PRIVACY POLICY FOR EMPLOYEES

INTRODUCTION

Dear employee, Telenet group is responsible for the collection and use of your personal data, and we protect it with due care. How we handle privacy is part of the responsibility we have to our employees. We aim to be clear about how important our employees' privacy is and how it is protected. Telenet group ensures compliance with all applicable laws and regulations, including the General Data Protection Regulation (AVG).

This Privacy Policy informs you on the processing of your personal data, which personal data is collected about you, what types of processing activities are carried out, with whom we share your data, how we protect it and what privacy rights you have.

I. Who are we?

We are Telenet group (with registered offices at Liersesteenweg 4, 2800 Mechelen). This privacy policy applies to employees (see further below) of the following entities of the Telenet group group:

- Telenet Retail BV
- Telenet Group NV
- Telenet BV

II. Who is protected by this privacy policy?

This Privacy policy applies to all our employees, i.e. all Telenet group employees and all other individuals employed by Telenet group, including those who are temporarily made available to Telenet group by a third party without being bound to Telenet group by an employment contract or a nominal service agreement. For the purposes of this privacy policy, the term “employee” shall include our current and former employees and everyone who works for Telenet group, including:

- independent service providers,
- personnel of our suppliers,
- consultants,
- interim workers,
- interns,
- student workers,
- volunteers.

This insofar as Telenet group processes personal data of these individuals.

Please note that there is a specific policy for job applicants which you can access when you open an outstanding vacancy on our vacancies' website.

III. Which personal data does Telenet group process, and why?

WHAT DATA DO WE PROCESS?

This policy applies to all personal data collected, processed and stored in the context of your employment relationship. Personal data is data relating to an identified or identifiable person. It is therefore any information that directly or indirectly identifies a natural person, such as a name, employee number, telephone number, address, date of birth, but also an IP address, a photo, a fingerprint, etc. We may process different categories of personal data related to our employees, always in accordance with the conditions of the applicable specific legal provisions or Collective Labor Agreements. You may find the summary of the data that we collect in the table below.

Identification details	Data that can identify you like your name and first name, address, e-mail address, phone number, identity card number, date of birth, place of birth, social security number, license plate, employee number etc.
Photos and videos	Images of you or videos, e.g. when you take part in an employee event, images from surveillance cameras, etc.
Communication data	Audio recordings (e.g. in the contact center), transcripts & summaries of the calls, chats with customers, etc.
Family data	Marital status, family composition, name of the spouse or partner, number of children, name and contact details of persons to be contacted in case of an emergency, etc.
Professional details	Overview of your career, CV, references, job application letter, training & development, resignation letter etc.
Contract data	Employment contract, payslips, tax documents information etc.
Financial details	Bank account number, salary, bonuses, other benefits granted by Telenet group, payments made by Telenet group, information regarding meal vouchers, pension plan, data related to your retirement, expense notes etc.
Mobility data	Information related to company cars, fuel card, other mobility plans, etc.
Logging and monitoring data	Logging data related to your usage of the Telenet group applications & devices, login and passwords to access Telenet group applications etc.
Collaboration data	Data regarding your online collaboration and communication on Telenet group platforms (e-mails in Outlook, posts on the intranet, meeting minutes, meeting recordings, chats in Teams, etc.)

Data relating to your presence in Telenet group buildings and to homeworking	Use of access badge, registration of days of presence at the office or of homeworking in the dedicated tools, connections to homeworking servers, registration of access to the technical buildings like the head ends, server rooms etc.
Prompts	Prompts used in AI tools provided by Telenet group
Health related data	Health-related data, to carry out our obligations regarding the employment legislation and social security, such as health monitoring at work, health assessments, occupational accidents, medical certificates with regard to incapacity for work, data related to pregnancy and maternity, birth, adoption or foster leave, etc.
Performance data	Disciplinary files, performance evaluation results, assessments, etc.
Mandates	Legal mandates (positions held in other organizations)
Extract of criminal record for security screening	For specific positions, we are required by law to screen our employees and collect criminal record abstracts
Behavioural data (cookies)	Data collected via cookies placed on the internal HR intranet pages (to analyse how the page visitors navigate, to count how many visitors consult the pages etc.)

Why do we process this personal data?

