

Verwerkersovereenkomst (DPA)

Laatst bijgewerkt: 1 oktober 2026 · gegenereerd op 02 oktober 2026

Dit document is beschikbaar in het Engels.

Preamble

This DPA supplements the framework agreement ("Agreement") between Logicc GmbH ("Logicc") and the Customer, which refers to this DPA (Logicc and the Customer together are the "Parties"). This DPA automatically enters into force upon conclusion of the Agreement and applies from the same date as the Agreement.

In the context of fulfilling the Agreement, Logicc processes the Personal Data provided by the Customer. The parties agree that Logicc processes such Personal Data on behalf of the Customer, either as a Processor if the Customer is the Controller, or as a Subprocessor if the Customer is itself a Processor. Therefore, this DPA applies if and to the extent that Logicc processes Personal Data for the Customer in the course of providing Services under the Agreement. The parties agree that this DPA replaces all existing data protection provisions that the parties have previously agreed in connection with the Services.

1. Definitions

1.1 "Customer Data" means all Personal Data uploaded in connection with the use of the Services, retrieved from connected third-party systems or processed when triggering actions in those systems on behalf of the Customer, and processed by Logicc on behalf of the Customer in the course of providing the Services.

1.2 "Controller" is the person or company that determines the purposes and means of Processing Personal Data.

1.3 "Processor" is the person or company that processes Personal Data on behalf of a Controller.

1.4 "Data Protection Laws" means all Data Protection Laws applicable to the Processing of Personal Data. For the EU and the EEA, this includes, in particular, the General Data Protection Regulation (GDPR) and the e-Privacy Directive 2002/58/EC, as well as the local laws of the member states on data protection.

1.5 "EEA" means the European Economic Area.

1.6 "EU" is the European Union.

1.7 "Personal Data" means any information relating to an identified or identifiable natural person.

1.8 "Processing" has the meaning specified in the GDPR and includes any operation or set of operations performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, distribution, or otherwise making available, alignment or combination, restriction, or erasure of Personal Data.

1.9 "Security Incident" means any unauthorized or unlawful breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

1.10 "Services" has the meaning set forth in the Agreement.

1.11 "SCC" means the standard contractual clauses for the transfer of Personal Data to third countries contained in the Annex to Commission Implementing Decision (EU) 2021/914 of June 4, 2021.

1.12 "Subprocessor" means any Processor engaged by Logicc to assist in the provision of the Services.

2. Subject matter of this DPA

2.1 This DPA sets out the rights and obligations of the parties in relation to the Processing of Customer Data by Logicc in connection with the provision of the Services.

2.2 For this purpose, the Customer hereby appoints Logicc as a Processor if the Customer acts as a Controller, or as a Subprocessor if the Customer itself acts as a Processor.

2.3 This DPA applies to all Customer Data as specified in Appendix 1 to which Logicc has access during the provision of the Services. This includes Customer Data provided to Logicc by the Customer for the provision of Services, Customer Data generated by Logicc during the provision of Services, or Customer Data to which Logicc gains access in other ways, e.g., directly from data subjects, in the course of providing Services. This DPA does not apply to data that is not considered Customer Data, including non-personal data provided by the Customer or data that is not processed as part of the Services.

3. Principle of processing on behalf of the Customer

3.1 Logicc takes appropriate technical and organizational measures to ensure that the Processing of Customer Data complies with the requirements of applicable Data Protection Laws and that the rights of data subjects are protected.

3.2 The Processing of Customer Data by Logicc and, where applicable, commissioned Subprocessors generally takes place within the EEA. Transfers of Customer Data to a third country outside the EEA only take place if Logicc ensures compliance with the requirements of applicable Data Protection Laws and if such transfers are supported by an appropriate legal basis, such as an adequacy decision, SCC, or other applicable safeguards.

3.3 The Customer is solely responsible for the legality of the Processing of Customer Data and for safeguarding the rights of the data subjects in the relationship between the parties. Should third parties assert claims against Logicc due to the Processing of Customer Data in accordance with this DPA, the Customer shall indemnify Logicc against such claims.

