

BASE Privacy Policy

Welcome dear Visitor, Customer, User of BASE products and services, interested reader: your privacy is important to you, and you are consequently interested in our privacy policy. We at BASE also attach great importance to your privacy and do our utmost to manage it with due care and in a responsible manner. We also aim to communicate clearly about this, which is why we have combined any relevant information regarding the collection and use of your data (referred to as 'personal data') in this privacy policy.

BASE will collect and use your personal data in accordance with applicable legislation and regulations at all times. This relates in particular to the General Data Protection Regulation, GDPR, and other applicable legislation such as the Electronic Communications Act. The legislation refers to the collection and use of your data as the 'processing of personal data'.

Good to know:

- BASE acts as reseller for devices such as handsets. In this case, the supplier of the product is responsible for the processing of personal data by the device and has its own privacy policy. This means that the BASE privacy policy does not apply to these products.
- For certain services such as, for example, the repair service for devices, BASE does not act as a data controller. The repair is registered to the repairer, namely [Dynagroup](#), who is data controller and therefore responsible for processing the data you provide to them via their website in the context of the repair. The BASE privacy policy is therefore not applicable.
- In case you buy a device in one of our stores and take out a loan for it, BASE will collect data within the context of the application and granting of the loan on behalf of the lender [Cofidis](#). BASE does not act as a data controller for this processing and the BASE privacy policy is therefore not applicable.
- The processing of cookies via our websites shall also be executed in accordance with this privacy policy at all times. For further information concerning cookies and how to manage your cookie preferences, please refer to the [BASE Cookie Policy](#).

What is covered in the BASE privacy policy?

1. Who are we?
2. Who is protected by this privacy policy?
3. Which personal data does BASE process, and why?
 - a. What data do we process?
 - b. How do we obtain this data?
 - c. Why do we process this data?
 - d. Summary table
4. How do we protect your personal data?
5. Do we pass on your personal data? And to whom?
6. How long do we keep your personal data?
7. The use of your personal data for commercial purposes
 - a. What levels of privacy are there?
 - b. How can you adjust your privacy level?
8. What are your privacy rights and how can you exercise them?
 - a. Overview of your privacy rights
 - b. How can I exercise my privacy rights?
9. Use of Generative Artificial Intelligence (AI)
10. How can I contact BASE regarding my privacy?
11. Stay informed about changes
12. Escalation to the supervisory authority

1. Who are we?

We are Telenet Group NV (trading under the commercial name BASE), with registered offices at Liersesteenweg 4, 2800 Mechelen, and registered in the CBE (Crossroads Bank for Enterprises) under number 462.925.669 (hereafter referred to as "BASE"). Telenet Group NV is a telecommunications company which, together with amongst others Telenet BV (Telenet and TADAAM brands), is part of the larger Telenet group ("Telenet Group Holding SA/NV"). Telenet Group Holding SA/NV is fully-owned by Liberty Global.

We are responsible for the collection and use of your personal data, and we safeguard it in accordance with the rules of good housekeeping. We determine which data we collect and use, why and how we achieve this, always in accordance with applicable legislation and regulations. We are the data controller.

2. Who is protected by this privacy policy?

Anyone using our products and services is protected by this privacy policy. 'Anyone' refers to natural persons (not companies or offices) whose identity we are familiar with (you are identifiable, an individual).

This includes:

- Our customers;
- Family members of our customers, if they also use BASE services;
- Our former customers;
- Potential future customers (prospects);
- Our suppliers' and partners' contacts;
- Our business customers' contacts;
- Our customers' contacts, where applicable (e.g. guardian);
- Visitors to our shops and/or offices/business premises;
- Visitors to our websites;
- Users of our mobile applications (apps);
- Participants in competitions, campaigns, surveys, webinars, events, etc.

As a BASE customer, it may happen that you allow family members, friends, visitors and employees to use the products and services of BASE. An example is giving them access to your Wi-Fi. This will mean that BASE processes their data, and this is therefore subject to the BASE privacy policy. BASE has no relationship with them, however, and consequently cannot notify them of this. We count on you, as a customer, to take your responsibility and inform them about this.

3. Which personal data does BASE process, and why?

BASE processes various categories of personal data in order to carry out its activities. This chapter aims to provide an insight into the categories of data we collect, how we obtain them and the purposes for which we process them.

Depending on which BASE service you use, we collect and use different types of personal data. The following is a description of the types of data, how we obtain them and why we collect and use them (referred to as 'processing purposes'). Further information concerning retention periods for this personal data can be found in Chapter 6 of this privacy policy.

a. Which data do we process?

The data we process can be divided into four types, i.e. user data, transactional data, derived data and sensitive data:

User data <i>This data is directly linked to you as a person, regardless of your products or services</i>	• Identification data: personal data that can identify you as a user of our products and services, such as your name and address, date of birth, ID card number, national registry number, a copy of your passport or ID card, CCTV images if you visit a shop or our offices, any images, audio files or videos you submit when taking part in our campaigns or competitions, etc.; • Contact data: personal data that enables us to contact you, e.g. your phone number, e-mail address, etc.; • Contract data: personal data related to your contract such as the products you use, your customer number, invoicing and payment details, contract and order confirmation, technical data such as personal data related to your devices, such as the model and number of your TV box, your IMEI number of your phone ...; • Your lifestyle and usage habits: personal data that provides information concerning your lifestyle such as whether you have a dog, whether your children are still small, whether you like to travel, etc.; • Family data: data about your family such as your marital status, your family members, etc.; • Financial data: bank account number, external credit rating, data relating to your financial position, e.g. homeowner, etc.; • Communication data: data relating to our communications with you, such as your interactions with our customer service (via email, phone, live chat, social media...), audio recordings and transcriptions of customer service calls, interactions with our Gen AI chatbot, etc.; • Your preferences: data relating to your privacy settings, your choice of communication channels via which you do or don't want to be contacted, settings on your TV box whether you want recommendations or not, etc.
Transactional data <i>This data is linked to the use of your BASE services and data that is created as a result of your use of BASE services.</i>	• Technical data: the MAC address of your laptop, the model and service number of your mobile phone or the software version you use with one of our apps. • Traffic data: this data is required in order to transmit your communication (to handle traffic via electronic communication networks). Technical and usage data may also be included if they relate to your communication;

