BALKANS
FORWARD
FOUNDATION

# DATA PROTECTION POLICY (GDPR)

# Balkans Forward Foundation

# DATA PROTECTION POLICY (GDPR)

## Table of Contents

# 1. Purpose

The purpose of this Data Protection Policy is to ensure that Balkans Forward Foundation ("the Foundation") collects, uses, stores, shares, and protects personal data in a lawful, fair, secure, and transparent manner.

The Foundation is committed to respecting privacy and protecting the rights of individuals whose personal data it processes, in line with the General Data Protection Regulation (GDPR) and other applicable data protection laws.

# 2. Scope

This policy applies to all personal data processed by or on behalf of the Foundation, in digital or physical form, regardless of where or how it is stored.

It applies to all persons acting on behalf of the Foundation, including the Founder, Board members, Executive Director, staff, consultants, interns, volunteers, external experts, and any other authorised persons.

This policy also applies, where relevant, to third-party service providers, consultants, contractors, and partners who process personal data on behalf of the Foundation.

# 3. Definitions

Personal data means any information relating to an identified or identifiable natural person.

This may include names, contact details, identification data, online identifiers, financial information, employment-related information, application materials, communication records, photographs, or other information linked to an individual.

Special category data means particularly sensitive personal data, including data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, biometric data, or genetic data. Such data requires a higher level of protection and may only be processed where there is a valid legal basis and, where required, an additional legal condition. OBJ

Processing means any operation involving personal data, including collection, recording, storage, use, disclosure, sharing, transfer, deletion, or destruction. OBJ

# 4. Data Protection Principles

The Foundation shall process personal data in accordance with the following principles:

Personal data must be processed lawfully, fairly, and transparently.
It must be collected for specific, explicit, and legitimate purposes and not used in ways incompatible with those purposes.
Only data that is necessary and proportionate for the relevant purpose shall be collected and processed.
Personal data must be accurate and, where necessary, kept up to date.
Personal data shall not be kept longer than necessary.
Personal data must be processed securely and protected against unauthorised access, misuse, loss, alteration, or disclosure.
The Foundation must be able to demonstrate compliance with these principles. OBJ

# 5. Lawful Basis for Processing

The Foundation shall process personal data only where there is a valid legal basis for doing so.

Depending on the context, this may include consent, contractual necessity, legal obligation, legitimate interests, protection of vital interests, or another lawful basis recognised by applicable law. The Foundation must identify the appropriate legal basis for each category or purpose of processing. OBJ

Where the Foundation relies on consent, consent must be freely given, informed, specific, and capable of being withdrawn.

Where the Foundation relies on legitimate interests, it must ensure that such interests are not overridden by the rights and freedoms of the individual concerned.

## 6. Categories of Personal Data Processed

The Foundation may process personal data where relevant to its legitimate work and operations, including in relation to:

staff, consultants, interns, volunteers, applicants, Board members, experts, donors, supporters, partners, event participants, training participants, contractors, service providers, and other individuals connected to the Foundation's work.

This may include contact details, CVs, contracts, payment-related data, correspondence, event registration data, communication records, monitoring and evaluation data, and other information reasonably necessary for organisational, legal, operational, or donor-related purposes.

The Foundation will avoid collecting or retaining unnecessary personal data.

## 7. Special Category and Sensitive Data

Where the Foundation processes special category data or other sensitive personal data, it shall do so only when strictly necessary, proportionate, and legally justified.

Such data shall be subject to heightened confidentiality, access restrictions, and safeguards.

Particular care must be taken when handling data relating to vulnerable individuals, human rights defenders, minority communities, beneficiaries, or persons who may face risks if their data is disclosed or misused.

## 8. Transparency and Information to Individuals

The Foundation shall take reasonable steps to ensure that individuals are informed about how their personal data is processed.

This includes, where appropriate, informing individuals about the purpose of processing, the type of data involved, the legal basis, who may receive the data, how long it will be retained, and what rights they have.

Where required, the Foundation shall provide privacy notices or equivalent information.

## 9. Data Subject Rights

Individuals whose personal data is processed by the Foundation may have rights under applicable law, including the right to request access, rectification, erasure, restriction, objection, withdrawal of consent where relevant, and, where applicable, data portability.

The Foundation shall respond to such requests in a timely and lawful manner, subject to applicable legal limitations and exemptions.

Requests relating to personal data should be directed to the Executive Director or another designated responsible person.

## 10. Data Access and Confidentiality

Access to personal data shall be limited to persons who need it for legitimate organisational, legal, compliance, or operational reasons.

All persons handling personal data on behalf of the Foundation must treat it as confidential and must not access, disclose, copy, share, or use it without proper authority.

Confidentiality obligations continue after the end of employment or engagement.

## 11. Data Sharing and Third Parties

Personal data may be shared only where there is a legitimate and lawful reason to do so.

This may include sharing with accountants, payroll providers, IT service providers, legal advisors, auditors, donors where required, event or training partners, or competent authorities where legally necessary.

Where third parties process personal data on behalf of the Foundation, the Foundation shall take reasonable steps to ensure that appropriate safeguards and contractual protections are in place. Controllers determine the purposes and means of processing, while processors act only on instructions and require appropriate contractual arrangements. OBJ

## 12. International Transfers

Where personal data is transferred outside the country or region in which it was collected, the Foundation shall ensure that such transfers are lawful and subject to appropriate safeguards where required.

Particular caution must be applied when using digital tools, cloud services, communication platforms, or international service providers.

## 13. Data Security

The Foundation shall implement reasonable and proportionate technical and organisational measures to protect personal data.

This includes secure storage, access controls, password protection, appropriate use of devices and systems, secure sharing practices, backups where relevant, and measures to reduce the risk of unauthorised access, accidental loss, or misuse.

All persons acting on behalf of the Foundation are responsible for handling personal data securely and in accordance with this policy.

## 14. Data Retention and Deletion

Personal data shall be retained only for as long as necessary for the purpose for which it was collected, or as required by law, donor rules, contractual obligations, or legitimate organisational need.

When personal data is no longer required, it must be securely deleted, anonymised, or destroyed in accordance with the Foundation's Document Retention and Archiving Policy.

## 15. Personal Data Breaches

Any actual or suspected personal data breach, including unauthorised access, disclosure, loss, theft, destruction, or accidental sharing of personal data, must be reported immediately to the Executive Director or designated responsible person.

The Foundation shall assess and respond to breaches promptly and, where required by law, notify the competent authority and/or affected individuals within the applicable timeframe.

# 16. Roles and Responsibilities

The Foundation acts as a data controller where it determines the purposes and means of processing personal data.

All persons acting on behalf of the Foundation are responsible for handling personal data responsibly and in accordance with this policy.

The Executive Director is responsible for oversight of implementation, coordination of responses to data protection issues, and ensuring that appropriate safeguards and procedures are in place.

The Board has oversight responsibility for ensuring that the Foundation maintains appropriate governance and accountability in relation to data protection.

# 17. Breach of Policy

Failure to comply with this policy may result in corrective or disciplinary action, depending on the seriousness of the breach.

Unauthorised access, disclosure, misuse, concealment, negligent handling, or deliberate abuse of personal data may be treated as a serious violation.

# 18. Related Policies

This policy should be read together with the Digital and Information Security Policy, Document Retention and Archiving Policy, Code of Conduct, Safeguarding Policy, Recruitment and Selection Policy, and any applicable legal or donor requirements.

# 19. Review of the Policy

This policy shall be reviewed periodically and updated as necessary to reflect legal obligations, organisational practice, technological developments, and good governance standards.