



FIRST EDITION / CORPORATE GOVERNANCE

DATA PROTECTION & PRIVACY POLICY

Aerospace Federation

PRIVACY BY DESIGN

LAWFUL INFORMATION FLOWS

ACCOUNTABLE DIGITAL SYSTEMS

Publication identity and use

Control field	Controlled value
Title / code	Data Protection & Privacy Policy / AF-PL-018
Edition / revision / language	First Edition / Revision 00 / English master text
Edition date	30 September 2026
Document owner	Information and Security Manager; designated privacy coordination function
Operating interface	P16 and P02; all AF processes, programs and information recipients
Institutional scope	Aviation, space, the whole defense industry, heavy and advanced industry, defense- and space-purpose mobility; all AF corporate and service activities.
Approval and effectivity	Actual authority, adoption, commencement, role holders and operating readiness shall be recorded through AF-FR-001 and AF-ML-001. The edition date is not approval evidence.
Relationship to existing files	Separate expanded policy. Existing AF source documents, prior policies and the final AF 9100:2026 files remain unchanged.
Distribution	Policy text may be published after authorized release. Completed case, declaration and personal-data records are protected according to their content.

Purpose-limited data. Protected rights. Accountable use.

This policy applies across governance, membership, committees, technical and assurance services, learning, events, awards, research, funding, partners, chapters and enabling functions. Requirements follow the actual relationship and lawful mandate; they do not create general authority over unrelated third parties.

Reading and implementation route

Read the numbered sections for requirements and responsibilities, then use the annexes for scope matrices, timelines, decision controls, communication models and records. The final annex identifies inherited AF requirements and the implementation controls added in this edition. Complete actual contacts, roles, approvals and jurisdiction-specific conditions before operational use.

“Shall” states a requirement following valid adoption; “should” states a recommendation; “may” states permission. Examples are synthetic. A template is evidence-capture space, not a completed approval or a factual public notice. Mandatory law and higher AF instruments retain their effect.

Contents

Clause and annex identifiers control references. Page numbers show where each section begins.

Section	Page
1 Purpose, principles and policy status	4
2 Scope, information and people	4
3 Applicable law and functional responsibility	4
4 Leadership, privacy coordination and independence	4
5 Processing inventory and lawful basis	5
6 Necessity, accuracy and permitted reuse	5
7 Transparency and consent	5
8 Sensitive information and children	6
9 Membership, governance and public registers	6
10 Assessment, education and professional evidence	6
11 Events, publications and communications	6
12 People, finance, grants and research	7
13 Privacy by design and impact assessment	7
14 Service providers and data-sharing arrangements	7
15 International access and controlled transfers	8
16 Information security and access control	8
17 Rights requests and response workflow	8
18 Limits, disputes and legitimate disclosure	8
19 Personal-data incidents and breach response	9
20 Retention, holds and defensible deletion	9
21 AI, profiling and emerging technology	9
22 Monitoring, training and assurance	10
23 Public notices, changes and operational release	10
Annex A Processing inventory and whole-federation map	11
Annex B Public privacy notice and purpose modules	12
Annex C Rights handling and protected disclosure workflow	13
Annex D Privacy screening and full impact assessment	14
Annex E Processor agreement — model terms and schedules	15
Annex F Data sharing and international-transfer review	16
Annex G Retention, holds and secure disposal	17
Annex H Breach assessment and communication pack	18
Annex I Jurisdiction, readiness and scenario checks	19
Annex J Source alignment, adoption and controlled release	20

1 Purpose, principles and policy status

1.1 Institutional commitment

Aerospace Federation shall process personal information lawfully, fairly, transparently and only for defined purposes, using necessary data, appropriate accuracy, justified retention, effective security and demonstrable accountability. These controls cover the entire federation, not only its website or assessment services. AF shall protect the people who participate in governance, membership, science, industry cooperation, education, events, awards, research, funding and independent assurance. Privacy shall be considered before information is collected or a system is selected, rather than added after a problem occurs.

1.2 Companion to existing AF controls

This policy expands AF-PL-005, AF-PL-006, AF-PR-014 and related record controls. It does not silently replace those files, alter the Constitution or amend AF 9100:2026. This is an internal operating policy with model notice and contract modules; it is not by itself a factual public privacy notice for every AF service. Actual controller identity, contacts, processing, providers, countries, legal bases and rights information shall be confirmed before a notice is published. Annex J distinguishes inherited duties from new policy controls.

2 Scope, information and people

2.1 Information within scope

Personal data means information relating to an identified or reasonably identifiable natural person, including identifiers, contact details, images, recordings, online identifiers, professional evaluations, communications and inferences. Pseudonymized data remains personal where re-identification is reasonably possible; removing a name does not necessarily anonymize a file. Confidential corporate and controlled technical information may need additional protection even when not personal. AF handling labels Public, Internal, Confidential and Restricted are not governmental security classifications.

2.2 Operational coverage

Apply the policy to employees, volunteers, officers, members, applicants, representatives, assessors, candidates, learners, researchers, donors, suppliers, witnesses, complainants and relevant visitors. Cover paper, email, devices, collaboration platforms, recordings, cloud services, spreadsheets, registries and AI-assisted work. Apply relevant controls to contractors and affiliated delivery under actual agreements. A separate chapter or partner does not automatically share AF's legal role; determine each party's responsibility from what it actually does.