	• Location data: personal data that enables us to determine the geographical location of your device such as, GPS determination which mobile phone mast or Wi-Fi point you are connected to; • Usage data: personal data that our systems create when you use our products. Including: ○ When surfing: the date, time, duration and location of an internet connection, the URLs you visit, as well as the internet volume used and the type of protocol or service (e.g. FTP, HTTP, Streaming, etc.); ○ Watching TV: For each TV box we keep a record of information such as which programs you watch, which films you watch and order from our TV library, what you record, what you pause, what you fast-forward or rewind, what your favorite TV channels are or which apps on our TV box you have recently used (both via cable and via our TV apps, both for live and near-live TV viewing, look-back TV and recorded programs); ○ When making a phone call: we process data relating to the telephone numbers, date, time, duration of a call, etc.; • Data concerning the content of your communication: such as the message you send in a text message, the content of a telephone call you make, the e-mail you send or receive, the video you watch on a website, etc. We obviously comply with the provisions of telecommunications secrecy at all times; • Behavioral data: E.g. data about how you navigate the menu of your TV box. Data concerning visits to our websites: we use cookies to collect certain data when you visit our website such as your IP address, which page you are viewing, what you put in your shopping cart, what your language preference is, etc. We also use cookies when you open our e-mails and use our apps (e.g. which software version you are using, the time and duration of use of the app, your navigation via the app, etc.) For further information about cookies, please refer to the BASE Cookie Policy.
Derived data <i>This data is derived from your user and your transactional data.</i>	Profiles: Your user and transactional data enables us to build up a profile about you. For example, if you use a lot of mobile data, we will deduce that you are a high user of mobile data. If you like watching sports programs, we may deduce that you are a sports enthusiast. We also rate your wifi or mobile network based on how well or badly it performs. Do you have children? Then we may deduce that you are a family with children. We also keep track of how you prefer to contact BASE (MyBASE app, e-mail, phone, etc.) to enable us to assist you via the right channels. The derived terms “high user”, “sports enthusiast”, “active MyBASE user”, “family with children” or “network/wifi score” are referred to as profiles. We distinguish between two types of profiles: • Service type: these are only used for service purposes such as network management analyses, maintenance planning, call center planning, customer care input to assist you in the event of problems. For example, if an installation appointment has been booked for you, you will be given the profile 'Installation appointment scheduled'. Or, when network measurements show that the mobile network is not functioning properly, your network will be allocated a bad score. • Commercial type: these are used to deliver appropriate advertising to the right target audience. We also use these profiles in analyses with a commercial purpose e.g. to find out how much customers would be willing to pay for a new functionality, or to investigate why customers are leaving BASE. It is up to you to decide how personal our advertising and analyses can be and which personal data we can use for this purpose. You can manage these choices via

	your privacy settings. Further information on this topic can be found in Chapter 7.
Sensitive data <i>Some personal data is of a more sensitive nature and is additionally protected by privacy legislation</i>	Privacy legislation places sensitive data in a separate category. This includes personal data relating to your health, sexual preferences, political opinions, ethnic origin, religion, biometric data, criminal record, etc. With regard to biometric data (personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or fingerprint data): In the context of identifying new customers in the online BASE shop, we may use this by comparing facial images (selfies) with the photo on an identity document using image recognition software. This processing is only possible after your explicit consent. Biometric data will not be stored in our systems under any circumstances. In addition, we provide alternative identification processes if you do not wish to give your consent to the processing of biometric data. With respect to other types of sensitive data, the following applies: As a rule, BASE does not collect or use this data. However, if you apply for a social tariff for health reasons, we are obliged to request a certificate concerning your medical condition to enable us to validate whether you are entitled to the social tariff. You may also be under guardianship. BASE is notified accordingly so we can manage your contract with your appointed guardian.

b. How do we obtain this personal data?

This is achieved in various ways:

- We receive the data directly from you, e.g. when you conclude a contract with us, when you contact our customer service desk, have a conversation with our chatbot, take part in a competition, complete a survey or contact form, download the BASE app.
- We allocate personal data to you for the use of our services, e.g. a TV box number, an IP address, phone number, SIM card number, customer number, login code(s) and password(s).
- Our systems also record personal data generated when you are using our products and services such as the TV programs you have watched, or the identification numbers of the devices linked to our mobile network or internet connection, call data, call numbers and transit volumes, location and time of calls, or web pages visited when visiting our websites.
- Finally, we also obtain personal data via third parties. The following are a few typical examples:
 - *We purchase data from specialized data companies to match with our own data (validate, supplement, correct...) to improve the quality of the data in our systems;*
 - *We buy data, such as your family composition and housing information, from specialized data companies (we call this socio-demographic data and consumer information);*
 - *We obtain data from partners (e.g. if you have given your consent, your building contractor may send us your data);*
 - *We obtain data on your mobile usage abroad from other telecom operators;*
 - *We obtain data via affiliated companies within the Telenet group, e.g. within the context of an acquisition;*
 - *We receive data concerning your interests via market research agencies (e.g. that you like to go to the cinema, you like to travel, etc.);*

- *We obtain data from social media channels such as Meta, Google, LinkedIn, etc. (e.g. when you use your social media profile to log in or when you contact us via this channel).*
- *We receive your data if you give your consent for this when using the itsme app;*

c. How do we process this personal data?

We process personal data for various purposes, always using only the data that is necessary to achieve the purpose. We have listed the purposes below. We also explain the legal basis for collecting and using your personal data.

In general, we only process your personal data when necessary:

- in connection with the preparation, implementation or termination of a contract;
- to comply with a legal obligation; and/or
- to protect our legitimate interests, in which case we will always try to strike a balance between our interest and respecting your privacy.

If the processing of your personal data is not necessary for one of these three reasons, we will always ask for your consent to process your personal data. As a customer, you can manage your consent via your privacy settings, or by contacting our customer service. You can always withdraw your consent. See Chapter 7 for further information.

The table below provides an overview of all purposes and legal grounds based on which we process your personal data.

Purposes	Description	Legal basis
Sales After-sales service Customer support	When you decide to become a BASE customer, we will ask you for certain personal data such as your name, address, telephone number, e-mail address, for the management of our contractual relationship. We also read your ID card, take a copy of your foreign passport if you don't have a Belgian ID card, or we take a copy of your ID card if you are entering into a credit agreement. We also allocate data to you such as a customer number and login data. This data is also used for customer administration and support purposes (e.g. complaints management).	Contract performance
	The personal data we collect when concluding a contract with us is also used for the purpose of preventing and combating fraud. We also use these data to correctly identify existing customers when they contact us, as we need to be sure that we are in contact with the right person (e.g. to make a change to a subscription).	Legitimate interest
	In the context of combating terrorism, we are legally obliged to conduct identity checks and maintain certain identity records.	Legal obligation
Products and Services Invoicing Dispute management	We use your data to set up, maintain and support your products and services, e.g. to establish your connection and transmit communications via our network and other operators' networks, to calculate your usage for invoicing purposes and to manage fault reports or complaints.	Contract performance

