Privacy policy Mobile Vikings

Contents

1. Intro **4**
2. Who are we? **4**
3. Who is in scope of this Privacy policy? **4**
4. What personal data do we collect and how long do we keep it? **5**
4.1. Collected data (information you provide to us) **5**
4.2. Obtained data (information we obtain from third parties) **6**
4.3. Observed or generated data (information we obtain through your use of our products and services) **6**
4.4. Derived data (information we derive from collected, obtained and observed or generated data) **7**
4.5. How long do we keep personal data? **8**
5. Personal data sharing with third parties **8**
●.1. Subcontractors, suppliers and partners **8**
●.2. Proximus SA **9**
●.3. Governmental entities **9**
6. For what purposes (excluding marketing and sales purposes) do we use your personal data? **10**
6.1. General **10**
6.1.1. Visitor management 10
6.1.2. Recording of electronic communications for quality control purposes 11
6.1.3. After-sales service, customer support and interactions with customer service 12
6.1.4. AI-Powered Customer Interaction Analytics 15
6.2. When you're becoming a customer **16**
6.2.1. Contract commencement purposes **16**
6.2.2. Assessment of new orders **17**
6.2.3. Social tariff **19**
6.3. When you are a customer or user **20**
6.3.1. Delivery of requested products and services **20**
6.3.1.1. Provision of our products and services **20**
6.3.1.2. Interconnection with other telecom operators **21**
6.3.1.3. Planning and organization of network infrastructure **22**
6.3.2. Customer management **23**
6.3.2.1. Billing and accounting **23**
6.3.2.2. Collection process **24**
6.3.2.3. Third-Party Services or Direct Carrier Billing **25**

6.3.2.4. Dispute management 27
6.3.2.5. Market research 27
6.3.2.6. Quality assurance, improvement, and development of (new) products and services 29
6.3.3. Comply with legal dispositions 30
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) 30
6.3.3.2. Processing of data based on art. 125 Belgian Electronic Communications Act 32
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) 34
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) 35
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) 37
6.3.3.6. Location sharing trough AML with Belgian emergency centers 38
6.3.3.7. Access of emergency services to the Central Number Database (CNDB) 39
6.3.4. Directory management 40
6.3.5. Fraud prevention and network security 41
6.3.5.1. Detection and prevention of telecommunications fraud 41
6.3.5.2. Network and information security 43
6.3.5.3. Network management 45
6.3.5.4. Internal Benchmarking 45
6.4. When you have ceased to be a customer or user 47
6.4.1. Archiving purposes 47
6.4.2. Contract termination purposes 47
7. For what marketing and sales purposes do we use your personal data? 48
7.1. When you're not a customer yet 49
7.1.1. Collection of contact data 49
7.1.1.1. Direct collection of contact data via events or on other occasions 49
7.1.1.2. Acquisition of prospect data relating to potential customers 50
7.1.2. Commercial prospection led by indirect sales partners 51
7.2. When you are a customer or user 52
7.2.1. Creation and enrichment of customer profile 52
7.2.1.1. Basic segmentation of our customers for direct marketing purposes 52
7.2.1.2. Consent-based segmentation of our customers and use of traffic data for

direct marketing purposes 53
7.2.1.3. Consumption profiling for the calculation of the most advantageous tariff plan 54
7.2.2. Promotion of our products and services 55
7.2.2.1. Promotion of our products and services via telephone and e-mail campaigns 55
7.2.2.2. Promotion of our products and services online (e.g. on social media) 56
7.2.2.3. Mobile Vikings Newsletters 57
7.2.2.4. Viking Deals 58
8. My Viking 58
8.1. The creation of a My Viking account 58
8.2. My account 59
9. How do we protect your personal data? 60
10. What are cookies (and related technologies) and how are they used? 61
11. What are my privacy rights and how can I exercise them? 61
11.1. You can access your personal data 61
11.2. You can have your personal data corrected 62
11.3. You can have your personal data deleted 62
11.4. Removal of data from the telephone directory 62
11.5. You can object to the use of certain personal data 62
11.6. You can withdraw a consent previously given 63
11.7. You can sometimes object to the fully automated processing of your personal data 63
11.8. You can ask to transfer your personal data 63
11.9. You can register to be included on the Do Not Call Me list 63
11.10. You can register to be included on the Robinson list 63
12. Changes in the Privacy policy 64
13. Contact details 64

1. Intro

At Mobile Vikings 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 policy, we will provide you with detailed information 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 Mobile Vikings SA (Kempische Steenweg 309/1, 3500 Hasselt).