4. Customer's right to issue instructions

4.1 Customer Data covered by this DPA will only be processed in accordance with documented instructions from the Customer, including instructions for the transfer of Customer Data to a third country. If Logicc is required by applicable law to process Customer Data without such instructions, Logicc will inform the Customer of the legal obligation prior to Processing, unless such notification is prohibited by law for reasons of public interest.

4.2 The Customer's right to issue instructions regarding the nature, scope, and procedures for Processing Customer Data is limited to the scope specified in this DPA and in the Agreement. If Logicc agrees to any instructions beyond this scope, the Customer shall reimburse Logicc for the associated costs and expenses.

4.3 The Customer shall issue their instructions in writing, by email (in text form), or by using the

functionalities of the Services.

4.4 Logicc may not use Customer Data for purposes other than the provision of the Services. This restriction does not apply to backup copies that are necessary to ensure proper Processing, or to data that is retained to comply with statutory retention obligations, or to anonymized or aggregated data that cannot be re-identified and is used exclusively for internal business purposes, such as analysis or service improvements. Customer Data and any anonymized or aggregated data derived from Customer Data will not be used to train AI models.

5. Subprocessors

5.1 Logicc will not engage any Subprocessors without the prior written consent of the Customer, which may be given either as individual consent or as general consent.

5.2 The Customer hereby grants its consent to the engagement of the Subprocessors listed in Appendix 2 with effect from the date of this DPA.

5.3 The Customer also grants its general authorization for the engagement of additional Subprocessors. Logicc shall inform the Customer of any intended changes to the list of Subprocessors, including the addition or replacement of a Subprocessor, at least 15 days before a new Subprocessor first processes Customer Data and shall give the Customer the opportunity to object to such changes. The Customer may object in writing on reasonable grounds within 15 days following notification, and the parties shall cooperate in good faith to resolve the objection.

5.4 If Logicc engages a Subprocessor to perform certain Processing activities on behalf of the Customer, Logicc shall impose on the Subprocessor the same data protection obligations as set out in this DPA. This shall be done by means of an agreement or other legally binding instrument in accordance with applicable Data Protection Laws, ensuring that the Subprocessor provides sufficient guarantees, in particular the implementation of appropriate technical and organizational measures to comply with the requirements of the GDPR and other applicable Data Protection Laws. The contracting parties clarify that it is sufficient if the level of protection offered by the Subprocessor corresponds to the level of protection provided for in this DPA.

5.5 If Logicc's engagement of Subprocessors is subject to Articles 44 et seq. GDPR, Logicc shall, where necessary, conclude the applicable SCC and ensure that its Subprocessors take appropriate technical and organizational measures to ensure compliance with applicable Data Protection Laws.

5.6 In the event that the SCC become invalid or are otherwise no longer recognized as a valid data transfer mechanism under the GDPR or other Data Protection Laws, Logicc may resort to any alternative guarantee permitted under Data Protection Laws, such as binding corporate rules (BCR) or other appropriate safeguards or exemptions permitted under Chapter V of the GDPR or equivalent Data Protection Laws.

5.7 If a Subprocessor fails to comply with its data protection obligations, Logicc shall be liable to the Customer.

5.8 The commissioning of a third party to provide ancillary services (e.g., telecommunications, maintenance, user support, cleaning, testing, or disposal of data carriers) does not constitute the commissioning of a Subprocessor. However, Logicc shall ensure that appropriate legal agreements are in place and control measures are taken to protect the security and confidentiality of Customer Data when third parties provide such ancillary services.

5.9 Connection to third-party systems authorized by the Customer via open interfaces (including the

Model Context Protocol) takes place on behalf of the Customer and using the Customer's access credentials. Data flows between the Platform and the connected third-party system, including actions triggered in that system, are instructed by the Customer. Operators of such third-party systems are not Subprocessors of Logicc to the extent that the Customer maintains its own contractual relationships with them. The Customer is responsible for the lawfulness of processing in the third-party systems and for the data protection grounds for access.

6. Customer's control rights

6.1 Logicc undertakes to provide, upon written request from the Customer and within a reasonable period of time, the information necessary to demonstrate compliance with the obligations under this DPA.

6.2 The Customer or an auditor appointed by the Customer may verify Logicc's compliance with this DPA. Audits shall be conducted during regular business hours and in a manner that causes as little disruption as possible to Logicc's operations.

