GENERAL DATA PROTECTION POLICY

Reference: GLAD-POL- 012
Version number: 1.0
Department: Global Legal Affairs Department

Written by	Reviewed by	Approved by
Global Legal Affairs Department	Marc Robert Fernandes, General Counsel	Nicolas Besins, CEO Alexandre Besins, CEO
Effective date: 29 July 2025	Review type: annual	

Table of contents

1. General 2

1.1 Purpose 2
1.2 Scope 2
1.3 Definitions & Abbreviations 3
1.4 Roles & Responsibilities 4

2. Principles relating to the Processing of Personal Data 5

2.1 Principle: Lawfulness, fairness and transparency 5
2.2 Principle: Purpose limitation 5
2.3 Principle: Minimization and accuracy 6
2.4 Principle: Limited retention 6
2.5 Principle: Security 7
2.6 Transfer of Personal Data outside the European Union 8
2.7 Processing of Sensitive Personal Data 8

3. Accountability and risk management 9

3.1 Privacy by Design and Privacy by default 9
3.2 Data Protection Impact Assessment 10
3.3 The Record of Processing activities 11

4. Associate training and awareness 11

5. Relations with Data Subjects 11

6. Management of Personal Data Breaches 12

7. Management of Third Parties 13

7.1 Qualification and contractualization 13
7.2 Processor due diligence 13

8. Relations with the Supervisory Authority 14

9. Monitoring compliance 14

ANNEX 1: Organisation and governance of Personal Data protection 15

1. Privacy Committee 15

2. Privacy Referents 15

3. Data Protection Officer (« DPO ») 16

4. IT department 16

1. General

1.1 Purpose

Besins Healthcare is committed to protect all Personal Data collected and processed within the scope of its activities, as well as to comply with applicable laws and regulations regarding the Processing of Personal Data. Capitalized terms have the meaning assigned to them in section 1.2 below.

The purpose of this General Data Protection Policy is to:

- Define Besins Healthcare's data privacy commitments in terms of compliance with the principles set forth by the Applicable Legislation.
- Define the roles and responsibilities of key contributors and stakeholders involved in the collection and processing of personal data.
- Ensure the implementation of appropriate methods and procedures, as well as appropriate governance and control structures for compliance with the Applicable Legislation.
- Ensure training, general knowledge and understanding by Associates of data privacy principles and best practices, beyond the legal requirements.

To aid in the understanding, some sections may be summarised by "key take" referring to the basic mandatory rule and this summary is identified by Rx. Compliance by Associates with these mandatory rules will be verified in accordance with the terms of the « Monitoring compliance » Section of this Policy.

This Policy is supplemented by the following policies and procedures:

- Data Subjects' Requests Procedure
- Data Breaches Management Procedure
- Privacy Impact Assessment Procedure
- Privacy by Design Procedure
- Data Retention Policy
- Legitimate interests balancing report
- Procedure for Supervisory Authority inspection.

1.2 Scope

The Policy applies to all employees, consultants and contractors under the direct authority of Besins Healthcare ("Associates"), and applies to all the Processing activities of Besins Healthcare, regardless of the Processing medium.

As a general principle and notwithstanding any mandatory rule to the contrary, in the event of conflicts between this Policy and the Applicable Legislation

- If the Policy provides higher protection than the one granted by the Applicable Legislation, the Policy shall apply;
- If the Applicable Legislation provides higher protection, the Applicable Legislation will take precedence over this Policy.

If there are any doubts regarding the interpretation of this Policy, please reach out to Besins Healthcare's DPO.

