

CORDAID DATA PROTECTION POLICY

This Policy is for general information purposes only and expert advice should be obtained before acting on the basis on any part of the information provided in this report. The authors do not provide any warranty, nor explicit or implicit, with regard to the correctness or completeness of the information contained in the report and assume no responsibility whatsoever for any errors or omissions contained in the report and shall not be liable in respect of any loss, damages or expenses of whatsoever nature which is caused by any use the reader may choose to make of this information.

Neither this report nor any part of it may be copied or disclosed to any third party or otherwise quoted or referred to, without the prior written consent of Cordaid.

Contents

1 INTRODUCTION.....	3
Purpose, Scope and Adherence monitoring.....	3
Internal controls.....	5
Compliance checks.....	5
Definitions.....	6
2. POLICY STATEMENTS - WHY DO WE OPERATE THE WAY WE DO?	8
Processing purposes	8
Categories of Personal data collected by Cordaid.....	11
Other policy statements related to Data Processing.....	12
3. DESCRIPTION OF ACTIVITIES - WHAT DO WE DO AND HOW?	14
Records of Processing Activities and Data Processing Impact Assessment.....	14
Information requirements (transparency principle).....	14
Direct Access to Personal Data.....	15
Data disclosure.....	15
Transfers of Personal Data to countries outside the EU	15
Data Subject’s Right of access	16
Data Subject’s Right to rectification, data portability, restriction of processing and deletion of Personal Data (Right to be Forgotten).....	16
Data Subject’s Right to Object to processing for fundraising and direct marketing.....	16
Verification in exercising Data Subject’s rights	16
Information security	16
Data retention.....	17
Data breach notification.....	17
Responsibilities of the Data Processor	17
Awareness and training.....	17
Complaints.....	18
Documentation.....	18
Approval and validity.....	18

1. INTRODUCTION

Purpose, Scope and Adherence monitoring

<p>Purpose:</p>	<p>This Policy describes Cordaid positions that data collection shall not violate any privacy, human rights, or individual and or public freedom. This Data Protection Policy strives to guarantee an adequate level of data protection as implemented by current European Data Protection legal frameworks. Cordaid is committed that Personal Data is processed lawfully, fairly, and in a transparent manner. Therefore, 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 evaluated twice a year as the execution of the GDPR law involves continuous learning about data processing within Cordaid.</p>
<p>Scope:</p>	<p>This Policy applies to (automated) processing of Personal Data by Cordaid and its affiliates worldwide, including:</p> <ul style="list-style-type: none"> ■ Stichting Cordaid Expats, ■ Cordaid Investment Management (CIM) B.V. ■ ICCO Group BV ■ Stichting ICCO ■ Fair Climate Fund BV <p>The following entities are in liquidation; however, the processing of personal data has not (completely) ended:</p> <ul style="list-style-type: none"> ■ Stichting Cordaid Participaties [in liquidation], ■ Corpav BV [in liquidation] ■ Fair&Sustainable Participações en Empreendimentos Sustentaveis do Brasil [in liquidation] <p>This Policy will be updated when these entities have stopped the processing of personal data.</p> <p>For the sake of readability Hereinafter referred to: 'Cordaid' or 'Controller' and as such includes all affiliates/ entities as stated above.</p> <p>For the purpose of this Policy, 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:</p> <p>a. Projects;</p>

	<ul style="list-style-type: none"> b. Fundraising; c. HR; d. IT; e. Legal; f. Procurement; g. Finance; h. Positioning & Communication i. Visitor registration to the offices
<p>Scope for local adaptations</p>	<p>This Policy is based on working in compliance with GDPR requirements, which is a requirement for the entire Cordaid organisation, including Country Offices. As Country offices are also bound by local law and regulations, Country Offices may draft an attachment with local adaptations. This attachment must be approved by the Owner of this Data Protection policy mentioned above.</p>
<p>Adherence Monitoring:</p>	<p>Adherence to this Policy will be monitored by the Data Protection Working Group. Monitoring will take place ongoing.</p> <p>The Controller has appointed Administrators for the Processing of Personal Data per functional domain.</p> <p>Within Cordaid, there is a Data Protection Working Group. This team assesses the implementation and effects of this Policy within the organisation and includes the appointed Administrators. The Data Protection Working Group reports to the Board of Directors (BoD) and includes representation for Cordaid globally.</p> <p>The Data Protection Working Group has the responsibility to:</p> <ul style="list-style-type: none"> ■ Meet on a monthly 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 this Policy; ■ Ensure compliance and privacy awareness training of Personnel; ■ Verify and assess if data processing is compliant with the Law and this Policy; ■ Manage the register of data processing; ■ Advise the internal organisation on GDPR questions and issues; ■ Compile and execute this Policy in a Plan-Do-Check-Act cycle; ■ Consult with Cordaid's external stakeholders on privacy compliance issues; ■ Consult with internal departments on a regular basis to discuss compliance with the technical, data, and back-office business processes.

Internal controls

The Data Protection Working Group and the board are responsible for the implementation of this Data Protection Policy.

Plan: The principles for the fair and lawful processing of Personal Data defined in this Policy;

Do: The implementation of data privacy and information security measures described in this Policy;

Check: Conducting compliance checks internally and externally as described;

Act: Analysis of non-compliance and adjustment of the process.

Compliance checks

The Data Protection Working Group will periodically check data protection policies, work instructions, and information security measures. They will do so by evaluating the record of data processing activities with the business process owners and by evaluating the quality of the information security and privacy measures. If compliance with data protection policy is seriously insufficient, Cordaid may impose a sanction on the responsible Personnel within the framework of the agreed terms of employment and legal possibilities. Processing Personal Data is a continuous process. Technological and organisational developments inside and outside Cordaid make it necessary to periodically see if one is still on track with this Policy.

Definitions

The Law	the General Data Protection Regulation (GDPR); European legislation on data protection that applies to Cordaids data processing. An overview of GDPR and other applicable legislation can be found in Annex 1 .
This Policy	This data protection policy including annexes;
B2C	Business to Consumer
B2B	Business to Business
Controller(s)	Stichting Cordaid including Cordaid affiliates worldwide (which fall under the governance & control of Cordaid) such as described in 'Scope'.
Data Subject	all natural persons of whom Cordaid processes Personal Data, including institutional and B2C donors, volunteers, employees, external consultants, beneficiaries, investors/investees, ambassadors, implementing partners, suppliers, stakeholders and other relations;
Personnel	Controller's staff, volunteers and interns
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, religious, physiological, genetic, mental, economic, cultural, or social identity of that natural person;
Processing	any operation or set of operations that is performed on personal data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Database/ filing system	any structured set of Personal Data that 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	an 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;
User	an 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;

Data Protection Working Group	an organized group of primary data owners at Cordaid who are responsible for the implementation and control of this data protection policy. This group meets every month or when there is a significant data incident. The group exists of staff of representatives of different departments and facilitated by the Senior Manager Compliance & QMS and is 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.

2. POLICY STATEMENTS - WHY DO WE OPERATE THE WAY WE DO?

Processing purposes

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

Projects

Personal Data is being processed of B2B contacts from institutional donors, governments, beneficiaries, subcontractors, independent consultants, consultant companies and suppliers, and Cordaid project managers.

The purposes of data processing to which this Policy 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 others identifying the UBO as required by Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft);
- 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.

Fundraising

Personal Data is being processed of (Potential) B2C donors, participants, leads, executors, notaries, and fellow heirs, legatees, and suppliers.

The purposes of data processing to which this Policy 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 the use of services, including the website;

- Registering and analyzing non-sales;
- Customer care, including answering questions and complaint handling;
- Prevention and detection of fraud, and
- Quality monitoring and compliance and financial auditing.

HR

Personal Data is being processed of (former) employees and applicants, suppliers, independent consultants Personal Data.

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

- The implementation of staff management policy;
- Quality control(s);
- Recruitment;
- Onboarding, internal mobility, and exit management;
- Personnel payroll, compensations, and benefits;
- Personnel 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;
- Contractual obligations with institutional donors: International institutional donors may ask for personal data in case of (integrity) breaches based on contractual obligations. This is more thoroughly described in HR policies In case local (labour) law offers a higher standard of data protection than the GDPR, local law prevails.

IT

Personal Data is being processed of employees, guests on the Wifi, and contact details of IT suppliers.

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

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

Legal

Personal Data is being processed of contract partners, employees, donors, and other persons related to Cordaid.

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

- Closing and storing agreements such as consultancy and service agreements
- Closing and storing power of attorneys
- Having a contract administration
- Handling claims and judicial disputes
- Supporting the Boards and Supervisory Boards and directors with the (organisation and decision-making of) the governance of Cordaid including registration with government- authorities and chamber of commerce

Procurement

Personal Data is being processed of contract partners, employees, suppliers, and other persons related to Cordaid's procurement process.

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

- Maintaining an up-to-date contract administration including contact details of contact persons
- Closing and storing agreements with suppliers

Finance

Personal Data is being processed of contract partners, employees, debtors, other persons related to Cordaid's finance process.

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

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

Positioning & Communication

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

- Research
- Control
- Communication

Visitor registration

Personal Data is being processed of visitors to Cordaid's offices.

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

- Safety
- Comply with regulations.

Cordaid will not process Personal Data for purposes other than those mentioned above. The exact processing may vary per legal entity/ per country, also depending on local legal regulations and requirements.

Categories of Personal data collected by Cordaid

1. 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

- Organisation information, including information from external sources such as Chamber of Commerce information/ third party information regarding turnover, management stockholders, 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 donors, participants, and leads, executors, 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;
- Working hours;
- Holiday leave, sick leave, pregnancy leave;
- Bank account number;
- Proof of Life questions and answers (for travelling employees and local country office employees)
- ICE contact details of related persons;
- Resumé;

- Copy of ID document;
- Work and residence permit;
- Social security number;
- Data constituting a personnel file: among other appraisals; learning budget; qualifications;
- Salary details, and
- Employment contracts.

IT: Personnel personal data

- Personal details / contact data;
- Job title, function, department, and
- Authorisations and access rights.
- Location data and IP numbers

Finance

- Name, address, contact details, social security number of personnel for salary payments
- Contact details of other parties and external consultants

Legal

- Personal data in contracts; name, job title, signature
- Personal data in legal files or concerning claims or disputes
- Personal data in Power of Attorney; name, contact detail, birth date and passport information
- Personal data in registration of Cordaid and its board members and directors with authorities of all kinds (government-agencies, chamber of commerce, ministries, EU etc.), such as for example but not limited to: Copy of passport, names of relatives, previous home addresses, CVs
- Information asked for on UBO-forms (different formats per bank); they usually include names

Procurement

- Personal data in contracts; name, job title, signature
- Contact data of relations: name, (company) email address, or phone number

Visitor registration

- Name, date and time of entry and departure
- Company name
- Purpose of visit
- Person to visit

Other policy statements related to Data Processing

2. Cordaid does not process special categories of data about its donors without prior explicit consent as GDPR requires. Instead, this data can be processed by Cordaid for the purpose of legacies. Such data will never be used for profiling and fundraising purposes.
3. 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.
4. Personal Data will be collected directly from the Data Subject when possible.

5. 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.
6. Personal Data will be processed lawfully, fairly, and in a transparent manner in relation to the Data Subject.

3. DESCRIPTION OF ACTIVITIES – WHAT DO WE DO AND HOW?

Records of Processing Activities and Data Processing Impact Assessment

As the GDPR requires (Art. 30 GDPR) Cordaid keeps a record of processing activities which can be found in the Cordaid Record of Processing Activities (Annex 2).

Information requirements (transparency principle)

Information regarding Data Processing by Cordaid shall be provided to the Data Subject (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 an extended privacy statement and a short privacy information notice and which will be an integral part of all online and offline registration forms.

Cordaid has a privacy statement, explaining in detail how Cordaid processes 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 within the context of a donation Cordaid uses contact details for direct marketing and fundraising. In that case, donors can "opt-out" by using their e-mail address or telephone number.
- For non-donors and Cordaid will ask permission to send unsolicited communications via e-mail and telemarketing.