The table below provides a summary of the purposes and legal bases of the processing of your personal data:

Purposes	Description	Legal basis
Employee administration and management	This purpose relates to all activities regarding employee administration and management including: Payroll administration, bonus calculation; Management of collective and other insurances, pensions; Work planning (planning and monitoring of tasks, workload and performance); Time registration and holiday planning; Management of your personal employee file; Career development, selection of training courses and study tracks; Mobility management.	**Contractual obligation**, in order to ensure the proper execution of your employment contract, such as the payment of your salary or the reimbursement of your professional expenses **Legal obligation**, to comply with the legal requirements, such as the obligation to electronically transmit data relating to employment contracts to administrative bodies in order to comply with social and tax legislation **Legitimate interest,** in order to ensure good human resources management as well as the development, monitoring and management of employees
Employee Health & Safety	Activities related to the safety, health, and welfare of people at work including: Absence management; Incident management; Reporting.	Legal obligation, the processing is necessary according to a legal obligation

		Legitimate interest, the processing is provided for in labor law, social security law or a collective agreement.
Security screening	Retrieval of the extract from the criminal record for the functions where a security check is to be done. This retrieval is done by a designated team at Security and is kept separately on a protected folder	Legal requirement, for specific functions, we are required by law to perform this security check (e.g., the Jambon law regarding the security guards)
IT Security, fraud and software management	Activities related to monitoring the use of IT infrastructure that is made available to the employees (telephone, e-mails, internet, applications), fraud prevention, fraud detection and license management.	Legitimate interest
Physical Security	Activities to assure the safety of goods and persons in and around our offices and buildings.	Contractual obligation Legitimate interest
Organization of employee events	Activities related to the organization of events including registering for participation, photographs, videos taken	**Consent**: in the relationship employer – employee consent does not constitute a legal basis as the employee is in a subordinate relationship with his/her employer and is not in a position to provide a free consent. Nevertheless, Telenet group believes it may rely on consent in exceptional circumstances where the consent can be freely given because employees will face no adverse consequences at all whether or not they give consent
Analytics and strategic workforce planning	Internal reporting, analytics and statistical insights, activities related to surveys such as ZOOM	Legitimate interest
Service quality control	Monitoring and analyzing interactions between customers and customer care team to monitor and improve customer experience and quality of service provided. Including call recordings for quality management	Legitimate interest
AI training	Activities related to the training of AI tools and the use of personal data to train large language models (LLMs)	Legitimate interest
Knowledge management and insights	Analyzing the use of provided applications including prompt monitoring	Legitimate interest
Analytics website visit	Cookies placed on website visit	If these cookies have no functional purpose but are intended to do analysis

		(such as count the number of visitors), consent is the legal ground

SPECIAL CASES

1. MONITORING THE USE OF IT TOOLS

Telenet group may collect data about you in the context of monitoring the use of your PC and access to the Internet, the IT systems, network and applications. This control is carried out to ensure the security, functioning of the IT tools made available to employees and the proper execution of obligations (stipulated in the labor contract or other contracts). In certain specific cases, also to ensure that employees respect Telenet group's ethical values and to protect the confidentiality of Telenet group's strategic, financial or commercial interests. The data that is collected for control purposes is confidential. In the event of a serious suspicion of illicit use or infringement, this data can be analysed according to certain very precise rules.

2. ACCESS TO THE EMPLOYEE'S BUSINESS E-MAILS AND DATA STORED ON HARD DISKS IN THE EVENT OF PROLONGED ABSENCE, SUSPECTED FRAUD, BREACH OF SECURITY POLICIES, DISMISSAL OR RESIGNATION

Telenet group may, in strict compliance with the principles of legitimacy, transparency, necessity and proportionality, access the employee's professional e-mails in the event of prolonged absence, investigation for fraud, suspected breach of the security policies, but also following the employee's dismissal or resignation. This access will only take place in cases where it is necessary to ensure the continuity of a service, to protect the interests of Telenet group and will always foresee in a four eyes principle (including security).

Every employee has the possibility to create a 'Private' Outlook folder in order to save his or her private e-mail communications. In the event of access to the e-mail inbox during a prolonged absence or investigation, any access to this folder by a person other than the employee in question is not allowed.

