

Privacy Statement

Table of Contents

Introduction	2
Glossary.....	2
Privacy Principles.....	2
Responsibilities	3
Who Is Affected?.....	4
Purpose: What data is involved?	4
Collection: How Is Data Collected?	4
On what legal grounds is the data processed?	5
To whom is the data disclosed?.....	6
How long do we retain the data?	6
Measures: How do we protect the data?.....	7
Applicable rights and remedies	8
1.1 Right to withdraw consent (Article 7.3 of the GDPR)	8
1.2 Right of access (Article 15 of the GDPR)	8
1.3 Right to rectification (Article 16 of the GDPR)	8
1.4 Right to erasure (Article 17 of the GDPR).....	8
1.5 Right to restriction of processing (Article 18 of the GDPR)	8
1.6 Right to data portability (Article 20 of the GDPR)	9
1.7 Right to object (Article 21 of the GDPR).....	9
1.8 Exercising a Right	9
Questions: Who to contact?.....	9
Changes	9

Introduction

PRAYON places great importance on the protection of your personal data. We process your personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (General Data Protection Regulation—GDPR), and the Belgian Law of July 30, 2018, on the protection of natural persons with regard to the processing of personal data. These provisions aim to manage, process, and secure citizens' personal data more effectively, both in Belgium and within the European Union.

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

Given the importance of this subject, we encourage you to read this statement carefully to familiarize yourself with our practices in this area.

Glossary

Personal data: Any information relating to an identified or identifiable natural person.

Processing: Any operation performed on personal data or a set of personal data.

Data Controller: A natural or legal person who determines the purposes and means of processing.

Recipient: A natural or legal person who receives personal data.

Consent: Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she signifies agreement to the processing of personal data concerning him or her.

Personal Data Breach: A breach of security leading, accidentally or unlawfully, to the destruction, loss, alteration, or unauthorized disclosure of personal data that has been transmitted, stored, or otherwise processed.

Privacy Principles

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

First and foremost, the purpose of this statement is to ensure compliance with applicable national and international legal standards in connection with all processing activities carried out to fulfill our contractual and legal obligations.

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

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

PRAYON has developed applications based on physical, technical, and administrative procedures that prevent any malicious use of personal data. These procedures specifically address access to the applications provided, access to personal data, the transfer of such data between **PRAYON** and third parties, and encryption within our databases.

If, despite these measures, a personal data breach occurs, **PRAYON** will take the necessary steps to respond effectively to the situation.

Responsibilities

PRAYON acts as the data controller with regard to the processing of your data. It is therefore considered responsible for the processing it performs on your personal data.

To comply with its obligations under the GDPR, **PRAYON** has committed, in particular, to:

- Review its data processing activities, maintain a record of processing activities, and ensure that the rights of data subjects are respected;
- Implement appropriate technical and organizational measures to ensure the necessary security of personal data;
- Comply with the principle of accountability, cooperate with the Data Protection Authority (DPA), and establish procedures to promptly identify, investigate, and report data breaches to the DPA (“Data Breach Procedure”);
- Ensure that the processors it designates provide sufficient safeguards regarding privacy; and
- Raise employee awareness of the operational challenges and impacts of the regulations.

Who is affected?

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

Given that our business is primarily focused on other businesses (“B2B”), this privacy statement applies to job applicants, employees, staff members, visitors, and contacts within our clients, subcontractors, and suppliers.

These individuals are hereinafter referred to as “data subjects.”

Purpose: What data is covered?

The data in question consists of information relating to the aforementioned data subjects. This data can be grouped into different categories based on its nature, such as:

1. Genetic, biometric, or health-related data
2. Racial or ethnic origin and cultural diversity
3. Political opinions or trade union membership
4. Religious or philosophical beliefs
5. Private and family life, sexual orientation
6. Identification data, language preferences, and personal characteristics
7. Criminal convictions and offenses
8. Employment 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 conduct its business activities.

Collection: How is data collected?

For job applicants, employees, and contractors, personal data is provided to **PRAYON** through the following communication channels:

- By submitting your resume yourself or through a staffing agency,
- Through the onboarding form completed at the start of the contractual engagement,
- Through your interactions with us,
- Through a medical examination,
- Through copies of the documents required for employment,
- Through the photo taken on the first day of work.

For subcontractors working on-site, personal data is provided to **PRAYON** through the following communication channels:

- Through the identity check conducted at the guardhouse to activate the access badge,
- Through service agreements,
- Through your interactions with us.

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

- Through a copy of your ID card to obtain an access badge,
- Through your interactions with us.

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

- Through contracts for the purchase or supply of goods or services,
- Through your interactions with us.

We may also collect data from credible third-party sources, whether commercial or public. The data in question primarily relates to the identification of contact persons or legal representatives, as well as their professional activities.

A contact form is available on the **PRAYON** website for any external inquiries. This form requires the entry of certain personal data, such as email address, last name, and first name. This data will be processed solely to respond to the inquiry and will then be deleted.

PRAYON also collects data from video surveillance cameras installed in and around our premises, in compliance with legal requirements. The footage is recorded exclusively for the purpose of ensuring the safety of property and people, as well as to prevent abuse, fraud, and other offenses of which the company and we ourselves might be victims.

On what legal grounds is the data processed?

PRAYON's processing of your data is based on the following legal grounds:

- For non-sensitive data of applicants: Article 6.1.a of the GDPR (consent for recruitment purposes); Article 6.1.b of the GDPR (implementation of pre-contractual recruitment measures taken at your request); Article 6.1.c of the GDPR (compliance with legal obligations regarding recruitment to which PRAYON is subject).
- For non-sensitive data of employees and contractors: Article 6.1.b of the GDPR (performance of the employment or contractor agreement); Article 6.1.c of the GDPR (compliance by PRAYON with its legal obligations, particularly regarding labor and tax law).

