ISO/IEC 27018:2025, Information security, cybersecurity and privacy protection: Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors (3rd edition, 2025-08)

PII protection in the public cloud

36 requirements. There is no accredited certificate for this standard. As of 07/2026.

ISO/IEC 27018 is not a management system standard but a set of guidelines with extended controls on top of ISO/IEC 27002:2022. There is no standalone accredited certificate against ISO/IEC 27018. The controls are taken into the Statement of Applicability of an ISO/IEC 27001 system, and the certificate is then issued against ISO/IEC 27001 with a reference to ISO/IEC 27018. The standard addresses the provider of a public cloud service that processes personally identifiable information on behalf of its cloud service customers. An organization that merely consumes cloud services does not take on that role and should sensibly assess the requirements against its providers, not against itself. For Leanshift this checklist is therefore above all a supplier assessment grid. Every point can be put to the provider as a question and secured through the data processing agreement under Article 28 GDPR. The outcome of such an assessment is an internal conformity record or a provider rating profile, not a certificate. On numbering: clauses A.2 to A.12 follow the privacy principles in Annex A of the standard, items numbered like A.11.6 are the additional controls listed there. Items numbered like 8.10 or 5.34 refer to controls from ISO/IEC 27002:2022 that the standard makes specific for the cloud. Items carrying the suffix (Grundsatz), meaning principle, are derived from the principle of the clause itself, where Annex A carries no dedicated additional control.

Company	Date	Prepared by

A.2 Consent and choice 2

A.2.1 **The cloud service provider supports the cloud service customer in meeting the rights of data subjects, such as access, rectification, erasure and objection. Responsibilities and deadlines are set out contractually.** Document

What proves it: Evidence is the data processing agreement under Article 28 GDPR with a clause on assistance with data subject rights, together with the technical means inside the service itself: export, correction and deletion features, or a documented support procedure with a response deadline. Question to the provider: which feature or process do you offer so that we can serve an access or erasure request within one month?

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.2 (Grundsatz) **Personally identifiable information belonging to cloud service customers is processed only on the customer's documented instructions. Obtaining consent from data subjects remains the task of the customer as controller, and the provider does not pre-empt that.**

What proves it: Evidence is the instruction clause in the data processing agreement plus proof that the provider makes no secondary use of the data, for example the privacy notice of the service and the product documentation. Question to the provider: do you process our customer data in any way outside our instructions, for instance for product improvement or model training?

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.3 Purpose legitimacy and specification 2

A.3.1 **The purpose for which the provider processes personally identifiable information is limited to delivering the agreed service and is named in the contract. No processing for the provider's own purposes takes place.** Document

What proves it: Evidence is the data processing agreement stating subject matter, nature, purpose and duration of the processing as well as the categories of data subjects under Article 28(3) GDPR. Question to the provider: please supply the contract annex that describes the processing purpose exhaustively. For small organizations the provider's standard data processing addendum is sufficient, provided it contains this information.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.3.2 **Personally identifiable information entrusted to the provider is not used for advertising, marketing or other commercial purposes of the provider without prior express consent. Delivery of the service is not made conditional on such consent.**

What proves it: Evidence is an explicit contract clause ruling out commercial secondary use, together with the terms of service. Question to the provider: confirm in writing that customer data is not used for advertising, profiling or the training of AI models. Where that commitment is missing, the service is unsuitable for personally identifiable information.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.4 Collection limitation 1

A.4 (Grundsatz) **Beyond the data the customer puts into the service, the provider collects no further personally identifiable information for its own purposes, such as telemetry, usage profiles or content analysis. Operational data and metadata that are collected are named and justified.**

What proves it: Evidence is a list of the data the service records alongside content data (access logs, telemetry, diagnostic data) with purpose and retention period, plus a screenshot of the setting that turns optional telemetry off. Question to the provider: which usage, telemetry and diagnostic data do you collect in addition, what do you use it for, and can we switch the collection off?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5 Data minimization 2

