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'.

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?

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"). The majority shareholder of Telenet Group Holding SA/NV is Liberty Global plc.

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;
- 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.

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 *This data is directly linked to you as a person, regardless of your products or services*	• **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, 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,…; • **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, etc.; • **Communication data**: data relating to our communications with you, such as your interactions with our customer service, audio recordings of customer service calls, 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, etc.

Transactional data
 	
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.
	• **Technical data**: 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 SIM card such as which mobile phone mast 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.);
	  ○ **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**: Data concerning visits to our websites: we use cookies to collect certain data when you visit our website such as 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 *This data is derived from your user and your transactional data.*	**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. We also rate your mobile network based on how well or badly it performs. 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", "active MyBase user" or "network 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. 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 *Some personal data is of a more sensitive nature and is additionally protected by privacy legislation*	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, 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 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 identification numbers of the devices linked to our mobile network, call data, call numbers and transit volumes, location and time of calls.

- Finally, we also obtain personal data via third parties. The following are a few typical examples:
    - *We request credit rating analyses for future customers from specialised firms;*
    - *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 Facebook, Google, LinkedIn, etc. (e.g. when you use your social media profile to log in or when you contact us via this channel).*

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, 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	Contract performance Legal obligation (e.g. in the context of counter-terrorism)

	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).	Legitimate interest (e.g. to prevent fraud)
Products and Services Invoicing Dispute management	We use your data to set up, maintain and support your 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. 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 (e.g. text message parking, purchasing tickets from De Lijn, participating in a text based vote or phone game, etc.), we will process certain data and pass it on to third parties in order to enable invoicing and payment of these amounts to these third parties.	Contract performance
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. We also process this data for technical and statistical analyses, and the results are reported anonymously within BASE.	Contract performance 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 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). 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.	Legitimate interest
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 will also send you newsletters and invitations to events or competitions, etc. Advertising is more effective if we tailor it successfully to your requirements, which is referred to as 'personalized' advertising. 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	Legitimate interest (e.g. for general advertising) Consent (e.g. for personalized advertising)

	choices via your privacy settings. You also have the option to completely opt out of advertising. Further information on this topic can be found in Chapter 7. We may also approach you when you are no longer a BASE customer or we consider you a potential future BASE customer, providing you have given appropriate consent. We may also approach you with a personalized offer when you call us or visit and log into our websites.	
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 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
Security	You will also be recorded by our security cameras in and around our 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. Your data may also be processed within the context of network and information security.	Legitimate interest 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. In addition to general tax and accounting obligations, 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.	Legal obligation
Anonymized reporting	We use your data, for example, to report internally and externally on the use of our services. We use the information obtained from these studies and analyses to evaluate our current portfolio of products and services and adapt it to new developments. We also use your location data (connection of your SIM card to the mobile phone mast) to create anonymous location reports ('how many people were in a certain location at a certain time?') for event organizations, supermarkets, cities/municipalities, etc. These reports are completely anonymized and cannot be traced back to a particular individual.	Legitimate interest

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.

• **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.

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 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	Specialised suppliers such as our call centers, IT support companies, data analytics companies, etc. The government (police, ombudsman), social media platforms (only if you have privacy setting 'Targeted', they cannot use this data for their own purposes). Companies in the Liberty Global and Telenet Group. Solely with your consent: specific partners (e.g. Itsme)
		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, user name, invoice, order confirmation, contract	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	Specialised 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 (e.g. Itsme)
		Lifestyle and usage habits	.e.g. leisure activities, travel habits	Purchase from third parties	- Marketing of own products - Marketing of third-party products	Legitimate interest Consent	13 months for existing and former customers	Specialised suppliers such as our call centers, IT support companies, data analytics companies, etc.
		Family details:	e.g. civil status, family members	Purchase from third parties	- Product and service provision, invoicing	Legitimate interest	As long as you are a customer.	Specialised suppliers such as our call centers,

					- Network management - Sales, after-sales service and customer support - Quality improvement - Fraud management - Marketing of own products - Marketing of third-party products - Anonymized reporting	Contract performance Consent	Up to 36 months for former customers	IT support companies, data analytics companies, etc.
		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.
		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	- 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. Other data: existing customer as long as you are a customer (privacy setting) or up to 24 months (survey answers), ex-customer: 36 or 24 months depending on type of data.	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc. Companies in the Liberty Global and Telenet group.
	Transactional data	Technical data:	e.g. 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	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.

				- Support for government applications and legal obligations - Marketing of own products - Anonymized reporting			Solely with your consent: specific partners (e.g. Itsme)
	Location data:	e.g. connection to mobile phone mast, GPS coordinates	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 - Anonymized reporting	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 (e.g. Itsme)
	Usage data	e.g. time of call, duration of call, URLs	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	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.
	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	Specialized suppliers such as our call centers, IT support companies, data analytics companies, etc.
	Behavioral data:	e.g. how you navigate our websites (data obtained via cookies)	When 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	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.

	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.
	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	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.
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.

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);
- Universities with respect to product development and innovation;
- Social media channels such as Facebook, 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;
- The Belgian Institute for Postal Services and Telecommunications (BIPT);
- The Telecommunications Ombudsman Service.

❖ **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 <u>not</u> 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. The following are a few typical examples:

- 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 (referred to as BM-ID) 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.

Personal data is also passed on to other telecom operators to enable network interconnection (connection to other operators' electronic communication networks) and roaming, and all relevant administration (invoicing and settlement between operators). This data transfer is not subject to your prior consent as this is necessary to fulfill the obligations of our agreement. The other telecom operators act as data controllers.

❖ **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. We make certain that sufficient contractual guarantees are in place to ensure that they maintain the same level of security when handling your data. 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.

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. The following are a few typical examples:

- Traffic data relating to communications and connections are never retained for more than 13 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.

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.

Just one last thing:

Please note that we may not always be able to delete all the requested personal data when you wish to exercise your "right to be forgotten". If the processing of the data in question is (or was) necessary, for example, for the provision of your service or because of legal requirements, we will only be able to delete the data after the retention period has expired. If processing is not necessary, i.e. in the context of direct marketing, we will be able to respond to your request. Further information concerning your privacy rights and how to exercise them can be found in Chapter 8 of this privacy policy.

7. Use of your personal data for commercial purposes

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

We also use your data for commercial purposes. Your personal data may be processed to promote similar BASE products and services, to better communicate about our brand or for analyses to enable us to enhance our customer knowledge. You decide which data we are allowed to use via the BASE privacy settings. BASE privacy settings are based on 2 levels, i.e. 'General' and 'Targeted'.

BASE applies a particularly strict policy for minors (below the age of 16): the personal data of minors is automatically assigned the most restrictive privacy level, i.e. privacy level 'General'. Other than that, and where required by law, BASE will obtain prior consent from the minor's parent(s) or guardian(s).

In addition to privacy levels, there are also communication channels. You can choose how you want to receive advertising, i.e. by post, e-mail, text message or telephone.

a. What privacy levels are there?

As stated above, you can decide which data we can use for commercial purposes, in accordance with your privacy level. This can range from not using your personal data for commercial purposes at all to a fully personalized BASE experience.

❖ **No use of your data at all (Full opt-out)**

Let us start with a full opt-out from commercial purposes: you will not receive any advertising from BASE. In such cases we combine privacy level 'General' with switching off all your communication channels. This is referred to as a 'full opt-out'.

Privacy level ‘General’ implies that no commercial profiles are created for you and you are not included in commercial analyses. Moreover, with a ‘full opt-out’ all communication channels will be switched off to ensure that you no longer receive commercial mail, e-mails, telephone calls or text messages from us.

You will continue to receive communications for service reasons, e.g. concerning upcoming works, changes to security settings, to notify you that you have reached your data limits or to send your invoice. You cannot stop these while you are still a customer.

❖ **Privacy level 1: General**

Privacy level ‘General’ implies that no commercial profiles are created for you and you are not included in commercial analyses.

If you choose privacy setting ‘General’, you will only receive general (non-personalized) commercial communications that are legally acceptable on the grounds of BASE's legitimate interests.

We only use a very limited set of your user data, such as your name, address, e-mail address, language preference, gender (for the correct title) and product portfolio. We do not use any of your transactional data for commercial purposes (but still use it for service reasons, otherwise you wouldn’t be able to call or surf). No commercial profiles are created. Your data will not be used in commercial analyses.