	We may send you communications for service purposes e.g. to notify you that your data limit has been reached, to ask you to reset your password or to send your invoicing documents. If you use third-party services and choose to pay via your BASE bill (so-called "Direct Carrier Billing"), we will process certain data and pass it on to the third parties in order to enable invoicing and payment of these amounts to the third parties. For example: SMS parking, purchase of ticket from De Lijn, participation in an SMS voting or calling game, payment for a streaming service subscription (Netflix, Disney+, Amazon Prime, etc.), purchase of digital services via Google (Play store), Apple (App store), Sony (PlayStation store)...	
Network management	Our analysis of network usage provides us with vital information about the usage and load on our network. This enables us to perform successful network management (routing traffic, solving malfunctions, monitoring peak and overload rates, etc.) and to improve our networks where necessary. To establish an optimal wifi connection and to provide support in the event of problems with your wifi network, we collect, via your modem, information about the devices connecting to your wifi network, about all connections to your wifi network, and about neighbouring wifi networks that may cause interference.	Contract performance
	In order to establish an optimal Wi-Fi connection and to provide support in case of problems with your Wi-Fi network, we collect information from your modem about the devices that connect to your Wi-Fi network, about all connections to your Wi-Fi network and about neighboring Wi-Fi networks that may cause interference. In connection with the assignment of receivables (factoring), we will transfer your data to the financial institution(s) with which we have entered into a contract for this purpose. We may also engage third parties to collect unpaid invoices (e.g., collection agencies).	Legitimate interest
Quality improvement	We may use your data to evaluate and improve our products and services. For example, we may check what type of unit you have in order to optimize the use of our apps or check the quality of your internet connection. We also aim to improve our products and services on the basis of customer feedback about our services (e.g. through market research) and data obtained during discussions with, or our interventions with, our customers. Certain telephone calls with our customer service desk are recorded for quality improvement and training purposes (this is indicated at the beginning of a call). In the event of a dispute, the recording may be listened to and used as evidence. We can install people counters in our stores; these track the number of visitors to our stores.	Legitimate interest
	If we are unable to find the cause of a persistent disruption on a line, we may temporarily record calls for analysis - subject to your prior consent.	Consent

Commercial use (marketing and direct marketing) for products from BASE and affiliated companies	Direct Marketing involves sending advertising and conducting analyses with a commercial aim. We may use your data to offer you new products, services or special promotions that we think may be of interest to you. For example, you may receive an e-mail with a promotion for a BASE product that you have not acquired yet. This kind of advertising may be sent via various channels (e.g. by post, e-mail, text message or telephone). We may also send you newsletters and invitations to events or competitions, etc. We may also approach you when you are no longer a BASE customer. If you have the privacy setting “Personalized communications about our products and services” enabled, as well as the “digital media” communication channel, we may share information with online platforms such as Meta, Google (YouTube), and Ads&Data about who we want to show our ads to—and who we don’t. So that they can decide whether or not to show you our ads on their platforms, we share your name, email address, and/or phone number with them. Emails from BASE may contain a small, invisible one-pixel image that can be used to let us know that the email has been opened. When the recipient of the email loads images, a message (an automatic request) is sent to the server upon opening the email, requesting the image. BASE records this request, which indicates that the email has been opened. A similar process may be used for links or attachments in the email.	Legitimate interest
	We may approach you with an offer as a future customer of BASE, for example if you have given your consent to this when registering for a competition.	Consent
Fraud management	When you become a BASE customer, we will ask you to read in your ID card to enable us to identify you and prevent identity theft. If you become an online customer, we will ask for your ID card number and national registry number for the same reason. We may also ask for proof of your family structure in order to prevent abuse. Depending on which BASE products and/or services you choose, we will also check your credit rating.	Legitimate interest
	To protect our customers from fraud (e.g., via smishing), traffic on our network is automatically monitored to identify and stop fraudulent messages where appropriate. This means that you may not receive certain messages intended for you because they have been identified by our algorithms as smishing attacks. This monitoring may include automatic screening of message content. This screening of content is strictly limited to what is necessary to efficiently combat fraudulent activity.	Legitimate interest
Security	You will also be recorded by our security cameras in and around our shops, offices and premises. These images are stored solely for the purpose of safeguarding the security of goods and people, and to prevent abuse, fraud and other offences which we and our customers could become the victim of.	Legitimate interest
	As part of network and information security, your personal data may be processed. Providing a secure network and communication service is an essential part of our service.	Contract performance
Support for government applications and legal obligations	In many cases we are required by law to retain and/or share personal data with government agencies.	Legal obligation

	We must, for example, pass on your location to the emergency services if you call 112. We may also be required, within the framework of a police or judicial investigation, to pass on specific data in a confidential manner to the competent authorities. We also support the prevention of malicious calls at the request of the Office of the Ombudsman for Telecommunications.	
Anonymized reporting	We use your data to report internally and externally on the use of our services. These reports are anonymized and thus cannot be traced back to any particular individual. For internal reporting purposes, we generate anonymous reports for analysis and statistical insights. For example, reports are generated on the use of our services, on the TV viewing behavior of our customers, on the traffic on our infrastructure in the context of network management, on the use of our applications, on the performance of our customer service... Viewer statistics are compiled based on your viewing behavior. These reports contain anonymous figures relating to the number of viewers per broadcast and are shared with TV stations, which use these insights to evaluate broadcast programs. Besides the viewer statistics, we also pass on pseudonymized data to TV broadcasters about your viewing behavior collected via your TV box (only in relation to their own TV channels). The broadcasters analyze this information to gain insight into how viewers watch their programs (e.g. live viewing, recording and later viewing, postponed viewing, re-watching...) and on this basis they can optimize their programming. The personal data we transmit are pseudonymized by stripping all data that allows to identify an individual, with the exception of your customer number which is scrambled (by means of tokenization). You are not identifiable from the transmitted data. This data is anonymous to the receiving TV stations.	Legitimate interest
<i>Publication in telephone directories and intelligence services</i>	Your contact data are not published by default in telephone directories and enquiry services directories, this is only possible with your consent. For this publication, we are legally obliged to pass on your contact data via the Central Numbering Database, which then makes them available to providers of telephone directories and enquiry services. You can read more about this publication via this link.	Consent
<i>Participation in campaigns, contests, etc.</i>	We may collect your data when you participate in contests, campaigns, or other projects organized (in part) by BASE, such as your contact information to manage your participation and keep you informed of contest results, as well as your images, audio and video material, or other material that you submit to us or make available to us in connection with those campaigns, etc., which we may use to select winners, produce and promote campaign-related content in accordance with the campaign terms and conditions, and to comply with our legal and administrative obligations.	Consent Contract performance

Just one last thing:

- The **content of your personal communications is confidential**. We process your data to make communications technically possible, but the content of your personal

communications that pass through our network (for example, telephone calls, e-mails and text messages) is protected by the provisions of **telecommunications secrecy**. Telecommunications secrecy means that, apart from any exceptions stipulated by law, BASE shall not become acquainted with the existence or content of such communications. BASE has implemented any necessary security measures and given adequate instructions to their employees to respect the secrecy of telecommunications.

One such exception is the automatic screening of text message content to combat smishing and other forms of SMS and MMS fraud. This screening is done using algorithms that help us detect and block fraudulent messages. This means that end users may not receive certain messages that were intended for them because they have been identified as smishing attacks. The screening of the content of communications is limited to what is absolutely necessary to efficiently combat fraudulent activities via SMS or MMS communications as permitted by Belgian Electronic Communications Law (art. 125, §1, 7°). This means that not all communications will be analyzed for content.

