proximus

DPO

Data Protection & Secrecy of Electronic Communications

Last update on 17/12/2024
Owner Data Protection Officer

Table of contents

1. Introduction

1.1 Policy purpose

The Proximus Group is committed to comply with all relevant data protection legislation and good practices relating to the processing of electronic communications data and personal data, as set out in this policy.

An important reason for treating electronic communications data and personal data with strict confidentiality is that this data is legally protected. Any failure by the entities of the Proximus Group or their employees, contractors and representatives to comply with these legal obligations can be subject to criminal, administrative and disciplinary sanctions.

It goes without saying that respect for electronic communications confidentiality and the privacy of our customers is essential if we want to win and retain customers and their trust.

The Proximus Group is committed to comply with all relevant legislation in respect of personal data, and to protect the rights and freedoms of individuals in accordance with a.o. the General Data Protection Regulation (**GDPR**[1]) and the Directive on privacy and electronic communications (**e-Privacy Directive**[2]), transposed into Belgian legislation via the Electronic Communications Act of 13/06/2005.

1.2 Policy scope

This policy applies to all employees and (sub)contractors of the Proximus Group and to all processing of personal data[3], including electronic communications data[4], by the Proximus Group either as a controller either as a processor[5]. This includes personal data of any of the following categories of data subjects[6]: active Proximus customers, prospects and former customers, job applicants, current Proximus employees and (sub)contractors and former Proximus employees and (sub)contractors.

For the purposes of this policy, the term "Proximus Group" refers to Proximus SA/NV, a public limited liability company under Belgian law (**Proximus**), and its subsidiaries. Subsidiaries may adapt or derive from this policy if necessary to address specific local legal requirements that diverge from the policy, ensuring compliance with applicable local laws.

Proximus Group's employees but also (sub)contractors and any third parties working with or for the Proximus Group, and who have or may have access to personal data, will be expected to have read,

[1] See definition of "GDPR" in Annex 1.
[2] See definition of "e-Privacy Directive" in Annex 1.
[3] See definition of "personal data" in Annex 1.
[4] See definition of "electronic communications data" in Annex 1.
[5] See definitions of "controller" and "processor" in Annex 1.
[6] See definition of "data subject" in Annex 1.

understood and to comply with this policy. Please note that in the remainder of this policy, the term 'Proximus employee' covers both employees as (sub)contractors of the Proximus Group.

This policy is in line with the GDPR and with the e-Privacy Directive.

The GDPR applies to all controllers that are established in the European Union (**EU**) who process the personal data of data subjects, in the context of that establishment[7]. It also applies to controllers outside of the EU that process personal data of data subjects who are in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
- to the monitoring of their behaviour as far as their behaviour takes place within the EU.

1.3 What Proximus employees must do?

This section aims at setting out an overview of the points of action that Proximus employees must take in order to comply with the requirements of this policy. The list below is non-exhaustive and simply aims at highlighting the most important requirements in an actionable form.

1.3.1 Apply the principles of personal data processing to the collection and use of personal data

- Only collect personal data that is directly relevant and necessary to accomplish the specified purpose(s) and only retain personal data for as long as is necessary to fulfil the specified purpose(s).
- Use personal data solely for the purpose(s) for which it was collected.
- Ensure that personal data is accurate, up-to-date and relevant to the purpose(s) for which it is collected.
- Secure personal data (paper and electronic) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Avoid accessing, collecting or storing personal data that is not necessary for their current job responsibilities.
- Always dispose of personal data securely when it is no longer necessary to fulfil the specified purpose(s).

1.3.2 Follow the privacy by design process

- Follow the privacy by design process[8] at the initial design phase of any system, product or process involving the processing of personal data.

[7] See definition of "establishment" in Annex 1.
[8] The privacy by design process is a process put in place to take data protection requirements into account in the design of any initiative involving the processing of personal data. See section 2.3.

- Implement the measures defined in the context of the privacy by design process to mitigate the risks that this processing activity may pose to the rights and freedoms of individuals.