1.3 Definitions & Abbreviations

Term	Description
Associate	Any employee, consultant, contractor, director and officer working under the direct authority of Besins Healthcare
Applicable legislation	set of regulations relating to the protection of Personal Data and applicable to the Processing of Personal Data by Besins Healthcare, namely Regulation (EU) 2016/679 on the protection of Personal Data (GDPR), and any other regulations relating thereto.
Consent	any free, specific, informed and unambiguous expression of will by which the Data Subject accepts, by a clear declaration or positive act, that Personal Data concerning them may be processed, prior to the initiating of such Processing activity.
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.
Data Breach/Personal Data Breach	security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Besins Healthcare's Personal Data transmitted, stored or otherwise processed.
Data Protection Impact Assessment (DPIA)	analysis to be carried out by Besins Healthcare for Processing operations likely to present a high risk to the rights and freedoms of Data Subjects.
Data Protection Officer ("DPO")	The person/entity appointed by Besins Healthcare, responsible for monitoring the protection of Personal Data and Besins Healthcare's compliance with the Applicable legislation.
Data Subject	Identified or identifiable individual to whom the Personal Data relates. This includes, among others, current and former customers, prospects and Associates.
GDPR	the "General Data Protection Regulation" i.e. European Regulation (EU) 2016/679 which entered into effect on May 25, 2018.
Personal Data	any information relating to a Data Subject, in particular by reference to an identifier such as a name, 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 term « Personal Data » includes Sensitive Personal Data.
Processing	any operation or set of operations performed on Personal Data whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, Transfer, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Term	Description
Processor	any natural or legal person who processes Personal Data on behalf of the Data Controller and according to its instructions (e.g. providers or suppliers).
Project Owner	The Besins Healthcare Associate who is conducting a business or other operational activity which comprises the Processing of Personal Data.
Recipient	natural or legal person, public authority, department or any other body to which the Personal Data are disclosed.
Sensitive Personal Data	refers to special categories of Personal Data defined in Article 9 GDPR (i.e. Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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) as well as Data related to criminal convictions and offences.
Supervisory Authority	the competent Data protection authority in charge of monitoring the application of the Applicable legislation in order to protect the fundamental rights and freedoms of Data Subjects.
Third Party	any natural or legal person, public authority, agency or other body other than the Data Subject, the Controller and persons who, under the direct authority of the Controller, are authorised to process the Personal Data.
Transfer	any communication, copy or movement of Personal Data via a network, or any communication, copy or movement of such Personal Data from one medium to another, whatever medium is chosen, to a country outside the European Union or to an international organisation, which is or is intended to be the subject to a Processing after such Transfer.

1.4 Roles & Responsibilities

Role	Responsibilities
Top Management	Appoint a Data Protection Officer to ensure Besins Healthcare's compliance with the Applicable Legislation and with the commitments made under this Policy.
Privacy Committee	Take day-to-day decisions on privacy governance following DPO recommendations (see Annex 1 Section 1)
Privacy Referents	Monitor compliance and implement remediation measures in their department, requesting DPO involvement as needed (see Annex 1 Section 2)
Data Protection Officer	Raise awareness, advise, monitor compliance, prepare remediation plans, draft privacy documentation and emit recommendations (see Annex 1 Section 3)
IT department	Advise and assist on information security, technical feasibility, and Data Breaches. (see Annex 1 section 4)

2. Principles relating to the Processing of Personal Data

In accordance with the Applicable Legislation, Besins Healthcare undertakes to comply with the principles hereafter when collecting and Processing Personal Data.

2.1 Principle: Lawfulness, fairness and transparency

Personal Data must be collected and processed in a lawful, fair, and transparent manner.

To that end, Besins Healthcare guarantees that any Processing operation relies on a lawful basis recognised by the Applicable Legislation such as:

- Data Subjects have given their Consent to the Processing of their Personal Data for one or more specific purposes;
- The Processing is necessary for the performance of a contract to which the Data Subject is a party or to take pre-contractual measures at the request of the Data Subject;
- The Processing is necessary to comply with legal obligations to which Besins Healthcare is subject;
- The Processing is necessary to further legitimate interests pursued by Besins Healthcare;
- The Processing is necessary to protect the vital interests of the Data Subject;
- The Processing is necessary to perform a task carried out in the public interest.

When a Processing operation is based on Besins Healthcare's legitimate interests, the Project Owner, with DPO support, assesses whether this interest is overridden by the Data Subjects' interests or fundamental rights and freedoms. This assessment and its outcome must be documented as part of Besins Healthcare's accountability obligations.

If Associates process Sensitive Personal Data, Besins Healthcare ensures compliance with the "Processing of Sensitive Personal Data" section of this Policy.