Personnel and applicants

- 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.

Personal Data will be deleted if the applicant requests it and, in any case, no later than 1 year after the application procedure has ended, unless the applicant has specified that he/she wants his/ her data to be removed after four weeks. The applicant is informed by the privacy statement on the website and with a short information notice on the online application page.

- Upon commencement of employment, the Personnel will be informed about the processing of his data for the purposes. The Personnel is informed about the purposes of personal data processing through the Legal Status Regulation (LSR). And can request a copy of this Data Protection Policy.

Institutional donors and third parties

- In case of data exchange between Cordaid and institutional donors for the purpose of reporting and (financial) accountability, such interactions 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 Policy. Where relevant, parties are informed about this Data Protection Policy and can request a copy.

Direct Access to Personal Data

- Only the administrator and designated users have direct access to Personal Data ensuring the correct processing of Personal Data for the specified purposes. Access right management is centrally managed and periodically checked by the Data Protection Working Group. Outcomes are reported to the Administrator. This will be a recurring agenda item in the Data Protection Working Group meeting.
- The individuals referred to in the first paragraph must treat Personal Data as confidential; therefore, all Cordaid Personnel sign a Cordaid Code of Conduct (Annex 4).

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 is directly involved in Cordaid's current activities and services. The template DPA can be found in Annex 8.

Anonymous data

When Personal Data is anonymized in a way that it 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 with 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.

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 organisations or institutional donors) that does not offer an adequate level of data protection. Standard contractual clauses (SCC) or Binding Corporate Rules (BCR's) need to be in place.

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 is being processed and, where that is the case, a transcript of that Personal Data. The Data Subject will receive a 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. Data subjects are informed about their rights through different privacy statements.

Data Subject's Right to rectification, data portability, 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 defend of a legal claim.

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.

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. Depending on the type of data subject and the confidentiality of the personal data involved, this may include name, birth date, ZIP code, and a copy of a passport (for example when a former employee request access).
- In order to verify the Data Subjects identity, Cordaid customer service will use the Cordaid Verification Matrix for Data Subject Requests (NL) (Annex 5).

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, primarily written with digital information in mind. Also applying is the Cordaid password policy, this one can also be found on the Cordaid Intranet.

Backup policy

The purpose of backing up data is to protect data in the organisation to be sure it is not lost. Information can be recovered in the event of an equipment failure, destruction of data, or disaster. Cordaid has a backup policy in place to assure business continuity and prevent the loss of data. Like many organisations, Cordaid has moved from physical servers to a cloud server. This has resulted in a

new back-up policy which is currently being revised and updated. The latest version of the backup policy is available at the IT department.

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 is processed. Hereafter, Cordaid will delete or anonymize Personal Data. In addition, Cordaid has issued a Policy for data retention periods within the organisation; the Cordaid Rationale for Data Retention (Annex 6). Specific data retention periods per (sub) processing are also defined in the Cordaid record of processing activities (Annex 2).

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 Personnel;
- 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 Senior Manager Compliance & QMS, and ICT manager;
- e. A record of each security incident in an incident register.

Responsibilities of the Data Processor

Cordaid obliges Data Processor to comply with this Policy. The obligation is for processors to provide sufficient guarantees to implement appropriate technical and organisational measures so that processing will meet the requirements of the legislation.

This Policy will be governed by the Cordaid Data Processor Agreement (Annex 8).

Awareness and training

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

Complaints

If a personnel member or other Data Subject believes that data protection legislation or this Policy are not respected by Cordaid, a complaint can be issued to the Cordaid customer service or directly to one of the Administrators.

Documentation

This Policy refers 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 this Policy or is available for inspection with the Administrators. In addition, this section provides a summary of the available documentation:

1. Cordaid Overview of applicable legislation (Annex 1)
2. Cordaid Record of Processing Activities (Annex 2)
3. [Cordaid's Privacy statement](#) (Annex 3)
4. Cordaid [Code of Conduct](#) (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)

Approval and validity

This Policy was approved by the Board of Directors on 24-04-2024 and is effective as of 24-04-2024. The Policy will be valid until declared obsolete by the Board of Directors.