1.3.3 Report personal data breaches and complaints

- Immediately report any suspected personal data breach in line with your internal reporting procedures. A personal data breach occurs when the confidentiality, availability or integrity of personal data is compromised.
- Report any complaints from data subjects about how their personal data is processed in line with your internal reporting procedures.

1.3.4 Complete required trainings

- Undertake and complete all required data protection and information security trainings.

1.4 Responsibilities

This section identifies and explains the roles and responsibilities of the different actors involved in complying with the data protection legislation. These roles are defined in a general manner to remain applicable across all subsidiaries of the Proximus Group, considering their respective needs and governance structure.

1.4.1 Proximus Group

Proximus or any of its subsidiaries may qualify both as a controller and processor[9] under the GDPR. Proximus or its subsidiary, in its role as controller/ processor is responsible for, and must be able to demonstrate compliance with the GDPR (accountability principle)[10].

Senior management and all those in managerial or supervisory roles throughout the Proximus Group are responsible for developing and encouraging good data protection practices within the group of companies.

1.4.2 All employees

Compliance with data protection legislation is the responsibility of all Proximus employees, i.e. both employees and (sub)contractors of the Proximus Group, who process personal data.

Section 1.3 sets out a non-exhaustive overview of the points of action that all Proximus employees must take in order to comply with the requirements of this policy.

[9] See definitions of "controller" and "processor" in Annex 1.
[10] The principle of accountability is explained in section 2.2.7.

1.4.3 Data Protection Officer

Where required by law, a Data Protection Officer ("DPO") will be designated to oversee the personal data processing activities of one or several subsidiaries of the Proximus Group. The DPO's responsibilities include, amongst others:

- Monitoring compliance with GDPR and other applicable data protection laws as well as Proximus' policies (including this policy);
- Informing and advising Proximus employees and management on data protection obligations;
- Reporting on requirements, risks and impacts related to data protection and privacy towards the management;
- Cooperating with the supervisory authorities and acting as a contact point for supervisory authorities and data subjects regarding data protection issues;
- Monitoring that Data Protection Impact Assessments (DPIAs) are performed for high-risk processing activities and providing advice during the DPIA process where necessary;
- Providing general training and awareness to ensure the organization understands and complies with the GDPR and other applicable data protection laws.

1.4.4 Supporting teams

Depending on the needs of the concerned subsidiary of the Proximus Group, various supporting teams provide specialized expertise to implement and maintain compliance with data protection requirements. These may include:

- Information security experts: ensuring the technical and organisational measures are in place to protect personal data against unauthorized access, breaches and losses and managing cybersecurity incidents.
- Legal experts: advising on the interpretation of the data protection requirements and ensuring compliance with applicable laws in contracts and operational practices.
- Data governance experts: assisting in maintaining accurate data inventories and ensuring proper data lifecycle management.
- Audit teams: monitoring and assessing compliance with data protection policies.

1.4.5 Governance bodies

Specific governance bodies comprising members of the management are responsible for overseeing and making decisions regarding data protection and GDPR compliance risks.

2. Policy: Data Protection

2.1 Consequences in case of non-compliance

2.1.1 GDPR

The GDPR has come into effect on the 25th of May 2018. There are no transitional provisions for existing personal data. This means that, from that date onwards, the Proximus Group has to fully comply with the GDPR.

The Proximus Group carries out processing activities where it qualifies as a controller and activities where it qualifies as a processor under the GDPR and risks sanctions in case of non-compliance with its obligations under data protection legislation.

The GDPR foresees different types of sanctions in case of non-compliance with the data protection rules, including reprimands, temporary or definitive bans on processing and fines of up to €20 million or 4% of the business's total worldwide annual turnover of the preceding financial year.

2.1.2 Electronic Communications Act of 13/06/2005

Possible sanctions in case of non-compliance with the e-Privacy Directive are provided in section 3.3.

2.1.3 Disciplinary actions

Any violation of this policy could result in disciplinary measures that may lead to dismissal, in accordance with the employment regulations applicable to you. Breaches of data protection legislation may also constitute a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.2 Principles of personal data processing

All processing of personal data must be done in accordance with the following data protection principles. Any new product and service involving the processing of personal data should follow the privacy by design process to ensure that these principles are taken into account in its design.

2.2.1 Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and transparently.

2.2.1.1 Lawfulness

The processing of personal data has to happen in a lawful way. For the processing to be considered lawful, it must be based on one of the legal grounds listed in article 6.1 of the GDPR, namely:

- Prior consent of the data subject;
- Performance of a contract;
- Compliance with a legal obligation of the controller;
- Protection of the vital interest of the data subject;
- Performance of the public interest or official authority; or
- Legitimate interest of Proximus or a third party.

There is no hierarchy within the list of legal grounds.

Specific legal grounds are necessary to process special categories of personal data[11].

Lawfulness also means that the processing of personal data may not be unlawful or illegal in a more general way. This implies that all processing activities must respect applicable criminal and civil laws and principles.

The appropriate legal ground for a processing activity is defined and documented as part of the privacy by design process which must be followed for any new initiative involving the processing of personal data.

2.2.1.2 Fairness

Personal data must be processed in a fair way. This means that:

- The Proximus Group handles personal data in ways data subjects would reasonably expect (transparency and reasonable expectations);
- The Proximus Group does not use personal data in a way that has adverse effects on the data subjects;
- The Proximus Group does not deceive the data subjects;
- The Proximus Group does not lure the data subjects into the processing of their personal data.

2.2.1.3 Transparency

The GDPR has increased requirements about what information should be made available to data subjects, which is covered in the 'Transparency' requirement. It defines which information relating to the processing of personal data must be provided to data subjects, as well as when and how this information must be provided.

The mandatory content of the information that must be provided to the data subjects is defined by articles 13.1 and 13.2 or 14.1 and 14.2 of the GDPR.

Information and communication relating to the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- in clear and plain language;
- in writing or by other means, including where appropriate, by electronic means; and
- provided free of charge.

The information relating to the processing of personal data must be provided to the data subjects within the timing laid down in articles 13.1 and 14.3 (a) to (c) of the GDPR.

2.2.2 Purpose limitation

Personal data shall only be collected and processed for specified, legitimate and explicit purposes and not further processed in a manner that is incompatible with these purposes. During the privacy by design

[11] See definition of "special categories of personal data" in Annex 1.

process it is checked and documented whether a personal data processing activity is justified by a valid purpose or whether a new purpose is compatible with the original purpose of processing.

2.2.2.1 Specified purpose

The purpose of the personal data processing must be established in advance and determined at the time of the collection or further processing of the personal data.

If the processing activity does not serve any specific purpose, it should not take place or be stopped immediately when the purpose becomes inexistent.

2.2.2.2 Legitimate purpose

A legitimate purpose is one which complies with any legal requirements. Furthermore, a legitimate purpose is a valid purpose. Not only does it have to be lawful, it also has to be reasonable and realistic.

2.2.2.3 Explicit purpose

An explicit purpose is one that is clearly revealed, explained and expressed. The purpose has to be explicit at the latest at the moment personal data is being collected or being further processed.

2.2.2.4 Compatible use

Personal data obtained for specified purposes must not be subsequently used for any other purpose that is not compatible with the purpose originally defined. Nevertheless, it is allowed to process personal data for a new purpose in cases where the data has been collected on the basis of legitimate interest, a contract or vital interests but only after checking that the new purpose is compatible with the original purpose.

2.2.3 Data minimization

Personal data must be adequate (sufficient to properly fulfil the specified purpose), relevant (with a rational link to that purpose) and limited to what is necessary in relation to the purposes for which they are processed.

If certain personal data is not strictly necessary for the purpose in question, it may not be collected or processed.

Data collection methods are reviewed as part of the privacy by design process to ensure that collected data is adequate, relevant and not excessive.

