Cordaid Data Protection Policy

Date: 25-5-2018
Version: 2.0
Document owner: Simone van Hamond

Contents

Cordaid DATA PROTECTION STANDARD

Article 1: Purpose

European data protection legislation demands that Personal Data is processed lawfully, fairly and in a transparent manner. The purpose of this policy is to give practical effect to the provisions of Data Protection legislation as determined by the General Data Protection Regulation (GDPR), according to the guidelines of the European Union.

This document will be revised twice a year as execution of the GDPR law involves continuous learning about data processing within Cordaid.

Article 2: Definitions

The law	:	the General Data Protection Regulation (GDPR);
The Standards	:	these standards, including annexes;
Controller(s)	:	Stichting Cordaid (including Country Offices) Stichting Cordaid Expats Stichting Cordaid Patricipaties CIM B.V., having their registered offices at Lutherse Burgwal 10 The Hague; Cordaid affiliates worldwide
Data Subject	:	all natural persons of whom Cordaid processes Personal Data, including institutional and B2C donors, volunteers, employees, beneficiaries, investors/investees, ambassadors and other relations;
Employee	:	natural person employed Cordaid;
Personal Data	:	any information relating to an identified or identifiable natural person, 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;
Processing	:	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;
Database/ filing system	:	any structured set of Personal Data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
Processor	**:**	a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller;
Administrator	**:**	individual who under the responsibility of the Controller manages the processing of Personal Data on a day to day basis, for the accuracy of such data, as well as for the retention, removal and disclosure of such data as defined in Article 4;
User	**:**	individual authorized by the Administrators to read, enter, modify and / or remove Personal Data, or to take notice of report on any processing of Personal Data;

GDPR Working group	:	organized group of primary data owners at Cordaid who are responsible for the implementation and control of this GDPR Standards. This group meets twice a year or when there is a major data incident. The group exists of Directors of PF&C, HR, ICT and CIM and facilitated by the Quality Assurance officer and Advised by the External DPO;
DPO	:	Data processing officer who consults the working group on legislation and implementation and data breach notifications;
Maintenance	:	activities relating to ICT maintenance and repair;
Disclosure	:	making Personal Data known and/or available to third parties and or Data Processors.

Article 3: Scope

These Standards apply to (automated) processing of Personal Data by Cordaid, constituting of the following legal entities.

1. Stichting Cordaid;
2. Stichting Cordaid Expats;
3. Stichting Cordaid Participaties, and
4. Cordaid Investment Management (CIM) B.V.

<u>hereafter referred to as **"Cordaid" or "Controller".**</u>

For the purpose of these Standards we maintain an alternative structure. As we document the processing of personal data within Cordaid per business process a.k.a. functional domain. Within Cordaid we identify the following domains:

1. Projects;
2. Fundraising;
3. HR;
4. IT;
5. Finance, and
6. Investment management (CIM) B.V.

These domains correspond with the Cordaid organizational structure as illustrated in **Figure 1**.

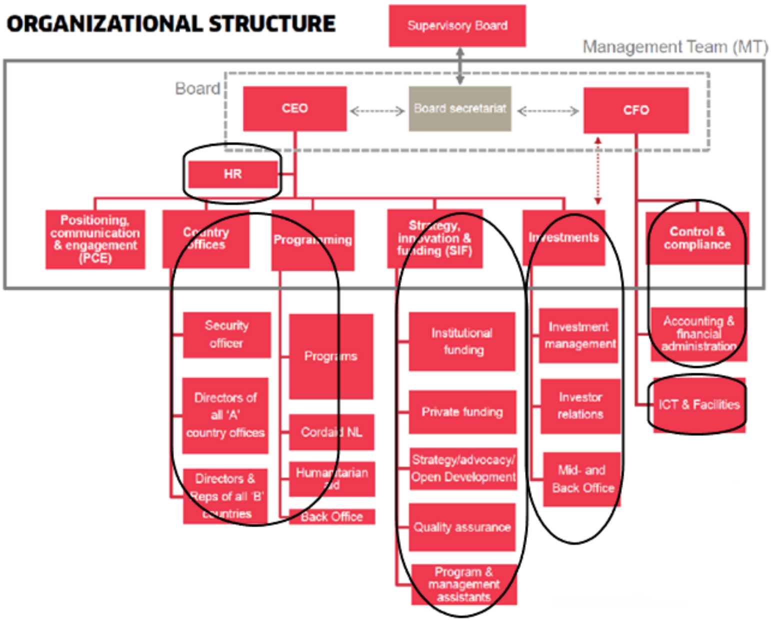

Figure 1: Cordaid organizational structure

Article 4: Data management

The Controller has appointed Administrators for the Processing of Personal Data per functional domain.

Within Cordaid there is a Data Protection Working Group. This team assesses the implementation and effects of this Standard within the organization and includes the appointed Administrators. The project team reports to Board of Directors and includes representation for Cordaid globally

The Data Protection Working Group has the responsibility to:

- Meet on a quarterly basis, with reporting of compliance results to the Board of Directors annually
- Inform itself of changes in law and regulation;
- Assess whether Cordaid Data Processing activities are conducted in accordance with the Law and these Standards;
- Ensure compliance and privacy awareness training of Employees;
- Verify and assess if data processing are compliant to the law and these Standards;
- Manage the register of data processing;
- Advise the internal organization on compliance issues;
- Compile and execute these Standard in a Plan-Do-Check-Act cycle;
- Consult with Cordaid's external stakeholders on privacy compliance issues;
- Report compliance results to the board;
- Consult with internal departments on a regular basis to discuss compliance of the technical, data and back-office business processes.

Article 5: Legitimate grounds for data processing

Personal Data is processed by Cordaid only if one of the following conditions is met:

- The Data Subject has given unambiguous consent, for example for sending unsolicited e-mail;
- The processing is necessary for the performance of a contract/ donation to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into this contract, for example when a Data Subject becomes a donor, registers as a volunteer, becomes an employee, beneficiary or investor, or participates in another activity initiated by Controller;
- The processing is necessary for compliance with a legal obligation to which the Controller is subject; for example, data retention for tax authorities or due diligence investigations into beneficiary Ultimate Beneficial Owners (UBO) required under Anti-Money Laundering and Anti-Terrorist Financing Act;
- The processing is necessary for the purposes of the legitimate interests pursued by the Controller, for example to provide the Data Subject with personalized information or fundraising requests.

The specified purposes for Cordaid Data Processing are stated in Article 7.

Article 6: Data Quality and proportionality of processing

The processing of Personal Data shall be:

- Non-excessive;
- Relevant;
- Limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’), and
- Accurate and up-to-date.

Articles 7, 8 and 9 explain how Cordaid implements these requirements in business processes.

Article 7: Purposes for data processing (purpose specification and use limitation principle)

Personal Data can only be processed for specified, explicit and legitimate purposes and not will not be processed further in a manner that is incompatible with those purposes. Cordaid has specified it’s purposes for data processing per functional domain.

a. Projects

Personal Data of B2B contacts from institutional donors, governments, beneficiaries, Subcontractors and independent Consultants and Consultant Companies and Suppliers and Cordaid project managers.

The purposes of data processing to which this Standard applies are:

- The performance of a contract with an institutional investor or beneficiaries or processing in order to take steps at the request of the investor and or beneficiary prior to entering into a contract;
- Client research/ customer due diligence among other identifying the UBO as required by Anti-Money Laundering and Anti-Terrorist Financing Act;
- Program management;
- Reporting in order to meet requirements of transparency and social responsibility;
- Accounting for the expenditure of subsidies, grants and other third-party cash flows;
- Institutional donor account management;
- Beneficiary account management;
- Enabling Visa applications for foreign visitors;
- (Financial) auditing and quality assurance.

b. Fundraising

(Potential) B2C donor, participant and lead, executors, notaries and fellow heirs, legatees, suppliers Personal Data.

The purposes of data processing to which this Standard applies are:

- performance of a donor, membership and/or purchase/ legacy or other agreement in which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Fundraising and marketing activities;
- Electronic communications such as e-mail newsletters, service mail and other (unsolicited) electronic messages;
- Analysis of use of services, including the website;
- Registering and analyzing non-sales;
- Customer care, including answering questions and compliant handling;
- Prevention and detection of fraud, and
- Quality monitoring and compliance and financial auditing.

c. HR

(Former) employee and applicant, suppliers, independent consultants Personal Data.
The purposes of data processing to which this Standard applies are:

- The implementation of staff management policy;
- Quality control(s);
- Recruitment;
- Onboarding, internal mobility and exit management;
- Employee payroll, compensations and benefits;
- Employee learning and development;
- Occupational health and safety;
- Taxes;
- Accountability for social security provisions such as health insurance, travel insurance, incident management; employee insurance agencies, executive agencies, and
- (Financial) auditing.

d. IT

The purposes of data processing to which this Standard applies are:

- General system administration and (IT) workplace management; issuing company equipment, authorizations and rights to Cordaid employees
- Maintaining licenses;
- Account and access management, and
- Quality and compliance control(s).

e. Finance

The purposes of data processing to which this Standard applies are:

- General accounting including maintaining and providing records of accounts receivable and payable, creditor and debtor overviews and general financial reporting;
- Billing;
- Employee time writing for third party donor and grant accountability on projects;
- Salary payments, and
- Financial Auditing.

f. Investments

The purposes of data processing to which this Standard applies are:

- the performance of a contract with an institutional investor or investee in order to take steps at the request of the investor and or investee prior to entering into a contract;
- client research/ customer due diligence among other identifying the UBO as required by Anti-Money Laundering and Anti-Terrorist Financing Act;
- Investment management;
- Reporting in order to meet requirements of financial law and other regulations regarding transparency and social responsibility;
- Accounting for investor expenditure;
- Investor account management;
- Investee account management, and
- (Financial) auditing and quality assurance.

Cordaid will not process Personal Data for other purposes than mentioned above.

Article 8: (Categories of) Personal Data (collection limitation principle)

a. Cordaid collects the following categories of personal data:

Projects: Personal Data of B2B contacts from institutional donors, governments, subcontractors, individual consultants and consultant companies, suppliers, beneficiaries and Cordaid project managers

- Organization information, including information from external sources such as Chamber of Commerce information/ third party information regarding turnover, management stock holders, loans etc.;
- B2B contact details;
- Beneficiary UBO (Ultimate Beneficial Owner);
- Information regarding funds, grants, subsidies and Institutional donors;
- Project information;
- Information regarding investment application, allocation and spending, and
- declarations/compensations/ advances, financial data, travel expenses.

Fundraising: (Potential) B2C donor, participant and lead, executor, notaries, fellow heirs, legatees Personal Data

- Personal details / contact data;
- Financial and administrative data;
- Donation order and contact history, participation data, complaints, questions and comments;
- Lifestyle characteristics / demographic and sociographic characteristics, and
- Data relating to the use of our electronic services such as the website (s).

HR: (Former) employee and applicant personal data

- Personal details / contact data;
- Job title;
- Work and education history;
- Financial and administrative data;
- Resumé;
- Social security number;
- Data constituting a personnel file: among other appraisals; learning budget; qualifications;
- Salary details, and
- Employment contracts.

IT: Employee personal data

- Personal details / contact data;
- Job title, function and department, and
- Authorizations and access rights.

b. Cordaid does not process special categories of data about its donors without prior explicit consent. This data can be processed by Cordaid for purposes of legacies. Such data will never be used for profiling and fund raising purposes.

c. Cordaid does not process Personal Data of Children (individuals under the age of sixteen) without the prior consent or authorization by the holder of parental responsibility over the child.

d. Personal Data will be collected directly from the Data Subject when possible.

e. When Personal Data is collected by a third party (lead generation or affiliate marketing), for fundraising purposes the Data Subject has to give his unambiguous consent.

f. Personal Data will be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

Article 9: Record of Processing Activities and Data Privacy Impact Assessment

Cordaid has a general overview of data applications used for all data processing. The **Data Application Overview** (**Annex 1)**. Furthermore, Cordaid keeps a record of processing activities as required in Article 30 GDPR, which can be found in the **Cordaid Record of Processing Activities (Annex 2)**. The record of processing activities also states and qualifies the existing information and privacy control measures, therefore also meeting the requirements of a Data Privacy Impact Assessment (DPIA) as required in Article 35 GDPR.

