Finnish Social and Health Data Permit Authority ver. 29.05.2026

FORM B – Assessment of the Information Security and Data Protection of the Processing Environment

Instructions

The requirements in this form concern the information security and risk management of another secure processing environment in accordance with the EU General Data Protection Regulation and Section 18 of the Secondary Use Act.

The assessment under this form focuses on the technical and organisational structures of the processing environment that ensure the secure and controlled implementation of personal data processing in accordance with the data permit decision.

This form relates to the assessment of a processing environment pursuant to Section 51 c of the Secondary Use Act where, based on the preliminary assessment carried out in Form A, it has been determined that the conditions are met to assess another secure processing environment.

Answer each item "Yes" or "No". "Additional information" is completed only where necessary, for example if the answer is "No" or if the implementation deviates from the standard. Each item specifies the required annex, which must be provided as a separate attachment to this form. The annexes are listed below.

- **Annex 1:** Architecture, segregation of the processing environment and network restrictions
- **Annex 2:** Description of access management (initial identification, MFA, granting/termination of access rights)
- **Annex 3:** Restrictions on data export (copying)
- **Annex 4:** Logging (content, protection, monitoring)
- **Annex 5:** Information security management (roles, risks, monitoring, response, deletion of the dataset)
- **Annex 6:** DPIA summary concerning risks related to the processing environment

Provide only the requested information in the annexes and indicate at the end of this form which annexes you submit.

If the processing environment is located **outside the EU/EEA**, also complete "**Additional Part C – Third Country**" at the end of the form.

1 Information on the future controller of the dataset

Organisation: _____
Business ID / identifier:_____
Contact person (management / responsible):_____
Email: _____
Phone: _____
Data Protection Officer / contact point: _____
Information Security Officer / CISO / equivalent: _____

2 Basic information on the target processing environment

Name of the processing environment: _____
Location: ☐ Finland ☐ EU/ETA (country: _____) ☐ Outside the EU/EEA (country: _____)
Administrator / service provider:_____
Contact details: _____

3 Self-assessment (Phase B) – Yes / No + annex reference

B1 Information security management (GDPR Articles 5(2), 24 and 32; Section 18 of the Secondary Use Act)

Section 18 of the Secondary Use Act requires that sufficient information security in the processing of personal data be ensured through risk management and by complying with the regulations and instructions of the authority responsible for the implementation and supervision of information security and data protection.

The General Data Protection Regulation additionally requires that the controller implements appropriate technical and organisational measures and is able to demonstrate compliance with the Regulation in the processing of personal data. Information security management ensures the systematic and continuous fulfilment of these requirements.

B1.1 Ownership and responsibilities (management + operational)

Required annex: Annex 5
Condition: The processing environment has a designated owner and defined information security responsibilities.

☐ Yes ☐ No

Additional information:

B1.2 Information security management system / risk management model

Required annex: Annex 5
Condition: The organisation / service provider responsible for the processing environment has an information security management system (ISMS) or a corresponding risk-based model in place.

☐ Yes ☐ No

Additional information:

B1.3 Incident management and notification

Required annex: Annex 5
Condition: Detection, response and notification of incidents are instructed and assigned, and the administrator of the processing environment has the capability to notify the controller without delay of suspected processing contrary to the terms of the data permit.

☐ Yes ☐ No

Additional information:

B1.4 Vulnerability management

Required annex: Annex 5
Condition: The processing environment is protected against malware and vulnerability management is in place.

☐ Yes ☐ No
Additional information:

B2 Restriction of access in accordance with the data permit (GDPR Articles 5(1)(c) and 32; Section 18 of the Secondary Use Act)

Section 18 of the Secondary Use Act requires that appropriate access control is implemented and that particular attention is paid to the enforcement of usage restrictions.

Under the General Data Protection Regulation, processing must be limited to what is necessary for the purpose, and access to personal data must be prevented where it is not justified.

Access control ensures that personal data are processed only to the extent necessary and only by persons for whom such processing is necessary.

B2.1 Reliable initial identification

Required annex: Annex 2
Condition: Users' identities are reliably verified before access to the dataset is granted.

☐ Yes ☐ No

Additional information:

B2.2 Multi-factor authentication (MFA) prior to access to datasets

Required annex: Annex 2
Condition: A personal user ID and MFA are required before access to datasets (a justified exception may be possible in a secured-area model).

☐ Yes ☐ No

Additional information:

B2.3 Access rights in accordance with the data permit only

Required annex: Annex 2
Condition: Access rights to the dataset are granted only to persons specified in the data permit and in accordance with the principle of least privilege.

☐ Yes ☐ No

Additional information:

B3 Data protection: isolation and prevention of export (GDPR Articles 5(1)(f) and 32; Section 18 of the Secondary Use Act)

Section 18 of the Secondary Use Act requires that sufficient information security is ensured so that data are not used or disclosed contrary to their intended purpose and that confidentiality obligations are fulfilled.