2.2.4 Accuracy

Personal data must be accurate and kept up to date.

In order to achieve optimal accuracy, personal data should, as much as possible, be obtained from the data subjects themselves. Personal data that is kept by the Proximus Group must be reviewed and updated as necessary.

2.2.5 Storage limitation

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for the purposes for which the personal data are processed. Personal data may not be stored for an indefinite period of time. The duration of the period can vary depending on the purpose for which the personal data is processed. During the entire period, the Proximus Group must be able to prove that the storage of the personal data is necessary for such purpose.

The appropriate retention period of the personal data is defined and documented as part of the privacy by design process which must be followed for any new initiative involving the processing of personal data.

The Proximus Group must ensure that personal data is securely anonymized, disposed of or destroyed at the end of its retention period.

2.2.6 Security of personal data

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The Proximus Group shall implement such technical and organizational measures required to ensure adequate security of personal data.

All personal data shall be classified and treated depending on their sensitivity level as defined in the Proximus Information Ownership and Classification Policy.

In assessing measures to ensure appropriate security of the personal data, a risk assessment will be carried out taking into account all the circumstances of the Proximus Group's processing operations as well as the extent of possible damage or loss that might be caused to data subjects if a security breach occurs, the effect of any security breach on the Proximus Group itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, following measures will among others be considered:

- Firewalls and internet gateways;
- Privacy enhancing techniques such as pseudonymisation and anonymisation;
- Identity & access management (incl. Public Key Infrastructure, Key Management Infrastructure, etc.);
- Threat & vulnerability management (incl. vulnerability scanning & patching, event logging & monitoring, malware protection and intrusion detection);
- Data leakage prevention;
- Encryption management;
- Application security (incl. SOA security, database security);
- Network and end user device protection;
- Security information & event management;
- Data, application and network segregation;
- Audit logs and monitoring;
- Supplier and Third Party Remote Access Management.

When assessing appropriate organisational measures, following measures will among others be considered:

- Data protection policy framework;
- Training & awareness for Proximus employees;
- Physical access controls;

- Adoption of a clear desk policy.

All Proximus employees are responsible for ensuring that any personal data which the Proximus Group holds and for which they are responsible is kept securely.

2.2.6.1 Integrity

Personal data must be properly secured in order to achieve and maintain their integrity. Data integrity needs to be taken into account during the entire lifecycle of any project or process.

2.2.6.2 Confidentiality

Personal data cannot be accessed by people who do not need them, as formulated in the *Need to know* principle: access to personal data must always be restricted to the persons who need it for the performance of their tasks. The Proximus Group needs to ensure that personal data are only processed by authorized employees or authorized equipment.

2.2.7 Accountability

As a controller, according to article 5.2 of the GDPR, the Proximus Group is not only responsible for ensuring compliance but also for demonstrating that processing operations comply with the principles of data processing listed in this policy and the requirements of the GDPR (**accountability principle**).

In order to be able to demonstrate compliance, the Proximus Group will keep traces and documentation of every decision taken and measure implemented to comply with principles of data processing enshrined in the policy, including by implementing a privacy by design process, maintaining records of processing activities and executing and documenting DPIAs where legally required, implementing and documenting technical and organizational security measures, implementing a personal data breach notification process, facilitating the exercise of the data subject's rights, etc. This documentation will be made available upon request to the supervisory authority and serves as proof of compliance with data protection regulation.

With regard to monitoring and control, Proximus applies the system described in section 4 of this policy.

2.3 Privacy by design process

In accordance with the GDPR principle of accountability[12], the Proximus Group must be able to demonstrate compliance to data protection regulation (e.g., GDPR, e-Privacy Directive) and ensure that the processing of personal data is compliant with applicable legislations.