- **Automatic decision-making:** BASE shall not make any automatic decisions - irrespective of whether or not they are based on profiling - that might have legal consequences for you or might significantly affect you, unless:
 - this is necessary to enter into or perform our agreement (e.g. credit check or shutting down your BASE products and services in the event of non-payment);
 - this is permitted by law (e.g. for the detection of tax fraud); or
 - if we have obtained your explicit consent. In such situations you will be notified in advance of the automated decision, of your right to demand human intervention and how you can challenge the decision. This is the case, for example, if you wish to become a customer via the online BASE shop and wish to use the online identification procedure provided which uses image recognition software.

BASE uses automatic decision making to identify new customers in the shops to prevent identity fraud. The identity document is read, or the number of the identity document is entered after which an automatic verification is done in the CheckDoc application of the FPS Home Affairs. If this verification reveals that the identity document is expired, stolen, forged or invalid for any other reason, we cannot accept the document and the requested service will be refused. You can file an objection to this with the FPS Home Affairs through this [link](#).

d. Summary table

The table below provides an overview of the different categories of personal data, which specific personal data they include, for which purposes it is processed, how we obtained it, what the legal basis is, how long we keep the data and with whom we share it.

We have tried to make the table below as comprehensive as possible, taking into account any potential processing operations by BASE. However, they do not always apply to everyone and depend upon your use of our services. If you use your mobile subscription solely to make calls, we will obviously have no data on your mobile data usage.

From whom?	Data type?	Data category?	Which Personal Data?	How was it obtained?	Purpose?	Legal basis	How long?	Whom do we share it with?
Customers, former customers	User data	Identification and contact details	e.g. name, address, date of birth, ID card number, copy of ID card, nationality, gender, National Registration Number, place of birth, telephone number, e-mail address	Received from customer when registering as a customer in a shop, via the online ordering platform, via the customer service department (call center), when applying for the social tariff, when concluding a credit contract or by entering the details in the BASE customer zone	- Product and service provision, invoicing - Network management - Sales, after-sales service and customer support - Quality improvement - Fraud management - Support for government applications and legal obligations - Marketing of own products - Anonymized reporting	Legitimate interest Legal obligation Contract performance	As long as you are a customer. Up to 3 years after you cease to be a customer	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman), the Central Numbering Database... Social media platforms (only if the 'digital media' communication channel is switched on in your privacy settings); they cannot use this data for their own purposes. Companies in the Liberty Global and Telenet Group. Solely with your consent: specific partners (see chapter 5)
		Sensitive Data: Biometric data	Facial image (selfie) and photo of identity document to enable image recognition	Upload of photo and scan of identity document in the BASE online shop	- Identification of new customers	Explicit Consent	No storage,	This data is shared in real time with a provider specializing in identity verification software (such as Onfido, for example) and are immediately deleted afterwards.
		Contract data:	e.g. products, customer number, username, invoice, order confirmation, contract, TV box model/number	Allocated to a customer when creating and managing a customer account	- Product and service provision, invoicing - Network management - Sales, after-sales service and customer support - Quality improvement - Fraud management - Support for government applications and legal obligations - Marketing of own products - Marketing of third-party products - Anonymized reporting	Legitimate interest Legal obligation Contract performance Consent	As long as you are a customer. Up to 10 years after you ceased to be a customer for certain data such as the contract	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman), Companies in the Liberty Global and Telenet Group. Solely with your consent: partners (see chapter 5)
		Lifestyle and usage habits	e.g. leisure activities, travel habits	Purchase from third parties	- Marketing of own products	Legitimate interest	13 months for existing and	Specialized suppliers such as our call centers, IT

			- Marketing of third-party products	Consent	former customers	support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
Family details:	e.g. civil status, family members	Purchase from third parties	- Product and service provision, invoicing - Network management - Sales, after-sales service and customer support - Quality improvement - Fraud management - Marketing of own products - Marketing of third-party products - Anonymized reporting	Legitimate interest Contract performance Consent	As long as you are a customer. Up to 36 months for former customers	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
Financial data	e.g. payment details (bank account number), payment habits	Derived from payments received from customer	- Product and service provision s, invoicing - Sales, after-sales service and customer support - Fraud management - Marketing of own products - Marketing of third-party products - Support for government applications and legal obligations	Legitimate interest Legal obligation Contract performance Consent	As long as you are a customer. Up to 36 months for former customers	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman) Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
Communication data	e.g. created contacts, answers to surveys, your preferences such as your privacy setting, recorded conversations with Customer Service.	Customer service call, visit to a shop, contact via the contact form, completed surveys, use of voice remote control	- Product and service provision, invoicing - Sales, after-sales service and customer support - Quality improvement - Fraud management - Marketing of own products - Marketing of third-party products - Anonymized reporting	Legitimate interest Contract performance Consent	Recording of calls with Customer Service: 30 days. Voice control: 0 (no retention) Other data: existing customer as long as you are a customer (privacy setting)	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)

						or up to 24 months (survey answers), ex-customer: 36 or 24 months depending on type of data.	
Transactional data	Technical data	e.g. MAC address, SSID, IMSI, IP address, the model and service number of your mobile phone or the software version you use for one of our apps	By allocation, when using BASE services	- Product and service provision, invoicing - Network management - Sales, after-sales service and customer support - Quality improvement - Fraud management - Support for government applications and legal obligations - Marketing of own products - Anonymized reporting	Legitimate interest Legal obligation Contract performance Consent	13 months for traffic data, 36 months for TV usage data	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman) Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
	Location data	e.g. connection to mobile phone mast, GPS coordinates, wifi connection	When using BASE services	- Product and service provision, invoicing - Network management - Sales, after-sales service and customer support - Quality improvement - Fraud management - Support for government applications and legal obligations	Legitimate interest Legal obligation Contract performance Consent	13 months	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman) Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
	Usage data	e.g. time of call, duration of call, URLs, TV programmes watched (viewing behaviour)	When using BASE services	- Product and service provision , invoicing - Network management - Sales, after-sales service and customer support - Quality improvement - Fraud management - Support for government applications and legal obligations - Marketing of own products - Marketing of third-party products - Anonymized reporting	Legitimate interest Legal obligation Contract performance Consent	13 months for traffic data, 36 months for TV usage data	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman) Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)

		Communication content	e.g. e-mails, text/multimedia messages, phone calls, voicemail recordings	When using BASE services	- Security - Fraud management - Quality improvement	Legitimate interest Contract performance Consent	No storage, except for recording of phone calls for quality purposes (depending on the case)	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc.
		Behavioral data:	e.g. how you navigate the TV box menu or our websites (data obtained via cookies)	When using BASE services, visiting our websites and apps	- Product and service provision , invoicing - Quality improvement - Marketing of own products - Marketing of third-party products - Anonymized reporting	Legitimate interest Contract performance Consent	36 months for existing customers, 3 months for former customers. Retention period for data obtained from cookies depends on the type of cookies (see BASE cookie policy)	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
	Derived data	Profiles	e.g. high consumer, Network score, MyBASE App user	Derived from user and transactional data	- Product and service provision , invoicing - Network management - Sales, after-sales service and customer support - Quality improvement - Marketing of own products - Marketing of third-party products - Anonymized reporting	Legitimate interest Contract performance Consent	120 months for existing customers, 24 months for former customers	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
	Sensitive data	Medical data	e.g. social tariff certificate, guardianship	Received from customer when creating and managing a customer's account	- Sales, after-sales service and customer support - Fraud management	Legitimate interest Contract performance	No storage certificate. Guardianship data are in line with the retention period for identification data	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group
Prospects	User data	Identification and contact details	Name, address, telephone number, e-mail address, ID check data (such as ID card number) in the customer creation process (e.g. online order cancelled)	Third-party purchases, registration for events, competitions, attempt to create customer file	- Sales, after-sales service and customer support - Quality improvement - Fraud management - Marketing of own products - Anonymized reporting	Legitimate interest Consent	Until withdrawal of consent (with continuous refresh)	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group

		Communication data	"Opt-out" setting, recording of customer service call	Customer service call, shop visit, contact via contact form	- Sales, after-sales service and customer support - Quality improvement - Marketing of own products	Legitimate interest Consent	Until withdrawal of consent 1 month for customer service recordings	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
Visitors	User data	Identification data:	Surname, first name, name of company represented, ID card, license plate, CCTV images	Visit BASE offices, BASE outlets	- Security	Legitimate interest	13 months	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman)
	Transactional data	Behavioral data:	Data obtained via cookies	Visit BASE websites and Apps	- Quality improvement - Marketing of own products - Marketing of third-party products - Anonymized reporting	Legitimate interest Consent	Retention period for data obtained from cookies depends on the type of cookies (see BASE cookie policy)	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group. Solely with your consent: specific partners (see chapter 5)
Participants in competitions, campaigns, surveys, webinars, etc.	User data	Identification data	Contact details, images, video or audio recordings	Received from the participant	- Organization of campaigns, participation management, communication with participants	Consent Contract performance	Retention period is linked to the duration of the campaign and additional agreements with the participants, if any.	Specialized suppliers such as our marketing campaign or brand activation partners, production companies Our partners co-organizing campaigns
		Content data	Content submitted by the participants in the course of campaigns or competitions, such as audio samples, video recordings, or other materials	Received from the participant	- Organization of campaigns, participation management, communication with participants	Contract performance	Retention period is linked to the duration of the campaign and additional agreements with the participants, if any.	Specialized suppliers such as our marketing campaign or brand activation partners, production companies Our partners co-organizing campaigns

4. How do we safeguard your personal data?

The protection of your personal data is a definite priority for BASE. To this end, we have implemented appropriate technical and organizational security measures to protect any personal data in our systems and databases as much as possible from unauthorized access and/or use, loss or theft. These measures are regularly tested, evaluated and, where necessary, adapted in order to guarantee an adequate level of security at all times.

Our data security policy fully complies with the international ISO27002 standard and includes guidelines relating to, amongst other things, access control, data encryption, the security of operations and communications, physical security, etc. A specialized security team is responsible for implementing and monitoring the guidelines to ensure that the security of our databases, networks, infrastructure and information systems is guaranteed.

The development or implementation of new systems, applications or new products is designed with the highest level of security in mind, and always focused on your privacy (the 'privacy by design' principle). Our security and privacy experts work in close cooperation with the development teams to ensure that the appropriate protection is in place, commensurate with the assessed risks associated with the processing of the personal data in question. Access control is an important aspect of our data security policy. BASE has implemented procedures to limit access to our databases, systems, equipment and networks to those who strictly need this access to perform their job. These individuals must maintain strict confidentiality and comply with any guidelines that safeguard the protection of personal data.

BASE also provides privacy and security specific training for its employees in order to clarify guidelines and procedures and to make them aware of the risks involved in the processing of personal data.

BASE also imposes stringent security requirements upon partners and suppliers who process your personal data on our behalf. Also relying on contractual guarantees, we ensure that, just like us, they process your data safely and in accordance with privacy legislation. We consequently expect our partners and suppliers to implement a data security policy and security measures in accordance with international standards and best practices.

5. Do we pass on your personal data? And to whom?

In order to be able to offer you our services we sometimes rely on third parties, who will have access to your personal data. Data transfers to third parties shall only occur for the purposes described in section 3.c of this privacy policy. We have listed the parties to whom we transfer data below.

❖ Transfer of personal data to third parties working on our behalf

Some of our databases are accessible to third parties who are working on our behalf and helping us to provide our products and services. The following are a few typical examples:

- Commercial agents who sell our products;
- Companies and self-employed technicians who maintain our network and install the installations;
- External call centers that assist our customers by telephone on a daily basis;
- Logistics companies that deliver our appliances to you;
- The management of our external legal archive (e.g. invoices), in both digital and paper format;

- Companies that manage our outgoing paper document flow (e.g. invoices);
- Credit management specialists who analyze the solvency of prospective customers;
- Collection agencies and legal service providers within the context of collecting our invoices;
- Cloud providers;
- Security firms (cyber security);
- Companies specializing in ICT in support of our IT Team;
- Companies specializing in telecommunications and network infrastructure;
- BASE affiliated companies (belonging to the Liberty Global or Telenet group, who manage technical platforms or software applications for us);
- Specialized big data companies (data brokers and data analysts) within the context of data enrichment and data analyses;
- Market research companies;
- Marketing agencies that assist us with various advertising campaigns;
- Partners with whom we cooperate for a specific action (e.g. a travel agency for a competition whereby you can win a city trip);
- Specialized cookie analytics companies (such as Google and Adobe);
- Specialized companies that support us in our fight against spam and other abuse through our websites (such as, for example, reCAPTCHA Enterprise, part of Google);
- Universities with respect to product development and innovation;
- Social media channels such as Meta, Google, LinkedIn, etc. relating to, for example, direct marketing campaigns via these channels (they cannot use this data to also supplement their own data).

The transfer of your data shall always be limited to the data they need to perform their task on our behalf. We ensure that they manage your data securely, with due care and in accordance with the rules of good housekeeping - just like we do - and we implement appropriate contractual safeguards for this purpose.

❖ **Transfer of personal data within the context of a legal obligation**

The law compels us to transfer certain personal data to a number of authorized bodies. The following are a few typical examples:

- Emergency centers;
- Judicial authorities;
- Belgian intelligence services;
- Fiscal authorities;
- Central Number Database;
- The Belgian Institute for Postal Services and Telecommunications (BIPT);
- The Telecommunications Ombudsman Service;
- FPS Economy for the social tariff.

❖ **Transfer of personal data to other Telenet group companies**

We may transfer your personal data to affiliated companies within the Telenet group. The following are a few typical examples:

- To keep you informed about the products and services provided by the entire Telenet group;
- In the event of non-payment, we can also pass on your payment habits to protect the justified interests of the Telenet group.

Within this context companies of the Telenet group qualify as separate data processors and any data processing agreements are contractually agreed between the respective companies.

❖ **Transfer of personal data to third parties in the context of an acquisition or merger**

We may transfer your personal data to third parties in the context of an acquisition or merger transaction. This also applies to the preparatory phase of the transaction. Again, data processing arrangements will be contractually defined in a data processing agreement between the respective companies.

❖ **Transfer of personal data to third parties not operating on our behalf**

We can only pass on your data to other companies (with their own privacy policies) that determine the purposes for processing your data themselves, subject to your prior consent.

We may also, in certain cases, transfer your personal data to other parties who determine their own purposes for processing your data. These third parties therefore act as data controllers (or joint-controllers) and their own privacy policies apply (also).

This transfer is only possible if you have given your consent, if the transfer is necessary to fulfill the obligations of our agreement or to meet the legitimate interests of BASE or a third party.

The transfer is limited to only those personal data which are necessary and relevant for the intended processing.

Some examples of data transfer with **your consent**:

- Transfer of your contact information (name, address, phone number) to directory providers and intelligence services providers through the [Central Number Database](#).
- Transfer of your device identification number ('IMEI'), SIM card ('IMSI' or 'ICCID'), mobile network operator code (which identifies your mobile network operator 'MNC') and mobile country code (which identifies the country you are in, 'MCC') to [Belgian Mobile Wallet SA/NA](#) for their mobile identity solution: the 'Itsme' app.
- BASE may also allow third parties to place cookies on our websites for their own marketing purposes or pass on collected cookie data to third parties. This will only be possible providing you have given your specific consent. For further information on this topic please refer to the [BASE Cookie Policy](#).

Consent is given through the choices you have made in your privacy settings or specifically for the intended data processing after we have informed you about it. Consent may be withdrawn at any time.

Some examples of data transfer **in the context of contract performance**:

- To enable network interconnection (connection to other operators' electronic communications networks) and roaming, as well as all relevant administration (billing and settlement between operators), we will transfer your personal data to other telecom operators.
- We offer customers the possibility of paying for third-party services via their BASE bill (so-called "Direct Carrier Billing"). If you wish to make use of this, we will receive and pass on certain data to these *third parties to enable the billing and payment of these amounts to the third parties*. Some examples of what these services may include:
 - SMS parking;
 - Purchasing a ticket from a transportation company (De Lijn);
 - Participating in an SMS voting or calling game;
 - Purchase of digital services through Google (Play store), Apple (App store), Sony (PlayStation store)...

- Where you wish to participate in campaigns or creative competitions organized jointly by BASE and our partners, we may share your personal data with such partners, for the winners selection and follow-up, in accordance with the respective Rules of Contest. For example,
 - Where you take part in the Generation You Got This! Campaign feat. Camille Yembe, the profiles that you create on third party platforms and/or other information that you submit will be shared with Camille and her record label, acting as a Joint Controller, for winners' selection. Where you are registered on such third party platforms, or when you enter into additional agreements with Camille and her record label for further processing, such as production of artwork, they will be solely responsible for the processing of your personal data.

An example of data transfer **based on legitimate interests**:

- In connection with the assignment of receivables (factoring), we will transfer your data to the financial institution(s) with which we have entered into a contract for this purpose.

❖ **International data transfers**

Your personal data is also processed outside the European Union (the European Economic Area, also referred to as EEA). In fact, many large IT suppliers, infrastructure providers and technology companies are not actually based in the European Union.

The following are a few typical examples:

- External call center - Morocco;
- Maintenance of IT systems 24/7 - India, China, US;
- Network infrastructure - China;
- IT security - India, US;
- Cloud providers - US;
- Interconnect and Roaming - worldwide;
- Software applications - US.

When transferring your personal data outside the EEA, we always respect the requirements of the privacy legislation regarding international transfers:

- We may transfer personal data to countries that the European Commission has determined to provide an adequate level of data protection in accordance with European privacy legislation (GDPR), and
- We may transfer personal data based on the relevant modules of the European Commission's standard contractual clauses.

Moreover, we have aligned ourselves with the guidelines regarding international data transfers issued by the European Data Protection Board. For each international transfer, we conduct a Data Transfer Impact Assessment to assess the legislation of the third countries and identify any practices that are incompatible with the obligations of the transfer mechanism. This analysis also allows us to identify additional security, contractual and organizational measures to protect the data from unauthorized access by the third country government authorities.

6. How long do we keep your personal data?

We are not allowed to keep personal data any longer than is necessary to achieve the purposes for which it was collected. We have defined a retention period for any personal data we process for each purpose. The retention period may consequently vary depending on the purpose. Please refer to the table under section 3.d for an overview of retention periods; that table always states the maximum retention period. The following are a few typical examples:

- Traffic data relating to communications and connections are never retained for more than 13 months;
- TV viewing behavior is stored for a maximum of 36 months;
- Recorded conversations with the BASE Customer Service are stored for a maximum of 30 days;
- Invoice data will be retained for a maximum of 7 years;
- Your contract and order confirmations are retained for a maximum of 10 years after you have left BASE as a customer;
- Where you take part in a contest, competition or campaign (co-)organized by BASE, your personal data will be retained for the duration of the campaign and follow-up.

Upon expiry of the applicable retention period(s), personal data is automatically deleted or anonymized. If you cease to be a BASE customer, we can still contact you up to 3 years after you left to notify you about a new offer.

7. Use of your personal data for commercial purposes

We use your data primarily to be able to provide you with a good service. For example, to perform the contract, to make your service work, to manage our network, to be able to support you properly as a customer, to inform you about your usage, to send you your invoice, etc.

In addition, we also use your data for commercial and analysis purposes. As a customer, you decide for yourself for which purposes BASE may use your data. We have developed a system of privacy settings for this, allowing for different degrees of data use. Of course, you also retain the right to object to any use of your personal data for commercial purposes (the so-called 'opt-out'). You can manage your choices via your privacy settings in My BASE. More information on how this works can be found in section b of this chapter.

Important to know:

- By 'customer' we mean the person who signed the contract. This is limited to private customers, self-employed persons and small businesses (such as sole proprietorship).
- Privacy settings are registered at contract level. This means that everyone who uses this product (e.g. TV products) within the same contract is subject to the same choices. To change the privacy settings, you must be the contract holder or administrator.
- If you are a former customer, your privacy settings remain in effect. You can, of course, always have these adjusted, as is the case for active customers.

a. What privacy settings are there?

As explained above, you can decide for yourself which data we may use for commercial purposes, based on your privacy settings. You can choose from various gradations, ranging from not using any of your personal data for commercial purposes at all, to a fully personalized experience. We have divided the choices into different categories, depending on the objective:

- Marketing for BASE products and services
- Viewing data for better programmes

In addition, you also have various communication preferences, per medium:

- E-mail
- SMS
- Digital media

If the digital media choice is switched on, we may show you advertisements for our products on the channels of social media platforms (Facebook, Google (e.g. YouTube), etc.) if you have an account there. We share your name, e-mail address and/or telephone number. This allows them to know whether you have an account. They cannot read your data: it is first converted into numbers and letters (hashing) using an encryption key. Facebook, Google, etc. also already have your name and e-mail address themselves and have likewise converted these into the same numbers and letters. This allows them to match your name and e-mail address with the data they also hold, and to know who is eligible to be shown the advertisement. After matching, they delete the uploaded data. They may not use it for any other purpose (e.g. to enrich their own files), which in any event would not be possible since it is unreadable to them. After matching, they know who is eligible for the advertisement. Which advertisements someone has received may be used by the platforms for AI training. For this, we refer you to the privacy policy of these platforms. It is possible to switch off the use of your data for AI training on these platforms.

For communication by phone and mail, you always have the following options for unsubscribing:

- **if you do not wish to receive commercial calls**, you can subscribe to the so-called “do-not-call-me” list via their website (www.dncm.be) or by phone on 02/882.19.75;
- **if you do not wish to receive commercial mailings**, you can subscribe to the so-called Robinson list (www.robinsonlist.be).

❖ Marketing

We wish to inform you about our offers and products. We naturally always want to do this in a way that is relevant to you, and not intrusive. We offer you the following privacy settings:

- **General information about our offer**

You only receive general, non-personalized offers and information from us. We only use your name, address, e-mail address and the products you have with BASE, without creating a data profile.

You can receive these offers via e-mail, SMS, post, the BASE app, websites or other channels for which you have given your approval.

- **Tailored information about our offer**

You receive personalized offers and information from us. To make this as relevant as possible for you, we create a data profile.

This includes data such as your name, address, e-mail address, products, family situation, age, customer service contact, visits to our websites or apps, programs you watched, and your general invoicing data such as overall internet and telephone usage.

For new customers, this setting, as well as the previous one, is switched on by default, but this can be changed at any time.

- **Tailored information about our offer, using traffic data**

You receive personalized offers and information from us. To make this as relevant as possible for you, we create a data profile.

This includes data about your name, address, e-mail address, products, family situation, age, customer service contact, visits to our websites or apps, programs you watched, detailed invoicing data, and detailed data from your internet and telephony traffic (what we call traffic data, such as the times at which you use the service, which devices you use, the connection to mobile masts, etc.). We consider it important to mention that the content of your communication is not processed.

❖ **Viewing data for improving programs**

In your viewing data we see how long and when you watch programs. We share this information, segment data, and the encrypted number of your decoder and your customer number with TV channels, such as Play Media, VRT and DPG Media. This way they know which programs are popular. We never share your name.

❖ **Opt-out**

Would you like none of your data to be used for commercial purposes at all? We understand! This can easily be done by switching off the marketing settings and deactivating all communication channels. This way, you will not receive any advertising from BASE whatsoever. No commercial profiles will be created about you and your data will not be included in commercial analyses.

Please note that you will still receive communications for service reasons, such as, for example, an announcement of works, a change to security settings, a warning that you are approaching your data limit, or your invoice. You cannot stop this for as long as you remain a customer.

Summary table

Setting	Advertising?	Based on what data?	Still communication for service?
Opt out (no marketing + all communication channels off)	Yes	None	Yes
Marketing			
General communication about our offer	Yes, but not personalized No, if you turn off all your communication channels.	Name, address, e-mail address, and product portfolio	Yes
Tailor-made communication about our offer	Yes, personalized No, if you turn off all your communication channels.	Name, address, e-mail address, products, family situation, age, customer service contact, visit to our websites or apps, programs you watched and your general billing information such as global internet and telephone usage.	Yes
Tailor-made communication about our offer, based on traffic data	Yes, personalized No, if you turn off all your communication channels.	Name, address, e-mail address, products, family situation, age, customer service contact, visits to our websites or apps, programs you watched, detailed billing information, and detailed data from your internet and telephone traffic.	Yes
Viewing dates for better programs	Yes	How long and when you watch programs. We share this info, segment data and the encrypted number of your decoder and your customer number	Yes

b. How can you adjust your privacy setting?

Being a BASE customer, you obviously retain control of your data for commercial use.

You can consult and adjust your privacy setting upon simple request via the:

- [BASE customer zone](#) (only for customers/users with an active account/profile and former customers for whom the BASE customer zone is still active)
- Through our Customer Service (after ID verification)
- [My BASE app](#)

Please remember that processing your preference may take a while (maximum 72 hours). Any adjustment to your privacy setting does not affect the lawfulness of previous processing operations.

You always have the option to enable or disable your communication channels. Changing your privacy settings does not affect your choice of communication channels, and vice versa.

Please also note: if you are a former customer, your privacy setting will continue to apply. You can also have this changed at any time as described above.

If you have never been a customer, e.g. you have participated in a competition or we have obtained your data from a third party and you do not want BASE to send you advertisements or to use your data for our commercial purposes, you can:

- Use the unsubscribe link which you can find at the bottom of the marketing e-mail from BASE;
- Contact us using [this form](#);
- Visit a [BASE shop](#) and ask a staff member to launch a request for 'Right to object' or a 'full unsubscription from all commercial communications'.

8. What are your privacy rights and how can you exercise them?

To give you more control over your personal data, you can easily manage it by submitting a request to exercise your privacy rights.

a. Overview of your privacy rights

❖ Your right of access

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 about you. We will initially provide you with an automatically generated standard report. If this does not meet your expectations, or if you need specific information, you can submit an additional request via the link included with the standard response.

❖ Your right to update personal data

You have the right to have incomplete, incorrect, inappropriate, or outdated personal data corrected. In order to keep your data up to date, we would ask you anyway to notify us of any change, such as a move, a change of e-mail address or a renewal of your identity card.

❖ Your right to the erasure of personal data (the “right to be forgotten”)

You have the right to have your personal data deleted if:

- your personal data is no longer needed for the purposes for which it was collected or otherwise processed by BASE;
- you withdraw your previous consent for processing and there is no other legal ground for (further) processing BASE can rely on;
- you object to the processing of your personal data, and there are no more compelling legal grounds for (further) processing by BASE;
- your personal data is being processed unlawfully;
- your personal data must be deleted in order to comply with a legal obligation;
- your personal data was collected when you were a minor.

Do bear in mind that we cannot always delete all the requested personal data, for example when processing of this data is required for the provision of your service, to exercise a legal claim, or because the data is needed in order to comply with a legal obligation or to fulfil a task which is in the public interest.

❖ **Your right to restrict the processing of data**

In specific cases you are entitled to limit the processing of your personal data. This is the case, for example, when you dispute the accuracy of personal data or when your data is no longer required to achieve the processing purposes, but you need it to instigate, exercise or substantiate a legal claim.

❖ **Your right to portability of personal data/the transfer of data**

You have the right to 'retrieve' your personal data, for example, in order to be able to change your service provider more easily. This can only be done for personal data that you have provided to BASE yourself, on the basis of consent or agreement.

❖ **Your right to object to the processing of your personal data**

You have the right to object if BASE uses your personal data for purposes other than those necessary for the implementation of an agreement or to comply with a legal obligation. You will need to submit a substantiated request (outlining the specific reasons why you wish to object to the processing) and BASE will, in the event of a justified request, stop the use of your personal data unless we have compelling reasons for not doing so.