Article 10: Information requirements (transparency principle)

Information regarding Data Processing by Cordaid shall be provided to the Data Subject (consumers private donors, employees, institutional donors and other third parties) in a concise, transparent, intelligible and easily accessible form, using clear and plain language

B2C donors, leads, participants and other relations

- When entering into a contract with Cordaid (donor agreement), donors, participants and other relations are informed of the purposes of data collection by means of a Privacy Disclaimer, which will be an integral part of all online and offline registration forms:
- Cordaid has a **privacy statement** explaining in detail how Cordaid processes consumer personal data that will be easily accessible online at all Cordaid web domains **(Annex 3)**
- When there's an existing relationship with a donor and contact data is obtained the context of a donation Cordaid uses contact details for direct marketing and fundraising. In that case donors can "opt-out" from the use of their e-mail address.
- For non-donors and Cordaid will ask permission to send unsolicited communications via e-mail

Employees

- Personal data of applicants are processed to assess:
  a) whether an applicant is suitable for a position, and
  b) for the settlement of any costs.

  The Personal Data will be deleted if the applicant requests it and, in any case, no later than 4 weeks after the application procedure has ended.
- Upon commencement of employment, the Employee will be informed about the processing of his data for the purposes stated in Article 7. The Employee is informed about this Privacy Policy and can request a copy.

Institutional donors and third parties

- In case of data exchange between Cordaid and institutional donors for the purpose of reporting and (financial) accountability such exchanges will be governed by a written agreement;
- Data of third parties, such as suppliers or institutional donors processed by Cordaid will be governed by this Standard. Where relevant, parties are informed about this Privacy Policy and can request a copy.

Article 11: Direct Access to Personal Data

- Only the administrator and designated users have direct access to Personal Data for the purpose of ensuring a correct processing of Personal Data for the specified purposes. Access right management is centrally managed and periodically checked by the GDPR working group. Outcomes are reported to the Administrator. This will be a recurring agenda item in the GDPR workgroup meeting
- The individuals referred to in the first paragraph must treat Personal Data confidential, therefore all Cordaid Employees sign a **Cordaid Employee Confidentiality Agreement (Annex 4).**

Article 12: Data disclosure

Without prior consent of the Data Subject, Personal Data can only be disclosed to Data Processors and third parties with a signed Data Processing Agreement (DPA) that are directly involved in Cordaid's current activities and services.

Anonymous data

When Personal Data is anonymized in a way that they cannot be directly or indirectly linked to the Data Subject, the anonymized data can be disclosed by Cordaid when the purpose of the disclosure is compatible to the original purpose of processing.

No third party data disclosure for commercial purposes

Cordaid does not disclose Personal Data to a third party unless the data is anonymized or the disclosure is necessary to comply with a legal requirement to which Cordaid is subject or when requested by Public authorities based on a legal claim.

Article 13: Transfers of Personal Data to countries outside the EU.

Cordaid will not transfer Personal Data to a company or processor in a country outside the EU (I.E. international and local partner organizations or institutional donors) that does not have a GDPR policy or signed DPA;

Article 14: Data Subject's Right of access

The Data Subject or his legal representative has the right to obtain from Cordaid confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case a transcript of that Personal Data. The Data Subject will receive an written overview of his Personal Data, This transcript will be provided as soon as possible, but no later than four (4) weeks after the request has been made.

Article 15: Data Subject's Right to rectification, restriction of processing and deletion of Personal Data (Right to be Forgotten)

- The Data Subject may submit a written request to rectify, complete or delete his data or to restrict data processing by Cordaid.
- Cordaid will inform the Data Subject within four (4) weeks in writing whether and to what extent it shall honor the request made. When a request is (partially) refused Cordaid will demonstrate the compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for Cordaid to exercise or defense of legal claim.

Article 16: Data Subject's Right to Object to processing for fundraising and direct marketing

- When a Data Subject objects to the processing of his data for fundraising or direct marketing purposes Cordaid will honor this request as soon as possible, but at least within four (4) weeks, by registering the Data Subject on an internal suppression file.

Article 17: Verification in exercising Data Subject's rights

- Before submitting the Data Subject's request Cordaid may ask a Data Subject to verify his or her identity by asking for initials, surname and email address.
- In order to verify the Data Subjects identity Cordaid customer service will use the **Cordaid Verification Matrix for Data Subject Requests (NL) (Annex 5).**

Article 18: Information security

IT security, Authorizations and access rights

Cordaid has an Information Security policy, this policy can be found on the Cordaid Intranet. This policy is meant for physical and digital information, however mostly written with digital information in mind. Also applying is the Cordaid password policy, this one can also be found on the Cordaid Intranet.