3 Applicable law and functional responsibility

3.1 Jurisdiction-specific obligations

Identify the actual legal entity, establishments, people affected, locations, service targeting, processing types and transfers before determining applicable obligations. A non-profit purpose, foreign incorporation, a federation title or a business contact does not by itself establish a privacy-law exemption. The legal register shall record rights, response times, breach duties, sensitive-data conditions, child-related requirements, transfer mechanisms and any registrations or representatives required. Mandatory obligations prevail over a generic AF target. Do not claim worldwide compliance or acceptance merely because this policy exists.

3.2 Controller, processor and joint roles

A controller determines the purposes and essential means of processing; a processor acts on documented instructions for a controller. Joint decisions require an appropriate allocation of responsibilities and transparent contact arrangements. Determine the role per activity rather than assigning one label to every relationship. Where AF processes for another controller, it shall follow lawful instructions, escalate questionable instructions and provide agreed assistance. A service contract or accreditation MoU is not automatically an adequate data-processing agreement.

4 Leadership, privacy coordination and independence

4.1 Accountable functions

The Council shall provide resources and review material privacy risks. Process owners remain accountable for their actual processing. The Information and Security Manager shall maintain the inventory, controls, incident and rights workflow with a designated privacy coordinator and deputies. The Legal and Integrity Coordinator shall support jurisdiction, protected-case and transfer analysis. Procurement shall verify provider terms before access. Staff and contractors shall use only approved systems and report concerns promptly; a privacy coordinator does not absorb every owner's responsibility.

4.2 Officer designation and conflicting roles

Assess whether a legally designated data protection officer, representative or other specialist is required and record the actual decision. Do not represent the Information and Security Manager or another person as a statutory officer without a proper appointment. Where a data protection officer is appointed, preserve the independence, direct escalation, resources and protection required for that role; duties that determine processing purposes or means shall be checked for incompatibility. Use independent external expertise when internal competence or separation is insufficient.

5 Processing inventory and lawful basis

5.1 Purpose-by-purpose record

Before collection or a material change, record the activity, owner, data subjects, fields and sources, purposes, legal role, lawful basis, sensitive-data condition if needed, notices, recipients, providers, countries, retention, security, rights and decision effects. Separate administration, technical evaluation, publicity and marketing purposes. Annex A supplies the record and representative service map; illustrative entries do not certify that a particular live AF system or data flow exists. Review the inventory on change and at least annually, with actual owner confirmation.

5.2 Selecting and documenting the basis

Identify a valid basis for each purpose under applicable law. A contract basis concerns processing objectively necessary for the relevant individual's contract; a corporate member's employee is not automatically the individual contracting party. Legitimate-interest reasoning, where available, shall state the purpose, necessity, alternatives, balancing, reasonable expectations and safeguards. Identify the actual obligation when relying on law. Public-benefit language does not create a public-task mandate. Consent shall not be chosen merely to avoid checking whether it is freely given or appropriate.

6 Necessity, accuracy and permitted reuse

6.1 Minimum information

Collect the minimum needed for a defined decision or service. Verify identity proportionately; do not routinely retain full identity documents, health records, complete bank records, classified files or unrelated private correspondence. Limit free-text fields and attachment instructions where unnecessary sensitive material is foreseeable. Separate fact, allegation, opinion and inferred score; keep sources and corrections traceable. A form's ability to accept a field is not justification for collecting it.

6.2 Accuracy and new purposes

Correct material inaccuracies without rewriting authentic historical acts. Identify disputed information and preserve a lawful explanatory record where needed. Before using information for a new purpose, assess compatibility, legal basis, notice and any consent or other condition required. A public professional profile, directory or social-media post is not permission for unrestricted profiling, scraping, resale or AI training. Do not repurpose examination, whistleblowing, donor or member evidence for unrelated promotion.

7 Transparency and consent

7.1 Layered and accurate notices

Provide understandable information at the legally appropriate time, including when data comes from another source. State the actual responsible entity and contact, purposes, data categories and source where required, legal bases, recipients, transfers, retention, rights, complaint options and significant automated use. Explain mandatory versus optional fields and consequences of not supplying necessary information. Provide activity-specific layers for membership, events, remote assessment, personnel, research and protected reporting. Accessible language shall not obscure meaningful limitations.

7.2 Consent and choice controls

Where consent is used, make it specific, informed, demonstrable and freely given, using separate choices for distinct optional purposes. No pre-ticked boxes, misleading design or unnecessary bundling with membership or essential service. Record the wording, version, time, method and person's choice. Withdrawal shall be as straightforward as giving consent and shall stop the consent-based future use, while lawful prior use and independently justified necessary records are explained. Employment, power imbalance and children require special care; a signed generic waiver is insufficient.

8 Sensitive information and children

8.1 Additional safeguards

Sensitive categories, criminal allegations, health, biometrics, financial vulnerability and highly identifying information shall receive a specific legal-condition and necessity review, restricted access, justified retention and appropriate safeguards. General consent, encryption or a contractual confidentiality clause does not by itself satisfy all special conditions. Separate incidental support information from evaluation and selection files. Use the least intrusive reliable proof for a justified eligibility or safety need and avoid inferring sensitive attributes from photographs or unrelated records.

8.2 Young and vulnerable participants

Program owners shall assess age-related permissions, guardian authority, understandable notices, safeguarding and lawful data use for the actual jurisdiction and activity. This policy does not prescribe one universal age of digital consent. Verify age or authority proportionately without excessive identification. As AF protective defaults, prohibit behavioral advertising and unnecessary profiling of children in AF services, and do not publish identifying child information or images without the required lawful safeguarding and permission process. A child's privacy request requires a case-specific authority and best-interests assessment.