This Privacy policy is applicable to all customers of “Mobile Vikings” and “JIM Mobile”.

3. Who is in scope of this Privacy policy?

With this Privacy policy, 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 policy 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 My Viking 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 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 websites and users of our mobile applications;
- Participants in competitions, campaigns, surveys, webinars, events, etc.

As a Mobile Vikings' 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 policy. 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 section 6 and section 7 of this Privacy policy.

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 collect personal data in various ways. For instance, when you create a My Viking account to access our products and services, you will be asked to provide certain information (e.g., your name, postal address, email address, phone number, date of birth, and national registry number).
We may also process your personal data in other situations, such as when you sign up for a special offer or promotion, submit an online application (e.g., for our newsletter or via our Chatbot), or interact with us through social media platforms (e.g., Facebook).

From the moment you become a Mobile Vikings 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, Mobile Vikings 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, 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,…);
- 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 at his disposal, …);
- 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 Mobile Vikings (website 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 section 6 and section 7 of this Privacy policy.

- 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, 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, ...) 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,…);
- Internal identifiers: Records that are used by Mobile Vikings to uniquely identify a customer or end-user (customer number, …);
- 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), 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, Viking Deal activities).

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,…);
- Leisure and personal interests: Information that provides an insight into leisure activities or personal interests of a customer or end-user (membership to sports clubs, interest in fashion, subscription to an automobile magazine,…);
- 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, …).

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 section 6 and section 7 of this Privacy policy.

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 us 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 we share personal data.

●.1. Subcontractors, suppliers and partners

- Call centers for customer service and support purposes
- Partners or call centers who sell Mobile Vikings services in our name and on our behalf
- IT service providers
- Identification and authentication service providers
- Network and telecommunications service providers
- Hardware providers
- Market research partners
- Courier services
- Installation technicians
- Billing service providers
- Payment service providers such as your bank
- Email service providers
- Marketing email providers
- Partners in the context of the loyalty programs 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

Mobile Vikings can enlist the services of subcontractors located outside the European Economic Area. Mobile Vikings 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.

●.2. Proximus SA

As Mobile Vikings was acquired by Proximus SA under Belgian public law (hereinafter: Proximus) in 2021, your personal data as well as data on the products and services you use, will be shared with Proximus:

- for the performance of Proximus' obligations in its role as mobile and broadband network operator (hereinafter: network operator) since Mobile Viking is using Proximus' network to provide the services. This concerns the processing activities that are:
    - (i) mentioned in section "6.3.1.2. Interconnection with other telecom operators"; section "6.3.1.3. Planning and organisation of network infrastructure" and "6.3.5.3. Network management" and,
    - (ii) certain legal obligations as stated in section 6.
      In case the data is processed by Proximus, it will be mentioned in the data activity (under "With whom do we share this data?");
- to prevent that you, as a (former) Proximus and Mobile Vikings customer, would receive promotions or advertisements for similar Proximus products or services you already use with Mobile Vikings;
- to make financial reports and analyses, which can be used both internally and externally (e.g. for reporting group results to Proximus shareholders).

The Proximus privacy policy can be consulted on the Proximus website, at Legal warnings for private and professional customers | Proximus. For non-mandatory data processing activities, you can disable this data processing at any time in your My Viking account.

●.3. Governmental entities

We have a legal obligation to share your personal data with certain governmental entities. As Proximus is Mobile Vikings' network operator, it will mostly perform the legal obligation in name and on behalf of Mobile Vikings.

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".

Apart from Proximus, 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
- 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 policy) 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 policy. The summary table is followed by an explanation of the purpose.

Each purpose includes the legal basis for processing your personal data. In cases where processing is necessary to comply with a legal obligation, to perform a contract to which you are a party, or to take steps at your request prior to enter into a contract, providing certain personal data may be a statutory or contractual requirement, or necessary to enter into a contract. Failure to provide such information may result in consequences, such as the inability to enter into or perform a contract.