Back-up

The below paragraph is a summary of the backup policy of Cordaid that can be found on the Cordaid intranet. The purpose of backing up data is to protect data in the organization to be sure it is not lost. Information can be recovered in the event of an equipment failure, destruction of data, or disaster. This backup policy applies to all equipment and data owned and operated by Cordaid Global Office and Country Offices. Backup time and backup tools can deviate in different offices, but a weekly full backup is mandatory.

Definitions used

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

- Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
- Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

Backup policy

Full backups are performed weekly on Friday 22:00. On Monday, Tuesday, Wednesday, Thursday, differential backups are made.

- Tapes that are not in the tape library are kept in a safe at Cordaid HQ.
- The tape drives are cleaned automatically.
- The Manager IT Global Office has delegated a member of the department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.
- The ability to restore data from backups shall be tested at least once per six (6) months.
- Users that need files restored must submit a request with the Self ServiceDesk tool and include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

Article 19: Data retention

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. Hereafter, Cordaid will delete or anonymize Personal Data. Cordaid has issued a standard for data retention periods within the organization: the **Cordaid Rationale for Data Retention (Annex 6).** Specific data retention periods per (sub) processing are also defined in the **Cordaid record of data processings (Annex 1 and 2).**

Article 20: Data breach notification

In the case of a Personal Data breach, Cordaid shall without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of it, notify the Personal Data breach to the supervisory authority, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of Data Subjects. When the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the Personal Data breach to the Data Subject without undue delay.

Cordaid has a **breach notification procedure (Annex 7)** and entails:

a. An instruction for Employees;
b. An instruction for Data Processors;
c. Requirements regarding the notification of a data breach by the Data Processor recorded in Data Processor Agreements;
d. An assessment of each security incident by the Manager marketing and fundraising;
e. A record of each security incident in an incident register.

Article 21: Internal controls

The GDPR working group and the board are responsible for the implementation of these data protection standards.

- **Plan:** The principles for the fair and lawful processing of Personal Data defined in these Standards;
- **Do:** The implementation of data privacy and information security measures described in these Standards;
- **Check:** Conducting compliance checks internally and externally as described in this article;
- **Act:** Analysis of non-compliance and adjustment of the process.

Audits

The GDPR working group will periodically check data protection policies, work instructions and information security measures. They will do so by evaluating the record of data processings with the business process owners and by evaluating the quality of the information security and privacy measures. If compliance with data protection standards is seriously insufficient, Cordaid may impose a sanction on the responsible Employees within the framework of the agreed terms of employment and legal possibilities. Processing Personal Data is a continuous process. Technological and organizational developments inside and outside Cordaid make it necessary to periodically see if one is still on track with these Standards.

Article 22: Responsibilities of the Data Processor

Cordaid obliges Data Processor to comply with these Standards. The obligation is for processors to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of legislation and these Standards will be governed by the **Cordaid Data Processor Agreement (Annex 8).**

Article 23: Awareness and training

Policies and measures are not sufficient to exclude risks in the field of data processing. It is necessary to continually raise awareness at Cordaid, making Employees aware of risks and encouraging (safe and responsible) behavior. The Cordaid e-learning platform will be used for training and awareness and is the responsibility of the Board of Directors.

Article 24: Complaints

If an Employee or Data Subject believes that data protection legislation or these Standards are not respected by Cordaid a complaint can be issued to the Cordaid customer service or directly to one of the Administrators.

Article 25: Documentation

These Standards refer to documentation in which Cordaid further describes the implemented data protection and information security measures to ensure that the processing of Personal Data takes place fairly and lawfully. This documentation is added as an Annex to these Standards or is available for inspection with the Administrators. This Article provides a summary of the available documentation:

1. **Cordaid Data Application Overview (Annex 1)**
2. **Cordaid Record of Processing Activities (Annex 2)**
3. **Cordaid Privacy Statement (Annex 3)**
4. **Cordaid Employee Confidentiality Agreement (Annex 4)**
5. **Cordaid Verification Matrix for Data Subject Requests (NL) (Annex 5)**
6. **Cordaid Rationale for Data Retention (Annex 6)**
7. **Cordaid Data Breach Notification Protocol (Annex 7)**
8. **Cordaid Data Processor Agreement (Annex 8)**
9. **Cordaid Compliance Plan (NL) (Annex 9)**

Article 26: Availability

These Standards are effective of 25-05-2018 and are available on the Cordaid Intranet.