Privacy and security by design

Just Software ApS · Approved · GDPR / personal data

Version	v1.3	**Approved on**	2 November 2026
Approval authority	CISO or CTO	**Next review due**	2 November 2027
Last reviewed	2 November 2026	**Review interval**	365 days
Relevant frameworks	—		

Privacy and security by design

Purpose, scope, and users

• Purpose: Make sure privacy and security are built into our products from the start.
• Scope: All new products and services, and major changes to existing ones.
• Users: Developers, product owners and security reviewers.

How security is implemented in code, pipelines and testing is defined in the Software development policy. This policy defines what each product must decide and document.

A. Risk assessment and requirements

• Start each new product or major change with a privacy and security risk assessment, using the Risk assessment methodology.
• Based on it, document for each product:
  • the personal data it collects and why, and whether that is proportionate to the service;
  • the privacy and security requirements it must meet;
  • the privacy by design strategy or strategies chosen (section B).
• Requirements are captured as acceptance criteria in Azure DevOps. The chosen strategy and key decisions are recorded in an ADR.
• Reassess when there are major changes.

B. Privacy by design

We choose at least one strategy per product:

• **Minimise and limit:** collect as little personal data, and as few types of it, as the service needs. Show only the personal data needed in the user interface. Pseudonymise or anonymise where possible (see the Anonymisation of support data procedure). Set a maximum retention time and delete personal data when it is no longer needed.
• **Separate and hide:** keep personal data in separate stores and combine it only when needed. Use opaque identifiers so that data cannot be linked across systems. Encrypt data in transit and at rest (see Encryption Standards). Give access only to those whose job requires it.
• **Aggregate:** use group-level data instead of individual records where possible, and no more precision than the purpose needs.

Privacy by default:

• Privacy-friendly settings are the default. Optional data sharing and optional features that process personal data (for example AI features) are off until the customer or user turns them on.
• We do not use browsing, profiling or usage data to track users, and we do not reuse information about other sites they visit.
• When we change privacy settings, existing settings are set to the most protective level.
• Consent is only asked for what the service actually needs, and the product works in full if the user declines optional processing.

C. Security by design

- **Attack surface:** for each new product or major change, map the attack surface across network, functionality and access rights, and remove what is not needed.
- **Secure defaults:** products are delivered with the highest reasonable security level as default.
- **No weakening by users:** users should not be able to lower security. If a product allows it, the reason and any compensating controls are documented in an ADR.
- **Least privilege:** users, services and integrations get only the access they need.

Records or evidence

- Per-product requirements and chosen privacy strategy (ADRs, acceptance criteria)
- Risk assessments for new products and major changes
- Attack surface mapping
- ADRs for default settings and any user-adjustable security settings
- Results of the privacy and security defaults check

Developer Habits

- Always apply at least one privacy strategy per product
- Make privacy-friendly and secure settings the default
- Never let users lower security without a documented decision
- Never give more access than needed

Recurring Tasks for Security Roles

Privacy and security defaults check

- Description: Before major releases, and at least yearly, check that default settings protect privacy and security
- Frequency: YEARLY
- Security roles: CISO

Product privacy and security review

- Description: Review the per-product requirements, chosen strategies and attack surface mapping. New products and major changes are reviewed when they occur.
- Frequency: YEARLY
- Security roles: CISO