9 Membership, governance and public registers

9.1 Participation information

Collect identity, representative authority, affiliations, eligibility and contact information needed for the actual membership or governance process. Separate internal verification from optional public profiles, images and marketing permissions. Common-control and electoral checks shall use necessary information without disclosing a person's complete private relationships. Secret ballots require separation between credential validation and vote choice with an independently verifiable audit trail. Do not expose identifiable voting preferences through analytics or casual access logs.

9.2 Status verification and public accountability

Public registries shall show enough authentic scope, issuer, dates, status and restrictions to prevent misleading use without disclosing home addresses, private contacts, exam results or protected technical evidence unnecessarily. Public disclosure of constitutional officers and resolutions follows actual transparency and legal obligations, with appropriate minimization. A request to delete an expired or adverse status shall be considered lawfully but shall not be used to manufacture a false current history. Corrected public entries retain an appropriate protected decision lineage.

10 Assessment, education and professional evidence

10.1 Evidence and remote work

Assessment information shall be limited to the exact route, object, profile and necessary evidence. Control images of workplaces, staff, screens, documents and live feeds under AF-PL-015. Recording is not automatic: define purpose, necessity, permissions, alternatives, access and deletion. Do not require unrestricted access to a person's entire device or household to verify a bounded task. Restricted technical evidence may require authorized local review rather than transfer; record limitations honestly.

10.2 Learning and credentials

Keep attendance, assessed learning, examination evidence and independent personnel credentials distinct. Verify identity without unnecessary permanent copies; protect exam material and raw practical recordings. Publish only the necessary credential identity, scope and state under the actual program. Do not send individual performance to an employer, sponsor or training provider without a valid basis and appropriate notice. Learning analytics and remote proctoring shall be proportionate, tested and subject to privacy-risk review; intrusive automated surveillance is not a default.

11 Events, publications and communications

11.1 Attendance, images and sponsors

Explain registration, badge scanning, directory visibility, recordings, photography and partner access separately. A sponsorship or exhibitor fee does not buy the participant list. Offer meaningful alternatives to optional promotional photography where practicable and preserve safety-critical attendance needs without expanding publicity. Speaker materials, recorded sessions and professional biographies require rights and privacy review. Do not treat venue attendance as blanket consent to all future promotion or external reuse.

11.2 Marketing, cookies and audience measurement

Distinguish necessary service messages from optional marketing. Maintain lawful permissions and practical opt-out controls; retain minimal suppression information only to honor choices. As AF policy defaults, do not sell personal information, supply attendee/member lists for third-party marketing without a valid separate permission basis, or activate nonessential advertising/tracking without the required lawful choice. Inventory cookies, pixels, analytics, embeds and meeting bots; do not describe a system as cookie-free or anonymous without checking actual behavior. Honor applicable opt-out mechanisms.

12 People, finance, grants and research

12.1 Employment, payments and support

Limit personnel, volunteer, supplier, donor and payment information to legitimate administration, legal duties and fair review. Separate health/support, conflict, disciplinary and payroll records by access. Bank or identity details shall not be placed in committee packs unnecessarily. Grant and scholarship selection shall use relevant eligibility and merit evidence, protect vulnerable applicants and disclose any lawful publication of awards. Do not publish an unsuccessful applicant's financial or personal difficulties as a transparency measure.

12.2 Research and sector intelligence

Define research objectives, roles, lawful basis, participant information, ethics, rights, data access and retention before work. Distinguish genuine anonymization from pseudonymization and assess re-identification through linkage, rare attributes or small samples. Prefer justified aggregation and minimize source personal data. Open-science or sector-benefit aims do not authorize unrestricted disclosure. Controlled secondary use, data sharing or AI training requires its own assessment; a research label shall not conceal a new commercial purpose.

13 Privacy by design and impact assessment

13.1 Early screening

Screen new or materially changed services, registries, databases, platforms, AI models, tracking, biometrics, remote monitoring and cross-border arrangements before procurement or live use. Consider scale, sensitivity, vulnerable people, systematic observation, data linkage, decisions with significant effects, novelty and barriers to exercising rights. Identify both actual legal impact-assessment duties and wider AF risk controls. A small user count does not remove serious consequence; a high commercial value does not justify disproportionate collection.

13.2 Assessment and approval gate

A documented impact assessment shall describe processing and flows, necessity and alternatives, risks to individuals, safeguards, consultation or specialist advice, residual risk, responsible actions and approval. Annex D supplies the full module. Seek any mandatory prior authority consultation before processing; no Council signature substitutes for it. A residual high risk, missing legal basis or unresolved controlled-transfer duty blocks launch until validly resolved. Reassess after a material change or incident, not merely on a fixed calendar.

14 Service providers and data-sharing arrangements

14.1 Due diligence and written terms

Before a provider receives data, assess competence, security, location, access, subprocessors, incident handling, retention, return/deletion, audit evidence and exit continuity. Determine whether it is a processor, independent controller or joint controller. A processor agreement shall state subject, duration, nature, purpose, data/people, instructions, confidentiality, security, subprocessor permissions, rights/incident assistance, audit, lawful disclosure and end-of-service handling. Annex E provides model terms and schedules. Marketing promises or a generic quality certificate are not proof of appropriate protection.

14.2 Continuing oversight

Review material provider changes and assess actual performance at least annually according to risk. Require prompt notice and lawful approval of changes that alter purpose, region, recipients or safeguards. Control support engineer and privileged administrator access, not just server location. No provider may independently train a model, advertise, sell or reuse AF data beyond a lawful separately approved purpose. At exit, verify return, accessible records, deletion of unnecessary copies, subprocessor action and continuity of required history.