6.1. General

6.1.1. 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 can be shared with public authorities.

In case of a planned visit to one of the Mobile Vikings offices, your name, contact and company details are collected for visitor management and access to the offices. 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 telephone conversations will be stored for a period of 1 month after the electronic communication has taken place. Or in case of chat or e-mail conversations, as long as necessary.

With whom do we share this data?

This data is shared with our customer support software tool.

The recording can also take place in name of Mobile Vikings 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 or e-mail conversations you might have with one of our agents.

These electronic communications are recorded and stored for 1 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 we 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 to which you are a party (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 a Mobile Vikings 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. 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?

This data is shared with our customer support software tool.

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 our network operator Proximus.

Additionally, depending on the channel used to address your question or problem to Mobile Vikings, some of your personal data might also be shared with the third party

acting on behalf of the customer (e.g., Telecommunications Mediation Service, Testaankoop / Testachats).

Mobile Vikings is committed to offer you the best customer experience both via the various customer service channels (phone, chat, contact form or FAQs on the Mobile Vikings 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, it is possible that you will first meet a digital assistant that will offer to assist you. Mobile Vikings 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, it is possible that you will be first 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.

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

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

  Mobile Vikings relies on IVR for effective call routing. This technology uses the personal data you provide (i.e., phone 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 Mobile Vikings website*
  You may also use a contact form to address Mobile Vikings with your question or issue. Mobile Vikings may request certain personal data (i.e., phone 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 Mobile Vikings website*
  The Mobile Vikings 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 Mobile Vikings.

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 Mobile Vikings, 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 our network operator Proximus.

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

If your question or problem is submitted to Mobile Vikings 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 Mobile Vikings

Next to the situations where you reach out to Mobile Vikings, Mobile Vikings might also reach out to you (e.g., to follow up on an open customer care ticket, 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). These types of communications can take place by phone call, e-mail, SMS,, e-mail.

6.1.4. AI-Powered Customer Interaction Analytics

Which categories of personal data will Mobile Vikings use?

- Collected data: identification and contact information.
- Observed and generated data: your interactions with our Mobile Vikings agents and/or our digital assistants (search bot, chat bot) through our various communication channels and features. This may include text, images, and other content you share with us.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) to improve your customer experience and enhance our services through advanced analysis.

With whom do we share this data?

Besides internal Mobile Vikings teams responsible for customer experience, your data may be shared with the following recipients:

- Our external AI providers such as Amazon Connect and Amazon Bedrock which help us analyze data using cutting-edge technology. Amazon Connect handles call recording and transcription, providing voice-to-text conversion while Amazon Bedrock provides Large Language Models (LLMs) to support multiple use cases, including natural language processing and advanced analytics.

How can I object?

If you have a specific reason, you can object to our use of your personal data for this purpose. This may impact your ability to fully benefit from our services. 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.

Mobile Vikings is committed to offering you the best possible experience. In the era of new technologies, Mobile Vikings has decided to elevate your customer experience through advanced analysis powered by Artificial Intelligence (AI), specifically generative AI.

Whenever you interact with Mobile Vikings via phone, chat, email, or other means, your interactions may be recorded, temporarily stored, and analyzed by our AI model. This analysis includes text analysis to understand the content of your messages.

This helps us improve your experience in several ways:

- We analyze the reasons why customers contact us to identify trends and resolve recurring issues before they occur again.
- Our intelligent customer support (e.g., search bot, chatbot) can respond quickly to your requests, making your interactions more efficient and freeing agents to focus on more complex issues.
- Your interactions are automatically translated and corrected to ensure clarity and accuracy.
- Agents receive response suggestions for simple requests, enhancing their efficiency.
- Requests are directed to the appropriate agents based on the subject and their expertise.
- The key points of your latest interactions are condensed for quick follow-up and analysis by our agents. This ensures that agents have the right context if you contact Mobile Vikings again, thus avoiding the need for you to repeat yourself.

This section concerns AI-based analysis of your interactions. AI analysis may use transcripts or interaction content but does not necessarily involve listening to or reviewing recordings. If you want to learn more about our recording of communications for quality control purposes, please refer to Section "6.1.2 Recording of electronic communications for quality control purposes of this Notice".

Please note that no special category of personal data is intended to be processed.

When using AI tools, we carefully select our suppliers and ensure they do not use your data to train their AI model.

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, 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 Mobile Vikings 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 a Mobile Vikings 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 Mobile Vikings customer.

With whom do we share this data?

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 Mobile Vikings 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 need to verify your identity via Itsme, a payment with your bank account or a copy of your Belgian identity card (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.

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 Mobile Vikings 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 at your previous operator and the transfer of services.

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 shared with Proximus.

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 Mobile Vikings. 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 Mobile Vikings (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 can be stored at a maximum up to 10 years after you have ceased to be a Mobile Vikings customer.

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.

Mobile Vikings no longer offers social tariff price plans now.

For Mobile Vikings customers who were eligible for a social tariff price plan before 1/03/2024, article 74 of the Belgian Electronic Communications Act imposes an obligation to continue offering specific telecommunications services at a reduced price, which is known as the social tariff. The Federal Public Service Economy is responsible to check if the eligible customers can still benefit from the social tariff.

The Federal Public Service Economy will notify Mobile Vikings when they are no longer eligible for the social tariff. When this occurs, Mobile Vikings 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 Mobile Vikings 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. The data can be stored at a maximum of 10 years after you have ceased to be a Mobile Vikings customer.

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 our network operator 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 accessing your My Viking account, we will need to process data to authenticate your log-in and ensure a secure authentication process;

- If you are using voice-to-voice or SMS services, 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.

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?

Proximus, acting as a mobile network operator for Mobile Vikings, processes the data to deliver electronic communication services. To ensure proper interconnection between networks, Proximus will both receive and share data with other telecom operators involved in that specific electronic communication.

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 Mobile Vikings 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.

6.3.1.3. Planning and organization of network infrastructure

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?

Signaling information will be stored for 14 days from the moment the signal has been sent out.

Our network operator Proximus stores aggregated data on end-user level for maximum three months. Aggregated data on network level will be stored for maximum one year.

With whom do we share this data?

Proximus, acting as a network operator for Mobile Vikings, may share the data with companies that assist them in the context of planning and organization of the network infrastructure.

Planning and building stable, reliable, flexible, and efficient network infrastructure is a fundamental requirement for operators like Proximus, acting as a network operator for Mobile Vikings.

Effective planning and organization of telecom infrastructure are crucial to ensure seamless connectivity and service reliability to its customers and end-users. By meticulously designing and managing the network and by analysing current network capabilities and shortcomings, Proximus can provide stable, high-speed internet and communication services, which not only enhances user experience but also supports the growing demand for data and digital services.

You can find more information on this specific topic on the Proximus website.

While Proximus is committed to ensuring the optimal performance of our telecommunication networks and services, it is therefore also analysing information relating to the use of the telecommunication networks with the aim of resolving and/or preventing network issues. For more information, see section “6.3.6.3. Network Management”.

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, 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 up to 10 years after you have ceased to be a Mobile Vikings customer 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 Mobile Vikings' behalf to provide billing-related services such as the transmission of invoices of professional customers via the Peppol network, 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 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; and/or
- on your My Viking account, via the App and online.

If you choose to pay your bills by means of direct debit, you authorize your bank to pay your Mobile Vikings 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 on your Mobile Vikings 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, 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 up to 10 years after you have ceased to be a Mobile Vikings customer 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 (mobile and internet) or other intermediary measures (e.g. speed throttling, minimal outgoing mobile services);
- 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 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?

We will keep billing-related data as long as necessary, for the duration agreed with the third-party provider.

With whom do we share this data?

Third-party service providers (such as online merchants who offer digital content, SMS-tickets for public transport, parking apps, etc.) 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 customer care department 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. 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 necessary 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 Mobile Vikings customer.

How long will we process this data for this purpose?

Your personal data will be kept for 10 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).

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.

6.3.2.5. 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 10 years after the end of your contract with Mobile Vikings.

The personal data processed in the context of market research and surveys are retained for the duration of the agreement with the relevant research partner.

With whom do we share this data?

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 Mobile Vikings 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 unsubscribe in the relevant invitation or you can opt-out for market research through the privacy preferences in your My Viking account. For more information on how 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@mobilevikings.be.

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

Mobile Vikings itself, or in cooperation with research partners, does 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.

6.3.2.6. Quality assurance, improvement, and development of (new) products and services

Which categories of personal data will we use?

- Collected data: Identification and contact information, Customer interactions, Survey specific information.
- Observed or generated data: Internal identifiers, Technical identifiers, Product and service subscription information, Product and service usage information, Hardware information, Personal data generated in the context of transmitting electronic communications.
- Derived data: Segmentation information.

What justifies this processing activity?

The processing of personal data for quality assurance is necessary for the performance of the contract to which you are a party (art. 6(1)(b) GDPR).

The processing of personal data for the improvement and development of (new) products and services is based on our legitimate interest (art. 6(1)(f) GDPR) to provide high quality and innovative products and services that meet the evolving needs of our customers as well as ensure smooth and satisfactory customer journeys (e.g. when customers are joining us, modifying a subscription, or seeking assistance for administrative or technical issues.…). .

How long will we keep this data?

Aggregated personal data can be processed for an unlimited time, if they do not include personal data. However, there are shorter retention periods for personal data that is not aggregated, as well as for personal data used for diagnostic purposes.

With whom do we share this data?

We may share your personal data with network and telecommunications service providers and suppliers of the hardware devices we provide to customers to enable our customers to use our products and services.

How can I object?

If the aggregated data includes your personal data and you have a specific reason (motivated request), you can object to our use of your personal data for the processing activity which is based on our legitimate interest. 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 ensuring high-quality performance and innovation of our products and services. To achieve this, we continuously monitor and evaluate their performance, investing in improvements and the development of new offerings. This involves collecting and analysing data on usage and customer feedback to ensure the quality of our products and services, enhance them and improve customer satisfaction.

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 Mobile Vikings (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?

- Proximus, acting as the network operator for Mobile Vikings, processes your traffic data and other location data. This includes the management of telecommunications traffic, combating fraud or malicious use of the network, complying with legal obligations by Mobile Vikings or Proximus collaborators 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 acting as Mobile Vikings' network operator 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, as the network operator for Mobile Vikings, 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 Mobile Vikings 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 Mobile Vikings' 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 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.

With whom do we share this data?

- Proximus, acting as the network operator for Mobile Vikings, processes your personal data for this purpose. Only 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 will handle the data (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 "6.3.5.2. 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 "6.3.5.3. 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); 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, and/or our network operator Proximus 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?

Proximus, acting as the network operator for Mobile Vikings, processes your personal data for this purpose.

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.

Mobile Vikings and its network operator, Proximus, have 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,…).

We store 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 Mobile Vikings (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, Proximus 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?

Proximus, acting as the network operator for Mobile Vikings, processes your personal data for this purpose.

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 Mobile Vikings - 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, our network operator 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 Mobile Vikings (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.

Mobile Vikings 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.

Mobile Vikings 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 via our network operator Proximus as well as to the emergency services as long as you have a subscription with Mobile Vikings.

With whom do we share this data?

Proximus, acting as the network operator for Mobile Vikings, processes this data. Your location data is shared with Belgian emergency centers (medical emergency service, fire department, police station,…).

Mobile Vikings 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, 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 Mobile Vikings (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 Mobile Vikings. 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, Mobile Vikings 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) 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 localize 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, Mobile Vikings 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 withdrawn your consent.

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 by contacting our customer service or by sending an e-mail to privacy@mobilevikings.be.

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 contact our customer service.

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. You have the right to access and rectify your data at any time via our customer service or by sending an e-mail to privacy@mobilevikings.be.

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 withdrawn your consent. You can withdraw your consent for the inclusion in telephone directories or directory enquiry services by contacting our customer service or by sending an e-mail to privacy@mobilevikings.be.

6.3.5. Fraud prevention and network security

6.3.5.1. Detection and prevention of telecommunications fraud

Which categories of personal data will we 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 Mobile Vikings (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 and by Proximus, both of which are 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. For this activity, we are collaborating with Proximus to bilaterally share data to prevent 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;
- 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.

6.3.5.2. 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?

Proximus, acting as the network operator for Mobile Vikings, processes 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.

Mobile Vikings, via its mobile network operator 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.

6.3.5.3. 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?

Proximus, acting as the network operator for Mobile Vikings, processes this data. We may share the data with companies that assist us in the context of network management and network provisioning.

Mobile Vikings, via its mobile network operator 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, Proximus can identify when an outage occurs in our mobile network or when the quality of certain connections is not optimal. By studying and analyzing network usage, Proximus 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 Proximus' network through this link.

6.3.5.4. Internal Benchmarking

Which categories of personal data will we use?

The actual list of categories of personal data processed will vary by benchmark, but can in any case include:

- Collected data: Identification and contact information, financial and billing data, customer interactions, survey specific information.

- Observed or generated data: Internal identifiers, technical identifiers, product and service subscription information, personal data generated in the context of transmitting electronic communications, consumption habits, product and service usage information.

- Derived data: Leisure and personal interests, family and household composition, segmentation information.

What justifies this processing activity?

Our legitimate interest (art. 6(1)(f) GDPR) in developing our economic activities and improving the operational efficiency of the company.

How long will we process this data for this purpose?

The input data for internal benchmarking can be stored for a multitude of different purposes – the retention period will depend on the purpose for which the input data is being processed.

Aggregated personal data can be processed for an unlimited time, if they do not include personal data. However, there are shorter retention periods for personal data that is not aggregated, as well as for personal data used for diagnostic purposes.

With whom do we share this data?

Mobile Vikings makes use of reporting and benchmarking tools provided by IT service providers.

We regularly look at how we're doing across different parts of our organization to spot what's working well and where we can improve. This is what we call internal benchmarking.

To achieve this purpose, we use tools that help us turn large amounts of data into clear, visual summaries. But don't worry — we don't look at individual people. The data is grouped together in a way that doesn't identify anyone personally. We also remove any direct identifiers like names or contact details before we start.

Here are some domains in which such benchmarks are being used:

- Products and services management: How many people are using a certain product or service, and how it changes over time.
- Operational performance: How well our internal processes are running, like order handling or fraud detection.
- Network management and rollout: How our infrastructure projects are progressing, such as the rollout of fiber networks.

- Marketing effectiveness: How well our campaigns are performing, including the opt-outs and conversions resulting from specific campaigns.
- Supplier performance: How much we're spending with suppliers and how well they're delivering.

This activity is strictly for internal use. We don't share these reports with third parties, and we don't use them for anything other than improving how we work. It's all about making our services better for you, while respecting your privacy every step of the way.

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 Mobile Vikings (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.

6.4.2. Contract termination purposes

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, Technical identifiers, Product and service subscription information, Hardware information, Billing 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 process the personal data listed above for this purpose until all outstanding amounts have been paid and the rented Mobile Vikings equipment has been returned.

With whom do we share this data?

In case you decide to switch providers, we will share your personal data with your new operator of choice.

When you decide to terminate your contract(s) with Mobile Vikings, we will process your personal data to manage the termination process. This personal data, collected when you became a Mobile Vikings customer and through your use of Mobile Vikings products and services, includes your name, address, telephone number, email address, customer number, the products, and services you wish to terminate, and any other relevant identifiers linked to your services and products.

You have the option to either cancel your products and services partially, entirely or to switch to another provider. If you choose to switch providers, we will facilitate the transfer of your products and services using your easy switch ID. This applies to fixed internet, mobile subscriptions and prepaid cards. We will ask you to provide the necessary information, such as your new operator's details and any relevant identifiers, to ensure a smooth transition.

Once you have cancelled your subscription(s), you will receive a confirmation along with all relevant information regarding the cancellation and related practicalities. For example, if you have rented any devices from Mobile Vikings (such as a internet box, WiFi booster, etc.), you will be informed of the return procedure.

After terminating the relevant contracts with Mobile Vikings, we may still process your personal data for other purposes. You can find more information about some of these purposes in sections "6.3.3. Comply with legal dispositions", "6.4.1. Archiving purposes" and "7.3.1. Ex-customer 'win-back' actions".

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 policy. The summary table is followed by an explanation of the purpose.

Each purpose includes the legal basis for processing your personal data. In cases where processing is necessary to comply with a legal obligation, to perform a contract to which you are a party, or to take steps at your request prior to enter into a contract, providing certain personal data may be a statutory or contractual requirement, or necessary to enter into a contract. Failure to provide such information may result in consequences, such as the inability to enter into or perform a contract.

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 or on other occasions

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), Proximus 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 the e-mail address privacy@mobilevikings.be. For more information on the various ways to exercise your rights, you can consult section 11 below.

We regularly organize events, contests or other occasions 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@mobilevikings.be. 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 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 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 subsidiairies of the Proximus Group:

- Fiberklaar (Proximus joint venture deploying fiber and organizing prospecting actions in this domain),
- Proximus (Proximus can send relevant leads to Mobile Vikings).

In practice, these third parties deliver 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. Commercial prospection led by Mobile Vikings" below.

7.1.2. 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 also authorized to selling our products and services (among the products of their other customers) specifically on their own website on the internet:

Astel
DPG Media

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, 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 Mobile Vikings.

- These companies use their own databases, for the benefit of multiple different clients – Mobile Vikings 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.

7.2. 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, Customer interactions.
- Observed or generated data: Product and service subscription information.
- Derived data: Segmentation information, Family and household composition, 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 5 years after the end of your contractual relationship with Mobile Vikings.

With whom do we share this data?

Mobile Vikings may share your Identification and contact information with Proximus, to avoid you being unnecessarily contacted for the promotion of a Proximus product or service you already have with Mobile Vikings. You can always switch off this data processing in your My Viking account.

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, by opting out from this option on your My Viking account. 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.

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, by opting out from this option on your account. 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 and use of traffic data 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.
- 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?

Your preference profile will be processed for 5 years after the end of your contractual relationship with Mobile Vikings.

The traffic data observed (*see description below*) and used to adapt offers and your preference profile are processed for a period of 2 years after creation.

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, by opting out from this option on your My Viking account. 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 on the basis of data on the usage of your Mobile Vikings services (mobile, and/or internet).

You can always withdraw your consent to the use these personal data for marketing profiling purposes by opting out from this option on your My Viking account. 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 Mobile Vikings (art. 6(1)(c) GDPR), namely the obligations foreseen in articles. 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 Mobile Vikings' compliance with a legal obligation, there is no possibility to object to this processing activity!

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.

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 5 years after the end of your contractual relationship with Mobile Vikings.

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 us at the e-mail address privacy@mobilevikings.be if you no longer wish to be called by us, be contacted via digital channels or receive postal mail from us. You can always restrict the channels via which you wish to be contacted, by opting out from this option on your My Viking account. 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 customers' personal data to spread awareness around these offers and promotions by contacting them directly, be it by phone or per e-mail.

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 Mobile Vikings' 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, by opting out from this option on your My Viking account. 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.
- Observed or generated data: Product and service subscription information.
- Derived and inferred data: 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?

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

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 in your My Viking account, or contact us at the e-mail address privacy@mobilevikings.be. 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 your Mobile Vikings products, your participation in the Viking Deal program, etc., 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 Mobile Vikings advertisement to men between 20 and 25 years with an interest in gaming. 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 your My Viking account. 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 policy.

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 via the webpage Legal and user information | Mobile Vikings.

7.2.2.3. Mobile Vikings 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 Mobile Vikings customer + 10 years after a person has ceased to be a Mobile Vikings 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 the relevant e-mails. You can always object (without a motivation)

to the processing of your personal data for the purpose of sending out newsletters by opting out from this option on your My Viking account. 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.

7.2.2.4. Viking Deals

For the specific processing of data in the framework of our Viking Deals, we refer to the Privacy Policy Viking Deals via Legal and user information | Mobile Vikings.

8. My Viking

Your My Viking account enables you to have a clear and concise overview of your customer account, your products and services and related bills and to participate in the Viking Deals.

This section is applicable to every processing of personal data of My Viking users.

8.1. The creation of a My Viking account

Which categories of personal data will we use?

- Title (Mr, Mrs, Ms)
- First name, last name
- (Installation) address
- Date & place of birth
- E-mail address
- Mobile phone number
- Customer number
- Preferred language

Upon creation of your account, Mobile Vikings will link a technical identifier to uniquely identify your My Viking account.

What justifies this processing activity?

The processing of some of your personal data for this purpose is necessary for the performance of the contract in the context of the creation of a user account, to uniquely identify you when creating a My Viking account and to enable you to log in to and use your account. Mobile Vikings processes your title and your preferred language based on a legitimate interest to address you in a correct manner and to display the information in a correct language.

How long will we keep this data in My Viking?

Your My Viking account will be available and your personal data will be processed as long as you are a Mobile Vikings customer. If you would like to have your account deleted, please contact our customer service.

With whom do we share this data?

The personal data you share with us when creating your My Viking account will not be shared with any third parties.

If you are using Viking Deals, we invite you to read the relevant Privacy Policy for Viking Deals (LINK).

8.2. My account

Once created, your My Viking account gives you an overview of the following details:

- Your personal account
- Overview of your Mobile Vikings products and services
- Overview of your consumption details
- Overview and evolution of your bills

Which categories of personal data will we use?

- Title (Mr, Mrs, Ms)

- First name, last name

- (Installation) address

- Billing address

- Date & place of birth

- E-mail address / login

- Mobile phone number

- Customer number

- Preferred language

- Subscription details

- Unique identifiers of My Viking equipment (router, WiFi booster,…)

- Consumption details (used data, calls, etc.)

- Technical identifier

- Easy Switch code

- Amount due & overview of latest bills

What justifies this processing activity?

The processing of your personal data is necessary for the performance of Mobile Vikings' contractual obligations in the context of My Viking and to offer you a core functionality of My Viking, namely, to display your customer details and details of your products and services in a transparent way and to follow up on the payment of your outstanding bills. Typically, this is the type of information a My Viking user is looking for when creating an account.

Some personal data elements are processed based on the legitimate interest of Mobile Vikings to make the My Viking account personalized for you as a customer and to make sure you are addressed in the correct way and language.

Mobile Viking has a legal obligation to provide free access to timely information on the level of consumption of the services included in the tariff plan.

How long will we keep this data in My Viking?

Your My Viking account will be available and your personal data will be processed as long as you are a Mobile Vikings customer. If you would like to have your account deleted, please contact our customer service.

With whom do we share this data?

The personal data you share with us when creating your My Viking account will not be shared with any third parties.

9. 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.

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

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

You can consult our cookie policy via the hyperlink "Cookie policy" on the webpage Legal and user information | Mobile Vikings.

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 Mobile Vikings (ex)customer, in most cases you can indicate your privacy preferences in your My Viking account (Web and in the App) or via our customer service. If you are a JIM Mobile customer, you can adapt your choices in your Customer zone. 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, either by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

You can submit a complaint to the Data Protection Authority

If you are not satisfied with the answer you receive from Mobile Vikings, 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.

Contact our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

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 your My Viking account or JIM Mobile Customer zone and you can change them there yourself. If that doesn't work, contact our customer service.

11.3. You can have your personal data deleted

In certain cases (e.g. when you don't have any Mobile Vikings 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 our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

11.4. Removal of data from the telephone directory

Contact our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

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.

Mobile Vikings (ex)customer

You can adapt the channels and preferences regarding communications for marketing purposes in your My Viking account or JIM Mobile Customer zone.

If that doesn't work, contact our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

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 contact our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

Not a Mobile Vikings (ex)customer

Contact our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

11.6. You can withdraw a consent previously given

Whenever you give us explicit consent to process personal data for specific purposes, you can withdraw the consent previously given at any time. You can do this in your My Viking account or JIM Mobile Customer zone.

If that doesn't work or if you have another request or question regarding the withdrawal of consent, you can contact our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

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 our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

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 our customer service, by e-mail: privacy@mobilevikings.be or by post: Kempische Steenweg 309/1, 3500 Hasselt.

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 Mobile Vikings.

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 policy

Changes can always be made to our Privacy policy. Therefore, consult this site regularly.

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

13. Contact details

If you have further questions about our Privacy policy, feel free to contact us.

By e-mail: privacy@mobilevikings.be

Address: Kempische Steenweg 309/1, 3500 Hasselt

Alternatively: you can call, mail or chat with our customer service.