

Privacy statement

Table of contents

Introduction	2
Lexicon.....	2
Privacy policy.....	2
Responsibilities	3
Who is concerned?	4
Subject: What data is involved?	4
How is data collected?.....	4
What are the legal bases for processing data?	5
Who receives the data?.....	6
How long do we keep data?	7
Measures: how do we protect data?.....	7
Applicable rights and remedies	8
1.1 Right to withdraw consent (articles 7.3 RGPD).....	9
1.2 Right of access (article 15 RGPD)	9
1.3 Right of rectification (article 16 RGPD)	9
1.4 Right to erasure (article 17 RGPD)	9
1.5 Right to restrict processing (Article 18 RGPD).....	9
1.6 Right to portability (article 20 RGPD)	9
1.7 Right to object (article 21 RGPD)	9
1.8 Use of a right	9
Questions: who to contact?.....	10
Modifications.....	10

Introduction

PRAYON attaches great importance to the protection of your personal data. We use them in accordance with Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), and the Belgian law of July 30, 2018 on the protection of individuals with regard to the processing of personal data. The aim of these provisions is to manage, process and secure citizens' personal data more effectively, in Belgium and within the European Union.

This privacy statement is also intended to inform you, as a customer, supplier, subcontractor, visitor, employee, worker or job applicant, about how we collect and process your data in the context of our relationship.

In view of the importance of this subject, we suggest that you read this declaration carefully to familiarize yourself with our practices in this area.

Lexicon

Personal data: Any information relating to a natural person who can be identified, directly or indirectly.

Processing: Any operation which is performed on personal data or sets of personal data.

Data controller: The natural or legal person who determines the purposes and means of processing.

Recipient: natural or legal person who receives personal data.

Consent: Any free, specific, informed and unambiguous expression of will by which the data subject accepts that personal data concerning him or her may be processed.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of personal data transmitted, stored or otherwise processed.

Privacy policy

PRAYON's philosophy is to protect the best interests of individuals with regard to the protection of personal data.

First of all, the spirit of this declaration is to ensure compliance with applicable national and international legal standards, in the context of all processing carried out in order to fulfill our contractual and legal obligations.

All activities carried out by **PRAYON** are carried out in accordance with the objectives described in the contracts binding the various parties concerned (employer, subcontractors, etc.). If, however, additional processing is required to extend the scope of the contract, explicit consent will be required to authorize the use of personal data.

The personal data collected by **PRAYON** is used for the purposes described in the contract and we undertake to ensure that all such data is authentic, complete and up-to-date at the time of processing.

PRAYON has developed applications based on physical, technical and administrative procedures which guarantee against any malicious use of private data. These procedures notably concern access to the applications made available, personal data, the transfer of such data between **PRAYON** and third parties, and encryption within our databases.

In the event of a personal data breach, **PRAYON will take** the necessary steps to deal with the situation effectively.

Responsibilities

PRAYON is directly responsible for the processing of your data. It is therefore considered responsible for the processing it applies to your personal data.

In order to comply with its obligations in relation to the RGPD, **PRAYON** has in particular undertaken to:

- Review its data processing activities, keep a data processing register and ensure that the rights of data subjects are respected;
- Implement appropriate technical and organizational measures to ensure the necessary security of personal data;
- Respect the principle of accountability, cooperate with the Data Protection Authority (DPA), and implement procedures for identifying, investigating and promptly reporting data breaches to the DPA ("Data Breach Procedure");

- Ensure that the subcontractors it appoints offer sufficient guarantees with regard to privacy; and
- Raise employee awareness of the challenges and operational impact of regulations.

Who's concerned?

Privacy regulations apply to all personal information relating to an identified or identifiable natural person. Legal entities, whatever their legal form, are excluded from the regulations.

In view of our business activity, which is mainly focused on companies ("B2B"), this privacy statement therefore applies to job applicants, employees, collaborators, visitors and contacts within our customers, subcontractors and suppliers.

These individuals are hereinafter referred to as the "persons concerned".

Subject: What data is involved?