The Proximus Group shall establish a process (**privacy by design process**) to assess compliance with the requirements under data protection regulation for any initiative involving the processing of personal data. The privacy by design process will enable the Proximus Group to anticipate and mitigate risks and privacy-

[12] The principle of accountability is explained in section 2.2.7.

invasive events before they occur, ensuring the correct implementation of data protection principles. The privacy by design process will also ensure that, at the initial design phase of any system, product or process, the Proximus Group considers:

- Whether the intended personal data processing activities complies with the data protection principles;
- the risks that these processing activities may pose to the rights and freedoms of individuals; and
- the possible measures available to mitigate the risks and demonstrate compliance with legislation.

2.4 Data Protection Impact Assessment

The Proximus Group shall perform an assessment of the impact of the envisaged processing operations on the protection of personal data whenever a processing activity is likely to result in a high risk to the rights and freedoms of individuals. Such assessment is called a Data Protection Impact Assessment (DPIA).

A DPIA is required at least in the following cases:

- a systematic and extensive evaluation of the personal aspects of an individual, including profiling;
- processing of sensitive data on a large scale;
- systematic monitoring of public areas on a large scale;
- large-scale and/or systematic processing of telephony, internet or other communication data, metadata or location data from or traceable to natural persons (for example Wi-Fi tracking or processing of location data of travellers in public transport) when the processing is not strictly necessary for a service requested by the person concerned.

The DPIAs shall contain and document at least the mandatory elements listed in article 35.7 of the GDPR.

2.5 Data subjects' rights

Data subjects have the following rights regarding the processing of their personal data:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (right to be forgotten)
- The right to restriction of processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making, including profiling.

The Proximus Group will design and maintain appropriate procedures and training to implement the above data subjects' rights and to handle data subjects' complaints about how their personal data has been processed by the Proximus Group.

The Proximus Group must put the appropriate means at the data subjects' disposal to allow them to exercise their rights and file their complaints.

Where required by law, the Proximus Group must execute the data subject's request and respond to it within the timing set forth in article 12.3 of the GDPR.

The Proximus Group ensures that no data subject will face retaliation or discrimination for exercising their rights under the GDPR or for filing a complaint regarding the processing of their personal data.

2.6 Consent

As explained in section 2.2.1.1 of this policy (**principle of lawfulness**), the processing of personal data must be based on one of the legal grounds listed in the GDPR. One of these legal grounds is the prior consent of the data subject. Whenever the processing of personal data is based on this legal ground, additional requirements need to be respected for the consent to be valid.

To be valid, the 'consent' must be collected in the form of a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

To obtain a valid consent, the data subject must have been fully informed of the intended processing and has signified his or her agreement, while in a fit state of mind to do so and without pressure being exerted upon him or her. Consent obtained under force or on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the absence of response to a communication. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, a specific consent should be given for all of them.

Where the Proximus Group provides information society services (i.e. online services) directly to children, it will ensure that it has obtained consent from the holder of parental responsibility over the child when processing personal data.

Proximus must be able to demonstrate, for every data subject involved, that a valid consent was obtained for all personal data processing activities for which the appropriate legal ground is consent.

2.7 Special categories of personal data

The processing of special categories of personal data[13], such as personal data revealing ethnic origin, religious beliefs, trade-union membership, or data concerning health[14], and the processing of judicial data[15] is in principle forbidden unless in specific circumstances, for example, if the data subject has given his or her explicit consent for such processing.

The specific legal requirements for processing special categories of personal data and judicial data shall be examined and documented as part of the privacy by design process.

[13] See definition of "special categories of personal data" in Annex 1.
[14] See definition of "data concerning health" in Annex 1.
[15] See definition of "judicial data" in Annex 1.

2.8 Personal data breaches

2.8.1 General

The Proximus Group shall maintain and implement appropriate procedure to manage personal data breaches[16].The supervisory authority must be notified where a personal data breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals. In such case, the supervisory authority must be notified without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach.

In addition, when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Proximus Group must communicate the personal data breach to the affected data subjects without undue delay.

In addition, under the e-Privacy Directive, the Proximus Group is obliged to notify any personal data breach in connection with the provision of a publicly available electronic communications service, to the supervisory authority, no later than 24 hours after the detection of the personal data breach where feasible. Detection of a personal data breach shall be deemed to have taken place when the Proximus Group has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the Proximus Group will also need to notify the subscriber or individual of the personal data breach, without undue delay.