15 International access and controlled transfers

15.1 Whole-flow assessment

Map where information is stored, accessed, backed up, supported and further transferred, including remote assessors, translators and cloud administrators. Identify applicable export restrictions and privacy-transfer requirements separately. A recipient's country, a common corporate group or an AF MoU does not automatically supply a valid transfer mechanism. Assess actual legal safeguards, necessary contractual measures, destination risks and supplementary controls before access. Record any onward-transfer and government-access limitations.

15.2 No unsupported global access

Do not claim a particular adequacy, certification or other transfer arrangement is available without verifying its current scope and the actual recipient. Use justified localization, restricted remote access, encryption with appropriate key control, redaction or other lawful alternatives where necessary. If essential lawful access cannot be arranged, restrict the activity rather than quietly transfer the data. An ordinary user's consent shall not become a routine substitute for an otherwise required systematic transfer framework. Annex F records the decision and monitoring triggers.

16 Information security and access control

16.1 Protection through the lifecycle

Use named accounts, least privilege, appropriate multifactor authentication, secure transmission and storage, role separation, logging, patching, tested backups and recoverable records. Protect cryptographic keys and administrative access; do not share passwords or publish sensitive evidence in open links. Classify and restrict export-controlled material separately. Verify permissions before onboarding and revoke promptly on role change or exit. Review access quarterly under AF-PR-014. Systems shall prevent unauthorized edits to decisions and support documented correction history.

16.2 Operational precautions

Use approved devices and repositories, minimize local downloads, secure printouts and removable media, and verify recipients before sending sensitive material. Separate production data from development/testing; use synthetic or properly minimized data where possible. Screen attachments and restrict unauthorized bots, screen capture and integrations. Test restoration quarterly and wider continuity annually under AF-PR-015. A successful backup, hash or login proves only the specific control tested, not overall data accuracy or privacy compliance.

17 Rights requests and response workflow

17.1 Recognizing and verifying requests

Receive requests for information, access, correction, deletion, restriction, portability, objection, consent withdrawal and other applicable rights through accessible routes, without insisting on a specific form or legal wording. Verify identity or representative authority proportionately; a simple marketing opt-out shall not routinely require a copy of identity documentation. Record original receipt and immediately identify the applicable legal clock. Locate data across owners and providers without exposing unrelated third-party or controlled information. Annex C supplies the workflow and record.

17.2 Action, reasons and time

Respond without undue delay within the applicable legal period. As a new AF service target, acknowledge within five calendar days and ordinarily complete the response within 30 calendar days, always using an earlier mandatory limit where triggered. A one-calendar-month legal period must not be assumed to equal 30 days. Any extension, pause, fee or refusal must have a valid applicable basis, reasons and timely notice; ordinary complaint extensions do not automatically apply. Explain action, partial restrictions, review/authority options and secure delivery. No unresolved request shall be marked completed merely because it was acknowledged.

18 Limits, disputes and legitimate disclosure

18.1 Balancing rights and evidence

Evaluate third-party rights, reporter confidentiality, protected investigations, privileges, legal holds, technical records and mandatory transparency individually. Apply the narrow lawful restriction required, using redaction or meaningful summaries where appropriate rather than blanket refusal. A deletion right does not automatically erase a necessary authentic decision; a retention preference does not automatically defeat the right. Record the legal reason, minimum retained information, period and review route. A requester shall not be penalized for exercising a right.

18.2 Authority requests and independent remedies

Authenticate legal requests, authority and scope before disclosure; involve competent advisers and disclose only what is lawfully required or justified. Preserve notice to affected persons where lawful and appropriate. Do not invent privilege or assume every foreign order authorizes unrestricted transfer. Complaints about handling use AF-PL-017 without delaying a privacy deadline or preventing a direct complaint to a competent authority. Publish actual relevant external remedy information in the service notice after jurisdiction verification.

19 Personal-data incidents and breach response

19.1 Immediate escalation and containment

Anyone suspecting loss, alteration, unauthorized access or disclosure shall notify the designated incident route immediately and preserve evidence safely. AF-PR-015 governs containment and continuity. Record detection and organizational awareness separately, affected systems/people/data, scope, risk, controls and uncertainty. As an additional AF response target, the incident lead shall open a documented privacy triage within four hours of awareness where a personal-data incident is suspected; protective action and earlier duties occur sooner. This is an internal target, not a universal statutory deadline.

19.2 Notification and recovery decisions

Determine affected jurisdictions, controller/processor roles, reportability thresholds, recipients, legal deadlines and contractual/technical notifications immediately. A provider acting as processor shall notify the responsible controller without undue delay under applicable terms and law; it shall not wait for final proof or a board meeting. A 72-hour or other period applies only where the actual law imposes it, not to every AF incident worldwide. Notify affected individuals when required, document justified non-notification and provide phased updates where needed. Recovery shall reconcile lost decisions, access and rights requests before authorized restart.

20 Retention, holds and defensible deletion

20.1 Record-specific periods

Apply AF-SC-001 with the current Constitution, applicable scheme, law and actual necessity. Constitutional instruments and corporate resolutions remain permanent; necessary assurance and case evidence retain the applicable seven-year baseline and any justified longer duty. Incidental event information, routine logs, support details and unnecessary identity copies require different, often shorter treatment. Assign each record's trigger and review date. A blank blanket retention promise is not an adequate schedule. Annex G preserves inherited AF defaults and explains legal/necessity qualifications.

20.2 Deletion, backups and anonymization

Suspend disposal only for a scoped valid hold; review at least every six months and on material case change. Delete securely or genuinely anonymize when the purpose and lawful duties end, recording scope, authority and verification without retaining the very data supposedly deleted. Backups follow their documented recovery cycle; preserve required held records separately instead of freezing every backup indefinitely. On restoration, reapply deletions, objections and status corrections before use. Pseudonymization is not deletion and public-blockchain storage of personal evidence is not an acceptable default.

21 AI, profiling and emerging technology

21.1 Controlled assistance

AI may assist search, drafting, transcription, translation, anomaly detection and administration only within approved purposes, data terms and competent human review. Do not supply protected evidence to an unapproved external model or accept vendor reuse for model training by default. Assess re-identification, leakage, inaccurate inferences, discriminatory effects, prompt manipulation, model changes and the rights of affected people. Record tool/version and material inputs where needed to reproduce a consequential result.

21.2 Human accountability and limits

No system shall autonomously impose membership discipline, award a grant, certify competence, accredit a body or decide an appeal. Human review must have access to underlying evidence and real authority to reject the output, not be a rubber stamp. As AF protective defaults, do not infer emotions or credibility from faces/voices for case, exam or employment decisions, and do not use broad biometric surveillance without separately justified lawful necessity and impact review. Digital twins, sensor feeds and privacy-enhancing methods remain subject to real validation and data minimization.

22 Monitoring, training and assurance

22.1 Ongoing control

Train staff, volunteers, assessors, committee secretaries and contractors before relevant access and refresh after material change or demonstrated need. Review permissions quarterly, providers and inventory at least annually, high-risk changes before release and incidents promptly. Sample notices against actual processing, test rights workflows and verify deletion/restoration rather than rely on a policy acknowledgment. Use de-identified or synthetic cases for exercises. Independent audit under AF-HB-009 shall examine actual processing and unresolved risks across the full portfolio.

22.2 Measuring results

Quarterly review shall consider rights timeliness, unresolved high risks, excess access, incidents, provider failures, valid consent/choice records, retention exceptions, corrected registries and completed remedial actions. Record denominators, original clocks and missing data. Low breach numbers may reflect poor detection; a signed agreement is not proof of provider performance. Management review shall fund required controls and record rejected options and residual risk within lawful limits.

23 Public notices, changes and operational release

23.1 Controlled publication

The model in Annex B shall be completed with actual identity, activities, contacts, providers, locations and rights before public release. Do not claim a designated officer, secure anonymous platform, particular hosting country, absence of cookies, data-sale practice or universal legal compliance without verifying the facts. Policy commitments are requirements for future conduct; public descriptions must report actual operation accurately. Material purpose or recipient changes require review and appropriate notice or new permission before use.

23.2 Adoption and review

Record real adoption, effective use, role appointments, applicable-law review, notices, supplier agreements, data flows, rights channels, incident contacts and tested controls through AF-FR-001 and AF-ML-001. This edition does not modify older files or prove implementation. Review at least annually and after material legal, technical or operational change. Annex I provides the jurisdiction and launch register; Annex J records source alignment and additional controls.

Annex A — Processing inventory and whole-federation map

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

DP-A01 | Processing activity record

Field	Instruction and entry space
Identity and ownership	Activity ID, service/process, actual legal entity, owner, controller/processor/joint role and counterpart. Record: _____
People, data and sources	Affected categories, necessary fields, source, sensitive elements, actual volume/scale and systems. Record: _____
Purpose and basis	Each purpose, lawful basis, additional sensitive-data condition, necessity/alternatives and legitimate-interest analysis where relevant. Record: _____
Notice and choices	Actual notice/version/timing, mandatory/optional fields, consent record, withdrawal and opt-out behavior. Record: _____
Recipients and locations	Internal access, recipients, providers/subprocessors, storage/support/backup countries and transfer basis. Record: _____
Retention and security	Record class, trigger/period/justification, holds, deletion method, access, logging and recovery. Record: _____
Rights and impact	Applicable clocks, significant automated effects, screening/impact assessment, risks, controls and review triggers. Record: _____

Representative activities — confirm actual processing

Activity	Purpose-specific information boundary
Membership and governance	Eligibility, representatives and lawful participation; optional publicity kept separate; ballot secrecy preserved.
Assurance and professional credentials	Identity, scope, necessary evidence and status; restricted case data not exposed in public registry.
Academy, events and awards	Registration, assessment and safe delivery; sponsor marketing and images separately reviewed.
People, finance and procurement	Necessary engagement, payee, transaction and conflict records; no unnecessary sensitive information in general files.
Research and support	Protocol, participant rights, selection evidence and justified dissemination; separate research and marketing.
Protected cases and disputes	Minimal intake plus restricted identity/evidence, lawful response and remedies; no uncontrolled sharing.
Web, platforms and remote work	Service operation, authentic access and defined analytics; nonessential tracking and bots reviewed before activation.

Annex B — Public privacy notice and purpose modules

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

MODEL ONLY — complete all factual fields and obtain authorized review before public use. The policy does not establish the actual controller or contact details.

Responsible organization: “[Verified legal entity] is responsible for [specified activities] under [role]. Contact us at [verified privacy route/address]. [Actual officer/representative, only if appointed] can be contacted through [route]. This notice was issued on [date/version].”

Collection and purposes: “For [service], we process [necessary data categories], obtained from [you/identified source categories], to [distinct purposes]. Our lawful bases are [purpose-by-purpose basis]; [additional condition] applies to [sensitive category] where relevant. [Specified fields] are necessary for [reason]; [specified fields] are optional. Not providing necessary data may mean [actual consequence], not loss of unrelated rights.”

Recipients and transfers: “Authorized personnel and [actual provider/recipient categories, or names where required] receive [necessary information] for [purpose]. We use [actual locations and transfer safeguards]. Obtain relevant information through [route]. No unverified transfer status or blanket worldwide hosting statement is included.”

Retention and decisions: “We retain [record categories] for [verified periods or meaningful criteria], subject to [necessary legal/technical holds]. [Actual significant automated processing or meaningful human decision arrangement] is explained here, including effects and available challenge. Optional choices and withdrawal work through [actual method].”

Rights and complaints: “Depending on the applicable law, you may seek access, correction, deletion, restriction, portability, objection or other relevant rights. Submit through [actual accessible route]; we verify authority proportionately and apply [verified response framework]. You may complain through [internal route] or [appropriate authority information], without losing non-excludable remedies. Restrictions are explained case by case.”

Supplemental layer

Supplemental layer	Additional information to state
Events and media	Badge scanning, photo/recording areas, optional publicity, sponsor access, withdrawal and alternatives.
Remote assessment/exams	Data observed or recorded, necessity, identity method, proctoring limits, access and deletion.
Whistleblowing/conflicts	Separate identity custody, safe contact, limited disclosure, fairness and protected external reporting.
Research/children	Protocol and use, consent/guardian basis where needed, support, publication and future-use limits.
Website/marketing	Actual cookies/embeds, purpose and duration, consent or lawful exceptions, opt-out/suppression and contact.

Annex C — Rights handling and protected disclosure workflow

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Step

Step	Required record / decision
1 Receive	Original request/time, requested action, actual identity context and safe response route; no mandatory form.
2 Identify clock	Applicable jurisdiction and exact deadline, unit, trigger and authorized extension rules; separate AF service target.
3 Verify proportionately	Use existing reliable account/relationship evidence first; obtain only necessary additional proof.
4 Locate	Search relevant owners, email, databases, case systems, paper and processors; track scope and reasonable search.
5 Assess limits	Item-level third-party/privilege/hold/controlled-data analysis; narrow redaction or reasons instead of blanket refusal.
6 Decide and deliver	Authorized action, correction/deletion/restriction, accessible secure copy, reasons and actual remedy information.
7 Verify completion	Recipients/processors notified where required, changes completed, necessary proof retained and remaining actions tracked.

DP-C01 | Rights-request case

Field	Instruction and entry space
Request and authority	ID, original time/zone, substance, verified requester/representative and actual affected records. Record: _____
Deadline and search	Legal/source basis, initial due date, AF target, search owners/systems, results and limitations. Record: _____
Decision and grounds	Action by item, withheld parts and legal basis, extension/notice if valid, reviewer and independent complaint route. Record: _____
Delivery and follow-up	Date/method, recipient verification, completed system/provider actions and retention of minimum response evidence. Record: _____

Synthetic clock check: an assumed one-calendar-month obligation triggered on 31 January 2027 ends on 28 February 2027; a 30-calendar-day corporate target would end 2 March and cannot replace the earlier legal limit. This demonstrates date arithmetic only. Identify the actual applicable legal rule before using the example.

Annex D — Privacy screening and full impact assessment

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Screening prompts

Screening prompts	Risk/obligation to examine
Sensitive data, allegations or vulnerable people	Additional lawful conditions, imbalance, confidentiality, support and significant consequences.
Systematic tracking, biometrics or remote monitoring	Necessity, less intrusive alternatives, visibility, observation limits and access.
Linking datasets or generating profiles	Unexpected reuse, inferred sensitive traits, error, discrimination and re-identification.
Large scale, novel technology or significant decisions	Actual scale/context, model limits, human control, enforceable rights and cumulative harm.
International or restricted information flow	Recipient/location, transfer safeguards, controlled-access permission and onward disclosure.

DP-D01 | Impact assessment and release gate

Field	Instruction and entry space
System and objective	Project, owner, actual role, purposes, information flow, categories, people, locations and intended outcome. Record: _____
Necessity and alternatives	Why each use is needed; less intrusive options; proportionality; lawful basis and notice. Record: _____
Risk analysis	Threat/impact on individuals, likelihood and severity reasoning, uncertainty and vulnerable groups; do not reduce to a commercial score. Record: _____
Controls and validation	Minimization, access, choice, security, retention, model limits, tests, responsible owners and evidence. Record: _____
Consultation and residual risk	Specialist/officer advice, people's views where appropriate, reasons for departures and mandatory authority consultation if required. Record: _____
Approval and follow-up	Actual competent approval, unresolved launch blockers, due actions, review triggers and demonstration of effectiveness. Record: _____

Release requires a valid purpose and legal basis, necessary information, appropriate safeguards, workable rights and transfer arrangements, and all mandatory prior processes completed. An unresolved high privacy risk shall not be accepted merely to meet a launch date.

Annex E — Processor agreement — model terms and schedules

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

MODEL TERMS. Incorporate into the actual contract after role and jurisdiction review. These terms do not fill missing party identity, instructions or a legally required transfer instrument.

