by law to comply with this list. They have to remove your telephone number and name from their call files, and are no longer allowed to call you about their products or services or promotional offers. Each company and organization is responsible for respecting the "Do Not Call Me" list. We have no powers to supervise or control this within companies other than Proximus.

For any complaints regarding unsolicited commercial calls, you can contact the Federal Public Service FPS Economy, SMEs, Self-Employed and Energy, Contact Center, Rue du Progrès 50, 1210 Brussels, call the toll-free number 0800 120 33, or contact the hotline: meldpunt.belgie.be, section "Vervelende telefoontjes" (unsolicited phone calls).

11.10. You can register to be included on the Robinson list

If you no longer wish to receive commercial letters from companies that are members of the Belgian Direct Marketing Association, you can register for your name to be put on the Robinson list via www.robinson.be.

12. Changes in the privacy notice

Changes can always be made to our privacy notice. Therefore, consult this site regularly.

Our privacy notice may be expanded or adapted in the future (e.g. to accommodate new developments). For this reason, we recommend that you consult the privacy notice regularly.

13. Contact details of the Data Protection Officer

If you have further questions about our privacy notice, feel free to contact our Data Protection Officer.

How do you contact the Proximus Data Protection Officer?

E-mail: privacy@proximus.com

Address: Boulevard du Roi Albert II 27, 1030 Brussels

Web form: link to web form