6.3 Logicc may provide current audit certificates, reports, or excerpts thereof from independent bodies (e.g., auditors, data protection officers, IT security departments, or data protection auditors) or suitable certifications from recognized IT security or data protection audits as evidence of compliance with this DPA.

7. Confidentiality obligation

7.1 Logicc shall ensure that all persons authorized to process Customer Data within the scope of this DPA are bound to confidentiality, either by contractual obligations or by statutory confidentiality obligations.

8. Technical and organizational measures

8.1 Taking into account the state of the art, the implementation costs, and the nature, scope, context, and purposes of the Processing, as well as the varying likelihood and severity of risks to the rights and freedoms of data subjects, both the Customer and Logicc shall take appropriate technical and organizational measures within their respective areas of responsibility to ensure a level of protection appropriate to the risk, in particular with regard to Security Incidents.

8.2 The technical and organizational measures taken by Logicc are listed in Appendix 3. The Customer confirms that these measures meet the requirements and ensure an appropriate level of protection for the Processing of Customer Data.

8.3 Logicc is entitled at any time to replace the technical and organizational measures with measures of equal or higher value, provided that these meet the requirements of this Section 8.

9. Logicc's information obligations

9.1 Logicc will inform the Customer immediately if Logicc becomes aware of a Security Incident.

10. Tasks to support the Customer

10.1 Taking into account the nature of the Processing, Logicc shall support the Customer with appropriate technical and organizational measures in fulfilling the Customer's obligations to respond to requests from data subjects and other obligations under Data Protection Laws.

10.2 Logicc will inform the Customer immediately if Logicc believes that an instruction given by the Customer violates Data Protection Laws.

11. Term

11.1 This DPA shall automatically enter into force upon conclusion of the Agreement and shall remain in force for at least the duration of the Agreement, unless otherwise specified.

11.2 Premature or other termination of the Agreement, for whatever reason, shall result in the automatic termination of this DPA. However, the provisions of this DPA shall remain in force to the extent necessary to ensure the proper completion of the Processing of Customer Data within the scope of this DPA in accordance with Data Protection Laws, in particular with regard to the deletion or return of Customer Data. Once such Processing has been completed, this DPA shall terminate without further notice.

12. Obligation to delete and return after termination

12.1 Upon termination of the Services, Logicc will either delete or return all Customer Data in accordance with the Customer's instructions. The Customer must inform Logicc of their choice within 30 days of the termination of Services. If no notification is received within this period, Logicc may delete the Customer Data unless further storage is required by applicable law. Storage and archiving obligations under applicable law remain unaffected by this. Logicc will confirm the deletion or return upon request by the Customer.

13. Data protection officer

13.1 Logicc will appoint a data protection officer if required by Data Protection Laws and, in this case, provide the Customer with the contact details of the data protection officer.

14. Remuneration

14.1 All Services provided by Logicc within the scope of this DPA are fully covered by the remuneration agreed in the Agreement, unless expressly stated otherwise in this DPA.

14.2 Insofar as Services within the scope of this DPA are designated as subject to remuneration, these Services shall be remunerated on a time and material basis at the rates agreed in the Agreement. If no remuneration rates have been agreed, Logicc's standard rates valid at the time of performance shall apply.

15. Liability

15.1 The liability provisions of the Agreement shall apply accordingly to this DPA.

15.2 Logicc cannot reclaim any administrative penalties or fines imposed directly on the Customer, unless they are attributable to a breach by Logicc of this DPA or Data Protection Laws. In such cases, Logicc's liability shall be limited to contributory negligence as determined by a final decision of a competent court or authority and shall be subject to the liability provisions of the Agreement.

16. Final provisions

16.1 This DPA is an integral part of the Agreement. In the event of a conflict between the provisions of the Agreement and this DPA, the provisions of this DPA shall prevail exclusively with regard to the Processing of Customer Data.

16.2 Logicc reserves the right to amend this DPA if necessary to reflect changes in applicable Data Protection Laws, regulatory requirements, or binding decisions by the competent supervisory authorities. Logicc will notify the Customer of such changes in writing or in text form (e.g., by email) at least 30 days in advance, unless an immediate change is required by law or regulation. If the Customer objects to such changes for legitimate reasons, the parties shall cooperate in good faith to find a solution acceptable to both sides. If the Customer objects to such changes and no mutually acceptable solution is reached within a reasonable period of time, the Customer may terminate the Agreement with regard to the Processing activities concerned by giving written notice.

16.3 Should any provision of this DPA be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions of this DPA. The same applies if and to the extent that a loophole appears in this DPA. In place of the invalid or unenforceable provision or to fill the gap, an appropriate provision shall apply which, as far as legally possible, comes closest to or corresponds to what the parties intended economically or would have intended according to the meaning and purpose of this DPA, had they considered this point.

16.4 In all other respects, the final provisions of the Agreement shall apply mutatis mutandis to this DPA.

Appendix 1: Details of Processing

1. Categories of data subjects

- Users of the Services
- Employees of the Customer
- Persons to whom data entered by users, retrieved from connected third-party systems or processed when triggering actions on behalf of the Customer relates

2. Types of Customer Data

- Names, email addresses of users and employees of the Customer
- Data entered by users
- Personal Data retrieved from third-party systems authorized by the Customer or processed when triggering actions in those systems on behalf of the Customer

3. Scope and type of Processing

- Communication content with LLMs
- Documents and information that the Customer uploads and stores on the platform
- Retrieval of data from third-party systems authorized by the Customer via open interfaces (including the Model Context Protocol)
- Transmission and processing of Customer Data when triggering actions in connected third-party systems on behalf of the Customer within the scope of the permissions granted by the Customer

4. Purpose of Processing

- Provision of Services in accordance with the Customer's instructions, including retrieval of data from connected third-party systems and triggering of actions in those systems on behalf of the Customer

Appendix 2: Subprocessors

Name: Microsoft Ireland Operations Limited

Address: The Atrium Building, Block B, Carmanhall Road, Sandyford Business Estate, Dublin 18, Ireland

Task: Provision of cloud infrastructure and LLM models via Azure OpenAI Service for processing user queries (input) and generating model responses (output)
Place of processing: EU

Name: Hetzner Online GmbH

Address: Industriestr. 25, 91710 Gunzenhausen, Germany
Task: Provision of cloud infrastructure for hosting the platform
Place of processing: Germany

Name: Google Ireland Limited

Address: Gordon House, Barrow Street, Dublin 4, Ireland
Task: Provision of cloud infrastructure for processing user requests (input) and generating model responses (output)
Place of processing: EU

Name: Amazon Web Services EMEA SARL

Address: 38 avenue John F. Kennedy, L-1855, Luxembourg
Task: Provision of cloud infrastructure, including infrastructure for processing user requests (input) and generating model responses (output)
Place of processing: EU

Name: Mistral AI SAS

Address: 15 rue des Halles, F-75001 Paris
Task: Provision of cloud infrastructure for processing user requests (input) and generating model responses (output)
Place of processing: EU

Name: Cloudflare Inc.

Address: 101 Townsend Street, San Francisco, California 94107, United States
Task: Provision of DDoS protection, web application firewall (WAF) and Content Delivery Network (CDN)
Place of processing: Place of use is place of Processing
Guarantee pursuant to Art. 44 et seq. GDPR: Standard Contractual Clauses (SCC) pursuant to Art. 46 (2) (c) GDPR and supplementary safeguards

Name: Stripe Payments Europe, Limited (SPEL)

Address: 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland
Task: Processing and administration of payment transactions
Place of processing: EU

Name: Clerk, Inc.

Address: 660 King Street, Unit 345, San Francisco, CA 94107, USA
Task: Authentication and authorization of platform users
Place of processing: United States
Guarantee pursuant to Art. 44 et seq. GDPR: EU-U.S. Data Privacy Framework (DPF) and Standard Contractual Clauses (SCC) as a fallback.

Name: Linkup Technologies SAS

Address: 28 avenue des Pépinières, 94260 Fresnes, France
Task: Provision of a web search function for AI applications to enrich responses with up-to-date information.
Place of processing: EU

Name: OpenAI Ireland Ltd.

Address: 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
Task: Provision of LLM models for processing user requests (input) and generating model responses (output)

Appendix 3: Technical and organizational measures

Taking into account the state of the art, the costs of implementation, and the nature, scope, circumstances, and purposes of Processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects, Logicc has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to maintain the security and confidentiality of Customer Data ("technical and organizational measures"). These measures include the following aspects:

1. Confidentiality

1.1 Physical access control

Logicc does not operate its own data centers or server rooms. The application is operated on cloud infrastructure in ISO/IEC 27001-certified data centers. Physical access control at the data centers is provided by the hosting providers in accordance with their contractually agreed technical and organizational measures. The following measures apply to Logicc's business premises:

- Digital access control system with individual access permissions for employees.
- Authentication using a personal access code or biometric factor.
- Logging of physical access events.
- Granting and revocation of physical access permissions according to operational requirements.
- Visitors and external service providers are admitted only by authorized employees and may not remain unattended in non-public areas.

1.2 System access control

Logicc will take appropriate measures to prevent unauthorized persons from using data processing systems.

- Technical measures:
- Use of individual user accounts and strong, unique authentication credentials.
- Use of multi-factor authentication or passkeys where technically supported, particularly for privileged or security-relevant access.
- Use of centrally approved password management to generate and securely store unique credentials.
- Change of credentials following known or suspected compromise or for other security-related reasons.
- Automatic locking of inactive sessions after a defined period.
- Central management of Logicc-provided endpoints to enforce and monitor security configurations, operating system updates, and device compliance.
- Full-disk encryption of Logicc-provided endpoints.
- Management of user permissions.
- Organizational measures:
- IT security policy governing the secure handling of passwords, credentials, and mobile devices.
- Use of Logicc-provided and centrally managed endpoints by employees when Processing Customer Data.
- Assignment of user accounts in accordance with the principle of least privilege.

- Regular security training for employees to raise awareness of phishing and other threats.

1.3 Data access control

Logicc will take appropriate measures to ensure that persons authorized to use the data processing systems can access only the Personal Data covered by their access authorization and that Customer Data cannot be read, copied, modified, or removed without authorization during Processing, use, or after storage. Logicc takes the following precautions:

- Technical measures:
- Implementation of a differentiated authorization concept that restricts access to Customer Data to the minimum necessary.
- Use of network and application filters, including a web application firewall for publicly accessible application endpoints.
- Comprehensive logging of all access to Customer Data in tamper-resistant audit logs in accordance with defined retention periods.
- Separate logging of security-relevant database access.
- Administrative access to hosting infrastructure only through encrypted and access-protected connections.
- Centralized, encrypted management of production secrets and cryptographic keys; access and provisioning are restricted to the persons and services that require them.
- Encryption of Customer Data at rest using strong, state-of-the-art encryption methods.
- Organizational measures:
- Policy for granting and revoking access rights based on the "need-to-know" principle.
- Regular and event-driven reviews of access permissions, particularly for privileged access.
- Specific authorization for access to particularly sensitive categories of data.
- Restriction of privileged access to a small group of persons for whom it is operationally necessary, in accordance with the principle of least privilege.
- Before being granted access, employees whose activities may give them knowledge of Customer Data are bound in text form to confidentiality and to protect third-party secrets pursuant to Section 203 of the German Criminal Code (StGB).

1.4 Separation control

Logicc will take appropriate measures to ensure that Customer Data collected for different purposes can be processed separately. Logicc takes the following precautions:

- Technical measures:
- Strict logical tenant separation within the central database through the use of Row-Level Security (RLS).
- Enforcement of tenant separation at the application level to prevent access to other tenants' data.
- Separate environments for development, testing, and production.
- A differentiated authorization concept governing access.
- Organizational measures:
- Policy on data classification and the separate Processing of data belonging to different tenants and purposes.
- Regular review of the technical and organizational measures for data separation.

2. Integrity

2.1 Transfer control

Logicc will take appropriate measures to reduce the risk that Customer Data may be read, copied, modified, or removed without authorization during electronic transmission or during its transport or storage on data carriers. Logicc takes the following precautions:

- Technical measures:
- Consistent encryption of all transmissions of Customer Data over external or public networks using at least TLS 1.3.
- Use of approved, access-protected transmission channels and cloud services for the exchange and provision of Customer Data.
- Organizational measures:
- Policy on the secure transfer and disclosure of Customer Data that prohibits the use of insecure channels.
- Employee awareness training on the risks of insecure data transmission.
- Clear rules on the use of cloud services and the transfer of data to third parties.
- Documented overview of regular retrieval and transmission procedures.

2.2 Input control

Logicc will take appropriate measures to ensure that it can subsequently be checked and determined whether and by whom Customer Data was entered into, modified in, or removed from data processing systems. Logicc takes the following precautions:

- Technical measures:
- Comprehensive logging of all entries, changes, and deletions of Customer Data in tamper-resistant audit logs in accordance with defined retention periods.
- Separate logging of security-relevant database access.
- Plausibility and validation checks during data entry.
- Traceability of changes through timestamps or versioning where technically provided for the relevant Processing operation.
- Organizational measures:
- Clear responsibilities for data entry and maintenance.
- Assignment of rights to enter, modify, and delete data based on an authorization concept.
- Regular and event-driven reviews of security-relevant logs.

3. Availability and resilience

Logicc will take appropriate measures to ensure that Customer Data is protected against accidental destruction or loss. Logicc takes the following precautions:

- Technical measures:
- Hosting of the application and Customer Data in ISO/IEC 27001-certified data centers.
- Daily backups of production Customer Data and of the systems and configurations required for secure operations.
- Storage of backups within the European Union and encryption using AES-256.
- Regular retention of backups for 14 days; deleted backups remain recoverable for 90 days through a soft-delete function.

- During the soft-delete period, deleted backups are retained solely for disaster recovery purposes, are not used in production, and are automatically and permanently deleted after the period expires.
- Monitoring of backup processes and regular review and documentation of backup results.
- Regular and event-driven testing of backup recoverability, at least once per quarter.
- Technical measures to detect and defend against malware and other security threats.
- Physical protection and redundancy measures implemented by the data center operators, particularly for power supply, air conditioning, fire protection, and storage systems.
- Organizational measures:
 - Documented backup and recovery concept based on the criticality of the data and systems and defining responsibilities, escalation paths, and automation-supported recovery steps.
 - Contingency plans for relevant failure scenarios that are regularly reviewed, updated, and tested.
 - Designated internal persons responsible for emergencies, technical security incidents, and necessary recovery measures.
 - Use of the contractually agreed standard availability and support services of the hosting providers.
 - Information security policy containing requirements for availability, recovery, and emergency operations.

4. Procedures for regular review, assessment, and evaluation

Logicc implements procedures for regularly reviewing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of Processing.

4.1 Data protection management

- An external data protection officer has been appointed. The data protection officer is supported in implementing data protection measures within the company by the managing director and a designated employee, who act as internal data protection coordinators.
- Implementation of a data protection management system (DPMS) based on established standards (e.g., ISO 27701 and BSI IT-Grundschutz), adapted to the size and complexity of the company.
- Regular internal reviews of data protection measures and processes, at least once a year.
- Documentation and handling of data protection incidents in accordance with a defined internal process.
- Regular employee training on data protection, at least once a year.
- Processes implementing the information obligations pursuant to Articles 13 and 14 GDPR.
- Formalized procedure for requests from data subjects.
- Integration of data protection checkpoints into risk assessments where possible and appropriate.
- Data protection impact assessments (DPIAs) are conducted as necessary for new Processing activities likely to result in a high risk.
- Data protection considerations form part of the company's general risk management.

4.2 Incident response management

- Use of monitoring restricted to technical error and performance information, with measures to avoid capturing prompts, model responses, document content, authentication tokens, and full request bodies.
- Documented incident response process for detecting, reporting, analyzing, responding to, and following up on security incidents and Personal Data breaches, including assessment of statutory

notification obligations.

- Designated internal incident response group and involvement of technical management in coordinating and handling security incidents and Personal Data breaches.
- Central documentation and tracking of security incidents and Personal Data breaches.
- Use of a web application firewall to protect publicly accessible application endpoints.
- Use of centralized spam, phishing, and malware protection mechanisms for business email communications.
- Regular employee training on handling security incidents and phishing attempts.
- Regular review and continuous improvement of the incident response procedure.

4.3 Secure software development and vulnerability management

- Protected development branches and controlled merge, approval, and release processes for changes to application code.
- Testing of changes in a test environment separated from production before deployment to production.
- Security, dependency, and vulnerability scans integrated into the development process and performed regularly.
- Identified vulnerabilities are prioritized according to severity and actual exposure and remediated promptly.