The data concerned is information relating to the persons concerned. These data can be grouped into different categories according to their nature, such as :

1. Genetic, biometric or health-related data
2. Racial or ethnic origin and cultural diversity
3. Political opinions or union membership
4. Religious or philosophical convictions
5. Private and family life, sexual orientation
6. Identification data, language choices and personal characteristics
7. Criminal convictions and offences
8. Professional data
9. Electronic communications data
10. Location data
11. Economic and financial data

PRAYON may collect data falling into one or more of these categories, to the extent necessary to fulfill its corporate purpose and commercial activities.

Data collection: how is data collected?

For applicants, employees and collaborators of the company, personal data is communicated to **PRAYON through the** following communication channels:

- By submitting your CV yourself or via the temporary employment agency,
- Via the commitment form completed at the start of the contractual service,
- Through the contacts you have with us,
- Via the medical check-up,
- Via a copy of the documents required for engagement,
- Via the photo taken on the first day of service.

For subcontractors working on the site, personal data are communicated to **PRAYON** through the following communication channels:

- Via the identity check carried out at the guardhouse to activate the access badge,
- Via service contracts,
- Through the contacts you have with us.

For visitors, personal data is communicated to **PRAYON through the** following communication channels:

- Via a copy of your identity card to obtain an access badge,
- Through the contacts you have with us.

For customers and suppliers, personal data is communicated to **PRAYON through the** following communication channels:

- Via contracts for the purchase or supply of goods or services,
- Through the contacts you have with us.

We may also collect data from credible third-party commercial or public sources. The data concerned mainly concerns the identification of contact persons or legal representatives, and professional activity.

A contact form is available on the **PRAYON website** for external inquiries. This form requires the insertion of certain personal data, such as e-mail address, surname and first name. This data will only be used to respond to the request, and will then be deleted.

PRAYON also has access to data from video-surveillance cameras installed in and around our premises, in compliance with legal requirements. Images are recorded exclusively for the purpose of protecting the security of goods and people, and preventing abuse, fraud and other offences to which we and our company may fall victim.

What are the legal bases for processing data?

The processing of your data by PRAYON is based on the following legal grounds:

- For non-sensitive candidate data: article 6.1.a RGPD (consent for the purposes of recruitment); article 6.1.b RGPD (performance of pre-contractual recruitment measures taken at your request); article 6.1.c RGPD (compliance with legal obligations relating to recruitment, to which PRAYON would be subject).
- For non-sensitive data of employees and collaborators: article 6.1.b RGPD (i.e. performance of the employment or collaboration contract); article 6.1.c RGPD (compliance with its legal obligations, by PRAYON, particularly in terms of social and tax law).
- For non-sensitive data of representatives or contact persons within our suppliers, customers and subcontractors: article 6.1.c RGPD (compliance with legal obligations to which PRAYON would be subject); article 6.1.f RGPD (fulfilment of legitimate interests of the parties concerned, i.e. the pursuit of their activities via contact persons).
- For sensitive data (linked to health or trade union membership) of workers and employees: article 9.2.c RGPD (exercise by **PRAYON** of rights and obligations relating to labor law, social security and social protection).
- For sensitive (biometric) data of subcontractors: article 9.2.a RGPD (your consent to the use of your fingerprints for the purpose of your identification, by the guard post, faster than via the presentation of your ID card).

Who receives the data?

PRAYON does not share data with anyone other than the intended recipients in the context of the contractual, legal or consent-based relationship. Unless explicitly stated otherwise, data is stored exclusively within the European Union.

Subcontractors, whose compliance with current regulations **PRAYON has checked**, may also receive personal data in order to meet contractual obligations arising from agreements concluded between you and us (meal voucher suppliers, temporary employment agencies, banking or insurance organizations, IT service providers, etc.).

How long do we keep data?

PRAYON undertakes not to keep data longer than the legal and/or necessary retention period to ensure the fulfilment of the corresponding processing purposes:

- The data of visitors and unsuccessful job applicants are kept for twelve (12) months following their last interaction with Prayon staff;
- The data of our workers and collaborators is kept for the duration of the contractual relationship, then stored in archived form for the following seven (7) years, in order to enable Prayon to demonstrate compliance with its legal and contractual obligations until the expiry of the applicable limitation periods;
- The data of our contact persons at our customers, suppliers and/or subcontractors is kept for the duration of our commercial relationship (actual or potential) with these entities, as well as for the period necessary for the expiry of the periods during which the responsibility of these entities or Prayon could be called into question as a result of this relationship (subject to the early departure of the contact persons concerned).

Measures: how do we protect data?

PRAYON guarantees its applicants, employees, collaborators, visitors, customers, suppliers and subcontractors an adequate level of data protection. Personal data is physically stored exclusively in data rooms located in the EU.

PRAYON implements administrative, technical and physical measures to protect data against accidental or unauthorized destruction, loss, modification, access or any other unauthorized processing of personal data. These procedures are drawn up and reviewed by the HR, Legal and IT Departments.

Administrative measures

Provisions relating to professional secrecy and confidentiality are included in our contracts and agreements. Access to data is defined according to the needs of the function.

Roles and responsibilities within the company are clearly defined, enabling these directives to be properly applied.

Technical measures

A firewall and antivirus software protect data on the servers. Other technical security measures include daily server backups, hard disk encryption, etc., and an external audit is carried out by the IT department to ensure security compliance.

The Office 365 Cloud and hard drive C are considered a personal area. This data will be destroyed 30 days after the employee's departure. Data inserted on hard drive Z is shared and will not be destroyed after the employee leaves. The employee must therefore take care not to insert any personal data.

Physical measurements

The cupboards in the personnel department, containing the workers' files with their personal data in paper format, are protected by a lock with a key at the end of each day. Computer and server rooms containing software and data are physically protected by a key lock and an alarm system.

Some of our servers are outsourced in the event of internal problems. In order to comply with the European Data Protection Regulation, we have checked the security measures implemented by this subcontractor. This meets our expectations in terms of personal data protection.

Information security incident management

The IT system logs, for a certain period of time, the various events occurring in the IT field. This information can be used to analyze any incidents that may have occurred, and as evidence in such cases. As part of the management of access to information on an as-needed basis, this logging data is of course protected.

If the incident is detected by someone other than the IT department, the latter will notify us as soon as possible.

If the incident concerns the loss, leakage or theft of personal data, the person who discovered the incident will also notify the person responsible for data protection at Prayon (Frédéric GEVERS - fgevers@prayon.com), who, with the help of the IT department, will take any necessary steps to report the incident to the appropriate authorities.

Applicable rights and remedies

N.B.: These rights are available under certain conditions laid down by the European Data Protection Regulation. Please refer to the articles indicated to check whether you meet the conditions required to exercise your rights.

1.1 Right to withdraw consent (articles 7.3 RGPD)

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time, without affecting the lawfulness of previous processing.

1.2 Right of access (article 15 RGPD)

You have the right to request confirmation from the data controller as to whether or not your personal data is being processed. In addition, you may request a copy of the data being processed, if applicable, subject to payment of the corresponding fee.

1.3 Right to rectification (article 16 RGPD)

You have the right to request that your personal data be corrected or completed.

1.4 Right to erasure (article 17 RGPD)

You have the right to request the deletion of your data.

1.5 Right to restriction of processing (Article 18 RGPD)

You have the right to request that your data be restricted. In this case, the data controller may only process your personal data for strictly defined purposes.

1.6 Right to data portability (article 20 RGPD)

You have the right to recover the personal data provided to the data controller in a structured, commonly used and machine-readable format, for possible transfer to a third party.

1.7 Right to object (article 21 RGPD)

You have the right to object to your personal data being processed for prospecting or direct marketing purposes.

1.8 Use of a right

Would you like to assert your rights? Contact Frédéric GEVERS (fgevers@prayon.com), or write to us: PRAYON S.A., Rue Joseph Wauters 144, 4480 ENGIS (BELGIUM).

When you exercise a right, we may ask you to prove your identity to prevent someone else from exercising your rights in your place. We may therefore ask you to provide us with a copy of the front of your identity card.

In the absence of a satisfactory response from us, you are of course free to lodge a complaint with the Belgian Data Protection Authority (contact@apd-gba.be).

Questions: who to contact?

Contact the Data Protection Officer:

Frédéric GEVERS

PRAYON S.A.

Rue Joseph Wauters, 144

4480 ENGIS

+32(0)4/273.92.80

fgevers@prayon.com

Modifications

This declaration was last amended on 22/02/2024. It may be amended or adapted at any time. Only the French version is an official version, and the other language versions are therefore provided for information purposes only. Consequently, the French version of this document will always prevail over the others in the event of contradiction.