2.8.2 Continuous improvement

In line with the Bold 2025 strategy, Proximus is dedicated to safeguarding the privacy and security of the personal data it processes. To uphold this commitment, Proximus recognizes the importance of continuous improvement in its data protection measures and commits to enforcing prioritization and timely implementation of necessary structural improvements to reduce the risk of data breaches, unauthorized access, ….

Furthermore, Proximus understands that the data protection landscape is constantly evolving, and new challenges may arise. As part of this policy, Proximus pledges to stay updated with the latest industry standards, best practices, and legal requirements to ensure that its data protection measures remain at the forefront of protection.

By enacting and adhering to these principles, Proximus demonstrates its firm commitment to protecting the personal data it processes. Through ongoing efforts to prioritize and implement structural improvements, Proximus aims to protect personal data and maintain the highest standard of data protection, building trust and confidence in its brand.

[16] See definition of "personal data breach" in Annex 1.

2.9 Sharing of personal data

The Proximus Group must ensure that personal data is not disclosed to unauthorized third parties either internally (i.e. within the Proximus Group) or externally (i.e. outside of the Proximus Group). All employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the personal data is relevant to, and necessary for, the conduct of the Proximus Group' business.

Sharing personal data constitutes a processing of personal data which is subject to all the principles listed in section 2.2 of this policy. In particular, the GDPR principle of lawfulness requires to have a lawful basis[17] for sharing personal data, and that this lawful basis is documented. The sharing of personal data should always be subject to appropriate security measures[18]. The lawfulness and other legal requirements applicable to sharing of personal data shall be checked and documented as part of the privacy by design process.

2.9.1 Exchange of data within the Proximus Group

The exchange of personal data between entities of the Proximus Group is not exempt from any restrictions and must comply with all the requirements related to the sharing of personal data explained in this section 2.9.

Moreover, all Proximus employees have to take into account any restrictions imposed by competition law (cf. Competition, Chinese Walls, Exchange of information and Down raids Policy).

2.9.2 Transfer of personal data outside the EU

The Proximus Group is fully committed to ensuring that there are adequate safeguards in place, as required by the applicable laws, to protect the personal data transferred by the Proximus Group to countries that do not have adequate data protection laws.

When transferring personal data to a country which is not a member of the European Economic Area (**third country**), one of the following tools pursuant to chapter V of the GDPR must be used to guarantee the adequate level of data protection:

- The recognition through a European Commission decision (**adequacy decision**) of an adequate data protection regime in the country where the recipient receiving the personal data is located.
- In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards.
  An example of such appropriate safeguards are the contractual arrangements with the recipient of the personal data, using, for example, the standard contractual clauses approved by the European Commission.

[17] The principle of lawfulness is explained in section 2.2.1.1.
[18] The principle of security of personal data is explained in section 2.2.6.

- Finally, if a transfer of personal data is envisaged to a third country that is not the subject of an adequacy decision and if appropriate safeguards are absent, a transfer can be made based on a number of derogations for specific situations for example, where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer.

2.9.3 Processors

The Proximus Group will identify for each standard product/service the role of its corresponding entity with respect to the processing of personal data (i.e. controller, processor[19]) and shall make sure that the correct contractual clauses are stipulated within the contract representing the correct responsibilities and obligations linked to that role.

In case an entity of the Proximus Group or the other party providing services to the Proximus Group acts as processor, the contract entered into by the parties shall specify the duties of the processor towards the controller in accordance with article 28 of the GDPR (**data processing agreement**).

2.9.4 Joint controllers

If an entity of the Proximus Group processes personal data as joint controller[20] together with one or more organisations, it shall enter into an arrangement with such organisation(s) setting out their respective responsibilities for complying with the GDPR requirements. The main aspects of the arrangement must be communicated to the data subjects.