R01 An appropriate lawful basis is identified for each Processing operation and documented in a record of processing activities.

Besins Healthcare ensures that its Processing operations are carried out in a visible and transparent manner. To that end, Besins Healthcare provides accessible and intelligible information to Data Subjects regarding the Processing of their Personal Data as required in the Applicable Legislation.

2.2 Principle: Purpose limitation

Before collecting Personal Data, the Project Owner must clearly defines the purposes for its collection. Such purposes must be determined, explicit and legitimate. Besins Healthcare ensures that the defined purposes align with its activities.

Personal Data must not be processed for additional purposes incompatible with the original purpose of its collection. Before reusing Personal Data for a different purpose, Besins Healthcare conducts a compatibility test to ensure the new purpose aligns with the original one. This test considers:

- The existence of a link between the two purposes;
- The context in which the Personal Data have been collected, in particular with regard to the relationship between the Data Subject and Besins Healthcare;
- The nature of Personal Data, in particular if it is Sensitive Personal Data;
- The possible consequences of the intended subsequent Processing for Data Subjects;
- The existence of appropriate safeguards.

Where the subsequent purpose is incompatible with the initial purpose, Besins Healthcare ensures that the Consent of the Data Subject is obtained.

R02 Personal Data must be collected only for specific, explicit and legitimate purposes and not be further processed in a manner incompatible with such purposes.

2.3 Principle: Minimization and accuracy

Personal Data collected must be adequate, relevant, and not excessive for the Processing purpose. Besins Healthcare ensures that only the strictly necessary Personal Data are collected.

Additionally, Besins Healthcare ensures Personal Data are accurate and updated as needed. Reasonable measures are taken to promptly erase or rectify any inaccurate Personal Data.

R03 Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purpose of the Processing. They must be accurate, complete, and updated as necessary.

2.4 Principle: Limited retention

Besins Healthcare ensures that Personal Data may only be retained in a form which permits the identification of Data Subjects for a period that does not exceed what is necessary to achieve the purposes for which they are processed.

Once this purpose has been achieved, Personal Data must be deleted or anonymized unless one of the following exceptions apply:

1) Personal Data may be archived to comply with mandatory retention periods (conservation of accounting documents, etc.) in order to be able to respond to requests for communication that may be addressed by certain legally authorised third parties (tax authorities, social organisms, etc.).

2) Personal Data may be archived to match legal statutes of limitation, essentially for evidentiary purposes (archiving of electronic contracts, etc.).

3) Personal Data may be retained for longer periods of time insofar as the Personal Data is processed exclusively for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are implemented to guarantee the rights and freedoms of the Data Subject, such as partial anonymisation or pseudonymisation.

To ensure compliance with this principle, Besins Healthcare defines, justify and document the different retention periods applicable to each Processing operation using the following guidelines:

- Legal obligations;
- Recommendations of Supervisory Authorities;
- Best practices;
- Statutes of limitation;
- Operational needs.

These retention periods are periodically reviewed and updated to reflect changes in the Applicable Legislation and practices within Besins Healthcare.

At the end of each retention period, Personal Data will be deleted without undue delay, either by erasure or anonymization. If deletion involves destruction, Besins Healthcare ensures effective removal from its systems, including third-party systems.

The requirements and implementation methods of the storage limitation principle are detailed in Besins Healthcare's dedicated policy (“Personal Data Retention Policy”).

R04 Retention periods are defined in the Data Retention Policy and all Project Owners are responsible to implement them.

2.5 Principle: Security

Besins Healthcare defines and implements appropriate technical and organizational measures to ensure the availability, confidentiality, and integrity of Personal Data throughout Processing. These measures consider:

- The severity and likelihood of potential harm from loss, alteration, or unauthorized access to Personal Data
- The characteristics of the Processing;
- Where applicable, the results of the Data Protection Impact Assessment carried out;
- The state of the art of security systems;
- The costs of implementation.

Besins Healthcare has an IT Security Policy detailing all technical and organizational security measures, which is regularly reviewed and updated. Besins Healthcare commits to regularly testing, evaluating, and improving security measures.

Besins Healthcare also ensures proper management of any Personal Data Breach in accordance with the Data Breach section of this Policy.

R05 Appropriate technical and organisational measures are implemented to ensure the security, integrity and confidentiality of Personal Data.

2.6 Transfer of Personal Data outside the European Union

Transfers of Personal Data require additional attention and safeguards. Besins Healthcare ensures that any Transfer of Personal Data is adequately secured and legally framed.

Besins Healthcare makes sure to:

- Identify all types of Transfers, including Transfers by Processors;
- Include specific contractual provisions in agreements with third party providers regarding data transfers and the localization of processing activities within the EU. Providers must ensure measures that guarantee a level of personal data protection equivalent to the Applicable Legislation.
- Secure all Transfers by taking appropriate technical and organisational measures;
- For Transfers to countries not recognized as adequate by the European Commission, legally frame the Transfer through appropriate safeguards.

The transfer of Personal Data to new recipients located outside the EU should not be carried out before requesting advice from the DPO, unless such recipient is located in a country deemed "adequate" by the European Commission: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

R06 Each Personal Data Transfer is adequately secured and legally framed in accordance with the requirements of the Applicable Legislation.

2.7 Processing of Sensitive Personal Data

Sensitive Personal Data may be collected ONLY IF the two following cumulative conditions are met: (1) there is a generic lawful basis for the processing (see section « Lawfulness, fairness and transparency »), AND (2) one of the following additional special conditions applies:

- The Data Subject have given its explicit Consent;
- The Processing is necessary for the purposes of carrying out Besins Healthcare's or the Data Subject's the obligations, or exercising their respective rights in the field of labour law, social security and social protection law;
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The Processing relates to Personal Data which are clearly made public by the Data Subject;
- The Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are requesting such Processing;
- The Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to Data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a

health professional when the data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy;
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- A specific condition provided for by the Applicable Legislation applies.

Besins Healthcare must take specific security measures for Sensitive Personal Data considering the risks their Processing may create for Data Subjects.

Data related to criminal convictions, offences, or security measures should generally not be collected, except in exceptional cases with DPO validation (e.g., verifying a job candidate's criminal record due to the specific nature of the position). When collected, it cannot be retained beyond completion of the initial purpose.

R07 The Processing of Sensitive Data is prohibited in principle. Any exception must be made in accordance with the conditions required by the Applicable Legislation and conveyed to the DPO for documentation and advice.

3. Accountability and risk management

All evidence of compliance with the Applicable Legislation must be documented.

3.1 Privacy by Design and Privacy by default

For any new project involving personal data processing, the Project Owner must implement measures to protect personal data from the initial design stage, throughout the project, and across the entire data lifecycle (from collection to destruction).

Project Owners managing a new project must follow these steps:

Step 1. Verify that all principles defined in Section 2 of this Policy are respected.
Step 2. List existing and planned technical and organisational measures to ensure the availability, integrity, and confidentiality of Personal Data.
Step 3. Conduct the DPIA pre-check to assess the level of risk (see Section 3.2).
Step 4. Carry out a Data Protection Impact Assessment if necessary.
Step 5. Implement security measures adapted to the level of risk.

The process to follow is detailed in Besins Healthcare's Privacy by design/by default checklist.

When the project involves entrusting all or part of the Processing to a Processor, Besins Healthcare ensures that the requirements of the section "Management of third parties involved" are respected.

R08 All projects must be designed to ensure the protection of Personal Data by design and by default.

3.2 Data Protection Impact Assessment

When a processing operation is likely to pose a high risk to the rights and freedoms of data subjects, Project Owner assisted by the DPO must carry out a Data Protection Impact Assessment (DPIA) before implementation, following the DPIA Procedure.

Besins Healthcare ensures that a pre-check is carried out for any new Processing operation to assess the level of risk of the Processing and, therefore, whether a DPIA should be conducted. This pre-check considers:

- Mandatory cases defined by the Supervisory Authority;
- The set of criteria set forth by the European Data Protection Board;
- The exemptions provided by the GDPR and the relevant Supervisory Authority.

The DPIA must be documented and:

- Describe the nature, scope, context and purposes of the Processing;
- Assess the necessity and proportionality of the Processing operations;
- Assess the existing safeguarding measures;
- Identify and assess risks to Data Subjects;
- Identify all measures susceptible to address and mitigate these risks.

For more information, please refer to EDPB Guidelines on DPIA.

R09 The necessity to carry out a DPIA must be assessed by the Project Owner for each new project and a DPIA is performed if required, prior to the beginning of the Processing.

The DPIA is a continuous process and will have to be reviewed regularly to ensure that the level of risk remains acceptable throughout the duration of the Processing, as the environment, particularly technical, may be subject to change, which in turn may require the implemented measures to be adapted.

Similarly, if a Processing operation does not at first stage require a DPIA but evolves afterwards, a DPIA may have to be carried out at a second stage.

R10 The need to perform a DPIA or update an existing one is considered for each major change in a Processing operation.

The DPO will consult the Supervisory Authority if the DPIA reveals that the processing poses a high risk to the rights and freedoms of data subjects, meaning the residual risk remains high even after implementing the risk remediation plan.

R11 When the DPIA shows that a high residual risk persists, the Supervisory Authority is consulted.

3.3 The Record of Processing activities

As Controller, Besins Healthcare must always maintain a Record of Processing activities.

To that end, Besins Healthcare designates the key actors involved in maintaining and updating the Record, their roles, and responsibilities.

R12 A Record of Processing activities under Besins Healthcare's responsibility is kept up to date.

4. Associate training and awareness

Besins Healthcare ensures that all its Associates are made aware of the issue of Personal Data protection and understands the intent and scope of the Applicable Legislation as well as the risks in the event of non-compliance. If relevant, Associates are trained on legislative or jurisprudential developments in the field of Personal Data protection as well as updates of applicable internal policies.

Besins Healthcare also provides specific training for Associates designated as Privacy Referents.

All new employees receive awareness/training appropriate to their tasks and level of knowledge.

Training will be provided using e-learning modules, dedicated webinars or internal training courses.

R13 All Associates are made aware of the general principles and challenges of Personal Data protection. Special in-depth training is provided to Privacy Referents.

5. Relations with Data Subjects

Besins Healthcare undertakes to guarantee the effective exercise of Data Subjects' privacy rights, which are:

1. Right to information: the right to have clear, precise and complete information about Besins Healthcare's use of their Personal Data.
2. Right of access: the right to obtain a copy of the Personal Data that the Controller holds on the Data Subject.
3. Right to rectification: the right to have their Personal Data rectified if they are inaccurate or obsolete and/or to complete them if they are incomplete.
4. Right to erasure / right to be forgotten: the right to have their Data erased or deleted, unless Besins Healthcare has a legitimate interest in keeping them.
5. Right to object: the right to object to the Processing of Personal Data by Besins Healthcare for reasons related to the particular situation of the Data Subject.
6. Right to withdraw Consent: the right to withdraw Consent at any time when the Processing is based on Consent.
7. Right to restriction of Processing: the right to request that the Processing of Personal Data be temporarily suspended.

8. Right to Data portability: the right to receive from the Controller Personal Data concerning them, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format.
9. Right not to be the subject to an automated decision: the right not to be subject to a decision based solely on automated Data Processing activity, including profiling, which produces legal effects concerning the Data Subject or similarly significantly affects him or her.

Additional rights may be granted to Data Subjects by local legislation.

To this end, Besins Healthcare defines and implements a procedure for the management of Data Subjects' rights in accordance with the requirements of the Applicable Legislation. This procedure establishes:

- The standards to be respected to ensure the transparent information of Data Subjects;
- The legal requirements that must be respected;
- The authorised means of submitting an application for each right, according to the category of Data Subjects;
- The business processes to manage these requests in accordance with the requirements hereinabove;
- The parties involved in these processes, their roles and responsibilities.

Requests submitted by data subjects exercising their rights are documented in a record to demonstrate compliance. The Data Subject Request Procedure outlines the content and methods for maintaining this record.

R14 Besins Healthcare and the DPO must develop and maintain a procedure relating to the management of the Data Subjects' rights, with requests being recorded in a dedicated record.

6. Management of Personal Data Breaches

In line with its security obligations, Besins Healthcare defines, documents, and implements a process to detect, qualify, and respond to personal data breaches. The procedure must include:

- A risk assessment matrix for the rights and freedoms of impacted data subjects, considering criteria defined by the Supervisory Authority
- Distribution of roles and responsibilities among all parties involved, including Besins Healthcare's processors
- Terms, conditions, modalities, and deadlines for notifying the Supervisory Authority and/or affected data subjects

Adequate technical and organizational measures are implemented to detect, investigate, and report personal data breaches. Additionally, Besins Healthcare's employees are trained and made aware of the procedure to follow in case of a suspected or confirmed data breach.

R15 Besins Healthcare and its DPO must develop and maintain a procedure for the management of Personal Data Breaches

In addition, Besins Healthcare maintains a record of Data Breaches for accountability purposes, logging all Data Breaches regardless of whether a notification is required.

R16 A record of Data Breaches is kept up to date.

7. Management of Third Parties

7.1 Qualification and contractualization

The Project Owner ensures that the Third Party involved is properly qualified (separate Controller, joint Controller or Processor) and that a written contract clearly defines the roles and responsibilities of each party with respect to Processing activities and data privacy obligations. If relevant, this contract includes at least the clauses required by the Applicable legislation. Please consult the DPO for this purpose.

When the Third Party acts as Processor, the signed contract must detail the Processing entrusted to the Processor by describing:

- The purpose and duration of the Processing;
- The nature and purpose of the Processing operations;
- The category or categories of Personal Data;
- The category or categories of Data Subjects;
- Instructions for Processing operations.

R17 A written contract is signed with each Third Party involved in the Processing. This agreement includes appropriate contractual clauses, in accordance with the Applicable Legislation.

7.2 Processor due diligence

Besins Healthcare undertakes to select Processors who offer sufficient guarantees regarding the implementation of appropriate technical and organisational measures.

In this respect, the Project Owner systematically performs a preliminary check to assess the guarantees offered by any Processor, in particular by means of questionnaires and/or documentation analysis. This verification must make it possible to evaluate the procedures for carrying out the Processing operations entrusted to it, security and confidentiality of Personal Data, and maturity of the Processor on the issue of Personal Data protection.

R18 A control of the guarantees offered by each Processor is carried out before entrusting them with Processing activities.

Processors are regularly audited to verify their ongoing compliance with contractual and regulatory requirements, according to modalities defined considering the nature and sensitivity of the Processing operations entrusted, the costs required and the resources available.

R19 Processors are regularly audited to verify their ongoing compliance with contractual and regulatory obligations.

8. Relations with the Supervisory Authority

Besins Healthcare fully cooperates with any Supervisory Authority when required to do so and provides all evidence of its compliance with the Applicable Legislation.

Besins Healthcare's Data Protection Officer acts as the main contact point for the Supervisory Authority, for:

- Consulting the relevant Supervisory Authority if a Processing involves a high residual risk for privacy;
- Notifying a Data Breach to the relevant Supervisory Authority when required;
- Handling all requests submitted by any Supervisory Authority (such as requests for access to the Record of Processing activities, requests for information, etc.)

Besins Healthcare defines a process in case of audit or inspection by a Supervisory Authority, which defines the roles and responsibilities of key actors in these controls.

R20 Besins Healthcare cooperates with Supervisory Authorities and defines a process in case of an audit.

9. Monitoring compliance

Privacy Referents are tasked with monitoring the compliance of their department and seeking the advice of the DPO whenever a new project is envisioned.

Additionally, an annual compliance check is conducted to evaluate Besins Healthcare's adherence to Data Protection policies and procedures, and the alignment of Processing activities with the Record of Processing activities. This check is performed by the DPO and relevant stakeholders.

Upon identifying non-compliance, the DPO and stakeholders develop a remediation plan, considering risks, costs, operational constraints, and available resources. Corrective measures are implemented promptly by stakeholders under the DPO's supervision.

R21 A framework for monitoring Besins Healthcare's compliance is implemented and complemented with remediation plans when necessary.