Clause

Clause	Required model obligation
1 Scope and instructions	The Processor shall process only the subject matter, duration, nature, purposes, personal-data categories and persons specified in Schedule E-A and on documented lawful Controller instructions, including transfers.
2 Confidential personnel	The Processor shall restrict access to authorized competent personnel bound by confidentiality and record relevant training and role changes.
3 Security	The Processor shall implement and maintain the measures in Schedule E-B, appropriate to risk, and promptly address material weaknesses without reducing agreed protection unilaterally.
4 Subprocessors	The Processor shall use only authorized subprocessors under the agreed specific/general written authorization process, give required change notice, allow the agreed response, impose equivalent duties and retain responsibility required by law/contract.
5 Rights assistance	The Processor shall promptly forward relevant requests and assist the Controller through agreed secure methods within the time needed for legal compliance; it shall not independently decide the Controller's response without authority.
6 Incident assistance	The Processor shall notify the Controller of a personal-data breach without undue delay and provide known scope, effects, measures and progressive updates; waiting for a final investigation is not permitted.
7 Assessments and consultation	The Processor shall supply necessary information and assistance for impact assessments, required consultation and evidence-based security/processing reviews.
8 Audit and accountability	The Processor shall make necessary compliance information available and permit proportionate agreed audits/inspections, protecting unrelated clients without defeating meaningful assurance.
9 Legal requests and unlawful instruction	The Processor shall inform the Controller of binding disclosure demands where lawful and of an instruction it considers unlawful; resolve or stop affected processing rather than silently broadening use.
10 Purpose restrictions	The Processor shall not sell, advertise with, independently profile or train reusable models on the data unless a separate lawful, expressly approved arrangement permits a defined new role/purpose.
11 Return and deletion	At service end, return or delete as instructed, including unnecessary copies/subprocessor data, except a verified law requires retention; document restricted lawful retention and deletion verification.
12 Continuity and changes	Preserve required records and access through exit, incident or reorganization. Material changes to locations, controls or uses require the agreed review and cannot silently defeat Controller obligations.

Required schedules

Field	Instruction and entry space
E-A Processing instructions	Real parties/roles, purpose, nature, duration, subject categories/data, authorized instructions and contacts. Record: _____
E-B Security and service	Measures, incident contacts/clocks, audit evidence, recovery, deletion and rights assistance. Record: _____
E-C Locations and subprocessors	Actual entities, access/support/storage/backup locations, authorization process, transfers and onward controls. Record: _____

Annex F — Data sharing and international-transfer review

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

DP-F01 | Recipient and transfer decision

Field	Instruction and entry space
Actual flow	Exporter/importer, legal roles, data/purpose, source and destination, support/backup/remote access and onward recipients. Record: _____
Applicable duties	Privacy and controlled-technology obligations, required permissions, verified current mechanism/scope and legal review. Record: _____
Risk and safeguards	Necessary data, government-access concerns where relevant, encryption/key control, redaction, localization, access/logging and enforceability. Record: _____
Recipient evidence	Due diligence, actual contract, subprocessor list, security/incident record, rights assistance and retention/exit. Record: _____
Approval or hold	Competent owner/legal authorization, exact allowed scope, remaining restrictions and next review. Record: _____
Change triggers	New recipient, country, purpose, system/model, law, incident or expired safeguard; action before continuing affected transfer. Record: _____

Examples: a local server with an overseas support engineer can still involve international access; an assessor viewing a live screen may receive personal or controlled data without downloading a file; an anonymized aggregate requires a real re-identification assessment. These examples are not a finding about AF's current infrastructure.

A sharing agreement shall identify roles, purpose, necessary information, notice/basis, rights handling, security, transfers, retention, breach responsibilities, disclosure to authorities, review and exit. Do not label a genuine independent controller as a processor simply to avoid its responsibilities.

Annex G — Retention, holds and secure disposal

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Inherited AF schedule — apply law and necessity

Class / information	AF baseline / qualification
R01 publications / R02 constitutional acts	Publication lineage and constitutional/corporate resolutions retained permanently under the applicable current instruments; incidental data separated.
R06 assurance evidence	At least 7 years after last relevant decision where AF 9100/AF-SR-001 applies; longer technical/legal needs recorded.
R08 contracts, projects and partnerships	Default 7 years after the latest relevant closure, final decision or contract end, subject to actual necessity/law.
R09 protected cases, complaints and disputes	Necessary evidence 7 years after closure/last related decision; not every irrelevant personal attachment.
R10 incidental event/learning administration	Up to 24 months after completion where justified; assessed credentials and financial evidence follow their proper classes.
R11 routine security/access logs	12 months if justified; material incident decisions 7 years after closure; sensitive raw data reviewed separately.
R12 audit, risk and review	Default 7 years after action/cycle closure, extended for justified continuing duties.
R13 research and safety knowledge	Approved public outputs permanent; raw study data default 5 years after closure only if lawful/necessary or another justified protocol period.
R14 backups	Rolling 90-day AF recovery baseline; isolate specific held records rather than retain all backup sets indefinitely.

DP-G01 | Hold or disposal action

Field	Instruction and entry space
Scope and authority	Record IDs/classes, trigger, purpose, current obligation, hold authority or disposal approval. Record: _____
Review and method	Holds reviewed at least every six months/on change; deletion/anonymization method, providers/backups and verification. Record: _____
Completion	Actual action/date, responsible person, exceptions, necessary proof, reapplication after restore and remaining custody. Record: _____

The table preserves selected existing defaults; it is not a universal legal retention schedule or a new period for all personnel/member data. Apply the full AF-SC-001 and current Constitution to the actual record.

Annex H — Breach assessment and communication pack

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

DP-H01 | Incident and notification record

Field	Instruction and entry space
Detection and awareness	Actual timestamps, reporter, suspected/confirmed facts, controller/processor role and secure response team. Record: _____
People, data and risk	Known/estimated scope, categories, sensitivity, countries, recipients, confidentiality/integrity/availability effects and uncertainty. Record: _____
Containment and evidence	Immediate measures, logs/originals preserved, competent responders and affected linked services. Record: _____
Legal clocks and decisions	Each jurisdiction, threshold, trigger, recipient/deadline, contractual/technical clock, notification or documented reason not to notify. Record: _____
Notices and updates	Minimum factual notice, actual delivery/receipt, affected-person advice, safe channel, outstanding facts and update dates. Record: _____
Recovery and correction	Verified restored data/access, reconciled status/requests, root cause, owners, effectiveness and authorized restart. Record: _____

Model individual notice: “We identified [confirmed incident] affecting [necessary categories] during [period]. The possible consequences are [bounded risks]. We have taken [actual measures]. You should consider [appropriate protective steps]. Contact [verified route] for support. [Specified facts] remain under investigation; updates will be provided through [route].” Do not include another person’s data, exploitable details or unsupported attribution.

The four-hour triage target is an added AF internal control; it does not replace without-undue-delay duties or any applicable 24-hour technical, 72-hour legal or other verified obligation. An outage does not suspend the obligation to assess reportability.

Annex I — Jurisdiction, readiness and scenario checks

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

Deployment requirement

Deployment requirement	Evidence required before relevant use
Actual legal entity and roles	Verified Controller/Processor identity, jurisdictions, contact/representative/officer requirements and authority.
Legal-clock register	Rights, complaints, breach and mandatory notice clocks with exact triggers, extensions and competent owner.
Notice and choice	Final activity-specific notice, actual optional choices, cookie/marketing behavior and withdrawal test.
Protected systems and providers	Real data inventory, access, agreements, transfers, secure handling and verified backups.
Rights and deletion rehearsal	Synthetic request, mixed evidence redaction, processor search, correction/deletion, hold and restore.
Privacy-risk gates	Completed screening, high-risk impact review, necessary prior approvals and recorded launch restrictions.
Children and sensitive data	Task necessity, proper conditions, safeguarding/permissions and minimal information.
Future changes	Monitor legal commencement dates, new tools/providers, uses and significant incidents; do not rely permanently on an old legal snapshot.

Scenario checks: a sponsor asks for an attendee list; a respondent requests a whistleblower identity; a remote assessment records a private room; a model provider changes its training terms; a records system restores deleted profiles; a statute gives a shorter request period than the corporate target. Each requires a recorded purpose, lawful basis, minimum information, actual independent review where needed and an appropriate action or hold.

Operational contact and legal-clock fields are deliberately uncompleted facts, not omitted policy rules. They must be populated from real AF arrangements; do not manufacture a Data Protection Officer, live portal, recipient or regulator contact.

Annex J — Source alignment, adoption and controlled release

NORMATIVE CONTROLS; EXAMPLES AND MODEL ENTRIES ARE INFORMATIVE

This annex distinguishes established AF requirements from the additional implementation controls authored for this policy. It does not amend a source document, authenticate a historic approval or establish that a reporting channel, appointed officer or digital service is already operating.

Inherited AF requirements and interfaces

Source	Preserved requirement / implementation interface
AF-CON-001 Articles 22, 24, 26–28	Lawful processing, independent remedies, authentic records, protected disclosure and accountable automation.
AF-PL-005/006; AF-PR-014/015	Purpose/minimization, handling classes, actual legal clocks, quarterly access/restoration checks and continuity.
AF-SC-001; AF-GD-003; AF-FR-021/022	Record classes, lawful holds, access/disposal, incident and recovery evidence.
AF-SR-001; AF-PL-015; AF 9100:2026	Exact public status, protected technical evidence, remote assessment and unchanged scheme requirements.

Additional controls in this edition

Control	Nature and approval boundary
Five-day acknowledgment / ordinary 30-day privacy service target	New AF service choices; earlier actual law controls, lawful extensions are separately documented.
Four-hour documented privacy-incident triage target	New internal response target, not a worldwide statutory deadline or permission to delay immediate protection.
No sale; limited optional marketing/tracking; child and AI defaults	New protective operational rules after adoption; actual public statements must still match verified practice.
Inventory, impact-assessment, notice and processor models	Expanded implementation controls; jurisdiction-specific legal conditions remain separately verified.

Controlled AF references: AF-CON-001; AF-QM-001; AF-ML-001; AF-PL-005; AF-PL-006; AF-PL-013; AF-PL-015; AF-PL-016; AF-PL-017; AF-PL-019; AF-PR-001; AF-PR-004; AF-PR-014; AF-PR-015; AF-PR-019; AF-HB-009; AF-GD-003; AF-SC-001; AF-FR-001; AF-FR-021; AF-FR-022; AF-SR-001; AF 9100:2026. Use the applicable current effective version. Where an older corporate instruction conflicts with the Constitution, record the conflict and complete the required controlled change; this file does not silently rewrite the earlier file. AF 9100:2026 remains unchanged.

Adoption and implementation record

Field	Instruction and entry space
Exact text	Record AF-PL-018, Data Protection & Privacy Policy, First Edition, Revision 00, 30 September 2026 and the approved file identity. Record: _____
Authority and approval	Identify actual approving organ/delegation, decision, reviewers, date and authenticated signatories. Record: _____
Commencement and transition	Enter the real effective date; affected contracts, rights, documents and pending cases; notices and transition actions. Record: _____
Owners and channels	Identify competent role holders/deputies, independent escalation, actual monitored contacts and operating hours. Record: _____
Readiness evidence	Record training, secure access, channel/record tests, case rehearsal and remaining restrictions. No fictitious test result. Record: _____
Master List and review	Add the proposed entry only through AF-FR-001 and AF-ML-001; assign next review and implementation checks. Record: _____

Proposed Master List entry: AF-PL-018 | Data Protection & Privacy Policy | Policy | First Edition | Revision 00 | 30 September 2026 | Approval/effectivity: enter actual record. R01 publication lineage; completed records follow their substantive record classes. Existing Master List and source files remain unchanged by delivery of this policy.