Privacy Policy & Data Processing Terms – Stichting Route 66

(GDPR / AVG compliant – Netherlands & Spain – Gran Canaria)

This Privacy Policy and Data Processing Terms (the “Policy”) applies to the processing of personal data by:

Stichting Route 66, a Dutch non-profit organisation with ANBI status, established at Voorhorsterbrink 18, 7431 ZD Diepenveen, The Netherlands, registered with the Dutch Chamber of Commerce under number 80876145, RSIN 861834227,and its official delegation in Spain:

La Delegación en Canarias de la Fundación Route 66,established at Calle de Arteara 17, 35108 Arteara, San Bartolomé de Tirajana, Las Palmas, Gran Canaria,registered in the Registro de Fundaciones de Canarias under number 399, CIF G44689545,hereinafter collectively referred to as “the Foundation”, “we”, or “us”.

This Policy describes how the Foundation collects, uses, stores, protects and processes personal data in accordance with:

- the General Data Protection Regulation (EU) 2016/679 (“GDPR” / “AVG”);
- applicable Dutch data protection legislation;
- applicable Spanish data protection legislation (including LOPDGDD);
- and relevant European programme requirements (ESC & Erasmus+).

By participating in any programme or project, registering, making use of our services, or interacting with our digital platforms, you acknowledge that you have read and accepted this Privacy Policy and Data Processing Terms.

Article 1 – Definitions

For the purposes of this Policy, the following definitions apply:

1. Personal Data
   Any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR.
2. Processing
   Any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organisation, storage, use, disclosure, erasure or destruction.
3. Data Subject
   The natural person whose Personal Data is processed, including Participants, Volunteers, Interns, Staff Members, Donors, partners, website visitors and applicants.
4. Controller / Data Controller
   The entity that determines the purposes and means of the processing of Personal Data.
   For the purposes of this Policy, Stichting Route 66 is the Data Controller.
5. Processor / Data Processor
   A party that processes Personal Data on behalf of the Controller.
6. Sub-processor
   A third party engaged by a Processor to assist in processing Personal Data.
7. GDPR / AVG
   The General Data Protection Regulation (EU) 2016/679 and its national implementations in the Netherlands and Spain.
8. European Programmes
   Projects and activities carried out under the European Solidarity Corps (ESC) and Erasmus+ frameworks.

9. Services
   All programmes, projects, activities, communications, registrations, digital platforms and administrative processes operated by or on behalf of the Foundation.

Article 2 – Role of the Foundation and Territorial Scope

1. The Foundation acts as the Data Controller for all Personal Data processed in relation to its programmes, projects, services and activities.
2. The Foundation is a Dutch legal entity with an official delegation registered in Spain. A substantial part of its operational activities are physically carried out on the island of Gran Canaria (Spain).
3. Personal Data may therefore be processed in:
   - The Netherlands, where the Foundation is legally established;
   - Spain, where programmes and projects are executed;
   - and within the European Union where authorised service providers and partners are located.
4. This Policy applies to all Personal Data processed by the Foundation, regardless of whether the processing takes place in the Netherlands, Spain, or any other EU Member State.
5. The Foundation processes Personal Data solely in accordance with:
   - GDPR requirements;
   - mandatory provisions of Dutch and Spanish data protection law;
   - and applicable European programme regulations.
6. Where activities are carried out on Spanish territory, mandatory provisions of Spanish law shall apply insofar as required, particularly with regard to:
   - data protection supervision;
   - rights of data subjects;
   - security and confidentiality obligations.
7. The Foundation ensures that all Personal Data processing is conducted lawfully, fairly, transparently and exclusively for clearly defined, legitimate and public-benefit purposes.

Article 3 – Legal Bases for Processing

1. The Foundation processes Personal Data only where there is a valid legal basis in accordance with Article 6 of the GDPR. Depending on the nature of the relationship with the Data Subject and the purpose of processing, one or more of the following legal bases apply:
   a. Consent
   Where the Data Subject has given explicit, informed and freely given consent for the processing of their Personal Data for one or more specific purposes, such as:
   - participation in programmes or projects;
   - use of photographs or video material;
   - receiving newsletters or communications;
   - participation in research, evaluation or awareness campaigns.
2. Consent may be withdrawn at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
   b. Performance of a Contract or Pre-contractual Measures
   Processing is necessary for the performance of an agreement to which the Data Subject is a party, or to take steps at the request of the Data Subject prior to entering into such an agreement, including:
   - registration for participation;
   - administration of programmes, projects and activities;
   - communication related to participation or cooperation;
   - insurance and safety administration.

3. c. Legal Obligation
   Processing is necessary for compliance with legal obligations to which the Foundation is subject, including obligations arising from:
   - Dutch and Spanish legislation;
   - financial and administrative regulations;
   - reporting duties towards tax authorities or regulatory bodies;
   - mandatory documentation and accountability within ESC and Erasmus+ frameworks.
4. d. Vital Interests
   Processing is necessary to protect the vital interests of the Data Subject or another natural person, particularly in emergency or safety situations where health or physical integrity is at risk.
   e. Public Interest and Public Benefit Mission
   Processing is necessary for the performance of tasks carried out in the public interest, in line with the Foundation's ANBI status and its mission to promote mental resilience, climate awareness, ecological responsibility and social connection.
   f. Legitimate Interests
   Processing is necessary for the legitimate interests of the Foundation, provided such interests are not overridden by the fundamental rights and freedoms of the Data Subject. Legitimate interests include, but are not limited to:
   - organisational administration and communication;
   - ensuring safety and integrity of programmes;
   - preventing misuse of services;
   - improving programme quality and effectiveness;
   - internal accountability and reporting.
5. Where Personal Data includes special categories of data as defined in Article 9 GDPR (such as health-related information), such data shall only be processed where:
   - it is strictly necessary for safety or emergency purposes;
   - explicit consent has been obtained from the Data Subject;
   - and appropriate safeguards are in place.
6. The Foundation shall never process Personal Data for commercial exploitation, profiling for marketing purposes, or any form of automated decision-making that produces legal effects or significantly affects Data Subjects.
7. Personal Data shall not be processed in a manner incompatible with the original purposes for which it was collected, unless required by law or explicitly consented to by the Data Subject.
8. In ESC and Erasmus+ Projects, processing of Personal Data is additionally based on:
   - contractual obligations under EU grant agreements;
   - mandatory monitoring, reporting and evaluation requirements;
   - compliance with European accountability and transparency standards.
9. The Foundation ensures that for every processing activity, the applicable legal basis is documented and can be demonstrated in accordance with the GDPR accountability principle.

Article 4 – Categories of Personal Data Processed

1. The Foundation processes only such Personal Data as is necessary and relevant for the execution of its public-benefit activities, in accordance with the principles of data minimisation and purpose limitation under the GDPR.
2. Depending on the nature of the relationship with the Data Subject (Participant, Volunteer, Intern, Staff Member, Donor, Partner or Applicant), the following categories of Personal Data may be processed:
   a. Identification Data
   - full name;
   - date of birth;
   - nationality;

    - gender (only where necessary and voluntarily provided).
3. b. Contact Data
    - postal address;
    - email address;
    - telephone number;
    - emergency contact details.
4. c. Administrative and Participation Data
    - registration forms and applications;
    - participation history in programmes and projects;
    - attendance records;
    - agreements, declarations and consent forms.
5. d. Financial and Donation Data
    - bank account details (where necessary for reimbursements or donations);
    - donation records and acknowledgements;
    - financial administration required under Dutch and Spanish law and EU project frameworks.
6. e. Insurance and Safety Data
    - proof of insurance coverage;
    - accident or incident reports;
    - emergency-related information.
7. f. Communication Data
    - emails and correspondence;
    - messages exchanged via authorised communication channels;
    - feedback and evaluation forms.
8. g. Media and Visual Material
    - photographs;
    - video recordings;
    - audio material;

      used only with consent or where legally permitted, for educational, reporting, documentation and awareness purposes.

   h. Project and EU Programme Data (ESC & Erasmus+)
    - participant identification numbers;
    - learning outcomes and Youthpass-related documentation;
    - reporting and monitoring data required by European authorities.
9. In exceptional cases, the Foundation may process special categories of Personal Data as defined in Article 9 GDPR, such as limited health-related information, but only where:
    - strictly necessary for safety or emergency situations;
    - explicitly consented to by the Data Subject;
    - protected by appropriate safeguards.
10. The Foundation does not intentionally process:
    - data relating to racial or ethnic origin;
    - political opinions;
    - religious or philosophical beliefs;
    - trade union membership;
    - genetic or biometric data;
    - sexual orientation or sexual life.

      Unless such data is voluntarily and explicitly provided and strictly necessary under legal obligations or safety requirements.

5. The Foundation does not engage in:
    - large-scale profiling;
    - automated decision-making;

- behavioural tracking for commercial purposes.

6. The Foundation ensures that all Personal Data processed remains:
    - relevant;
    - accurate;
    - up to date;
    - limited to what is strictly necessary for its lawful and public-benefit purposes.

Article 5 – Purposes of Data Processing

1. The Foundation processes Personal Data solely for specific, explicit and legitimate purposes that are directly connected to its public-benefit mission and operational activities.
2. Personal Data is processed for the following purposes:
   a. Organisation and Execution of Programmes and Projects
    - registering participants, volunteers, interns and staff;
    - managing applications, selections and placements;
    - organising logistics, accommodation, activities and schedules;
    - ensuring safe and responsible participation.
3. b. Safety, Health and Emergency Management
    - ensuring physical and emotional safety during activities;
    - responding to accidents or emergencies;
    - fulfilling insurance and incident reporting obligations;
    - implementing risk prevention and safeguarding procedures.
4. c. Administrative and Legal Compliance
    - fulfilling obligations under Dutch and Spanish law;
    - complying with financial, tax and accountability requirements;
    - maintaining proper organisational records as required for ANBI status;
    - meeting contractual obligations with partners and authorities.
5. d. European Programme Compliance (ESC & Erasmus+)
    - fulfilling monitoring, reporting and evaluation duties;
    - managing Youthpass documentation and learning outcomes;
    - complying with EU grant agreements and programme guidelines;
    - communication with National Agencies and EU institutions.
6. e. Communication and Information Sharing
    - communicating with participants and partners before, during and after projects;
    - providing programme updates and organisational information;
    - responding to inquiries and requests.
7. f. Awareness, Education and Public Communication
    - documenting activities and impact for educational and awareness purposes;
    - sharing stories, results and learning outcomes related to:
        - mental resilience,
        - climate awareness,
        - ecocentric learning,
        - the transition from ego-centred to eco-centred thinking,
        - and the movement from “I” to “we”;
    - strengthening public understanding of sustainable and conscious living.
8. g. Quality Improvement and Evaluation
    - collecting feedback and evaluations;
    - improving programme design and learning methods;
    - strengthening organisational effectiveness and integrity.
9. h. Donations and Support Administration
    - processing donations and maintaining donor records;
    - issuing confirmations or acknowledgements where applicable;
    - ensuring transparency and accountability of funds.

10. The Foundation shall not process Personal Data for purposes that are incompatible with the above, and shall never use Personal Data for:
    - commercial exploitation;
    - sale or trade of data;
    - targeted advertising;
    - behavioural profiling for marketing purposes.
11. All processing activities are guided by the principles of:
    - purpose limitation;
    - data minimisation;
    - transparency;
    - integrity and confidentiality;
    - proportionality.
12. Where Personal Data is intended to be used for a new purpose that is not compatible with the original purpose, the Foundation shall:
    - inform the Data Subject in advance;
    - identify a new lawful basis for processing;
    - and obtain additional consent where required by law.

Article 6 – Data Sharing and Recipients of Personal Data

1. The Foundation treats all Personal Data with strict confidentiality and shares such data only where this is necessary, lawful and consistent with the purposes described in this Policy.
2. Personal Data may be shared with the following categories of recipients, solely to the extent required for the proper functioning of the Foundation and its programmes:
   a. Internal Recipients
    - authorised staff members, coordinators and volunteers of the Foundation who require access to Personal Data for organisational, safety, administrative or project-related purposes;
    - only on a strict need-to-know basis and under confidentiality obligations.
3. b. European Institutions and National Agencies (ESC & Erasmus+)
    - the European Commission;
    - National Agencies;
    - authorised EU project partners;
4. where required for:
    - participant registration;
    - monitoring and evaluation;
    - reporting and accountability;
    - Youthpass and project certification processes.
5. c. Service Providers and Processors
   The Foundation may use external service providers that act as Data Processors, including but not limited to:
    - cloud and storage services (e.g. email, document management, collaboration platforms);
    - website hosting and form providers;
    - accounting and financial administration services;
    - communication and project management tools.
6. These providers process Personal Data solely on behalf of the Foundation and in accordance with written data processing agreements that comply with Article 28 GDPR.
   d. Insurance Companies and Emergency Services
    - where necessary in case of accidents, emergencies or insurance claims;
    - strictly limited to the information required to protect vital interests and fulfil legal obligations.
7. e. Legal and Regulatory Authorities

    - where required by law, court order or regulatory obligation under Dutch, Spanish or EU legislation.
8. The Foundation does not sell, rent, trade or commercially exploit Personal Data under any circumstances.
9. Where Personal Data is shared with third parties acting as Processors, the Foundation ensures that:
    - a written data processing agreement is in place;
    - appropriate technical and organisational security measures are implemented;
    - confidentiality is contractually guaranteed;
    - processing takes place only for specified and legitimate purposes.
10. Personal Data shall only be shared with third parties outside the Foundation when:
    - the Data Subject has given explicit consent;
    - the sharing is necessary for the performance of a contract or legal obligation;
    - the sharing is required for EU project compliance;
    - or the sharing is necessary to protect vital interests.
11. The Foundation ensures that all recipients of Personal Data operate within the European Union or within countries that provide an adequate level of data protection as recognised by the European Commission.
12. In the event that Personal Data must be transferred to a recipient outside the European Economic Area (EEA), the Foundation shall ensure that appropriate safeguards are in place, including:
    - Standard Contractual Clauses (SCCs);
    - or other lawful transfer mechanisms recognised under the GDPR.
13. The Foundation maintains an up-to-date register of all categories of recipients and Processors involved in the processing of Personal Data, in accordance with the GDPR accountability principle.

Article 7 – Data Security Measures

1. The Foundation takes appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required under Article 32 of the GDPR. These measures are designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
2. Security measures implemented by the Foundation include, but are not limited to:
    - controlled access to systems and data based on role and necessity;
    - strong password policies and, where possible, multi-factor authentication;
    - secure storage of physical documents in locked and access-restricted environments;
    - secure digital storage through encrypted or access-controlled platforms;
    - regular updates of software and systems;
    - protection against malware, viruses and unauthorised network access;
    - secure backup procedures to prevent data loss.
3. Access to Personal Data is strictly limited to authorised persons who require such access for the performance of their tasks. All persons with access to Personal Data are bound by confidentiality obligations.
4. The Foundation ensures that all staff members, volunteers and partners who process Personal Data receive appropriate awareness and guidance on data protection, confidentiality and information security.
5. Where the Foundation engages Processors or Sub-processors, it ensures that:
    - they provide sufficient guarantees regarding data security;
    - they implement appropriate technical and organisational measures;
    - such measures are contractually required in accordance with Article 28 GDPR.
6. The Foundation regularly evaluates and updates its security practices in light of:
    - technological developments;

    - organisational changes;
    - emerging risks;
    - guidance from supervisory authorities.
7. In the event of a Personal Data breach that is likely to result in a risk to the rights and freedoms of Data Subjects, the Foundation shall:
    - notify the competent supervisory authority without undue delay and, where required, within 72 hours;
    - inform affected Data Subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms;
    - document the breach, its effects and the remedial actions taken.
8. The Foundation maintains internal procedures for identifying, managing and mitigating data security incidents and Personal Data breaches.
9. The Foundation recognises that complete security cannot be guaranteed and therefore continuously strives to maintain and improve its protection measures in line with the principle of accountability and best practice standards.

Article 8 – Data Retention Periods

1. The Foundation shall retain Personal Data only for as long as is necessary to fulfil the purposes for which it was collected and processed, in accordance with the principles of storage limitation and proportionality under the GDPR.
2. Retention periods depend on the nature of the data, the purpose of processing and applicable legal, administrative and funding obligations, including those arising from Dutch, Spanish and European legislation and from ESC and Erasmus+ programme requirements.
3. As a general framework, the following retention periods apply:
   a. Participation and Programme Data
   Personal Data relating to participation in programmes and projects (such as registrations, attendance records, evaluations and agreements) shall be retained for a maximum period of seven (7) years after the end of participation, unless a longer retention period is required by law or EU programme regulations.
   b. ESC and Erasmus+ Project Data
   Personal Data processed within the framework of ESC and Erasmus+ Projects shall be retained for the period required by the applicable EU grant agreements and auditing obligations, which may extend up to ten (10) years or longer where required by European funding rules.
   c. Financial and Donation Records
   Financial administration data, including donation records and reimbursement documentation, shall be retained for the period required under Dutch and Spanish fiscal and accounting legislation, typically a minimum of seven (7) years.
   d. Communication Data
   General correspondence and communication records shall be retained for as long as necessary to handle the communication purpose and any follow-up obligations, after which they shall be securely deleted or anonymised.
   e. Media and Visual Material
   Photographs, video recordings and audio material shall be retained for as long as they remain relevant for educational, reporting and awareness purposes, subject to the consent given by the Data Subject and the right to withdraw such consent.
   f. Incident and Safety Records
   Data relating to accidents, incidents or safety reports shall be retained for as long as necessary to meet legal obligations, insurance requirements and potential liability considerations.
4. Where Personal Data is no longer necessary for the purposes for which it was collected and no legal obligation exists to retain it, the Foundation shall ensure that such data is:

    - securely deleted; or
    - anonymised in such a way that identification of individuals is no longer possible.
5. The Foundation shall periodically review stored Personal Data to determine whether continued retention is necessary.
6. Data retention may be extended where required:
    - for the establishment, exercise or defence of legal claims;
    - for compliance with legal obligations;
    - for obligations arising from European funding and accountability frameworks.
7. The Data Subject may request deletion of Personal Data in accordance with Article 11 of this Policy (Rights of Data Subjects), unless retention is required by law or overriding legitimate grounds apply.

Article 9 – Rights of Data Subjects

1. The Foundation respects and guarantees all rights of Data Subjects as laid down in the GDPR and applicable Dutch and Spanish data protection legislation.
2. The Data Subject has the right to:
   a. Right of Access
   To obtain confirmation as to whether or not Personal Data concerning them is being processed and, where that is the case, to access such data and information about the processing.
   b. Right to Rectification
   To request the correction of inaccurate Personal Data and the completion of incomplete Personal Data without undue delay.
   c. Right to Erasure (“Right to be Forgotten”)
   To request the deletion of Personal Data where:
    - the data is no longer necessary for the purposes for which it was collected;
    - consent is withdrawn and no other legal basis applies;
    - the data has been unlawfully processed;
    - deletion is required by law.
3. This right is subject to legal exceptions, including obligations to retain data for legal, financial or EU programme requirements.
   d. Right to Restriction of Processing
   To request limitation of processing where:
    - the accuracy of the data is contested;
    - the processing is unlawful but deletion is not desired;
    - the Foundation no longer needs the data but the Data Subject requires it for legal claims.
4. e. Right to Data Portability
   To receive Personal Data in a structured, commonly used and machine-readable format, and to transmit that data to another controller where technically feasible and legally applicable.
   f. Right to Object
   To object, on grounds relating to their particular situation, to the processing of Personal Data based on legitimate interests or public interest tasks.
   g. Right to Withdraw Consent
   To withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing prior to withdrawal.
5. The Data Subject may exercise these rights by submitting a written request to the Foundation using the contact details provided in this Policy.
6. The Foundation shall respond to such requests without undue delay and in any event within one (1) month of receipt, unless the request is complex or numerous, in which case the period may be extended by two (2) additional months, with notice to the Data Subject.

7. The Foundation may request additional information to verify the identity of the Data Subject before processing any request, in order to protect Personal Data against unauthorised access.
8. The exercise of Data Subject rights is free of charge, unless the requests are manifestly unfounded or excessive, in which case a reasonable administrative fee may be charged as permitted by law.
9. The Foundation shall inform the Data Subject if a request cannot be fully or partially fulfilled and provide the legal grounds for such refusal.
10. The Data Subject has the right to lodge a complaint with a supervisory authority, including but not limited to:
    - the Dutch Data Protection Authority (Autoriteit Persoonsgegevens);
    - the Spanish Data Protection Authority (Agencia Española de Protección de Datos – AEPD);
    - or the competent authority in the country of habitual residence or place of the alleged infringement.
11. The exercise of Data Subject rights shall not affect the Foundation's obligation to comply with mandatory retention periods, European funding requirements or legal obligations.

Article 10 – Contact Details and Data Protection Responsibility

1. The Foundation is responsible for ensuring compliance with this Privacy Policy & Data Processing Terms and with all applicable data protection laws and regulations.
2. The Data Controller for all Personal Data processed under this Policy is:

Stichting Route 66
Voorhorsterbrink 18
7431 ZD Diepenveen
The Netherlands

Chamber of Commerce (KvK): 80876145
RSIN: 861834227

Official delegation in Spain:

La Delegación en Canarias de la Fundación Route 66
Calle de Arteara 17
35108 Arteara
San Bartolomé de Tirajana
Las Palmas
Gran Canaria, Spain

Registro de Fundaciones de Canarias: 399
CIF: G44689545

3. For all questions, requests or complaints relating to Personal Data and data protection, the Data Subject may contact the Foundation via:

Email: info@r66gc.com
Website: www.r66gc.com

4. The Foundation shall designate a responsible contact person for data protection matters, who acts as the internal point of contact for:
    - handling Data Subject requests;

    - supervising GDPR compliance;
    - communication with supervisory authorities;
    - coordination of data protection procedures.
5. Where required by law, the Foundation may appoint a Data Protection Officer (DPO). If a DPO is appointed, the contact details shall be published on the Foundation's website and made available to Data Subjects.
6. The Foundation ensures that all communication relating to Personal Data and data protection is handled confidentially, professionally and in a timely manner.
7. Data Subjects are encouraged to contact the Foundation first in case of any questions, concerns or complaints regarding the processing of their Personal Data, so that issues can be addressed in an open and solution-oriented manner.

Article 11 – Governing Law, Supervisory Authorities and Complaints

1. This Privacy Policy and Data Processing Terms shall be governed by and interpreted in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the applicable data protection laws of the Netherlands and Spain.
2. As Stichting Route 66 is a Dutch legal entity with an official delegation in Spain and carries out a substantial part of its activities on Gran Canaria, the Foundation falls under the supervisory competence of:
    - the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), and
    - the Spanish Data Protection Authority (Agencia Española de Protección de Datos – AEPD),

    depending on the nature and location of the processing activities.
3. Where Personal Data is processed primarily in Spain or in direct relation to activities physically carried out on Spanish territory, the Spanish Data Protection Authority (AEPD) shall be the competent supervisory authority.
4. Where Personal Data is processed primarily in the Netherlands or relates to the legal, administrative and organisational management of the Foundation, the Dutch Data Protection Authority shall be the competent supervisory authority.
5. Data Subjects have the right to lodge a complaint with a supervisory authority in the Member State of their habitual residence, place of work, or place of the alleged infringement, in accordance with Article 77 GDPR.
6. Before submitting a complaint to a supervisory authority, the Foundation encourages Data Subjects to first contact the Foundation directly, so that any concerns can be addressed in a constructive and solution-oriented manner.
7. Complaints relating to Personal Data processing may be submitted to the Foundation via:
   Email: info@r66gc.com
   Website: www.r66gc.com
8. The Foundation shall make reasonable efforts to respond to complaints promptly, transparently and in accordance with applicable legal obligations.
9. The submission of a complaint shall not affect the Data Subject's right to seek judicial remedy or to contact a supervisory authority at any time.
10. Nothing in this Article shall limit the rights of Data Subjects under the GDPR or applicable national data protection legislation.

Article 12 – Updates and Amendments to this Policy

1. The Foundation reserves the right to amend, modify or update this Privacy Policy and Data Processing Terms at any time, in order to reflect:
    - changes in applicable legislation or regulations;
    - developments in European or national data protection requirements;
    - changes in organisational structure, programmes or operational processes;

    - new guidance from supervisory authorities;
    - technological or security developments.
2. The most recent version of this Policy shall always be the version published on the official website of the Foundation or otherwise made available to Data Subjects in written or digital form.
3. Amendments to this Policy shall enter into force no earlier than fourteen (14) days after publication or communication, unless:
    - a shorter period is required by law; or
    - the amendment is necessary to address urgent legal, security or safety risks.
4. Where amendments materially affect the rights or obligations of Data Subjects, the Foundation shall make reasonable efforts to inform Data Subjects in advance through appropriate communication channels.
5. Continued participation in programmes or projects, or continued use of the services of the Foundation after the effective date of an amendment, constitutes acceptance of the updated Policy.
6. If a Data Subject does not agree with an amendment, they may withdraw from participation or request the cessation of processing of their Personal Data, insofar as legally possible and subject to mandatory legal or contractual obligations.
7. Amendments shall not have retroactive effect, unless explicitly required by law.
8. The Foundation shall archive previous versions of this Policy for accountability and reference purposes.

Updated January 2026