The GDPR correspondingly requires protection against unauthorised or unlawful processing.

To fulfil these requirements, the processing environment must be technically isolated and unauthorised export or transfer of personal data must be prevented.

B3.1 Protection of network connections

Required annex: Annex 1
Condition: The processing environment is separated from other networks so that the dataset is not exposed to threats via network connections.

☐ Yes ☐ No

Additional information:

B3.2 Prevention of data export (copying)

Required annex: Annex 3
Condition: Users are prevented from exporting personal data from the environment in violation of the data permit.

☐ Yes ☐ No

Additional information:

B3.3 Encryption in transit and key management (where necessary)

Required annex: Annex 1
Condition: Traffic over public or less protected networks is encrypted and key management is in place.

☐ Yes ☐ No

Additional information:

B4 Logging and traceability (GDPR Articles 5(2), 24 and 32; Section 18 of the Secondary Use Act)

Section 18 of the Secondary Use Act requires active monitoring of personal data processing. The GDPR requires accountability, i.e. the ability to demonstrate lawful processing.

Logging and traceability enable monitoring, verification of compliance with permit conditions, and detection and investigation of incidents and misuse.

B4.1 Minimum content of logs

Required annex: Annex 4
Condition: Logs enable, at a minimum, traceability of user-specific logins and logouts in the processing environment.

☐ Yes ☐ No

Additional information:

B4.2 Protection and regular monitoring of logs

Required annex: Annex 4
Condition: Logs are protected as sensitive data and monitored regularly.

☐ Yes ☐ No

Additional information:

B4.3 Logs available upon request

Required annex: Annex 4
Condition: Logs can be provided to the data permit authority upon request without undue delay.

☐ Yes ☐ No

Additional information:

B5 End of the data permit: termination of access and deletion of the dataset (GDPR Article 32)

Personal data may be retained in identifiable form only as long as necessary. This requires that access is terminated and data are deleted or rendered unusable when processing ends.

B5.1 Automatic termination of access upon expiry of the data permit

Required annex: Annex 2
Condition: Access to the dataset is terminated when the data permit expires.

☐ Yes ☐ No

Additional information:

B5.2 Deletion of the dataset within a defined period and verifiability

Required annex: Annex 5
Condition: Datasets are securely deleted within a defined period and deletion produces a verifiable record/report.

☐ **Yes** ☐ **No**

Additional information:

B6 Data Protection Impact Assessment (DPIA) (GDPR Articles 35 and 89; Section 18 of the Secondary Use Act)

A DPIA is required where processing is likely to result in a high risk. It identifies risks and determines measures to ensure compliance with usage restrictions, confidentiality and the protection of data subjects.

B6.1 DPIA for the processing environment

Required annex: Annex 6
Condition: A DPIA in accordance with Article 35 GDPR has been carried out for the processing environment.

☐ **Yes** ☐ **No**

Additional information:

4 Annexes

Select the annexes submitted. **Note: Provide only information relevant to the description.**

☐ Annex 1 Architecture, segregation of the processing environment and network restrictions
☐ Annex 2 Description of access management (initial identification, MFA, granting/termination of access rights)
☐ Annex 3 Restrictions on data export (copying)
☐ Annex 4 Logging (content, protection, monitoring)
☐ Annex 5 Information security management (roles, risks, monitoring, response, deletion of the dataset)
☐ Annex 6 DPIA summary concerning risks related to the processing environment

5 Declaration by the future controller

The recipient of the decision (the controller under the data permit) undertakes to comply with the technical and organisational arrangements concerning the processing environment described in this Form B and its annexes throughout the validity of the data permit, insofar as they are approved in the data permit decision.

The recipient undertakes to ensure that processing takes place only in the approved processing environment and that the required level of protection is maintained continuously.

The recipient undertakes to notify Findata in advance of any material changes that may weaken information security or affect risk management, access control, monitoring, logging, data export, subcontractors or the location of the processing environment. Such changes require prior approval by Findata. If not approved, the data permit may be revoked.

We confirm that the information provided is correct and up to date. We undertake to comply with the restrictions of the data permit, protect the dataset, prevent unauthorised export, terminate access and delete the dataset upon expiry of the data permit.

Place and date: _____

Name, title (management): _____

Signature / electronic confirmation: _____

ADDITIONAL PART C – THIRD COUNTRY (if applicable)

Complete if the processing environment is located outside the EU/EEA.

Transfer outside the EEA requires a valid GDPR transfer mechanism, a case-by-case assessment and, where necessary, supplementary safeguards.

C1 TIA and supplementary safeguards

Condition: The effectiveness of the transfer mechanism has been assessed case by case by the controller and supplementary safeguards have been identified/implemented where necessary.

☐ Yes ☐ No

Additional information:

C2 Subcontractors and onward transfers

Condition: Subcontractors and onward transfers have been identified and managed by the controller (locations and agreements).

☐ Yes ☐ No

Additional information: