DATA PROTECTION POLICY
PURATOS GROUP

Puratos
Reliable partners in innovation

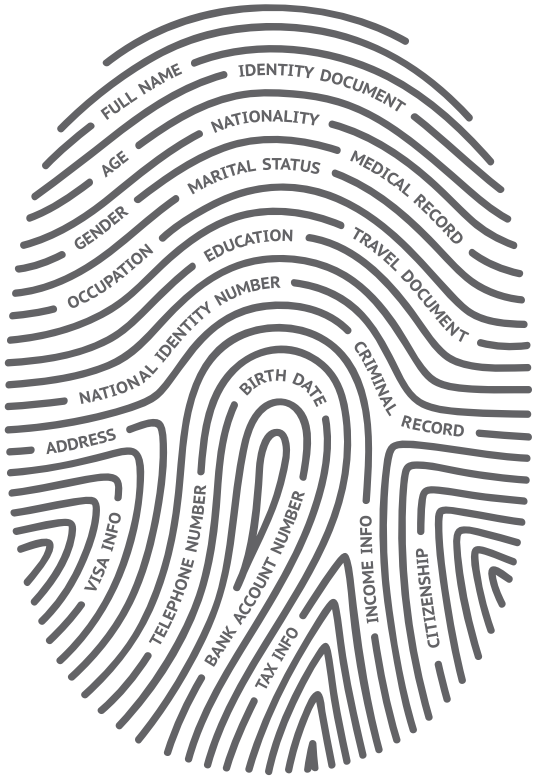
Contents

1. Purpose of this policy

The Puratos group highly values the relationship with its customers, distributors, employees, job applicants, suppliers, visitors and other stakeholders. The group aims at providing an adequate level of personal data protection to enhance its business relationships, trustworthiness and its reputation.

This data protection policy is inspired by the principles of European Union General Data Protection Regulation 2016/679 ('GDPR'). The GDPR aims at protecting EU citizens in the global and digital economy which has caused their personal data being spread across the globe. It's exceedingly difficult for individuals to know exactly what data is being collected about them, and what is happening to the data that they share with companies. The GDPR puts transparency at the centre, giving individuals the insights and control they need to feel comfortable sharing their personal data.

This data protection policy thus aims to provide a framework applied worldwide within the Puratos group in order to achieve an adequate level of personal data protection, to the benefit of all parties involved.



2. Scope of this policy

This policy applies to the processing of personal data by the entities of the Puratos group. Personal data is any information relating to an identified or identifiable living natural person, such as biographical information (names, dates of birth, ...), workplace data (addresses, position, phone numbers and email addresses, ...), an online identifier (IP address), and so on.

This policy comprises generally accepted data protection principles without replacing the existing local laws. It supplements the different national data protection laws that apply to the operations of the Puratos group.

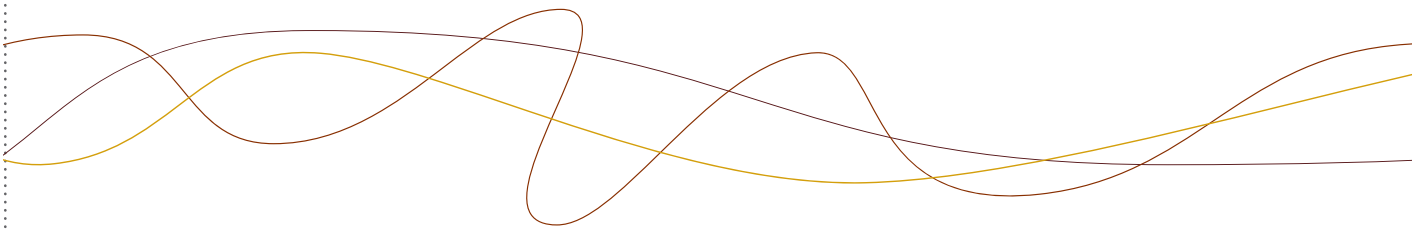
Each Puratos entity commits to fully comply with the applicable national data protection laws and with this policy.

If there is a reason to believe that compliance with legal obligations would contradict obligations under this policy, the Puratos entity concerned shall inform the Data Protection Team (dataprivacy@puratos.com) in order to find a practical solution that meets the aim of this policy.

This policy does not apply to the data of legal entities, such as companies or other organisations with a legal personality.

This policy does not apply to anonymous data, such as statistical data. However, the mere absence of a name does not imply that the data is anonymous, it should be impossible to directly or indirectly trace the data to an individual person.

This policy may be amended under coordination of the Puratos Data Protection Team. You can find the most recent version of this policy externally on the Puratos corporate website and internally on a dedicated section of the Puratos intranet.



3. Definitions

Controller	The natural or legal person, public authority, agency or other body who, 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 applicable law, the controller or the specific criteria for its nomination may be provided for by applicable 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	An identified or identifiable natural person who's personal data are processed. 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	Any information relating to an identified or identifiable natural person ('data subject').
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 that 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	The natural or legal person, public authority, agency or other body that processes personal data on the controller's behalf.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
Recipient	A natural or legal person, public authority, agency or another body, to which the personal data is disclosed, whether a third party or not. However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with applicable law will not be regarded as recipients; the processing of this data by those public authorities will comply with the applicable data protection rules according to the purposes of the processing.
Restriction of processing	The marking of stored personal data with the aim of limiting its processing in the future.

4. Principles relating to the processing of personal data

4.1 Lawfulness and fairness

Personal data must be processed in a lawful and fair way in relation to the data subject.

Any processing of personal data will only be lawful to the extent that the processing is based on a valid processing ground. When special categories of personal data are being processed, specific processing grounds apply.

4.2 Transparency

It must be transparent to natural persons that their personal data are collected, used, consulted or otherwise processed and to what extent. Any information and communication relating to the processing of those personal data must be easily accessible and understandable, using clear and plain language. In particular, data subjects must be informed on the identity of the controller, the purposes of the processing and their rights.

4.3 Purpose limitation

The purposes for which personal data are processed must be explicit and legitimate and determined at the time of the collection of the personal data. The personal data cannot be further processed in a manner that is incompatible with those purposes.

4.4 Data minimisation

The personal data that are being processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4.5 Accuracy

Personal data must be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

4.6 Storage limitation

Personal data cannot be longer processed than strictly necessary for the processing concerned. As from the moment the personal data is not necessary anymore for achieving the purpose of the processing, it must be anonymised or deleted.

Personal data can therefore only be kept during a limited storage period, which must be justified in light of the applicable purpose. As from the expiration of the storage period, personal data must be anonymized or deleted, including personal data residing on back-up servers or servers hosted by third parties.

4.7 Integrity and confidentiality

Personal data must be kept confidential and secured so that it does not get corrupted.

Confidentiality arrangements must be put in place with employees, consultants and other parties accessing personal data. In addition, a role based permission system must ensure that those persons can only access those personal data which they need for the exercise of their job/function.

4.8 Accountability

The Puratos entities must be able to demonstrate compliance with the principles of lawfulness, fairness, transparency, data minimisation, purpose limitation, storage limitation, integrity and confidentiality. The data protection policies, controls, procedures, guidelines, checklists and other measures that constitute the data protection framework must be systematically documented.

4.9 Data protection by design and by default

Data protection principles must be proactively implemented when developing and designing processing operations.

The strictest privacy settings (in relation to the amount of data collected, the extent of the processing, the period of storage and its accessibility) must be applied by default to any processing. .

The respect of the data protection by design and by default principles must be a functional requirement in the entire lifecycle of Puratos operations involving the processing of personal data.

5. Lawfulness

Puratos processes personal data for the following purposes and in that regard relies on the below identified processing grounds.

5.1 Management of customers

Personal data of the contact persons of customers can be processed where necessary:

- for the execution of the contracts with such customers (eg delivery of goods, creation of personal account on the website, registration to an event, provision of training); or,
- in order to send information to such customers about similar products and services.

Personal data of prospects can be processed where necessary in order to take steps at the latter's request prior to entering into a contract.

5.2 Management of suppliers

Personal data of the suppliers can be processed for the execution of contracts with such suppliers.

5.3 Management of employees and job applicants

Personal data of employees and job applicants can be processed for the management of human resources, which includes the administration of workforce (eg payroll), the management of workforce (eg promoting employee well-being, managing careers and evolution, preventing abuse the company's rules and resources, evaluation and monitoring), internal and external communications and recruitment. This processing can be based on the legal authority of the employer, on the execution of (future) labour contract and on the legitimate interests of the relevant Puratos entity and its stakeholders.

5.4 Management of visitors and prospects

Personal data of visitors (such as contact persons of customers, or suppliers and prospects present in the offices, visiting the website, attending an event) can be processed in order to answer and manage the specific requests of such visitors: eg providing access to offices, sending newsletters or other direct marketing, registration for events. This processing can be based on Puratos' legitimate interests or the consent of the visitors concerned.

5.5 Management of risks and claims

Personal data of those persons in contact with Puratos can be processed for the prevention and detection of unlawful activities (such as fraud or abuse of company's resources) and for dispute management (such as the defense of legal claims). This processing can be based on the legitimate interests of the relevant Puratos entity and its stakeholders because it contributes to safeguarding and promoting the economic, commercial, social and financial interests of the Puratos group.

5.6 Research

All personal data can eventually be aggregated for the purpose of research and development, including statistics about sales, market analysis, development of products and services. This processing can be based on the legitimate interests of the relevant Puratos entity and its stakeholders because research and development can lead to enhancement of customer experience, improvement of Puratos products and services, and innovation, which may eventually result in an advantage for all persons concerned by Puratos products and services.

5.7 Global management at a group level

Personal data of customers, suppliers, employees, job applicants and visitors can also be processed by Puratos NV at group level for the global management of such customers, suppliers, employees, job applicants and visitors and for the global management of unlawful activities. This processing can be based on the legitimate interests of Puratos NV, the other Puratos entities and their stakeholders because global management at a group level is necessary for the efficiency, consistency and continuity of the Puratos group operations and contributes to safeguarding and promoting the economic, commercial, social and financial interests of the Puratos group.

5.8 Special categories of personal data

Some personal data such as data about ethnicity, data about religious and political convictions, data relating to criminal facts, health data, data regarding sexual orientation, biometric data and genetic data are considered as special categories of personal data because of their highly sensitive nature. These data are subject to more stringent rules and may only be processed with a specific processing ground (e.g. specific rights and obligations in the field of social law). If there are plans to process highly sensitive data, the Data Protection Team must be informed in advance.

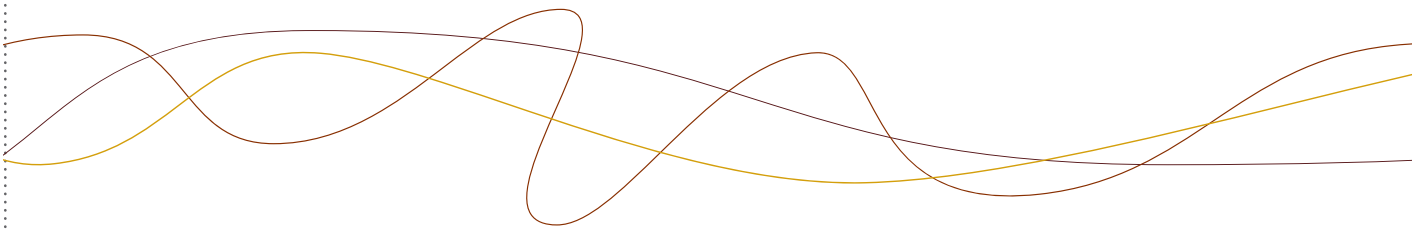
5.9 Automated individual decision-making

The data subject shall have the right not to be subject to a decision based solely on automated processing of his/her data, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless the data subject has given his or her explicit consent, when it is necessary for entering into or performing a contract, or if is authorised by law.

In case of automated individual decision-making based on consent or on a contract, the data subject must be given meaningful information about the reasoning involved, as well as the significance and the envisaged consequences for him or her and suitable measures must be implemented, such as the right for the data subject to obtain human intervention, to express his or her point of view and to contest the decision.

5.10 Data protection impact assessment

In order to enhance compliance, where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment must be carried out to evaluate, in particular, the origin, nature, particularity and severity of that risk.



6. Data subjects' rights

The Puratos group commits to respect the "Data subjects' rights" in line with the relevant data protection legislation. These rights, which are linked to specific legal conditions, are the "Data subjects' right" to:

- **Access** their personal data and obtain from the controller details about the processing.
- **Rectify** inaccurate personal data.
- **Object** to the processing of their personal data if, for example, the processing is based on the legitimate interests or pursues direct marketing purposes.
- **Erasure** if, for example, the data is no longer needed for the processing, the data subject objects to the processing, or the personal data is processed unlawfully.
- **Restrict** the processing of personal data in cases where, for example, the lawfulness of the processing or the accuracy of the data is contested. Once restricted, the controller may only store the personal data, cannot use it further and can only lift the restriction after informing the data subject about it. Each recipient to whom the personal data has been disclosed must be informed of any rectification, erasure or restriction that has been carried out.
- **Portability** if the processing is based on consent or the performance of a contract, meaning that data subjects have the right to receive their personal data which they have provided themselves, in a structured, commonly used and machine-readable format. Personal data which are derived or inferred from the personal data provided by the data subject are not covered by the right to data portability.

7. Security and confidentiality

Puratos entities and their employees must take sufficient technical and organisational measures to protect personal data from accidental or unauthorised destruction, accidental loss, unauthorised modification or access. These measures must be adequate in light of the state of the art, the cost and the nature of the data, and must be evaluated and tested at regular intervals.

Security and confidentiality requires measures to enhance awareness of data protection issues in the organization such a, for example, training of all functions confronted with personal data and allocation of responsibilities.

Techniques such as data minimisation, storage limitation, pseudonimisation, encryption, confidentiality, integrity and logging must be taking into consideration when dealing with data processing operations.

8. Processors

Puratos entities must verify that any processor, i.e. any provider processing personal data on their behalf, has implemented appropriate technical and organisational security measures. When considering these measures, the state of the art, the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons must be duly taken into account. Puratos entities must enter into a processing agreement with each of their processors in accordance with the applicable policies.

9. Transfer

The transfer of personal data is free within the countries of the European Union/European Economic Area and other countries deemed by the European Commission to provide for an adequate level of personal data protection.

When personal data is transmitted by a Puratos entity acting as controller in the European Union/European Economic Area to recipients in countries that do not provide an adequate level of protection, the relevant Puratos entity must ensure that appropriate safeguards are implemented such as, for example, standard data protection contractual clauses, binding corporate rules, approved codes of conduct and approved certification mechanisms.

In case a data subject claims that this policy has been breached by a Puratos entity in a third country without adequate level of protection that has imported the data, the Puratos entity that has exported the data undertakes to support the data subject in asserting his or her rights in accordance with this policy against such importing Puratos entity.

10. Golden rules for everyone within Puratos

As a good practice, anyone working at Puratos must comply with the following ten golden rules.

"Everyone sticks to their own jobs"

1. Do not consult personal data that is not intended for you (e.g. do not take notice of e-mails that are not intended for you).
2. Use the personal data only and, where necessary, for the performance of your duties within Puratos.
3. Your possible access to Puratos' databases is strictly personal and may not be passed on to others, inside or outside our organisation.

"Handle the personal data safely"

4. Keep the personal data only on the provided secure network drive and avoid printing. Keep paper lists or files with personal data in closed cabinets.
5. Do not allow personal data to circulate outside the organisation unless strictly necessary.
6. Ensure that laptops, USB sticks, smartphones, etc. with personal data are not left unattended or lost. Secure access with sufficiently strong passwords.