A.5.1 **Temporary files created while processing personally identifiable information, such as scratch storage, caches or rollback journals, are securely erased within a defined period.**

What proves it: Evidence is an operating or deletion procedure with a stated retention period for temporary data, backed by the system configuration, for example a cache TTL or a scheduled clean-up job with its execution log. Question to the provider: after what period are caches, temporary files and intermediate states deleted, and how is that monitored?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

8.11 **Wherever operations, testing or support do not require live data, personally identifiable information is masked, pseudonymized or anonymized. The volume of data processed stays limited to what the service actually needs.**

What proves it: Evidence is a ruling on which environments may see live data, plus screenshots or scripts of the masking used in test and development systems. Question to the provider: do your support and development teams work with production data, and if so, under which safeguards? For small organizations it is enough to have a rule that test systems run exclusively on generated sample data.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.6 Use, retention and disclosure limitation 3

A.6.1 **Where the provider receives a legally binding request to disclose personally identifiable information, for example from a public authority, it informs the cloud service customer beforehand, as far as the law permits.**

What proves it: Evidence is a contractual notification clause and an internal process for authority requests with a named owner. Question to the provider: do you notify us before handing over data, and do you publish a transparency report on requests from authorities? A current transparency report is strong evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.6.2 **Where the provider discloses personally identifiable information to third parties, it records the event so that it can be traced: who received the data, when it happened, which data was involved and on what basis the disclosure rests.** Document

What proves it: Evidence is a disclosure register or ticket history carrying those fields, even if it holds no entries. An empty but maintained register is acceptable and is the practical route for small organizations. Question to the provider: do you keep a register of data disclosures, and can we obtain extracts from it?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

8.10 **Personally identifiable information is deleted once the agreed retention period expires or the contract ends, including copies held in backups after their rotation cycle.**

What proves it: Evidence is a deletion concept with retention periods per data category, the backup retention period and a deletion log or deletion confirmation. Question to the provider: how long does our data live on in your backups after termination, and do we receive written confirmation of its deletion?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.7 Accuracy and quality 2

A.7 (Grundsatz) **The provider does not alter the personally identifiable information entrusted to it on its own initiative. Corrections and updates are made solely on the instruction of the cloud service customer or through features the customer operates itself.**

What proves it: Evidence is the editing features of the service together with their change history, plus the instruction clause in the data processing agreement. Question to the provider: can we correct records ourselves, and is every change logged so that it can be traced?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

8.13 **The integrity of personally identifiable information is protected in storage, in transmission and on restore. Backups exist and their restorability has been tested.**

What proves it: Evidence is the backup configuration, checksum or integrity mechanisms, and at least one documented restore test per year with date and result. Question to the provider: how often do you test restores, and what recovery time do you commit to in the service level?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8 Openness, transparency and notice 2

A.8.1 **The use of subcontractors that process personally identifiable information is disclosed before the contract is concluded. Changes to the list are notified to the customer in good time, so that the customer can object or terminate.** Document

What proves it: Evidence is a current list of subprocessors, published or made available contractually, with name, country and processing purpose, plus a notification rule under Article 28(2) GDPR. Question to the provider: where do we find your subprocessor list, how much advance notice do you give on changes, and how can we object?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8 (Grundsatz) **Before the contract is concluded, the provider makes available understandable information on how personally identifiable information is processed, which safeguards are in place and in which jurisdictions the processing happens.**

What proves it: Evidence is the privacy notice, a security whitepaper, a trust center page and the data processing agreement including the technical and organizational measures as an annex. Question to the provider: please supply the current list of technical and organizational measures as a contract annex, not just marketing material.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.9 Individual participation and access 2

A.9 (Grundsatz) **The service gives the cloud service customer the technical means to serve access, rectification and erasure requests from data subjects on its own, for example through export, search and deletion features.**

What proves it: Evidence is the product documentation of the export and deletion features, backed by an internal trial run: work through one access request end to end and note how long it takes. Question to the provider: can we find, export and delete all data on a single individual without your support?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.34 **Where the customer cannot handle a data subject request itself, the provider assists within an agreed period. Requests that data subjects send directly to the provider are passed on to the customer rather than answered by the provider.**

What proves it: Evidence is the corresponding clause in the data processing agreement with a concrete response deadline, plus a support ticket history as a real example. Question to the provider: what deadline do you commit to for assistance with data subject rights, and what does it cost?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.10 Accountability 4

A.10.1 **Breaches involving personally identifiable information are reported to the cloud service customer without undue delay, stating the scope, the data affected, the cause and the measures taken. A notification process with responsibilities and deadlines is defined.** Document

What proves it: Evidence is the incident response plan with its escalation chain, the contractual notification deadline (24 to 48 hours works in practice, so that the customer can still meet the 72 hour deadline under Article 33 GDPR) and records of past incidents or of an exercise. Question to the provider: within what period do you report an incident, through which channel, and which information do you supply with it?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.10.2 **Security policies, operating procedures and the related records are retained for a defined period, so that the processing can be reconstructed after the fact.** Document

What proves it: Evidence is a retention rule with the version history of the policies, for example through a document register or a version control system carrying the approval date. Question to the provider: how long do you keep policy versions and the related records, and do we get access to them in the event of an audit?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.10.3 **A defined arrangement exists for the return, transfer and destruction of personally identifiable information at the end of the contract, naming formats, deadlines and the treatment of copies.** Document

What proves it: Evidence is the exit clause in the data processing agreement plus a deletion confirmation after the contract ends. Question to the provider: in which format and within what period do we get our data back, when are all copies destroyed, and do we receive written confirmation?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.35 **The effectiveness of the safeguards is reviewed independently at regular intervals, for example through internal audits, penetration tests or third party assurance reports. Results are made available to the cloud service customer in a suitable form.**

What proves it: Evidence is an ISO/IEC 27001 certificate with a Statement of Applicability that includes the ISO/IEC 27018 controls, or a SOC 2 report, together with current penetration test summaries. Question to the provider: please supply the certificate, its scope and confirmation that ISO/IEC 27018 is reflected in the Statement of Applicability. Check whether the scope really covers the service you use.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11 Information security 13

A.11.1 **Everyone with access to personally identifiable information is bound to confidentiality, whether employed directly or engaged externally.** Document

What proves it: Evidence is signed confidentiality agreements or undertakings that remain in force after the engagement ends. Question to the provider: are all staff and service providers with data access bound to confidentiality in writing?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.2 **Printouts and other paper copies containing personally identifiable information are created only where strictly necessary. The permitted extent is governed by a rule.**

What proves it: Evidence is a rule on handling printouts, which in data centers is typically a blanket ban on printing in areas holding customer data. Question to the provider: is customer data printed at all in your operations, and if so, under what conditions?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.3 **Restores from backups are authorized in advance and logged, including the person who triggered the restore and the data affected.** Document

What proves it: Evidence is the restore log with timestamp, originator and scope, usually produced automatically by the backup tool. Question to the provider: do you log every restore, and can we inspect those logs in the event of an audit?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.4 **Storage media carrying personally identifiable information that leave the premises are protected against unauthorized access and loss, as a rule through encryption and a transport record.**

What proves it: Evidence is proof of encryption (full media encryption), transport and handover records, and a media inventory. Question to the provider: do media carrying customer data ever leave your sites, for instance for backups, and how are they protected in transit?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.5 **The use of unencrypted portable media and devices for personally identifiable information is prohibited or limited to justified exceptions with documented approval.**

What proves it: Evidence is a removable media policy plus technical enforcement, for example enforced device encryption or USB ports blocked through device management. Question to the provider: can staff copy customer data onto unencrypted devices, and what prevents that technically?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.6 **Personally identifiable information transmitted over public networks is encrypted. The mechanisms in use reflect the current state of the art.**

