Personal Data Protection Policy

February 2024

Policy version control

Title	Personal Data Protection Policy
Written by	data protection officer (external)
Reviewed by	Director Internal Operations, General Counsel
Approved by	Management Team
Distribution list	All GARDP Staff and Committees members

Revision history

Version	**Reasons and Changes**	**Date**
Version 1.0	Approved policy by OMT	May 2023
Version 1.1	Update to the Swiss legal references.	February 2024

Contents

1. Introduction

Personal data is any information which identifies an individual, directly, or indirectly, and in any forms. Personal data shall be protected as its unlawful, illegitimate use or dissemination can damage the privacy of the individuals to which they belong, and cause them harm, sometimes in an irreversible manner.
This Data Protection Policy defines the objectives set by GARDP (as defined below) for the protection of individuals whose personal data is collected or received by GARDP, stored, and used internally, or otherwise transferred externally, and the good practices that must be applied within GARDP to ensure the protection of the rights and freedoms of these individuals (**data subjects**). It is meant also to inform GARDP internal and external stakeholders about the practices it has implemented to comply with all data protection laws and ethical principles applying to the protection of personal data processed by GARDP.

2. Data protection at GARDP

GARDP Foundation ("**GARDP**") a Swiss foundation established pursuant to article 80 et seq. of the Swiss Civil Code with registration number CHE 331.930.936 having its principal office at 15 Chemin Camille-Vidart, 1202 Geneva, Switzerland.

GARDP accelerates the development and access of treatments for drugs-resistant infections. Working together with governments, the private sector, academic institutions, and civil society, we drive the development of innovative solutions to tackle antibiotic resistance. For this, GARDP uses personal data to allow GARDP to achieve its mission. Protecting individuals (staff, consultants, partners, experts, suppliers, patients, clinical trials staff, participants to clinical research studies, and others (as the case may be) and their data is a responsibility from a legal and ethical point. GARDP is committed to sustainable developments to protect the personal data of the individuals working with us or contributing to our research programs.

The protection of personal data is of utmost importance to GARDP. As outlined under section 2.2 of GARDP's **Code of Ethics**, GARDP is continually assessing (as defined below) privacy to the maximum extent possible and comply with the Swiss Federal Act on Data Protection (2023, "**FADP**") as well as European General Data Protection Regulation (2018, "**GDPR**"). Along the above principle, GARDP collects and maintains personal data as necessary to allow GARDP to achieve its mission. GARDP ensures that personal data is kept in accordance with strict security controls. To ensure that individuals whose personal data is used by GARDP are applied the same level of protection across all territories, GARDP has chosen to apply the most protective standard: the Regulation (**EU**) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the **processing** of personal data and on the free movement of such data - General Data Protection Regulation (GDPR).
GARDP recognizes however that, operating in different parts of the world (notably in Switzerland), any applicable national data protection laws ought to be considered in case they set forth more stringent requirements. This policy does not override any other applicable national data protection laws.

Among others, GARDP applies the following principles whenever handling personal data:

- Collecting and using personal data fairly and lawfully. GARDP strives to be transparent and open regarding data collection. GARDP will only use personal data for the purposes for which it was given or received or other legitimate and legal purposes.
- Respecting individual rights and choices. GARDP respects data subject's requests as to how their personal data is collected, processed and used by GARDP and its partners, donors, collaborators and service providers. This includes the right to access, correction and removal of data.
- Managing data responsibly. Confidentiality and integrity of personal data is essential to maintain trust in GARDP and to allow GARDP to achieve its public benefit mission. GARDP is committed to taking necessary measures to protect personal data from the risks of unauthorized use or disclosure.

3. Purpose

The purpose of this policy is to inform about GARDP's commitment to personal data protection compliance, to set out the responsibilities and outline the principles that must be applied to the processing of personal data.

This policy works in association with other GARDP policies, for instance but not limited to, GARDP IST Policy and Code of Ethics, as well as with GARDP personal data protection procedures, for instance but not limited to, GARDP procedure for managing **data subjects' requests** and GARDP procedure for managing **personal data breaches**.

This policy has been approved by GARDP. Any breach of this policy will be taken seriously.

4. Applicability

This policy is applicable to GARDP:

- To all "**GARDP Members"** which include employees, support staff, volunteers, interns, apprentices and trainees, agency staff employed by GARDP, consultants or contractors, staff seconded to GARDP from other organizations, and GARDP's Board, Audit Committee, Scientific Advisory Committee or any other Committee members (GARDP Member is further defined in the Code of Ethics)
- to all personal data, regardless of the media on which that data is stored, and regardless of the role of GARDP in processing this data, whether **data controller** (the most frequent role for GARDP) or **data processor** (unless otherwise specified, the principles stated in this policy apply to both roles).

Country-specific or function specific data protection requirements might apply and will be reflected in the local version of this policy or in function specific procedures. Other entities members within the GARDP Network should align with this policy and this is a requirement for GARDP's conducted activities.

5. The Data Protection Steering Group

GARDP has setup a Data Protection Steering Group, with expertise from different teams, namely the legal department, the information technology department, the director of internal operations, the clinical operation leader, the external affairs department, the human resources department and data protection officers ("DPO").

The Data Protection Steering Group has oversight for:

- Putting in place this policy in line with the relevant data protection principles and laws and keeping this policy updated in line with changes in legislation and guidelines from data protection authorities.
- Develop awareness and provide training regarding data protection.
- Monitoring the compliance of GARDP organization and operations with personal data protection laws, identify gaps and risks.
- The progress of IT projects when data protection and / or information security is concerned.

6. Data protection fundamental principles

There are several principles that GARDP Members shall consider when handling all types of personal data. Typically, GARDP Members will process personal data:

- When involved in clinical research for example patient data, the research team or collaborators,
- When dealing with HR management and this does not apply only to the HR department, for example managers' tasks (sickness management, annual performance reviews, recruitment, interviews) concerning members of their team.
- When dealing with external individuals for example working in External Affairs or the Communication department.
- When using GARDP's CRM, a database holding an important amount of personal data both internal and external.

This includes physical (paper-based) as well as electronic data.

The data protection principles state that personal data shall be:

1. **Processed fairly, lawfully and in a transparent way (*lawfulness, fairness and transparency*).**

   To ensure that data processing is lawful, GARDP must identify a valid legal basis for its use of personal data, applying to every activity that requires the use of personal data. Given the complexity of data protection in this area, please consult with the legal department and DPO for review and validation of the legal basis to apply.

   GARDP must always ensure our use of personal data does not affect individuals and consider any adverse impact on them. We demonstrate

openness through data protection / privacy notices and, for clinical studies, participant information sheets.

2. **Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (*purpose limitation*).** Whilst GARDP must only use personal data for the purposes we specify, it may also re-use that data for compatible purposes. For example, secondary use of data may be allowed in clinical research following a specific exemption, certain conditions and with safeguards in place. Please consult with the legal department or the DPO before envisaging to re-use personal data.

3. **Adequate, relevant and limited to what is necessary (*data minimisation*).** GARDP Members shall only collect data that is relevant for the intended purpose. Collecting information that is not going to be used means that it is unnecessary and therefore unlawful. For example, asking an individual who wants to attend an event their email address is necessary, asking them unrelated personal details are not relevant and therefore shall not be collected.

4. **Accurate and kept up to date (*accuracy*)**: reasonable measures should be taken to ensure the accuracy of data and should it be inaccurate, it should be deleted or rectified without delay.

5. **Kept secure and protected from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data by implementing appropriate technical and organisational measures (*integrity and confidentiality*).**
   This applies to personal data held electronically, and also applies to paper-based documents. Be careful when handling personal data and only share on a need-to-know basis. Keeping personal data secure is achieved through robust IT systems and controls as well as organisational measures such as training provided to staff, policies and standard operating procedures in place. The IST Policy should be read and applied in conjunction with this policy.

6. **Kept for no longer than is necessary (*storage limitation*).**

7. The principles also include a **responsibility to document and demonstrate how GARDP complies with the law (*accountability*).**

In general, when a GARDP Member intend to start a new activity where personal data is going to be processed or an already existing process is changed by collecting more information on a data subject or introducing a new system or transferring data to a new third party or country for example, GARDP Members should contact GARDP's DPO.

While designing systems and drafting procedures related to personal data processing, GARDP shall ensure that the design aligns to the above data protection principles and that it enables data subjects to exercise their rights. DPO can support GARDP Members during this process, which is called "data protection by design".

7. Rights of data subjects

The aim of personal data protection is to protect the rights and freedoms of individuals from which we process data. GARDP Members shall be aware of these rights, be able to identify them and know how to handle them.

There are strict deadlines defined by the data protection laws for the processing of a data subject's right request. To be compliant in any situation, GARDP has 30 calendar days to respond as a maximum. It is recommended however to respond as soon as possible. Note that it can be complex and time consuming to locate someone's data. An identity check is required in most circumstances, this is managed by the DPO and GARDP must provide the information (in the example of a right of access) in a format that will be understood and readable.

These rights are:

- The right to be informed,
- The right of access,
- The right of rectification,
- The right of erasure,
- The right of restriction,
- The right to object,
- The right to portability,
- The right over automated decision making,
- The right to be informed of a data breach,
- The right to complain to a supervisory authority.

For more information about these rights, please consult the GARDP data protection procedure "Managing Data Subjects Requests" and the dedicated SharePoint site for the Legal team:
https://dndi.sharepoint.com/sites/GARDPLegalPublic

Should a GARDP Member receive a data subject's right request, they must contact immediately the legal department and/or the DPO at dataprivacy@gardp.org.

8. Processing of sensitive data

The right of processing sensitive personal data is more limited and subject to conditions, such as implementation of appropriate safeguards or specific legal basis. Typical functions that will process sensitive data are within the research environment and the HR department, Research will require medical information for example to answer the research question and HR has legal obligations to collect sensitive information concerning medical details (sickness record, disability details for example) or ethnical background (for diversity and equity purposes) as the case maybe. This includes processing sensitive personal data for scientific, historical, research or statistical purposes where appropriate safeguards (anonymization where possible; alternatively, encryption or pseudonymization) need to be put in place.

The processing of data from clinical studies is considered as a large-scale processing of sensitive data and may generate high risks for the study subjects (data subjects). High risk means that an event such as loss of confidentiality, loss of integrity of data can have a big impact and consequences for an

individual. For example, a malicious person illegally obtaining personal data that GARDP process will use this to steal someone's ID, blackmail, targeted campaign to sell medical devices or medications, where the individual will be left feeling with feelings of fear, violation of privacy, untrust towards GARDP. Other processing activities such as those using new technologies or making use of large-scale publicly accessible personal data (e.g. from social media) or are meant to systematically monitor the behaviour of data subjects (e.g. If a research study monitored a participant through a medical device) may also generate high risks, even when they are not involving sensitive data. A **Data Protection Impact Assessment (DPIA)** shall be conducted to understand how such processing activities may affect data subjects before starting data collection. If appropriate, a competent data protection authority may have to be consulted.

A DPIA will include: a description of the processing, its purposes and the legal basis, an assessment of the necessity and proportionality of the processing in relation to its purpose, an assessment of the risk to the data subject and the risk mitigation measures in place and demonstration of compliance. GARDP Members shall ask the advice of the DPO before conducting a DPIA and shall ask the DPO for conducting an evaluation of a DPIA after GARDP Members have completed it and before submitting it to management for validation.

9. Records Of Processing Activities (ROPA)

GARDP maintains records of its personal data processing activities and shall make the records available on request of a competent data protection authority. These records include (but are not limited to) descriptions of the personal data types, data subject types, processing activities, processing purposes, outsourcing parties, third-party recipients, storage locations, transfers, retention period and a description of the security measures in place. The register is maintained by a designated and trained functional representative and managed by the DPO.

10. Obligations when outsourcing data processing activities.

GARDP is also responsible and accountable for the data that is processed on its behalf and under its instructions. The outsourced party is a **data processor**. GARDP has numerous relationships for example in a research study. GARDP has data processors such as CROs, study sites, laboratories. For other internal functions, GARDP may have data processors such as mailing compagnies, translation services, communication and marketing organisations, accounting services for example.

The concept of a relationship with outsourced parties is also compounded by the fact they can themselves outsource to sub-processors some of the tasks GARDP has entrusted them with. GARDP is obligated to demonstrate oversight of the entire chain of processing and is accountable and should carry out due diligence when contracting with another organisation by evaluating the risk to the personal data at play.

GARDP must ensure that the outsourced party (including any sub-processors) has implemented appropriate organisational and technical measures to adhere to the principles outlined in this policy. GARDP must also ensure that

appropriate contractual provisions are put in place to clarify the obligations of both parties in respect to ensuring data protection and ensuring the rights of individuals will be protected. Regulation in terms of data protection of the country of the receiving party will also have to be considered.

GARDP Members are required to seek experts' advice and contact the legal department and / or the IST department and / or the DPO before engaging with new outsourced parties. The data protection framework worldwide is changing at a rapid pace and to ensure legal and technical appropriate measures are in place, GARDP Members shall keep contractual arrangements reviewed and up to date.

11. Transfer of data outside the territory of the data subjects

Understanding how data flows across information systems, between GARDP's offices, between GARDP and its collaborators or services providers is important. The personal data might not be under the same data protection legislation when it flows to a country different from the country where it has been originally collected or from the country where the data subjects are located to another country (a third country). Additionally, the information being transferred must be evaluated both in transit (which tool / interface is used for the transfer) and at rest (the systems receiving the information are secure) with the data recipient in terms of information security. GARDP Members shall ensure that personal data is not transferred without the appropriate advice and contract. Specific legal conditions must be fulfilled to ensure that a transfer is legitimate. GARDP Members should contact the DPO or the legal department to ensure appropriate safeguards are in place when personal data is transferred to a third country.

12. Data protection incidents and breaches

Handling personal data contains risks. Incidents and data protection breaches can happen. GARDP Members shall be aware of what a personal data breach is, avoid them by following this policy and if it occurs, know how to report them.

There are three types of personal data incidents and breaches:

- An unauthorised disclosure of personal data (loss of confidentiality)
- An unauthorised modification of personal data (loss of integrity)
- The personal data is not available or has disappeared (loss of availability)

As a GARDP Member, if you discover a data protection breach or an incident that may represent a risk for the protection of personal data, you must immediately contact the legal department, IST and the DPO. If the breach is serious, we have a legal obligation to report it within 72 hours of becoming aware of it. This will require GARDP to assess the possible reputational damage, take remediation actions to mitigate the impact of the data breach and to inform its Board of Directors of the data breach and actions taken.

More details about personal data breaches can be found in the GARDP data protection procedure "Managing Personal Data Breaches" and the dedicated SharePoint site for the Legal team.
https://dndi.sharepoint.com/sites/GARDPLegalPublic

13. Personal data protection policy monitoring

The Data Protection Steering Group shall perform oversight of the compliance of GARDP with personal data protection laws, identify gaps and risks and report them where needed to GARDP Management Board.
Oversight may take place through internal auditing of personal data processing operations, review of training records, review of accesses granted to personal data or any other, setup and monitoring of key data protection indicators, or any other appropriate means.

This policy, its objectives and effectiveness are reviewed by GARDP Management Team regularly, based on a report and recommendations made by the Data Protection Steering Group. Improvements and updates will be made, and a new version of the policy will be published as needed.

Who to contact

For any questions regarding this policy, please contact GARDP's DPO at dataprivacy@gardp.org.

ANNEXE I

Glossary

Personal data means any information relating to a natural person (**data subject**), whether it relates to his or her private, professional, or public life. This data can be for example a name, photo, email address, bank details, medical information, IP address, social networks sites posts or a combination of the data that directly or indirectly identifies the person. Personal data includes pseudonymized data which can be attributed to a data subject by the use of additional information (e.g. a code attributed to the data subject and kept in a correspondence table); but excludes anonymous data or personal data rendered anonymous in such a manner that it can be demonstrated in a documented manner that the data subject is not or no longer identifiable.

Special categories data is personal data that is **sensitive** and if lost, corrupted, stolen would have a high detrimental impact on the individual concerned. These categories of data require extra safeguards. They are data relating to race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data (either physical or mental health), sex life or sexual orientation, social security number, administrative or criminal proceedings and sanctions.

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

Data subject means 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.

Data subject request means a request made by a data subject to exercise its rights under the applicable data protection law, e.g. right to be informed about the processing of its personal data, right to have its personal data be rectified, right to have its personal data be erase, right to lodge a complaint to GARDP or to a competent data protection authority.

GARDP Member means employees, support staff, volunteers, interns, apprentices and trainees, agency staff employed by GARDP, consultants or contractors, staff seconded to GARDP from other organizations, and GARDP's Board, Audit Committee, Scientific Advisory Committee or any other Committee members (GARDP Member is further defined in the Code of Ethics)

Personal data breach means 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.

Data controller means the natural or legal person who determines the purposes and means of processing personal data.

Data processor means the natural or legal person who is responsible for processing personal data on behalf of a data controller.

Data protection officer (DPO) have at least the following tasks: (a) to inform and advise GARDP management and staff who carry out processing of personal data on their obligations pursuant to applicable data protection laws, regulations and guidelines (the data protection framework); (b) to monitor compliance with this policy and to the data protection framework, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance; (d) to cooperate with the concerned data protection authorities; (e) to act as the contact point for the concerned data protection authorities on issues relating to processing and to consult them, where appropriate, with regard to any other matter.

Competent data protection authority means an independent public authority which is established by a state pursuant to its law, and which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the state of that data protection authority; (b) data subjects residing in the state of that data protection authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that data protection authority.