****

Signed by:
Nicolas Besins
Signer Name: Nicolas Besins
Signing Reason: I approve this document
Signing Time: 23 July 2025 | 11:22:52 AM CEST
EFBAF1F55011429FB35DB28EA5893B93

Nicolas Besins
CEO

Signed by:
Alexandre Besins
Signer Name: Alexandre Besins
Signing Reason: I approve this document
Signing Time: 23 July 2025 | 11:22:48 AM CEST
27805063219341429B04B281A7ABE547

Alexandre Besins
CEO

ANNEX 1: Organisation and governance of Personal Data protection

Each Associate working at Besins Healthcare is responsible for the protection of Personal Data. We value the data privacy of our Associates, our partners and customers, and of the patients we serve. We reflect this value in our operational policies, procedures, and practices.

Please note that main contributors identified in this section must adopt the roles and responsibilities set forth herein to ensure that this Policy is implemented in a consistent and coordinated manner within Besins Healthcare. Please contact the DPO if you need support to implement such roles and responsibilities.

1. Privacy Committee

The Privacy Committee guarantees Besins Healthcare's strong commitment to the protection of Personal Data as a strategic asset of the company. In this respect, the Privacy Committee must:

- Ensure the implementation of an adequate Personal Data protection governance, defining roles and responsibilities within Besins Healthcare and allowing the DPO to be involved, in an appropriate and timely manner, in all Data protection matters;
- Communicate to all employees the appointment of a DPO, their missions and how to contact them;
- Validate the GDPR compliance documentation from time to time;
- Ensure that the DPO:
    - Has the necessary resources and means to carry out their missions;
    - Does not receive any instructions with regard to the performance of their missions;
    - Receives appropriate training;
    - Can report directly to the Privacy Committee.

2. Privacy Referents

In each department processing Personal Data, Privacy Referents designated by the department head and whose identity is communicated to the Privacy Committee must:

- Ensure compliance with this Policy and related procedures.
- Involve the DPO from the design phase of new projects involving Personal Data.
- Facilitate communication between project owners of their departments and the DPO when Data Protection Impact Assessments are carried out.
- Document and justify in writing any deviations from the DPO's recommendations.
- Respond to DPO information requests regarding Personal Data matters.
- Provide all relevant documentation related to the Processing operations of their department.
- Record any new Processing operation in Besins Healthcare's Record of Processing activities.

3. *Data Protection Officer (« DPO »)*

Besins Healthcare's leadership has appointed a Data Protection Officer (DPO) to ensure its compliance with the Applicable legislation and this Policy.

The DPO has several missions within Besins Healthcare:

- Inform Associates and raise awareness about Personal Data Protection;
- Ensure compliance with the Applicable legislation and this Policy;
- Advise business departments on privacy principles for new projects, issue recommendations, and suggest alternatives if needed;
- Inform and alert, if necessary, Besins Healthcare's top management of the risks induced by projects and/or non-compliance with issued recommendations;
- Determine if a Data Protection Impact Assessment (DPIA) is needed and advise on its execution;
- Assist in assessing and responding to Personal Data Breaches, acting as a contact point for notifications to Supervisory Authorities and Data Subject;
- Analyse, investigate, audit, and control compliance, supporting business departments in remediation plan implementation;
- Establish and maintain accountability documentation;
- Submit an annual report to the top management;
- Interact with the Supervisory Authority.

The DPO provides specific training to appointed individuals.
The DPO prepares and sends to Besins Healthcare's leadership an annual report on activities relating to Data protection within Besins Healthcare. The DPO defines, collects, and summarizes indicators that highlight the level of compliance with internal policies and procedures and, in general, the Applicable legislation.

4. *IT department*

For each project, the IT department provides support and expertise to:

- Assess of the context and criticality of the project;
- Conduct an information security risk analysis, especially for pre-checks before DPIA execution.
- Advise on adequate security measures to reduce, avoid or transfer risks;
- Assess of the level of security of Processors involved and negotiate with them to incorporate Besins Healthcare's security requirements into the contract;
- Coordinate with the DPO to monitor, detect and respond to security incidents qualifying as Data Breaches.