ACCRÉDITATION SANS FRONTIÈRES

ASF Data Protection Policy

The comprehensive GDPR policy governing every category of personal data ASF processes

Version 1 · 2026
Paris · Geneva · Tbilisi

ASF-DATAPROTECT-001-v1 · Published Paris, 12 September 2026 · Next review 12 September 2029

Document Control

Document Title	ASF Data Protection Policy
Document Reference	ASF-DATAPROTECT-001-v1
Version / Edition	Version 1
Status	Published
Date of Publication	12 September 2026
Place of Publication	Paris, France
Issuing Authority	ASF International Standards Council, Accréditation Sans Frontières
Language of Origin	English
Effective Date	12 September 2026
Next Scheduled Review	12 September 2029
Supersedes	None — consolidates data protection provisions previously stated only partially, across Section 11 of How ASF Develops and Revises Standards and the ASF IT & Data Security Policy

Table of Contents

Foreword

Section 11 of How ASF Develops and Revises Standards addresses confidentiality of applicant information. The ASF IT & Data Security Policy addresses the technical and organizational security of ASF's systems. Neither is a comprehensive data protection policy in the sense the General Data Protection Regulation actually requires: a documented lawful basis for every category of personal data ASF processes, defined retention periods, a clear statement of data subject rights, and — given ASF's own genuine footprint across Paris, Geneva, and Tbilisi — an honest treatment of international data transfer. This document is that policy.

> *ASF is registered in Paris, France — squarely within the European Union, and squarely within GDPR's reach. This is not a policy ASF adopts by choice; it is a policy ASF is legally required to have, in substance and not merely in name.*

1. Purpose and Scope

This policy governs how ASF processes personal data across every category it holds — complainant identities under the ASF Public Complaints & Feedback Policy, whistleblower reports under the ASF Internal Whistleblower Protection Policy, survey and personnel records, and applicant organization data — consistent with the General Data Protection Regulation, Regulation (EU) 2016/679 [1].

2. Why This Matters: The Real Enforcement Evidence

This is not a theoretical compliance exercise. The Commission Nationale de l'Informatique et des Libertés — France's own data protection authority, with direct jurisdiction over ASF given ASF's Paris registration — issued eighty-three sanctions totaling €486.8 million in 2025, compared with roughly €55 million the year before: a nearly ninefold increase in a single year [2]. Across the European Union as a whole, data protection authorities assessed nearly €1.2 billion in GDPR fines in 2025, with cumulative penalties since the regulation's introduction exceeding €7.1 billion [3].

A specific, recurring finding in GDPR enforcement is directly relevant to how this policy is structured: undocumented, “just in case” data retention — keeping personal data longer than any actual purpose requires, without a documented justification — is now treated as an independent basis for sanction, separate from any other violation [2]. This is precisely why Section 4 of this policy defines a specific retention period for every category of data ASF holds, rather than a general commitment to “reasonable” retention.

3. Lawful Basis for Processing

Consistent with Article 6 of the GDPR, every instance of personal data processing at ASF is justified under one of six lawful bases, determined and documented before processing begins [4–5]:

- Consent — the individual has clearly agreed to a specific processing purpose
- Contract performance — processing is necessary to deliver a service the individual requested
- Legal obligation — processing is required to meet a legal requirement
- Vital interests — processing is necessary to protect someone's life
- Public task — processing is necessary for a task carried out in the public interest
- Legitimate interests — processing serves a genuine interest of ASF's, balanced against the individual's own rights and freedoms

4. Data Categories, Basis, and Retention

Data Category	Lawful Basis	Retention
Complainant identity (Complaints Policy)	Legitimate interest — investigating a genuine concern	Duration of investigation + 3 years
Whistleblower report	Legitimate interest — organizational integrity	Duration of investigation + 3 years
Survey and accreditation records	Contract performance	Full accreditation cycle + 10 years
Personnel competence records	Legal obligation / contract performance	Duration of role + 5 years
Sentinel event reports	Vital interests / legitimate interest	Indefinite — aggregate learning function

Where a specific document (the ASF Sentinel Event Policy, the ASF Public Complaints & Feedback Policy) already states a retention or confidentiality rule for its own data category, that rule governs; this table exists so every category is visible in one place, not to override any more specific existing rule.

5. Data Subject Rights

Consistent with Articles 15 through 22 of the GDPR, any individual whose personal data ASF holds may exercise the following rights, and ASF responds within one month of a request [1, 6]:

- Right of access — confirmation of whether ASF processes their data, and a copy of it
- Right to rectification — correction of inaccurate or incomplete data
- Right to erasure — deletion of data where no lawful basis for continued retention exists
- Right to restriction — limiting how ASF uses the data while a dispute about it is resolved
- Right to data portability — receiving data in a portable format, where technically feasible
- Right to object — objecting to processing based on legitimate interest, which ASF then stops unless a compelling justification overrides it

> *A complainant's right to request their own data does not override the confidentiality protections owed to them under the ASF Public Complaints & Feedback Policy — these rights work alongside that policy's own protections, not instead of them.*

6. International Transfers — The Tbilisi Question

ASF genuinely operates across three jurisdictions: Paris, France, within the European Union; Geneva, Switzerland, which the European Commission has recognized as providing an adequate level of data protection; and Tbilisi, Georgia, which sits outside the European Economic Area and has not received an EU adequacy decision. Consistent with GDPR Chapter V, any personal data ASF transfers to or processes from its Tbilisi operations requires its own documented safeguard — Standard Contractual Clauses or another approved transfer mechanism — rather than an assumption that data can move freely across all three locations on the same terms [1, 7].

> *This is not a hypothetical compliance point for ASF specifically — it is a real, live requirement given ASF's own genuine, three-city operational footprint, not a generic clause copied from a template built for a single-country organization.*

7. Data Protection Contact

Consistent with Article 37 of the GDPR, ASF designates a data protection contact responsible for overseeing this policy's application, advising on data protection questions, and serving as the point of contact for a data subject rights request or a query from a supervisory authority [1]. Where ASF's processing does not meet the specific threshold requiring a formal Data Protection Officer, ASF nonetheless maintains this designated contact as a matter of genuine accountability, not only minimum legal compliance.

8. Accountability and Records

Consistent with the accountability principle in Article 5(2) of the GDPR — the obligation not merely to comply, but to be able to demonstrate compliance on request — ASF maintains a record of processing activities covering every data category in Section 4, reviewed as part of the annual ASF Management Review Procedure [1, 7].

9. Relationship to Other ASF Processes

- The technical and organizational security measures protecting this data are governed by the ASF IT & Data Security Policy, not restated here
- A data protection incident is handled under Section 6 of the ASF IT & Data Security Policy, including the 72-hour regulatory notification requirement
- Confidentiality specific to a complainant or whistleblower's identity remains governed by the ASF Public Complaints & Feedback Policy and the ASF Internal Whistleblower Protection Policy respectively; this policy governs the broader data protection framework those specific protections sit within

References

[1] European Union. General Data Protection Regulation (EU) 2016/679. 2016.

[2] Legiscope. GDPR Compliance Guide 2026: Data Storage & Retention, citing CNIL 2025 sanction data.

[3] CNiC Solutions. Cybersecurity Compliance Statistics 2026: GDPR, HIPAA, PCI & CMMC Data. 2026.

[4] Drata. GDPR for US Companies: A Practical Guide to Compliance. 2026.

[5] Usercentrics. GDPR Data Retention: Compliance Guidelines and Best Practices. 2026.

[6] GDPR Local. Data Subject Rights and Responsibilities.

[7] Skillcast. Legal Basis for Data Processing under GDPR.

Annex A — Data Subject Rights Request Form

Completed by ASF's data protection contact upon receiving a data subject rights request.

Requester name: _____

Nature of relationship to ASF (complainant / whistleblower / personnel / other):

_____

Right(s) Requested

☐ Access

☐ Rectification

☐ Erasure

☐ Restriction

☐ Portability

☐ Objection

Date received: _____

Response due (within one month): _____

Response provided on: _____

Index

Every ASF document that mentions confidentiality assumes a real data protection framework sits underneath it. This is that framework, made explicit rather than assumed.