Product: GDPR-sovelluskirjasto

Last edited 01.09.2023

Basic information

Who gave the information? *

MET-1-1.1

Please state in which role you provide the product information.

Manufacturer/service provider

Brief introduction of the product

MET-1-2.1.

Briefly describe the product in English.

Sovelluskirjasto.fi / GDPR-library EU is Due Diligence tool for software buyers. We offer you as a software vendor possibility to maintain gdpr-information of your product in the library.

Introduction page (if any)

MET-1-3.1

https://sovelluskirjasto.fi/

1-5 categories describing the product.

System management and support programs, Data management and processing

1. The product's general terms and conditions

Is there an age limit for users in the service?

GEN-1-3.1

No

Country of manufacture/home country of the service provider *

GEN-1-5.1

Suomi

ISO certifications

GEN-1-6.1

ISO certifications granted to the manufacturer (27001, 27701).

Blank/not answered

Is there a mobile app for the service?

GEN-1-7.1

Blank/not answered

License type GEN-1-8.1

Named user

Is virtualization possible? GEN-1-9.1

No

Service-specific Privacy Notice (if any) GEN-2-1.1

https://www.sovelluskirjasto.fi/en/privacy-policy/

Data security description of the service (if any) GEN-2-2.1

Blank/not answered

Contact information of the data protection officer GEN-2-3.1

Blank/not answered

Are there advertisements or links to commercial services in the service? * GEN-2-4.1

If the service contains commercial content, describe in more detail what and for what age the commercial content is intended.

No

Does the service use cookies for which users' consent is asked? GEN-2-5.1

Consent is required for so-called non-necessary cookies, which may be related, for example, to tracking by third parties. On the other hand, cookies related to login and service functions do not require separate consent.

No

2. User management (end users)

Is the service used with personal usernames? UMA-1-1.1

If there are parts of the service that require logging in, are personal usernames and passwords used for them?

Yes

Are there at least two user levels in the user management of the service: administrator and end user? UMA-1-2.1

Having at least two user levels means that it is possible to have administrators in the service who can manage the usernames and access rights of other users.

No

Additional information

Customers who have signed an agreement get basic user rights to the service.

Can access rights be limited according to the employees' job duties, taking into account the rights of different user groups? UMA-1-3.1

The responsible controller must be able to control system access rights in accordance with the roles and tasks of users.

No

Additional information

There is no need to limit users' access rights in the service.

What options does the service have to integrate user management into the organization's centralized user registry and single sign-on (SSO)? UMA-1-4.1

If necessary, provide additional information about the integration possibilities.

Blank/not answered

Additional information

SSO integration is coming later.

Is it possible to log in with usernames of other service providers? UMA-1-5.1

Is it possible to log in to the service with e.g. Google, Microsoft, Facebook or Apple ID's?

No

Can multi-factor authentication (MFA) be used for logging in? UMA-1-6.1

No

Is strong user authentication possible? UMA-1-7.1

Is it possible to obtain strong identification from users of the service, for example, using an electronic identity card or banking IDs?

No

Are comprehensive log data about the activities of all logged-in users saved? * UMA-2-1.1

The responsible controller must ensure that the necessary log information is collected about the use of information systems and the disclosure of information from them, if the system requires logging in.

Yes

Is every access to personal data saved in a log? UMA-2-2.1

Is information stored in the log, for example, if the administrator views the information of other users?

Yes

3. Technical data protection

What kind of integrations (interfaces) are involved in the system and how are they protected from outsiders? * TDP-1-1.1

The responsible controller must implement the transfer of protected data in the data network using an encrypted or otherwise protected data transfer connection or method. Data transfer must be arranged in such a way that the recipient is verified or identified securely before the transfer of protected data.

The service has a REST API. Use of the interface requires the conclusion of an agreement and a customer-specific password. An encrypted network connection is used for data transfer.

Does all personal data processing in the service take place in such a way that the network connection is encrypted and the user or the parties to the data transfer are verified? TDP-2-1.1

When confidential information is transferred in information networks, the data is encrypted with an encryption solution that has no known vulnerabilities and supports modern encryption strengths and settings. In addition, the recipient is verified or identified in a sufficiently secure manner before the transfer of protected data. The requirement applies to both functions intended for users and interfaces in the service.

Yes

Is it possible to use the service so that all personal data is stored only in encrypted form? TDP-2-2.1

For example, is the personal data stored in the database in an encrypted form instead of the data being in plain language? In addition, it is required that the data intended for decryption (encryption keys) be kept separately from the stored data.

No

Is the data content of the service backed up at least once a day and is it possible to restore the backup quickly if necessary? * TDP-3-1.1

The verification and recovery processes are designed and implemented in such a way that they meet the requirements of data protection legislation regarding data integrity and usability.

Yes

Can multi-factor authentication (MFA) be required on all users at login? TDP-4-2.1

Requiring multi-factor authentication means that the service can be configured to require every user to activate it.

No

Are security updates for software components related to the service installed regularly without any delay? TDP-5-1.1

Yes

Has data security been audited by an external party? If so, by whom? * TDP-5-2.1

The responsible controller must ensure that appropriate data security measures have been implemented in the information system being used.

No

Are regular data security and vulnerability tests performed on the service? TDP-5-3.1

The resilience and usability of information systems essential to the performance of the duties of the responsible controller must be ensured by sufficient testing on a regular basis.

Yes

Additional information

The data security of the server is regularly monitored.

4. Data protection

What role does the service provider give itself in terms of data security? DPR-1-2.1

With regard to the personal data it processes, the service provider shall determine whether it acts as a controller, a joint controller or only as a processor of the client organization.

For the role of controller

Is it possible to make the name of the client organization and a link to its own privacy notice visible to users in the service? DPR-1-4.1

Users of the service should always see which entity is the controller related to the service, and it should provide information about the processing of personal data.

No

Does the service provider have access to personal data stored by the client organization? * DPR-1-5.1

Is the personal data stored in the service in such a form that the service provider has access to it? Are there other functions in the service that result in the service provider getting access to personal data?

Yes

Additional information

The service provider creates user accounts for the customer's employees and manages them.

Does use of the service generate a register of which the service provider is a joint controller with the client organization? DPR-1-6.1

No

Is a personal data register of users generated for the service provider of which it is the controller? DPR-1-7.1

Yes

Additional information

The service provider creates user accounts for the customer's employees and manages them.

Does the service provider have, for each sub-processor, an up-to-date list of sub-processors of personal data, which shows the name, location, processing purpose and possible grounds for transfer outside the EU/EEA area? * DPR-1-8.1

The responsible controller must receive information about all processors related to the service. in the processing of data, only processors that implement adequate protective measures should be used.

Yes

Link to the list of sub-processors (if any) DPR-1-9.1

Blank/not answered

Does the service provider or one of its sub-processors process personal data outside the EU/EEA area? DPR-1-10.1

The service provider has identified the international transfers of personal data outside the EU/EEA area related to its operations and the grounds for transfer used for them, and has ensured that the transferred personal data is guaranteed, by the legislation of the third country or by the supplementary protection measures used, a level of personal data protection that essentially corresponds to the level of EU data protection legislation.

Yes

Additional information

In Macedonian co-operation firm

If personal data is processed outside the EU/EEA area, on what grounds is personal data transferred? DPR-1-11.1

Standard clauses adopted by the Commission (Article 46:2(c) and Article 46:2(d))

Additional information

Personal data is primarily processed within the EU/EEA area only. Personal data may, however, be transferred outside the EU/EEA especially if a services provider we use is located outside the EU/EEA.

If personal data were to be transferred outside the EU/EEA to a country that is not included in the EU Commission's decision on an adequate level of data protection, we will make sure that the processing, transfer and storage of your data is carried out on the grounds required by law and with adequate protection mechanisms, such as using the standard contract clauses confirmed by the EU Commission.

Can personal data be transferred to non-secure third countries such as the United States? * DPR-1-12.1

Non-secure countries refer to countries whose authorities may have access to personal data, or whose legislation does not guarantee the same level of data protection as the EU data protection legislation.

No

What personal data does the service provider process? * DPR-2-1.1

List of registered groups and types of personal data to be processed.

Company name (employer)

Name of the person
Email address
Username and password
Log history of data entries and edits in the service, mainly: (1) who entered/edited data, (2) entries/edits made, (3) time stamp – this data is collected to ensure reliability of data in the service
Customary contact and billing details required for billing and invoicing paid services
Customary correspondence with users

Is the service also intended for processing special personal data (e.g. health data)? * DPR-2-2.1

Is the service specifically designed for the processing of special personal data referred to in the EU General Data Protection Regulation?

No

Can the required and optional fields related to users be defined by the administrator? DPR-2-3.1

Yes

Does the service provider provide users with comprehensive information about the processing of personal data in the service? DPR-2-4.1

Yes

Does the service provider process personal data in accordance with data protection legislation? * DPR-2-5.1

Service provider's own declaration of the product's GDPR compliance.

Yes

What procedures are in place to ensure that data is not used for other purposes? DPR-2-6.1

The service provider must process personal data only for purposes according to the DPA agreement and the instructions given by the controller.

Blank/not answered

Does the service have a function for pseudonymizing personal data? DPR-2-7.1

No

Is there profiling, scoring or evaluation of people in the functions of the service? DPR-2-10.1

Related to the need to do an impact assessment.

No

Are users' location data processed? * DPR-2-11.1

Related to the need to do an impact assessment.

No

Can the service define the retention periods of personal data or its criteria? * DPR-2-12.1

It must be possible to define the period for which the personal data are processed.

No

Additional information

The customer must inform the service provider when the data of its employees must be deleted.

Can users' personal data be anonymized instead of deleted? DPR-2-13.1

No

Has the service provider identified, in its privacy policy, all personal data that is clearly related to the use of the service? DPR-3-1.1

The controller and the service provider must identify all the personal data they process.

Yes

Does the service provider guarantee that the rights of the data subjects are realized in accordance with the EU General Data Protection Regulation (GDPR)? * DPR-4-1.1

Assurance given by the service provider about the safeguarding of the rights of data subjects, such as verification and rectification of data.

Yes

Additional information

The service provider uses personal data of the customer's employees only in accordance with the agreement and GDPR.

How and when are personal data deleted? * DPR-4-4.1

It must be possible to define the period for which the personal data are processed.

The customer must inform the service provider when the data of its employees must be deleted.

5. DPA Agreement

Is it possible to enter into a data processing agreement agreement (DPA) with the service provider? * DPA-1-1.1

The controller must enter into an agreement with the processor that meets the requirements of the EU General Data Protection Regulation.

No

Link to standard template for a DPA agreement (if available) DPA-1-2.1

Blank/not answered

Is the personal data to be processed specified in the DPA? DPA-1-3.1

Not answered

Are the purposes of personal data processing specified in the DPA? DPA-1-4.1

The processor shall process personal data only for the purposes according to the DPA agreement and the instructions given by the controller.

Not answered

In connection with the DPA, is it possible to give instructions that the service provider must taken into account when processing personal data? DPA-1-5.1

The controller must issue instructions regarding the processing of personal data and ensure that personal data is processed in accordance with them.

Not answered

Does the DPA stipulate that the service provider is responsible for the confidentiality obligation of its employees? DPA-1-6.1

The DPA agreement must ensure the confidentiality of personal data processing.

Not answered

Does the DPA stipulate that the service provider allows monitoring and auditing by the controller? DPA-1-7.1

Requirement of the EU General Data Protection Regulation for a DPA agreement.

Not answered

Does the service provider have a designated contact person for data protection issues? DPA-1-8.1

Not answered

Is deletion of data defined in the DPA? DPA-1-9.1

When the processing of personal data ends, the service provider is responsible for deleting the data or returning it to the controller.

Not answered

If sub-processors are used in the processing of personal data, is compliance with the EU's General Data Protection Regulation (GDPR) and the implementation of sufficient protective measures ensured in the contract? DPA-2-1.1

The service provider must only use processors that implement adequate protective measures in accordance with the EU's General Data Protection Regulation.

Not answered

Sub-processors under the DPA agreement or a link to the list of sub-processors (if any) DPA-2.2.1

Blank/not answered

The service provider undertakes to report all data security breaches without any delay DPA-3-1.1.

The service provider must notify the controller in writing of a personal data breach without undue delay after becoming aware of it.

Not answered

Does the processor or any of its sub-processors process personal data outside the EEA? * DPA-4-1.1

The service provider must identify the international transfers of personal data outside the EU/EEA area related to its operations and the grounds for transfer used for them, as well as ensure that the transferred personal data is guaranteed a level of personal data protection, in the legislation and practices of the third country, that essentially corresponds to the level of the EU's General Data Protection Regulation.

No

Additional information

There is no DPA agreement for the service

If personal data is processed outside the EEA, on what grounds is personal data transferred? DPA-4-2.1

A legal ground for transfer is required for the transfer of personal data outside the EU/EEA area.

Not answered

If the EU Commission's Standard Contractual Clauses (SCC) are used as the grounds for the transfer of personal data, which standard clauses are they? DPA-4-3.1

Standard clauses on data transfers to third countries (Article 46) on the Commission's website: Standard clauses for data transfers to third countries https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Not answered

Can personal data be disclosed to the authorities of a third country? * DPA-4-4.1

If personal data is transferred outside the EU/EEA to a country where the authorities can access the personal data, the controller must assess whether so-called supplementary safeguards are needed.

No

If data is transferred outside the EU/EEA area, does the service provider have documentation that helps in assessing the effects of data transfer (transfer impact assessment, TIA)? DPA-4-5.1

If personal data is transferred outside the EU/EEA, the controller must assess whether so-called supplementary safeguards are needed. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Not answered

If data is transferred outside the EU/EEA area, what additional protection measures are used? DPA-4-6.1

Blank/not answered

gdpr@sovelluskirjasto.fi