3. INSIGHTS AND ANALYTICS

Your personal data can be used in internal analytics that help Telenet group in making informed decisions, determine a proper HR strategy and create insightful reporting. Access to employee-level data is limited to the dedicated People Analytics team and only shared outside this team on an aggregated basis.

This includes, for example

- Analytics regarding telework supporting better resource management in hybrid work scenarios: data retrieved from the access badge system is processed to calculate the presence in the office and is reported on a team level basis. Team results are reported regardless of team size. As this points to objective and observable behaviour, we do

not apply the minimum threshold of 5 employees as we do with sensitive and subjective data like ZOOM results.

- Analytics regarding usage of the Microsoft applications for an optimal license distribution: statistical data retrieved from the Microsoft platform provides (quantitative) insights in your usage of the Microsoft applications (using Teams, Outlook, …). The statistics are not reported on but are used by Digital Workplace to prioritize and optimize software license distribution, for example for Microsoft Copilot licensing.

- Analytics regarding Viva Insights: aggregated reports on the Viva Insights metrics, enriched with the ZOOM results, provide meaningful insights in culture, meeting cost, work life balance etc.

- Analytics regarding hardware monitoring and asset management: statistical data regarding your PC (e.g. statistics on PC crashing, memory usage, apps installed) is collected and aggregated for insights in asset management and device allocation.

- Expedition T data driven individual recommendations: based on the qualifications you entered in Expedition T, internal vacancies and learning activities are recommended to you in Expedition T.

- Analytics for HR KPIs: data retrieved from the Zoom surveys, from the access badge system, and from HR applications (related to payroll and reward, collaboration, performance management, career path & learning) are combined for insightful correlations and reported on, on an aggregated basis.

4. DATA FOR AI TRAINING AND THE USE OF AI TOOLS PROVIDED BY TELENET GROUP

Telenet group offers multiple AI-supported tools. There are situations where AI tools will process your personal data. It is always contractually stipulated that the AI provider may not reuse the Telenet group data (and thus your personal data) e.g. to further train its AI model. An example of an AI tool that will process personal data is Agent Assist. Agent Assist is a tool that transcribes customer conversations and suggests a summary after the conversation. The tool also improves agent performance by providing real-time support during conversations, including instant feedback, live listening to questions and whispering answers to agents. This AI tool will listen in on the conversation and convert the conversation to a transcript. An instruction (a prompt) will also be given to a Gen-AI language model to summarize the transcription. Upon delivery of this summary, the transcription and instruction will be removed from the Gen-AI language model. The Gen-AI language model provider does not reuse the transcription. Just as the recordings are kept at Telenet group for one month, the transcripts are also kept for one month.

If Telenet group itself wants to train a gen-AI model, this is always done initially with non-personal data or synthetic data. Depending on the situation, it may still be necessary to use personal data for this purpose. In case such AI models need to be trained with personal data, these will be added to this privacy policy and the possibility of offering an opt out here will be considered.

To validate whether this agent assist has made a good transcription, it may be necessary at the development stage to listen to the recordings and compare them to the transcription. If you prefer not to, Telenet group offers you the right to opt out of the use of your recordings for this purpose (an opt out). See below title VIII (privacy rights) to read how to exercise the right to opt out.

As using AI tools is new, it is necessary to get coaching on prompting. The AI bot on the Genius platform improves the way the call center agents find the most optimal answers in the Genius articles. An overview of the prompts used by the call center agents can be pulled by the team coach to train in better prompting.

For more guidance on how to use AI, please visit the dedicated AI page on Tellit (Everything you need to know about GenAI) and the AI policy (Search Policy Documents).

5. Data Leak Prevention, Vulnerability and Malware Management

Specialized software may be installed or connected to all systems to detect potential security problems and data leakage risks in real-time.

This software provides alerts on identified vulnerabilities or threats, enabling us to address them promptly and effectively. Monitoring is generally performed in a global and non-individual manner. However, individual checks may be conducted in specific circumstances, such as preventing illegal or defamatory acts, protecting the company's economic interests, and ensuring the safety and proper functioning of the company's systems. This includes for example:

- IP logging and blocking of trusted/suspicious locations or IP ranges;
- Web monitoring to block, detect and investigate virus infections, abuse, data leaks;
- Monitoring to detect and investigate virus infections, abuse and data leaks;
- Virus scanning of e-mail;
- Overseeing email usage to check if internal emails are being forwarded to personal addresses;
- E-mail analysis in suspicion of fraud or legal infringement;
- Usage of data leak prevention capabilities on Telenet group applications to detect abuse and data leaks;

IV. HOW DO WE PROTECT YOUR PERSONAL DATA?

We take appropriate measures to protect the personal data that we use. To this end, we have implemented technical and organizational security measures to protect the personal data contained in our systems and databases as much as possible against unauthorized access and/or use, loss or theft.

These measures are regularly tested, evaluated and, where necessary, adapted in order to guarantee an adequate security level at all times.

Our information security policy is fully based on the international ISO 27002 standard, and contains guidelines with regard to access control, data encryption, security of operations, security of communications, physical security, etc. A specialized security team is responsible for the implementation and follow-up of the guidelines, so 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 security in mind, and always taking your privacy into account (the 'privacy by design' principle). Our security and privacy experts work closely together with the development teams to ensure that the appropriate protection is in place, commensurate with the assessed risk associated with the processing of the personal data.

Access control is an important aspect of our information security policy. Telenet group has implemented procedures to limit access to our databases, systems, equipment and networks to those persons who strictly need this access to perform their job. These persons must observe a strict obligation of confidentiality and comply with all guidelines for ensuring the protection of personal data. Access to the data of our employees in their employee file is limited to HR and management on a “need-to-know” basis. With regard to electronic information, users must authenticate themselves and enter a password before access is granted. Printed files regarding employees are stored in lockable cabinets in the HR office.

Telenet group also provides privacy and security-specific training for its employees, in order to clarify the guidelines and procedures to its employees and to make them aware of the risks involved in processing personal data.
Telenet group also imposes high security requirements on its partners and suppliers who process your personal data on our behalf. Partly by means of contractual guarantees, we ensure that, just like us, they process your data safely and with respect for the privacy legislation. We therefore expect our partners and suppliers to implement an information security policy and security measures that are grafted onto international standards and best practices.

V. DO WE TRANSFER YOUR PERSONAL DATA? TO WHOM?

Your personal data may be shared with the following parties:

THE THIRD PARTIES WHO PROVIDE SERVICES TO TELENET GROUP ACTING ON OUR BEHALF

Your personal data may be used by our suppliers who provide service to Telenet group for the same purposes stated above. It goes without saying that we only provide or make accessible the personal data that the provider needs to provide the service and they process your personal data on our behalf.

Here are a few examples:

- The social secretariat that carries out the payroll administration on our behalf;
- Talent platforms that help us map your skills;
- Digital workplace providers (such as Microsoft Office, etc);
- Companies specialized in ICT support and cybersecurity;
- Training companies;
- The companies responsible for access control and security in the buildings;
- Companies helping us deliver gifts to our employees;
- Companies helping us organize events for our employees;
- Documents management and storage platform Doccle (This data is processed for the purposes of automatically sending your payslips and tax documents to your Doccle account, enabling the storing of such documents. Please note that Telenet group is not involved nor responsible for the further storage and accessibility of your employment documents on/via your individual Doccle account, which shall outlast the termination of your employment relationship with Telenet group. This further processing of your personal data is under the responsibility and control of Doccle and subject to Doccle's terms, including its Privacy Policy).

TRANSFER OF PERSONAL DATA TO THIRD PARTIES WHO DO NOT WORK ON OUR BEHALF (ACTING AS CONTROLLERS)

We can also transfer your data to other companies who determine their own purposes for processing your data. This implies that their privacy policy is applicable.

Here are some examples:

- Fuel card providers (e.g. Eneco, Blossom, Total);
- Vehicle leasing & renting companies (e.g. Arval, Blue Bike). Leasing companies collect and process a multitude of data regarding your use of the company car (like location data, usage metrics etc). Check out their privacy policy;
- Insurance companies (e.g. Van Breda);
- Pension funds (e.g. the Telenet group pension fund, called IPB, processes your personal data to manage your supplementary pension rights);
- Electric car charging stations;
- SKIPR card (mobility);
- Degroof Petercam;
- Eco-cheques, meal vouchers (Sodexo, Edenred, Monizze);
- Work travel agencies.

OUR CUSTOMERS AND PARTNERS

In the context of our normal business activities, our partners (customers or all persons who make use of our services, suppliers and other (potential) contract parties), with whom you work in the capacity of employee, will receive your business contact details that is required for such activities.

IN THE CONTEXT OF POSSIBLE REORGANIZATIONS AND ACQUISITIONS

Your personal data may also be consulted by third parties who are involved in such possible transactions (in the context of a so-called "due diligence", for example), and this exclusively for the purposes of such a transaction. In such a case, the transfer of the relevant data is based on the legitimate interest of Telenet group, its shareholders and the third parties concerned with a view to the proposed transaction.

IN ORDER TO COMPLY WITH LEGAL REQUIREMENTS

Personal data may also be provided to other third parties in order to comply with legal requirements, such as:

- The tax authorities;
- Social security institutions;
- Labour inspection services;
- Prevention advisors;
- Bailiffs.

INTERNATIONAL DATA TRANSFERS

Your personal data is also processed outside the European Union (the European Economic Area, also called EEA). It's a fact that many large IT suppliers, infrastructure providers and technology companies are not based in the European Union.

Some examples:

- IT security – US (Crowdstrike);
- Support and maintenance – India (Cognizant);
- Digital workplace – US (Microsoft);
- Training, L&D – US (Datacamp);
- Cloud data storage – US (AWS).

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.

VI. How long do we retain your Personal Data?

We only retain your personal data as long as necessary for the purposes set out in this Privacy policy. In general, personal data is retained for the entire duration of the employment, under either an employment contract or a service agreement. After the termination of the employment, Telenet group must still retain personal data for a period depending on the processing purpose. After the applicable retention period(s) has(have) expired, the personal data will be deleted or anonymized.

Examples: Telenet group is legally obliged to retain all data that is part of the personnel register for a period of 5 years**.**

VII. Do we make use of so-called "automated individual decision-making"?

In principle, we do not make use of such automated individual decision-making. If such automated decision-making were to be used in the future, it will be implemented in accordance with the GDPR, and it will be ensured that the rights of the employees will be safeguarded at all times.

VIII. The privacy rights of our Employees

Based on the GDPR, you have the following rights in connection with the processing of your personal data by Telenet group. These rights are not absolute and exercising them may be subject to certain conditions and exceptions, as provided for in the GDPR.

YOUR RIGHT OF ACCESS

You have the right to know at any time from Telenet group whether or not we are processing your personal data, and, if we are processing your data, to view that data and receive additional information about the processing. You also have the right to receive a free copy of the processed data in an understandable form. Telenet group may request a reasonable compensation to cover the administrative costs of any additional copy that you request. If access to the personal data is refused, the reason for this will be communicated.

YOUR RIGHT TO THE CORRECTION OF PERSONAL DATA

You have the right to immediately have incomplete, incorrect, inappropriate or outdated data corrected. In order to keep your data up-to-date, we would ask you in any case to notify us of any changes, such as a move, a change of e-mail address or the renewal of your identity card. These changes can be communicated via a RM ticket.

YOUR RIGHT TO ERASURE (THE 'RIGHT TO BE FORGOTTEN')

You have the right to have your personal data deleted in the following cases:

- Your personal data is no longer necessary for the purposes for which it has been collected or otherwise processed by Telenet group;
- You withdraw your prior consent to the processing, and there is no other legal basis that Telenet group could invoke for the (further) processing;
- You object to the processing of your personal data and there are no more weighty, legitimate reasons for the (further) processing by Telenet group;
- Your personal data is processed in an unlawful manner;
- Your personal data must be deleted in order to comply with a legal obligation;
- Your personal data was collected when you were still underage.

Bear in mind, however, that we are not always able to delete all the requested personal data, for example, if the processing of this data is necessary in order to comply with our legal obligations.

YOUR RIGHT TO THE RESTRICTION OF PROCESSING

You have the right to obtain the restriction of the processing of your personal data if one of the following aspects applies:

- You dispute the accuracy of this personal data: the use will be restricted for a period sufficient to enable Telenet group to verify the correctness of the data;
- Your personal data is processed in an unlawful manner: instead of the deletion of your data, you may request the restriction of its use;
- Telenet group no longer needs your data for the original processing purposes, but requires it for the lodging, exercising or substantiation of a legal claim: instead of the deletion of your data, its use is restricted to the lodging, exercising or substantiation of the legal claim;
- As long as no decision has been reached regarding the exercising of your right to oppose the processing, you may request the restriction of the use of your personal data.

YOUR RIGHT TO OBJECT TO THE PROCESSING OF YOUR PERSONAL DATA.

You have the right to oppose the processing of your personal data on the basis of your specific situation if the processing takes place within the context of a legitimate interest of Telenet group, or in the context of the general interest. Telenet group will discontinue the processing of your personal

data unless it can demonstrate compelling and legitimate reasons for the processing that outweigh your reasons, or if the processing of the personal data relates to the lodging, exercising or substantiation of a legal claim (for example, the filing of a request at a court).

YOUR RIGHT TO THE TRANSFERABILITY OF PERSONAL DATA, OR "DATA PORTABILITY"

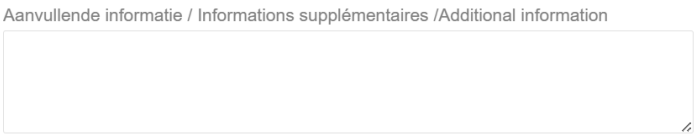
You have the right to 'recover' your personal data, for example, if you were to change your employer. This is only possible for the personal data you yourself have provided to Telenet group, based on consent or after agreement. In all other cases, you will not be able to exercise this right (for example, if the processing of your data takes place on the basis of a legal obligation).

This right involves 2 aspects:

- you may ask Telenet group to return the personal data concerned to you in a structured, standard and machine-readable form; and
- you may ask Telenet group to directly transfer the personal data to another data controller. You will thereby be responsible for the correctness and security of the (e-mail) address that you provide for the transfer. Telenet group has the right to refuse this if the transfer is not possible from a technical point of view.

HOW CAN I EXERCISE MY PRIVACY RIGHTS?

You can exercise your privacy rights via the online Privacy page on the Intranet (Tellit): Employee privacy (sharepoint.com). Formulate which right you want to execute in the field additional information:



Does this involve any costs? You can exercise your privacy rights free of charge, unless your request is manifestly unfounded or excessive, in particular if it is repetitive in nature. In accordance with the privacy legislation, we are, in such a case and at our discretion, entitled (i) to charge you a reasonable fee (taking into account the administrative costs involved in providing you with the requested information or communication, as well as the costs associated with implementing the requested measures), or (ii) to refuse to comply with your request.

In which format will I receive an answer? If you submit your request electronically, the information will also be provided electronically, if this is possible and unless you request otherwise. In any case, we will provide you with a concise, transparent, understandable and easily accessible reply.

When will I receive an answer? We will respond to your request as soon as possible, and in any case within one month of the receipt of your request. Depending on the complexity of the requests and on the number of requests, this period could be extended by a further two months, if necessary. If the response period is extended, we will notify you accordingly within one month of receipt of the request.

What happens if Telenet group does not comply with my request? In our reply, we will always inform you about the possibility of filing a complaint with a supervisory authority, and of lodging an appeal with the court.

What if I don't have access to Tellit? Then you can forward your query to privacy@telenet group.be. Please know that an additional identification check should take place.

IX. How can I contact Telenet group about my privacy?

- I want to exercise my privacy rights

You can exercise your rights by submitting a request via a form/support ticket on Employee privacy (sharepoint.com)

- I want to report a privacy breach to the Data Protection Officer

You can report a privacy breach via Privacy Incident First Aid Kit (sharepoint.com)

- I have another question about the processing of my personal data

You can pose your question the form on Employee privacy (sharepoint.com) or by contacting your HR Business Partner directly.

You can also send your question, complaint or request by letter to the attention of the Data Protection Officer (or "DPO"):
Telenet group BV, Liersesteenweg 4, 2800 Mechelen or use the e-mail address privacy@telenet group.be

X. Adjustments to this Privacy policy

Telenet group may review this Privacy policy at any time, for example following (i) new or amended legislation, rules and regulations, including recommendations from the Data Protection Authority or other government agencies such as, for example, the BIPT, or (ii) changes in Telenet group activities and processes.

XI. Escalation to the supervisory authority

The Data Protection Authority is an independent body that ensures that your personal data is processed in accordance with the law. If you have a complaint in connection with the processing of your personal data by Telenet group, 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 update: January 2025