A substantiated request is not required when it comes to processing within the context of Direct Marketing activities (including profiling). You always have the right to oppose the use of your personal data for Direct Marketing purposes without having to provide a reason. Two options are available:

- ***You no longer wish to receive any kind of commercial communication?*** You can exercise your 'right to object' via the BASE customer zone (Request: 'Full unsubscription from all commercial communications') and we will then make sure that you no longer receive any commercial communications from us. Bear in mind that we will still contact you with respect to performance of your contract or if the law obliges us to do so. If you do not wish to use your BASE customer zone account, you can go to a BASE shop to do so or contact us using this form.
- ***Do you wish to choose the channel via which you receive commercial communications?*** You can opt to receive commercial communications only via e-mail or text message. To deactivate a channel, simply make your preference known to our [customer service](#) or through your privacy settings.

Furthermore, anyone (including former customers and prospects) can make use of these unsubscribe options:

- if you do not wish to receive commercial calls, you can subscribe to the so-called "do-not-call-me" list via their website (www.dncm.be) or by phone on 02/882.19.75;
- if you do not wish to receive commercial mailings, you can subscribe to the so-called Robinson list (www.robinsonlist.be);
- if you no longer want to receive commercial text messages, you can reply "STOP" to the number that sent you the text message;
- if you no longer wish to receive commercial e-mails, you can use the unsubscribe option in the relevant e-mail.

Remember: the fact that you no longer wish to receive commercial communications from us does not affect our right to contact you with respect to the performance of your contract, or if we are obliged to do so by law.

b. How can I exercise my privacy rights?

You can exercise your privacy rights in two ways:

- **Are you a BASE customer?** Sign in via the [BASE Customer Zone](#) and select “GDPR request” (or launch your request [here](#))
- **Are you not (no longer) a customer or do you not have an active account in the BASE customer zone?** If so, you can visit a [BASE](#) shop to submit your application.

To ensure that the request is made by the right person, we will need to verify your identity. If you launch your request via the BASE customer zone, your successful login and password will serve as your identification. If you submit your request via a BASE shop, we will ask you to identify yourself by means of your identity card. If we cannot identify you with certainty, we will not be able to respond to your request.

Remember: due to complexity, a different application procedure applies when exercising the privacy rights listed below. This concerns:

- The right to restrict the processing of data; and
- The right to object to the processing of your personal data if it is not for Direct Marketing purposes.

If you wish to exercise these rights, please submit your request to the Data Protection Officer (or “DPO”) using this form, . Again, we will ask you to identify yourself before acting upon your request.

Is there a charge? You can exercise your privacy rights free of charge, unless your request is manifestly unfounded or excessive, in particular due to its repetitive nature. In such cases we have the right and the option - in accordance with privacy legislation - (i) to charge you a reasonable fee (which takes into account the administrative costs of providing the requested information or communication and the costs involved in taking the requested measures), or (ii) to refuse to comply with your request.

In which format will I receive a reply? If you submit your request electronically, the information will be provided electronically where possible, unless you request otherwise. In any event, we will provide you with a concise, transparent, understandable and easily accessible response.

When will I receive a reply? We will respond to your request as soon as possible, and, in any event, within one month of receipt of your request. Depending on the complexity of the requests and the number of requests, this period may be extended by a further two months, if required. If the deadline is extended, we will inform you accordingly within one month of receiving the request.

What if BASE does not respond to my request? We will always inform you in our response about the possibility of submitting a complaint to a supervisory authority.

9. Use of Generative Artificial Intelligence (AI)

How BASE uses AI

Like many other technology companies, BASE uses artificial intelligence (AI), including generative AI ("Gen AI"), to improve and increase the efficiency of its services. This includes, for example, answering questions through our Gen AI chatbot, optimizing our network, detecting fraud or faults, and supporting our customer service. AI helps us to help you faster and better, but does not replace BASE's ultimate control over, and responsibility for, these processes.

Your data is not used to train AI models

BASE draws a clear distinction between *using* AI technology to help you, and *training* AI models with your data.

Your personal data is not used to train public or external generative AI models (such as, for example, large language models that are also used by other companies). When BASE deploys AI technology from external partners, this is done within a strictly defined and secured framework: your data remains the property of BASE, is not shared with third parties for their own purposes, and is not used to improve or train the underlying AI models of those partners.

Our Gen AI chatbot

BASE offers an AI-powered chatbot to help you more quickly with your questions. This chatbot uses generative AI technology to understand your question and formulate a tailored answer based on our own knowledge base and data about your account or contract.

What this means for you:

- **You always know when you are talking to a chatbot.** BASE makes it clear when you are communicating with an automated system rather than an employee.
- **Your conversations are not used to train AI models.** The content of your chat conversations is used solely to help you at that moment (and, where necessary, in a follow-up contact), and to monitor the quality of our own services — not to train or improve underlying AI models, including those of our technology partners.
- **You can always be referred to an employee.** For more complex questions, complaints, or whenever you would simply prefer to, you can switch to a human customer service employee at any time.
- **Your data is processed securely.** Data processed via the chatbot remains subject to the same security measures and retention periods as your other personal data held by BASE, as described elsewhere in this privacy policy.

Gen AI in the call center

BASE uses Gen AI in the call center; this technology listens in on the call and produces transcripts of it. These transcripts are used for analyses relating to the operation of the call center and the quality of the calls.

10. How can I contact BASE about my privacy?

❖ I want to exercise my privacy rights.

- Are you a BASE customer? Sign in via the [BASE Customer Zone](#) (or launch your request [here](#)).
- Are you not (no longer) a customer or do you not have an active account in the BASE customer zone? If so, you can visit a [BASE shop](#) to submit your application or contact us via [this form](#).

❖ I would like to adjust my privacy level.

You can consult and adjust your privacy setting upon simple request via the:

- [BASE customer zone](#);
- [BASE shops](#);
- [My BASE app](#)

❖ I would like to report a breach of privacy to the Data Protection Officer.

Report a breach of privacy using [this form](#).

❖ I have another question about the processing of my personal data.

If you have a question about the processing of your personal data and cannot find the answer in this privacy policy, please contact us using [this form](#).

You can also send your question, complaint or request by letter for the attention of the Data Protection Officer (or "DPO"):

Telenet Group NV (BASE)
Liersesteenweg 4
2800 Mechelen

11. Keep up to date with changes

BASE may amend this privacy policy from time to time, for example in response to market developments and new processing activities at BASE. We would consequently advise that you always consult the latest version of this policy on our website (<https://www.base.be/en/legal-information/privacy-policy.html>) We will, of course, notify you in advance of any content change via our websites or other commonly used communication channels and, when required by law, we will ask for your prior consent for our (new) processing activities.

In the event of contradiction, our general terms and conditions and the extraordinary terms and conditions that apply to specific BASE products and services shall take precedence over this privacy policy.

12. Escalation to the supervisory authority

The Data Protection Authority is an independent body which ensures that your personal data is processed in accordance with the law. If you have a complaint concerning the processing of your personal data by BASE, or if you wish to initiate a procedure for mediation, you can contact the Data Protection Authority via [this link](#).

Last Updated 31/07/2026