- For non-sensitive data of representatives or contact persons at our suppliers, customers, and subcontractors: Article 6.1.c of the GDPR (compliance with legal obligations to which PRAYON is subject); Article 6.1.f of the GDPR (pursuit of the legitimate interests of the parties concerned, namely the conduct of their business activities through contact persons).
- For sensitive data (related to health or union membership) of employees and staff: Article 9.2.c of the GDPR (**PRAYON's** exercise of rights and obligations under labor law, social security, and social protection).
- For sensitive data (biometric data) of subcontractors: Article 9.2.a of the GDPR (your consent to the use of your fingerprints for identification purposes at the security checkpoint, which is faster than presenting your ID card).

To whom is the data disclosed?

PRAYON does not share data with anyone other than the recipients specified under the aforementioned legal bases for processing. Personal data is physically stored in data centers that comply with GDPR requirements.

Processors, whose compliance with applicable regulations has been verified by **PRAYON**, may also receive personal data to fulfill contractual obligations arising from agreements between you and us (meal voucher providers, temporary staffing agencies, banking or insurance institutions, IT service providers, etc.).

How long do we retain the data?

PRAYON is committed to not retaining data for longer than the legally required retention period and/or as long as necessary to fulfill the corresponding processing purposes:

- Data on visitors and job applicants who were not hired is retained for twelve (12) months following their last interaction with Prayon staff;
- Data on our employees and contractors is retained for the duration of the contractual relationship and then archived for the seven (7) years following its conclusion, to enable Prayon to demonstrate compliance with its legal and contractual obligations until the applicable statute of limitations expires;
- The data of our contacts at our customers, suppliers, and/or subcontractors is retained for the entire duration of our business relationship (current or potential) with these

entities, as well as for the period necessary until the expiration of the time limits during which the liability of these entities or Prayon could be called into question as a result of this relationship (subject to the early departure of the relevant contacts).

Measures: How Do We Protect Data?

PRAYON guarantees an adequate level of data protection for its applicants, employees, staff, visitors, customers, suppliers, and subcontractors. Personal data is physically stored in data centers that comply with the requirements of the GDPR.

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

Administrative Measures

Provisions regarding professional secrecy and confidentiality are included in our contracts and agreements. Access to data is defined according to job requirements.

Roles and responsibilities within the company are clearly defined, ensuring the proper implementation of these guidelines.

Technical Measures

A firewall and antivirus software protect the data on the servers. Other technical security measures are in place (daily server backups, hard drive encryption, etc.), and an external audit is conducted of the IT department to ensure compliance with security standards.

The Office 365 cloud and the C: drive are considered personal areas. Data stored in these locations will be deleted 30 days after the employee leaves the company. Data stored on the Z: drive is shared and will not be deleted after the employee leaves. Employees should therefore take care not to store any personal data there.

Physical Security Measures

The filing cabinets in the HR department, which contain employees' files with their personal data in paper format, are locked with a key at the end of each workday. The rooms housing the computers and servers containing software and data are physically secured with a key lock and an alarm system.

Some of the servers are outsourced in case of internal issues. To comply with the European General Data Protection Regulation, we have verified the security measures implemented by this third-party service provider. These measures meet our expectations regarding the protection of personal data.

Information Security Incident Management

The IT system logs various events occurring within the IT environment for a certain period of time. This information can therefore be used to analyze any potential incidents and serve as evidence in such cases. These log data, within the framework of managing access to information based on need, are of course protected.

If the incident is detected by someone outside the IT department, that person will notify the IT department as soon as possible.

If the incident involves the loss, leakage, or theft of personal data, the person who discovered the incident will also notify Prayon's Data Protection Advisor (Frédéric GEVERS – fgevers@prayon.com), who, with the assistance of the IT department, will take any necessary steps to report the incident to the relevant authorities.

Applicable Rights and Remedies

Note: These rights are subject to certain conditions set forth in the European General Data Protection Regulation (GDPR). Please refer to the articles listed below to verify whether you meet the requirements to exercise your rights.

1.1 Right to Withdraw Consent (Article 7.3 of the GDPR)

When the processing of your data is based on your consent, you have the right to withdraw that consent at any time, without affecting the lawfulness of any processing that took place prior to the withdrawal.

1.2 Right of access (Article 15 of the GDPR)

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, upon payment of the corresponding fees.

1.3 Right to Rectification (Article 16 of the GDPR)

You have the right to request that your personal data be rectified or supplemented.

1.4 Right to erasure (Article 17 of the GDPR)

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

1.5 Right to restriction of processing (Article 18 of the GDPR)

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

1.6 Right to data portability (Article 20 of the GDPR)

You have the right to receive the personal data you have provided to the data controller in a structured, commonly used, and machine-readable format, for the purpose of transferring that data to a third party.

1.7 Right to Object (Article 21 of the GDPR)

You have the right to object to the processing of your personal data for direct marketing or promotional purposes.

1.8 Exercising a Right

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

When you exercise a right, we may ask you to verify your identity to prevent someone else from exercising your rights on your behalf. We may therefore ask you to provide us with a copy of the front side of your ID card.

If you do not receive a satisfactory response from us, you are, of course, free to file a complaint with the Belgian Data Protection Authority (contact@apd-gba.be).

Questions: Who to contact?

Contact our data protection advisor :

Frédéric GEVERS

PRAYON S.A.

Rue Joseph Wauters 144

4480 ENGIS (BELGIUM)

fgevers@prayon.com

Changes

This statement was last updated on September 9, 2026. It may be modified or amended at any time. Only the French version constitutes an official version; other language versions are therefore provided for informational purposes only. Consequently, the French version of this document will always take precedence over the others in the event of any discrepancy.