2.10 Training & awareness

The Proximus Group will promote training and awareness programmes and shall make resources available in order to raise awareness and provide with general as well as specific trainings on data protection relevant to the day-to-day roles and responsibilities. Proximus employees must undertake and complete all required data protection and information security trainings.

2.11 Records of processing activities

In line with article 30 of the GDPR and to ensure that the Proximus Group understands the personal data that it processes, the purposes for which it processes it and the level of risk related to the processing of such information, the Proximus Group will maintain a record of processing activities in which all personal data processing activities managed under the responsibility of Proximus, as controller, joint controller and processor, are documented.

[19] See definitions of "controller" and "processor" in Annex 1.
[20] See definition of "joint controller" in Annex 1.

3. Policy: Secrecy of Electronic Communications

3.1 Principle

Electronic communications confidentiality protects the content of calls and electronic communications data such as numbers called, the time of communication, internet connection, and the confidentiality of private numbers (**electronic communications data**[21]). Both the content of a communication as data regarding the communication must be treated as confidential.

Protection of the content of the communication

A person who is not participating in a communication (i.e. mobile, fix and data communication) does not have the right to attempt to consult the content of the communication that he or she is transferring. It is also forbidden to record the content of communications.

Protection of the data related to a communication

It is forbidden to intentionally discover, disclose, change or destroy data regarding electronic communications related to other persons or to identify the persons concerned.

3.2 Exceptions

A number of situations to which this prohibition does not apply to a telecommunications operator and its employees are defined by law (see non-exhaustive list below).

Please contact the competent counsel in the Legal department to assess if any of the exception can be applied. Examples of exceptions:

- It is necessary to check the network to ensure that it is functioning properly or to ensure that the telecommunications service is provided properly;
- the consent of all the parties participating in the communication has been given;
- The data regarding electronic communications (not the content of the communication) is used for the following specific purposes:
  - billing and interconnection payment;
  - direct marketing with the customer's consent;
  - offering tracking and traffic data services;
  - traffic management;
  - fraud detection.

There are also regulatory exceptions to electronic communications confidentiality for judicial authorities, the emergency services, the Belgian Institute for Postal services and Telecommunications, the mediation service for telecommunications.

[21] See definition of "electronic communications data" in Annex 1.

Moreover, there are also legal exceptions which allow the registration of a communication for quality control in call centers and as a proof of commercial transactions.

3.3 Consequences in case of non-compliance

Any non-compliance with the ePrivacy Directive can be subject to fines up to 800.000€ and prison sentences up to 4 years.

4. Monitor and review

In order to monitor compliance of the Proximus Group with the data protection legislation, the Proximus Group shall:

- maintain a framework defining the appropriate internal controls and independent supervision mechanisms to monitor compliance with relevant data protection laws and with data protection policies and procedures;
- develop, maintain and apply a privacy by design process in order to evaluate whether new products/service initiatives involving personal data processing comply with data protection requirements;
- perform ad-hoc compliance reviews performed by the Data Protection Officer;
- perform ad-hoc audits by internal auditors or trusted third-party auditors.

Annex 1: Definitions

Biometric data - personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

Consent of the data subject - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data concerning health - personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data subject – any living individual who is the subject of personal data held by an organisation.

e-Privacy Directive (Directive on privacy and electronic communications) - the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector. The Directive has been transposed into Belgian law by the Act of 13 June 2005 on electronic communications.

Electronic communications data - traffic data and location data. Traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Location data, which means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

GDPR (General Data Protection Regulation) - the Regulation 2016/679 EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Genetic data - personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Joint controller – a controller which determine the purposes and means of processing of personal data jointly with one or more other controllers.

Judicial data - personal data relating to criminal convictions and offences or related security measures.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling – any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory authority (Gegevensbeschermingsautoriteit / Autorité de protection des données) - an independent public data protection authority which is established by a Member State. In Belgium, this is the 'Gegevensbeschermingsautoriteit' / 'L'autorité de protection des données' aka Supervisory Authority.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.