Your location data (the connection of your SIM card with mobile phone masts) is not included in the anonymous reports that we make available to cities, towns, shopping centers, etc.

Finally, at this level we do not share any data with social media platforms such as Google (e.g. YouTube), Facebook, etc. This means that the advertising campaigns you may see on these platforms are not personalized.

❖ **Privacy level 2: Targeted**

This level represents personalized advertising for BASE products. We use your user and transactional data to build commercial profiles (derived data) and include them in commercial analyses. You will receive this personalized advertising whenever your communication channels are switched on.

To find out more about user data and transactional data, please refer to section 2.a of this privacy policy. We would like to stress that we don’t use all the content of this data. For example, we will not use the copy of your ID card, your photograph (if we have one), sound and image recordings, national registration number, etc. in commercial analyses or to build up profiles of you.

As a new BASE customer, you will automatically be activated in privacy setting ‘Targeted’, which means that we use your personal data to build commercial profiles and perform commercial analyses with the aim of providing you with personalized advertising for our BASE products and services. Obviously, you will remain in control of your data for commercial use, which means that you can object to personalized advertising at any time by adjusting your privacy setting to 'General’.

Contrary to the ‘General’ level, your location data (the connection of your SIM card with mobile phone masts) is included at this level in anonymous reports that we make available to cities, towns, shopping centers, etc. Please note that these reports are completely anonymous. For example, a

report may be provided on how many people visited the Grand Place in Brussels during the holidays, or how many people drive into Mechelen via the motorway.

We may show you advertisements for our products on the channels of social media platforms (Facebook, Google (e.g. YouTube), etc.) if you are an account holder. We may let them know who we want to show or not show the advertising to. We share your name, e-mail address and/or telephone number. This is how they know whether you have an account. They cannot read your data as it is first converted into numbers and letters (hashing) in accordance with a specific key. Facebook, Google, etc. will also have your name and e-mail address and will have converted this information into the same number and letter sequences. This enables them to match (compare) your name and e-mail address with the data they have and as such they know who can be shown the commercial. Once matched, the uploaded data will be deleted by them. They cannot use it for any other purpose (e.g. to supplement their own files), which wouldn't be possible anyway as they cannot read it. Once the data has been matched, they know who is eligible for the advert. They must also delete this data upon termination of the campaign (the period during which the advertisement is shown).

Summary table

Privacy setting	Do you receive advertising?	On the basis of which data?	Do you still receive communications about our service?
I do not want advertising and I do not want to be profiled: 'Full opt-out' (privacy setting 'General' + all communication channels switched off)	No	Not applicable	Yes
I do not want to be profiled: Privacy setting 'General'	Yes, but not personalized No, if you have your communication channels switched off	Name, address, e-mail address, language preference, gender (for correct title) and product portfolio	Yes
I would like to receive advertising tailored to my preferences (my profiles): privacy setting 'Targeted' = our default level	Yes No, if you have your communication channels switched off	User and transactional data. Derived data	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
- BASE shops
- 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.

With each privacy setting, you also have the choice to switch your communication channels on or off. Changing the privacy level has no effect on your communication channels.

If you do not wish to receive any further advertising and you do not want your data to be used for any commercial purposes ('full opt-out'), you can request 'a complete removal of all communications' (i.e. the right to object). With a request of this nature your privacy level will be set to 'General' (if it is not already set to that) and all communication channels will be switched off. How to make a "right to object" request is explained in Chapter 8.

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. Remember to include the term 'privacy' in the subject line;
- 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.
- ***Do you wish to choose the channel via which you receive commercial communications?*** You can opt to receive commercial communications only via e-mail, text message, mail or phone. To deactivate a channel, simply make your preference known to our customer service or visit one of our BASE shops.

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 (www.dncm.be);
- 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, clearly indicating 'privacy' in the subject line. 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. 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.

❖ **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 and remember to include the 'privacy' in the subject line.

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

Telenet Group NV
Liersesteenweg 4
2800 Mechelen

10. 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.

11. 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 https://www.gegevensbeschermingsautoriteit.be/burger/acties/klacht-indienen.

Last Updated 03/08/2022