"Document any new/extended processing operations"

7. Inform your department manager and the Data Protection Team about any project of new/extended processing operations.
8. Before starting the new/extended processing, wait green light from the Data Protection Team, ensure that data protection principles are effectively taken into account, and ensure that the inventory of Puratos' processing has been updated accordingly.

"Report any problems"

9. Immediately forward any question or complaint from a person with regard to his/her personal data to the Data Protection Team (dataprivacy@puratos.com).
10. If you become aware of a (possible) loss, destruction, unauthorised access to or use of personal data, even if you are not 100% sure whether it qualifies as a personal data breach, immediately report this incident to your department manager and the Data Protection Team.

11. Data Protection Team

The Data Protection Team is responsible for this Policy and strives to implement and maintain compliance with national and international data protection rules on a continuous basis.

The Data Protection Team coordinates the handling of data subjects' requests. The Data Protection Team coordinates cooperation with the supervisory authorities and acts as a contact point for dealing with their requests and delivering information.

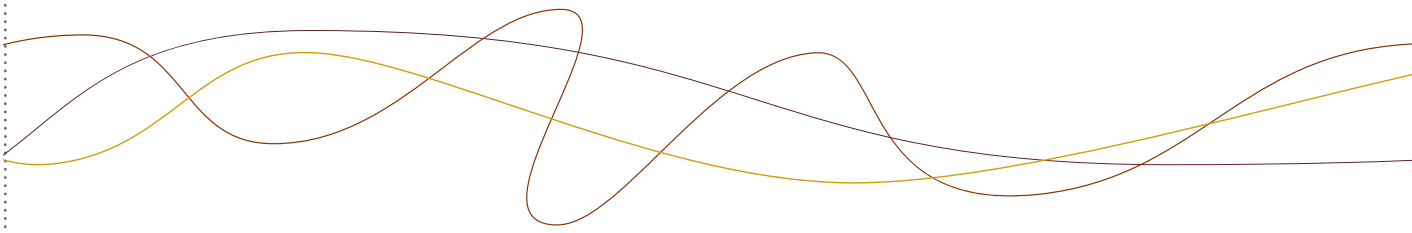
The Data Protection Team supervises the monitoring of compliance with this policy and may perform regular checks, reviews and audits of documents, procedures and operations.

The members of the Data Protection Team receive appropriate resources, training and guarantees of independence in order to ensure that the Data Protection Team is able to manage its tasks effectively.

The contact details of the Data Protection Team are: dataprivacy@puratos.com;
and Data Protection Team, Puratos NV, Industrialaan 25, 1702 Groot-Bijgaarden.

12.3. Data protection incidents

All employees must inform their department manager and the Data Protection Team immediately when becoming aware of a violation of this Policy or of a security incident which could involve a personal data breach, in accordance with the applicable procedure.



13. Responsibilities

The executive bodies of the Puratos entities and the department managers are accountable for the processing activities in their area of responsibility. They commit to effectively implement the appropriate technical and organizational measures to ensure compliance with the applicable laws and with this policy. They must closely co-operate with the Data Protection Team in order to achieve an adequate level of protection and to handle effectively the requests of supervisory authorities and data subjects. They manage that the Data Protection Team is duly informed in case of data protection incident and in case of new or extended processing activities, especially when they involve special categories of personal data or are likely to pose special risks to the rights and freedoms of individuals.

Breach of data protection rules may be criminally prosecuted in various jurisdictions and may result in damages claims. Breaches for which individual employees are responsible may lead to sanctions under employment law.

www.puratos.com

Puratos NV/SA - Industrialaan 25, Zone Maalbeek - B-1702 Groot-Bijgaarden, Belgium
T +32 2 481 44 44 - F +32 2 466 25 81 - E info@puratos.com

Puratos
Reliable partners in innovation