



POLICIES | FIRST EDITION

IAF DATA PROTECTION AND PRIVACY POLICY

Responsible data use and
privacy in automotive activities

STABLE RELEASE

Document No. IAF-POL-012 | Revision 01

Data lifecycle, individual rights and security
Privacy governance and incident response
Implementation records and references

International Automotive Federation

English master text | 14 September 2026

iaf.com

Publication identity and use

Protect personal data throughout IAF membership governance and automotive programmes.

Control	Publication record
Document	IAF-POL-012 Data Protection and Privacy Policy
Edition and revision	First Edition Revision 01 Stable Release
Text issued	14 September 2026 English master text
Policy owner	Information Lead and designated Privacy Lead
Approving authority	Competent Presidential Council authority under IAF-CON-001
Operational commencement	The actual approval reference and effective date are recorded in the controlled approval notice and IAF-RG-001.
Classification	Public core policy. Completed case records and operational details are classified according to their content.

How to apply this policy

Apply the numbered requirements to the relevant activity and use the annexes with the existing IAF forms. Record the responsible person, authority, evidence and dates for each decision. “Shall” states a requirement; “may” permits a justified choice within the stated authority.

Authority and document control

Mandatory law and the filed corporate instrument prevail, followed by the lawfully adopted Constitution and the applicable policies and programme rules. This policy supplements the IAF quality documentation. It does not amend constitutional offices, grant an external mandate or establish that operational appointments and systems are already in place.

The Constitution identifies 05 May 2025 as its designated effective date. This newly issued policy takes operational effect through its actual competent approval notice. The Secretariat maintains the master text, related instructions and revision history under IAF-PR-001.

Contents

The policy requirements and operating procedures are followed by implementation records and document references. Annex templates support the existing IAF forms and do not replace required competent decisions.

1 Purpose scope and governing principles	4
2 Accountability and operational roles	5
3 Processing inventory and lawful basis	6
4 Transparency collection and public information	7
5 Sensitive data children and research	8
6 Security access and system controls	9
7 Providers disclosures and international transfers	10
8 Individual rights request procedure	11
9 Personal data incident procedure	12
10 Retention holds and secure disposal	13
11 Privacy assessment audit and change	14
12 Publication commencement and contact control	15
Annex A Controller and privacy notice schedule	16
Annex B Request incident and assessment records	17
Annex C Selected jurisdiction requirements	18
Annex D Document alignment and activation record	19

Related policy series

IAF-POL-009 Whistleblowing Policy
IAF-POL-010 Appeals and Complaints Policy
IAF-POL-011 IAF Mark Usage Policy
IAF-POL-013 Conflict of Interest Policy

1 Purpose scope and governing principles

1.1 IAF shall process personal data lawfully, fairly and transparently for specified purposes, collect only what is necessary, maintain accuracy, limit retention and protect confidentiality, integrity and availability. The responsible operating entity shall be able to demonstrate these controls through records and effective oversight.

1.2 This policy applies to personal data in membership, governance, elections, assessments, accreditation and certification schemes, AutoSafe, AutoID, Academy activities, events, awards, employment, procurement, partnerships, research, communications, complaints, appeals and protected reporting. It covers paper records, email, cloud services, websites, recordings and data held by service providers.

1.3 Personal data is information relating to an identified or identifiable person. A business contact, sole trader record, image, voice, device identifier or vehicle record may be personal data where linked to a person. Pseudonymized data remains personal data where reidentification is possible; effective anonymization requires a documented assessment.

1.4 A controller determines the purposes and essential means of processing. A processor acts on a controller's documented instructions. Joint controllers determine purposes and means together. IAF's role shall be established for each processing activity from actual responsibilities, not assumed solely from a contract label.

1.5 This policy implements the Constitution and supplements IAF-POL-004 and IAF-PR-019. It is a global internal baseline; mandatory local rules apply according to the entity, persons, activity and jurisdiction. Annex C records selected legal requirements without asserting that every jurisdiction applies to every IAF activity.

1.6 Signing the Constitution, Membership Memorandum or a cooperation agreement does not provide blanket consent to all personal-data processing. Membership cooperation duties shall not require unlawful disclosure, irrelevant personal information or unrestricted access to another organization's records. Each processing purpose requires its own valid basis and safeguards.

2 Accountability and operational roles

2.1 Before processing begins, the operating entity shall record its exact registered identity, address, responsible office, contact route and applicable jurisdiction. The published privacy notice shall identify the actual controller. Federation branding alone shall not obscure which legal person is responsible for an activity.

2.2 The competent governing authority approves this policy and necessary resources. The Information Lead controls security and information operations. The designated Privacy Lead advises on notices, lawful bases, rights, risks and incidents and maintains the processing register. Appointment as Privacy Lead is not a claim that a statutory Data Protection Officer has been appointed.

2.3 Where legal criteria require a Data Protection Officer, representative, local registration or supervisory notification, the entity shall meet those requirements before or within the legally prescribed period. A required Data Protection Officer shall have suitable expertise, independence, protected access and no conflicting responsibility for determining the processing they oversee.

2.4 Each process owner shall identify the data used, purposes, persons affected, systems, recipients, lawful basis, retention and risks. The owner shall approve access according to need and ensure that staff and providers follow this policy. Outsourcing processing does not remove the controller's accountability.

2.5 The Quality Manager coordinates document control, audit and corrective actions. Ethics and Appeals functions retain independent access needed for their mandate, subject to lawful safeguards. An official implicated in a case shall not use privacy administration to suppress evidence or obtain unrestricted access to protected case data.

2.6 Employees, committee members, assessors and providers shall follow instructions, protect credentials, verify recipients and report suspected incidents promptly. Training shall occur before access and periodically thereafter. Material noncompliance shall receive proportionate action under the applicable employment, contract, membership or scheme process.

3 Processing inventory and lawful basis

3.1 Maintain a processing activity register identifying the controller role, purpose, data subjects, categories, sources, lawful basis, special-data condition where needed, recipients, locations, transfers, retention, security measures and responsible owner. Update it before a new activity or material change and review it at least annually.

IAF activity	Purpose and basis to establish before use
Membership and representatives	Verify identity, corporate authority, accession, contacts and dues. Distinguish contract with an individual from business-contact processing for a corporate member.
Technical programmes and registers	Evaluate competence and evidence, issue decisions and enable proportionate verification. Limit public fields to the scheme purpose and justified lawful basis.
Governance and integrity	Administer elections, declarations, complaints, appeals and reporting. Identify applicable legal duties and legitimate interests with extra safeguards for sensitive allegations.
Academy events and awards	Deliver the requested service, assess outcomes, manage entries and communications. Treat optional publicity and marketing separately.
Research and vehicle data	Define the project, linkage risk, collection authority and safeguards. An automotive or research purpose alone is not a lawful basis.

3.2 Where consent is used, it shall be specific, informed, freely given, recorded and as easy to withdraw as to give. Do not bundle optional publicity, marketing or unnecessary disclosure into membership or service acceptance. Withdrawal affects future consent-based processing and does not erase an independently lawful retention duty.

3.3 Where legitimate interests are legally available and relied on, document the purpose, necessity, reasonable expectations, impact and safeguards, including objection handling. Contract necessity applies only to processing objectively needed for the relevant contract with the person. Record the specific legal obligation where that basis is used.

4 Transparency collection and public information

4.1 Provide a clear activity-specific privacy notice when collecting data and, for indirectly obtained data, within the applicable legal period. Identify the controller, purposes, bases, categories and sources where relevant, recipients, transfers, retention, rights, contact and authority complaint route. Explain required fields and consequences of not supplying them.

4.2 Collect personal data through approved forms and systems with proportionate identity checks. Corporate membership evidence should establish the entity and authorized representative without collecting unrelated directors' identity documents or personal financial information. Redact unnecessary identifiers from resolutions and supporting documents where the evidential purpose permits.

4.3 Public registers shall disclose only the fields needed to verify a defined status or result. Normally use entity name, relevant scope, identifier, status and a business contact where justified. Do not publish private addresses, identity documents, complaint allegations, signatures or reporter identities. Review the risk of identifying sole traders and Individual members.

4.4 Meeting and event notices shall explain photography, recordings and publication. Use a valid basis and practical options where appropriate; do not assume attendance is consent to every use. Recordings shall have a defined purpose, access and retention period, and shall not replace a necessary accurate formal minute.

4.5 Websites shall distinguish essential service technologies from analytics, advertising and other optional tracking. Apply consent or other requirements under the relevant local rules, provide a genuine choice where required and maintain a current technology inventory. This policy does not assert that a particular cookie or consent system is already installed.

4.6 Marketing shall have a valid privacy and electronic-communications basis, a clear sender and an effective opt-out. Maintain a minimal suppression record where necessary to respect an objection. Ordinary membership administration and safety or status notices shall not be repackaged as compulsory promotional consent.

5 Sensitive data children and research

5.1 Health, biometric identification, criminal allegations and other legally sensitive categories require the applicable additional condition and enhanced safeguards. Determine the actual legal category in each jurisdiction. Where Turkish law applies, assess whether an Individual membership record constitutes association or foundation membership data within its special-category rules.

5.2 Conflict declarations and integrity cases shall collect the interest or allegation needed for the decision, not unnecessary details of relatives' lives. Restrict identity and allegation files, use summaries where sufficient and verify a lawful condition before retaining criminal-conviction or offence data. An internal allegation shall not be recorded as a conviction.

5.3 Before involving children or persons needing additional protection in learning, events or research, assess age-related rules, capacity, notices, safeguarding and any required parental authorization. Use age-appropriate explanations and minimize identity evidence. Do not publish a child's location, profile or images without a valid basis and appropriate safeguards.

5.4 Vehicle telemetry, location, driver behavior, images, connected-device identifiers and maintenance histories may identify drivers, owners or workers. A vehicle identifier is not automatically anonymous. Limit collection to the defined assessment or research purpose and separate identity links where possible.

5.5 Research and pilot projects shall document lawful collection, participant information, access, retention, publication and any reidentification risk. Anonymized outputs shall be checked against linkage with other available information. Sharing for a new research purpose requires a documented compatibility and legal assessment; a broad cooperation promise is insufficient.

5.6 Do not upload restricted case files, personal assessment evidence or confidential member records into unapproved artificial intelligence services. Approved use requires a documented purpose, provider terms, transfer review, data minimization and human responsibility. No significant membership, disciplinary or technical decision shall be made solely by an automated score without an expressly lawful and approved process and required safeguards.

6 Security access and system controls

6.1 Classify information as Public, Internal, Confidential or Restricted under IAF-POL-004. Apply role-based access, least privilege and individual accounts. Use multi-factor authentication for privileged, critical and remote access and protect authentication secrets. Shared uncontrolled accounts shall not be used for restricted cases or decision records.

6.2 Approve access before granting it, review privileged and restricted access at least quarterly and remove or adjust it promptly when a role ends or changes. Recusal under IAF-POL-013 shall remove case access as well as voting rights where needed. Retain access logs proportionate to security and accountability purposes.

6.3 Use approved managed devices, supported software, timely security updates, encryption appropriate to risk, secure transfer channels and protected backups. Test restoration and incident contacts. Do not send restricted attachments to broad mailing lists or personal accounts; verify recipients and use access-controlled links where appropriate.

6.4 Paper and physical evidence shall have secure storage, controlled removal, visitor safeguards and authorized destruction. Remote work shall protect screens, conversations, printing and devices. Disposal shall prevent practical recovery of personal information, with a record appropriate to the data and medium.

6.5 Systems shall preserve evidence integrity and separate environments where needed. Use non-sensitive test data where possible. A processor or administrator shall not reuse production data for product development, model training or unrelated analytics without documented controller authorization and an independent lawful assessment.

6.6 Security measures shall be based on actual risk, including safety implications, sensitive cases, scale and foreseeable harm. Review vulnerabilities and control failures through IAF-PR-017 and business continuity under IAF-PR-020. Security certification or contractual promises do not replace checking that controls operate in the IAF service.

7 Providers disclosures and international transfers

7.1 Before engaging a provider, assess its role, competence, security, locations, subprocessors, incident support, deletion and exit arrangements. A processor agreement shall cover documented instructions, confidentiality, security, subprocessors, rights assistance, incident notification, audit information, return or deletion and restrictions on independent reuse.

7.2 A disclosure to another controller shall have a defined purpose, lawful basis and minimum dataset. Joint-controller arrangements shall allocate responsibilities transparently without removing data subjects' rights. An international partnership or Memorandum does not itself establish a lawful basis for every exchange.

7.3 Record where data is hosted, accessed and supported. Remote access from another country may constitute a transfer under applicable law. Before a restricted international transfer, verify the relevant adequacy decision, approved safeguard or narrowly applicable exception and any required transfer-risk assessment and supplementary measures.

7.4 Where European data protection transfer rules apply, use the applicable lawful mechanism and assess whether it operates effectively in the circumstances. Where Turkish transfer rules apply, use the current Article 9 framework and meet the required approval or notification steps; a standard contract must be notified to the Authority within five business days following signature.

7.5 Requests from public authorities shall be verified, recorded and assessed for legal authority, scope and disclosure limits. Notify the person where lawful and appropriate. Emergency disclosure requires a documented lawful basis and necessary scope. Neither a senior office nor an informal external request authorizes unrestricted access.

7.6 Review providers and transfers when services, countries, ownership, subprocessors or law change. An unacceptable risk shall trigger mitigation, suspension of the affected transfer or an orderly alternative. Ending a contract shall include data return, deletion, revoked access and retained evidence of completion, subject to lawful holds.

8 Individual rights request procedure

8.1 Any recipient of a request concerning personal data shall forward it promptly to the verified Privacy Lead route. Record actual receipt, the right sought, jurisdiction and deadline. A request need not name a statute or use the IAF form. Do not require the person to complete a general complaint or appeal first.

8.2 Verify identity and representative authority only to the extent necessary. If reasonable doubt remains, request proportionate additional information through a secure route. Do not routinely request a full identity document when a safer existing account or limited check is sufficient. Record any lawful effect on the response clock; do not assume clarification automatically pauses it.

8.3 Search relevant systems, paper files and providers. Assess access, correction, deletion, restriction, portability, objection, consent withdrawal and automated-decision rights as applicable. Protect other persons' rights through justified redaction rather than blanket refusal. A legal hold may limit deletion but shall not automatically defeat access or correction.

8.4 Respond within the applicable statutory period. Under applicable European rules, the normal limit is one calendar month, with up to two further months where the legal conditions are met and notice is given within the first month. Under Turkish Law 6698, respond as soon as possible and no later than 30 days. These periods are not interchangeable.

8.5 The response shall explain action taken, data provided, any restriction or refusal and its reasons, and the competent complaint or judicial route. Use a secure delivery method and record actual dispatch. Requests are ordinarily free; any fee or refusal for abuse shall meet the specific legal test and shall not be used to deter a legitimate request.

8.6 Complete corrections or restrictions in relevant systems and notify recipients where required. Log the outcome in IAF-FR-024 with a restricted evidence link. A complaint about handling may follow IAF-POL-010, but shall not suspend statutory rights or the person's right to approach the competent authority.

9 Personal data incident procedure

9.1 A personal data breach may involve accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Anyone who suspects an incident shall notify the Information Lead or the verified alternative immediately, preserve evidence and avoid further disclosure. A processor shall notify the controller without undue delay under its agreement and applicable law.

Stage	Required action
Immediate response	Record discovery and awareness times; protect people; contain access or disclosure; preserve logs and originals; activate the incident team.
Initial assessment	Aim to establish scope and notification responsibilities within 24 hours. This internal target does not delay an earlier legal duty.
Risk and notification	Identify affected data and people, likely consequences, safeguards, controller and processor roles, jurisdictions and legal deadlines.
Recovery and follow-up	Restore safely; communicate verified updates; address causes; test corrective actions; close only with documented residual risk and ownership.

9.2 Where European rules apply, notify the supervisory authority without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to result in risk to individuals. Notify affected people without undue delay where likely high risk, subject to the legal exceptions. Record the reasoning for notification or non-notification.

9.3 Where Turkish rules apply to unlawfully obtained personal data, notify the Board without delay and within 72 hours of awareness, and affected people within the shortest reasonable period after identification. Do not import the European unlikely-risk exception to defeat the Turkish duty. Explain delay and provide phased information where permitted.

9.4 Notifications shall use the applicable required content and channels and identify known facts, likely consequences, measures and contact. Lack of a completed investigation is not a reason to miss a deadline. The incident record shall track supplemental information, communications and any linked whistleblowing or technical safety case.

10 Retention holds and secure disposal

10.1 Each record category shall have a purpose-based retention period, trigger, legal basis, owner and disposal method in IAF-RG-012. Periods in the existing quality schedule are planning baselines subject to legal and necessity review, not universal legal minimums. Retain only the data needed for the documented purpose.

Record category	Existing IAF baseline and limiting control
Constitutional governance	Permanent institutional resolutions; minimize personal attachments. Ordinary election audit records normally seven years.
Membership	Seven years after end of membership, subject to justified obligations and removal of unnecessary identity copies.
Technical outcomes	Ten years after final withdrawal or end of reliance; configuration-based ongoing reliance may require a documented longer active record.
Complaints appeals and corrective actions	Seven years after final verified closure, with earlier deletion of unnecessary identities and irrelevant evidence.
Competence and interests	Five years after role end, subject to necessary linkage to decisions and any lawful hold.
Data requests and incidents	Five years after closure, subject to a documented need and local requirements.
Routine access logs	Twelve months from creation unless a justified security need or scoped hold requires another period.

10.2 Other categories, including financial records, providers, training and publications, follow the approved category-specific schedule. The owner shall not default every personal record to the longest available period. Review active and archived holdings at least annually and delete or anonymize material whose purpose has ended.

10.3 A hold shall state the legal or evidential reason, records covered, authorized owner and review date. Release it when the reason ends. Use IAF-FR-030 to authorize disposal and preserve the minimal disposal evidence; a hold does not permit unrestricted access or indefinite retention of unrelated data.

11 Privacy assessment audit and change

11.1 Apply privacy by design and by default before introducing a new programme, portal, monitoring system, research dataset, recording practice, public register or automated tool. Assess necessity, less intrusive options, access, retention, rights, provider roles, transfers and foreseeable harm before collecting data.

11.2 A Data Protection Impact Assessment shall be completed before processing likely to create high risk where required by law and whenever IAF's risk assessment identifies a need. Examples warranting screening include systematic vehicle-location monitoring, large-scale sensitive data, biometric identification and significant automated evaluation.

11.3 The assessment shall describe the processing, purpose, necessity, proportionality, risks to people and measures. The process owner shall obtain Privacy Lead input and any required Data Protection Officer advice. Where unresolved high risk requires consultation with an authority, complete it before beginning the affected processing.

11.4 Material changes shall be approved through IAF-PR-002 and IAF-FR-003, with updated notices, contracts, inventories and training. Record decisions about compatibility of a new purpose. Do not rely on an old broad consent or an undocumented assumption that all Federation activities are the same purpose.

11.5 Audit shall examine actual access, deletion, rights responses, incident readiness, processor controls and public notices. Report trends and corrective actions without exposing case identities. Measure missed deadlines and control failures as well as training completion; a written policy alone is not evidence of effective protection.

11.6 The competent governing authority shall review material risks, resources and action effectiveness at least annually. The policy owner shall review legal changes with competent jurisdiction-specific advice. Where a legal entity or data location changes, reassess applicable law, representative duties and transfer arrangements before continuing affected processing.

12 Publication commencement and contact control

12.1 The core policy may be published. Completed operational schedules containing staff access details, security information, case references or sensitive contact arrangements shall remain Internal, Confidential or Restricted as appropriate. Publish only the contact information necessary for individuals to exercise their rights.

12.2 Before using a public privacy notice, complete Annex A with the actual controller identity, address, verified privacy contact, activity details and applicable authority route. A federation-wide notice may link to programme-specific notices, but shall not conceal different controllers or processing purposes.

12.3 Test the rights request and incident routes, including absence and outage coverage. Record monitoring frequency, deputies, notification authority and access controls. Do not advertise a Data Protection Officer, registered representative, certification, hotline or registration status without a current factual basis.

12.4 The competent Presidential Council authority approves this policy and resources through document control. The Secretariat shall record actual approval and operational effective date, distribute instructions and enter IAF-POL-012 Revision 01 in IAF-RG-001. Approval of this document is distinct from completing the factual notices and system controls.

12.5 Changes affecting people shall be communicated clearly and before new processing where required. Retain prior notices and their effective periods so that the information given at collection can be established. A later notice does not retrospectively legalize processing without a valid basis.

12.6 Review at least annually and after material legal, organizational, programme or security changes. Where local law imposes stronger requirements, document and apply the local addendum. Conflicting operational text shall be corrected through IAF-PR-001; statutory rights and notification duties shall remain effective throughout the correction.

Annex A Controller and privacy notice schedule

Complete one schedule for each controller and activity or a clearly defined group of activities. The approved public notice shall use actual service details and plain language.

Notice field	Required content
Controller	Exact registered name, address, registration details as required, relevant IAF role and applicable jurisdiction.
Contact	Verified privacy contact; Data Protection Officer or representative details only where actually appointed.
People and data	Affected groups; categories; direct or indirect sources; required and optional information.
Purpose and basis	Each purpose and its lawful basis; legitimate interest where used; additional condition for sensitive data.
Recipients and transfers	Recipient categories; processors or independent controllers; countries and safeguards; how to obtain relevant information.
Retention	Category period or intelligible criterion, trigger, lawful holds and any longer necessary reliance.
Rights and choices	Applicable rights; how to request them; consent withdrawal; objection; authority complaint route and contact.
Special processing	Automated decisions and safeguards if any; children; recordings; research; public register and optional publicity.
Control	Notice version, approval, effective date, public location, related programme notices and next review.

Public request wording

“To ask about your personal data or exercise an applicable right, contact the privacy office identified in this notice. Tell us the activity involved and what you would like us to do. We may request proportionate information to confirm identity. You do not need to complete an IAF complaint or appeal before exercising a statutory data protection right.”

Annex B Request incident and assessment records

Record	Minimum fields and completion
Rights request with IAF-FR-024	Receipt time; person and representative; activity; right; jurisdiction; identity check; deadline; search owner; disclosure review; response; delivery; recipient updates; closure.
Incident with IAF-FR-024	Discovery and awareness times; reporter; systems; controller role; data and people; containment; evidence; risk; each legal deadline; notification decision and reasons; recipients; updates; recovery.
Processing activity register	Controller and owner; purpose; persons and data; source; basis; sensitive-data condition; recipients; systems and countries; safeguards; retention; notice; risk assessment.
Provider and transfer assessment	Provider role; locations; subprocessors; terms; security evidence; rights and breach support; transfer mechanism; risk assessment; approvals; notification; exit controls.
Impact assessment	Processing description; necessity; alternatives; risks to people; measures; consultation; residual risk; approval; any authority consultation; review triggers.
Hold and disposal with IAF-FR-030	Record category; trigger; basis; relevant hold; owner; review date; authorized method; date completed; verification and minimal disposal evidence.

Access and record separation

Use the general action register only for a reference, owner, dates and status. Store identifying requests, incident evidence, health or offence information and security details in separately controlled files. A report to management should summarize risk and action without reproducing unnecessary personal data.

Operational rehearsal

Before activation and at least annually, test a rights request, a simulated breach escalation and a provider notification using non-sensitive test data. Confirm that receipt clocks, deputies and escalation work in practice and record corrective actions.

Annex C Selected jurisdiction requirements

This annex identifies selected rules requiring distinct controls. Applicability depends on the actual operating entity and processing. The Privacy Lead shall maintain the complete obligations assessment in IAF-RG-010 and obtain competent local advice where needed.

Framework	Requirements to preserve
European data protection rules	Record territorial applicability, Article 6 basis and any Article 9 or 10 condition. Rights response normally one calendar month; qualifying extension up to two further months with first-month notice. Breach authority notice under Article 33 and high-risk individual notice under Article 34 are distinct.
Turkish Law 6698	Record applicable processing and special-category conditions, transparency and security duties. Respond to controller requests within 30 days. A Board complaint may be made within 30 days of learning the response and in any event within 60 days of the original application, subject to the statutory route.
International transfers	Apply the relevant current transfer framework. A Turkish standard-contract mechanism requires notification within five business days of signature. An IAF Memorandum is not itself a statutory transfer safeguard.
Breach notification in Türkiye	Apply Board Decision 2019/10 to unlawfully obtained data: notify the Board without delay and within 72 hours of awareness; notify affected persons in the shortest reasonable period after identification.

Official legal sources

[Regulation 2016/679 on protection of personal data](#)

[Personal Data Protection Law 6698 as amended](#)

[Board Decision 2019/10 on breach notification](#)

Annex D Document alignment and activation record

Controlled reference	Application
IAF-CON-001	Protect governance records, confidentiality and fair access. Retain institutional resolutions and proportionate election evidence according to their distinct purposes.
Membership Guide and Memorandum	Verify corporate authority and accession; distinguish contract acceptance from optional consent and the lawful basis for representatives' data.
Accreditation and Committees Guides	Protect technical evidence, competence records, declarations, minutes and independent decision access.
IAF-POL-004 and IAF-PR-019 / 020	This policy supplies detailed privacy, rights, incident and continuity controls alongside existing information-security rules.
IAF-POL-009 / 010 / 011 / 013	Apply restricted case handling, statutory clocks, minimal public claims and proportionate conflict declarations.
IAF-PR-018 / 024 / 028	Control providers, partnerships, research and cross-border exchanges.
IAF-FR-024 / 030 and IAF-RG-010 / 012	Use request, incident, hold, disposal, obligations and retention controls with the fields in this policy.

Before operational use

Record the actual controller and verified channels, appointed owners, processing inventory, lawful bases, notices, provider agreements, transfer controls and justified retention schedule. Complete any legally required officer, representative, registration or impact-assessment steps. Record approval and commencement without backdating.

Continuing control

The policy owner shall retain a release checklist and report incomplete operational controls to the competent authority with an action owner and deadline. Processing that lacks a lawful basis or required safeguard shall not begin merely because this policy has been published.