What proves it: Evidence is the TLS configuration (current protocol version, no outdated ciphers) and an external configuration test as a report. Practical for small organizations: run a free TLS scan once a year and file the result. Question to the provider: which transport encryption do you enforce, and is encryption at rest active?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.7 **Paper records containing personally identifiable information are destroyed in a way that rules out reconstruction.**

What proves it: Evidence is shredders of an adequate security level or destruction certificates from a service provider working to DIN 66399 or an equivalent standard. Question to the provider: how do you destroy paper records relating to customers, and are destruction certificates on file?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.8 **User IDs are assigned uniquely to one person and are neither reissued nor shared. Shared accounts exist only in justified exceptions and with additional traceability.**

What proves it: Evidence is a user list from the identity system free of group accounts, together with the rule that administrative work is carried out under a personal account. Question to the provider: does your operations staff work with personal accounts, and is multi-factor authentication mandatory?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.9 **The provider can state at any time which persons or roles are allowed to access personally identifiable information, and keeps that overview up to date.** Document

What proves it: Evidence is an access rights overview by role, backed by a recurring access review with date and result. For small organizations a half-yearly export of the user list, signed off, is enough. Question to the provider: how many of your staff can access our data, and how often do you review that?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.10 **User accounts are managed across their whole life cycle: creation, modification and prompt deactivation when someone leaves or changes role.**

What proves it: Evidence is an onboarding and offboarding procedure with a checklist, plus logs of deactivated accounts with timestamps. Question to the provider: within what period do you withdraw access from staff who leave, and how do you evidence that?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.11 **The security and privacy obligations of the provider are fixed contractually, including the technical and organizational measures, the binding effect of the customer's instructions and the customer's right to audit.** Document

What proves it: Evidence is the signed data processing agreement under Article 28 GDPR with the annex of measures and an audit or information right. Question to the provider: please supply the signed data processing agreement including its annexes, not merely a reference to general terms of service.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.12 **Subcontractors that process personally identifiable information are subject to at least the same obligations as the provider itself. Their selection and ongoing monitoring is governed by a defined process.**

What proves it: Evidence is the flow-down of obligations in the contracts with subcontractors (Article 28(4) GDPR) and a supplier assessment carrying a date. Question to the provider: how do you assess your subcontractors, and which evidence do you require from them?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.11.13 **Before storage space is reused, it is ensured that no data of previous users remains accessible, neither on physical media nor in virtualized environments.**

What proves it: Evidence is the sanitization or overwrite procedure applied when storage is released, records of media destruction, and the tenant separation described in the architecture document. Question to the provider: how do you ensure that reused storage holds no residual data from other customers?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.12 Privacy compliance 3

A.12.1 **The countries in which personally identifiable information is stored and processed are named and known to the cloud service customer. Changes to the storage locations are notified.** Document

What proves it: Evidence is the provider's overview of sites and regions, in the contract or in the documentation, plus a screenshot of the region setting of the service in use. Question to the provider: in which countries does our data sit at rest, from which countries is it accessed, for example in support, and can we pin the region?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.12.2 **Transfers of personally identifiable information to third countries are known, justified and covered by appropriate safeguards.** Document

What proves it: Evidence is standard contractual clauses or an adequacy decision, backed by a transfer impact assessment, which for small organizations may be short: data categories affected, destination country, risk, additional measures taken. Question to the provider: on which legal basis do you transfer data to third countries, and which supplementary measures do you apply?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.31 **The legal and contractual requirements applying to the processing of personally identifiable information are identified and kept current as the legal situation changes. Conflicting jurisdictions are assessed.**

What proves it: Evidence is an overview of the applicable requirements (GDPR, national rules, sector specific duties) with an owner and a review date. In a small organization a one page list reviewed annually is enough. Question to the provider: are you or your subcontractors subject to jurisdictions that allow authorities to access our data, and how do you deal with that?

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification