

Algemene voorwaarden en DPA

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

Dit document is beschikbaar in het Engels.

General Terms and Conditions (GTC)

Preamble

These GTC govern the legal relationship between Logicc GmbH ("Logicc") and the Customer (Logicc and the Customer together referred to as the "Parties") with regard to the use of services.

These GTC are supplemented by the provisions in separate documents referred to in these GTC, such as the Data Processing Agreement ("DPA") and the information provided during the ordering process, which is documented in the order confirmation. In the event of a conflict between these documents, the following order of precedence shall apply: DPA, information in the order confirmation, these GTC.

1. Definitions

1.1 "Authorized User" means any person at the Customer to whom the Customer may grant access to use the Services in accordance with these GTC.

1.2 "Authorized Volume" means the usage parameters and limits for the use of the Platform in accordance with the service description.

1.3 "Confidential Information" means all information, documents, and files disclosed by one Party to the other Party in written, electronic, oral, or other form, which are designated as confidential by the disclosing Party or which, by their nature, are to be treated as confidential.

1.4 "Customer" refers to the person or company specified as the customer in the respective order process.

1.5 "Customer Data" means all data processed in connection with the use of the Services.

1.6 "Documentation" refers to the applicable technical and functional documentation relating to the Services provided by Logicc, including the technical and functional specifications, which are updated from time to time in accordance with these GTC.

1.7 "Effective Date" means the start of the term upon Logicc sending the order confirmation.

1.8 "Intellectual Property" means, without limitation, all patents and other rights to inventions, copyrights, trademarks, registered designs, and other industrial property rights, as well as all associated exploitation and usage rights.

1.9 "Services" means (i) the provision of access to AI applications and the hosting of corresponding data via the Platform, and (ii) consulting services that may be made available to the customer under these GTC. The services are described in the service description on the Logicc website at www.logicc.com and are specified in more detail in the order confirmation.

1.10 "Platform" refers to the online platform through which the Customer is given access to third-party AI applications and on which Customer Data is hosted.

1.11 "Term" means the original contract term and, if applicable, any extension period as specified in the order confirmation.

2. General provisions

2.1 Logicc's Services are intended exclusively for business customers. Logicc does not offer its services to consumers or natural persons beyond their commercial or professional activities, and the use of its Services by such persons is not permitted.

2.2 The Customer's general terms and conditions are rejected. They shall only become part of the contract if and to the extent that Logicc has expressly agreed to their validity in writing.

2.3 By completing the order process, the Customer submits a binding order. The contract under these GTC comes into effect when Logicc sends the order confirmation. The acceptance period is five business days. If Logicc does not accept the Customer's offer within this period, the Customer is no longer bound by its offer.

2.4 Logicc may offer the Customer an extension of the scope of Services if available. The Customer is then free to place a supplementary order and thus extend the existing contract. The above provisions on the conclusion of the contract apply accordingly.

2.5 The agreement on characteristics or other descriptions of the performance of the Services shall only be deemed a guarantee in the legal sense if and to the extent that they are expressly designated as a guarantee in writing in a separate guarantee document.

2.6 The Customer is obliged to take the necessary precautions and create the technical conditions to enable Logicc to provide the Services.

2.7 In its role as the controller of personal data in connection with the use of hosting and access to AI applications on the Platform, the Customer is obliged to inform Authorized Users and other affected data subjects about the processing in accordance with the provisions of the applicable data protection law. In this respect, Logicc acts in the role of a processor under the DPA.

3. Customer account and Authorized Users

3.1 The Customer must create an account to access the Platform. The Customer undertakes to keep its account information up to date, accurate, and complete at all times. The Customer is responsible for maintaining the confidentiality of the login information and will immediately notify Logicc of any loss, misuse, or unauthorized disclosure of such login information as soon as the Customer becomes aware of it. Logicc is not liable for any damage or loss resulting from the Customer's breach of the aforementioned obligations.

3.2 The maximum number of user accounts licensed by the Customer is specified in the order confirmation (insofar as access to the platform is to be via user accounts and no direct access via API has been agreed). Authorized Users include only (i) employees of the Customer and (ii) service providers of the Customer who do not compete with Logicc and who are permitted to use the Platform at the customer's place of business or in the presence of the customer's employees. The Customer is responsible for ensuring that access to a user account is not used in parallel and/or by multiple users.

3.3 The Customer is obliged to inform its Authorized Users of the rights and obligations agreed in these GTC before they start using the software solution on the Platform. The Customer is liable for breaches of duty by its Authorized Users or other third parties who violate obligations under these GTC that are within the Customer's sphere of influence.

4. Prohibited uses

4.1 Except to the extent expressly permitted by these GTC or required by law, the license granted under these GTC is subject to the following restrictions:

- the Customer may not exceed the authorized volume or use functions of the platform that are not covered by the order confirmation.
- the Customer may not allow unauthorized third parties to access or use the Platform,
- the Customer may not use the Platform to provide services to third parties, unless otherwise specified in these GTC,
- the Customer may not make any changes to the Platform unless this is permitted in accordance with the Documentation; and
- the Customer shall not, either directly or indirectly, reverse engineer, decompile, disassemble, or otherwise attempt to gain access to the source code, object code, or underlying structure, ideas, know-how, or algorithms relevant to the Platform, unless permitted by statutory law.

4.2 The Customer agrees not to use the Platform to

- process data on behalf of third parties who are not Authorized Users of the Customer;
- send unsolicited communications, junk mail, spam, or other forms of unsolicited messages that violate spamming or other laws;
- engage in unlawful conduct, including, but not limited to, violating the privacy or personal rights of any person;
- to store or transmit content that infringes the intellectual property rights of third parties;
- compromise or disrupt the integrity or performance of the Platform and its components;
- publish, transmit, upload, link, send, or store illegal, racist, hateful, offensive, defamatory, obscene, or discriminatory content;
- post, transmit, upload, link, send, or store viruses, malware, Trojan horses, time bombs, or similar harmful software.

4.3 Logicc has the right (but not the obligation) to suspend access to the Platform or remove data or content transmitted via the Platform without liability (i) if Logicc can reasonably assume that the Platform is being used in violation of these GTC or applicable law, (ii) if requested to do so by a law enforcement or other authority, or if necessary for other reasons to comply with applicable law, provided that Logicc makes commercially reasonable efforts to notify the Customer before suspending access to the Platform, or (iii) if permitted under the other provisions of these GTC.

4.4 Logicc will use commercially reasonable efforts to notify the Customer at least twelve hours prior to any suspension, unless Logicc determines in its reasonable discretion that a suspension with shorter or simultaneous notice is necessary to protect Logicc or its customers.

5. Hosting and access to AI applications

5.1 Logicc advises the Customer that content generated by AI applications may contain errors and inaccuracies. This content has not been checked or verified, but is automatically generated and may be incorrect or out of date. Logicc accepts no liability for any damage that may arise from the use of this content. Use is at the Customer's own risk.

5.2 After the contract has been concluded, Logicc will set up the Platform for use by the Customer and notify the Customer when it is ready for use. This may take up to three days.

5.3 Logicc reserves the right to subcontract services within the scope of these GTC. This applies in particular to the hosting providers and the providers of the AI applications as specified in the order confirmation. The AI applications used within the scope of the Services and available via the Platform are operated by third-party providers. The AI applications may be used within the scope of the Services to the extent permitted by the third-party provider. The available AI applications and their range of functions may change during the term of the contract.

5.4 Logicc has no influence on the specifications of the AI applications and does not assume any warranty or liability for a specific range of functions. Access to the available AI applications is subject to the corresponding terms of use and license conditions, which also describe the individual functionalities and system requirements of the AI applications.

5.5 Logicc is entitled to update the Platform regularly. All updates are subject to the provisions of these GTC. Logicc is only obliged to change or adapt the Platform if this is necessary to maintain the Platform in accordance with the state of the art. Otherwise, Logicc is not obliged to make further developments unless this has been expressly agreed between the Parties.

5.6 The Platform is subject to a regularly scheduled maintenance window. Logicc shall endeavor, to the extent economically reasonable, to schedule maintenance windows at times that minimize the impact on the Customer's users. While most maintenance work can be completed during the regularly scheduled maintenance windows, from time to time maintenance work must be performed outside of the scheduled maintenance windows to ensure the integrity and security of the services. In such cases, Logicc will inform the Customer of the planned maintenance work as early as technically feasible. The regularly scheduled weekly maintenance windows and any period of unavailability due to maintenance work for which the Customer is notified at least 24 hours in advance are considered scheduled maintenance.

5.7 Provided that the relevant commitment is included in the order confirmation, the following availability commitments (service levels) apply.

- The provider shall make commercially reasonable efforts to make the platform available with a minimum availability of 95% in each calendar month. Availability is the percentage resulting from the total minutes in a calendar month minus the minutes during which the Platform was unavailable outside of scheduled maintenance, divided by the total minutes in that calendar month.
- If Logicc fails to meet the promised availability, the Customer is entitled to receive a service credit of 10%. Logicc only offsets service credits against future payments of fees owed by the Customer. Service credits do not entitle the Customer to a refund or any other payment. Unless otherwise specified in the order confirmation, the Customer's sole and exclusive remedy for non-availability is to receive service credits, provided that a availability commitment has been made.
- Logicc will send the Customer an availability report for each calendar month. To receive a service credit, the Customer must submit a written or email request to Logicc within one week of receiving the availability report. If availability is lower than the promised availability, Logicc will issue the service credits to the Customer within one calendar month after the calendar month in which the credit was requested. If the Customer fails to submit the request for service credits and the other information required above, the Customer is not entitled to service credits.
- The promised availability does not apply to unavailability or other performance issues: (i) caused by factors beyond Logicc's reasonable control, including force majeure or Internet access problems or related problems outside the Platform's point of delivery; (ii) resulting from voluntary acts or omissions by the Customer or a third party or a breach of contract by the Customer; (iii) resulting from the Customer's failure to comply with the specifications described in the Documentation; (iv)

arising from the Customer's equipment, software, or other technology and/or the equipment, software, or other technology of third parties; or (vi) arising from the suspension or termination of the Customer's right to use the Platform in accordance with these GTC.

6. Consulting Services

6.1 Logicc provides consulting Services within the scope individually agreed with the Customer and documented in the order confirmation. The Customer bears the risk of whether the Services ordered meet the Customer's requirements and needs. Logicc is not obliged to provide consulting Services with a scope and objective other than those agreed, unless the Parties agree on an adjustment (change request).

6.2 Logicc provides the consulting Services as mere services on a time-and-material basis (Dienstleistungen). The Parties agree that the consulting Services are not subject to acceptance and that no specific success is owed, but rather the proper and careful performance of the consulting Services, unless the Customer and Logicc have expressly agreed in writing that acceptance shall take place.

6.3 All deadlines relating to the provision of consulting Services are estimates and are not binding, unless the Customer and Logicc have expressly agreed in writing that they are binding.

6.4 If Logicc is unable to provide Services in whole or in part due to problems on the part of the Customer and the Customer fails to inform Logicc of this in a timely manner, the Customer will be charged for the time required by Logicc.

6.5 All content provided by Logicc to the Customer for the preparation and performance of the Services is the intellectual property of Logicc. The Customer is only granted the rights to this content as set out in these GTC.

6.6 If the consulting Services are provided on site at the Customer's premises, the Customer agrees to provide the necessary access to its premises, including access to the Customer's computer systems and other facilities. The Customer shall designate a contact person with the authority to make decisions and to provide Logicc with all necessary and relevant information in a timely manner.

6.7 Logicc decides which consultant is assigned and reserves the right to replace a consultant at any time. It is at Logicc's discretion whether the consulting Services are provided at the Customer's premises or remotely. Even if consulting services are provided on site at the Customer's premises, Logicc has the exclusive right to issue instructions to the consultants deployed.

7. License and right of use

7.1 Logicc provides the Customer with access to the Platform as part of a software-as-a-service model. The Customer's right of use is limited to the term agreed in these GTC. Subject to the restrictions contained in these GTC, Logicc grants the Customer a non-exclusive, revocable, non-transferable, and non-sublicensable right to access the Platform (and the Documentation) during the Term and to use it exclusively for the purposes described in the Documentation for its internal business purposes. Without the express consent of Logicc, the Customer may not allow any affiliated companies or third parties to access the Platform. The license is granted per user account (insofar as access to the Platform is to be via user accounts and no direct access via API has been agreed). A user account is set up for each named Authorized User.

7.2 Logicc grants the Customer a non-exclusive, revocable, non-transferable, and non-sublicensable

right to use the content of the consulting Services, insofar as this has been actively transferred to the Customer by Logicc, subject to the restrictions contained in these GTC, exclusively for agreed purposes for its internal business purposes. Without the express consent of Logicc, the Customer may not allow any affiliated companies or third parties access to the Platform.

8. Remuneration

8.1 The Customer shall pay Logicc the remuneration specified in the order confirmation. Depending on the agreement, fees for the use of the Platform are payable for specific queries to the AI applications (price per token) and/or fees per user account (price per user). Unless otherwise agreed, a basic fee is also payable. Consulting Services are billed as specified in the order confirmation.

8.2 Unless otherwise specified in the order confirmation, in particular if no advance payment or advance debit by credit card or other means of payment is specified in the order process, all fees shall be paid to Logicc within 30 days of the invoice date. Complaints about invoices must be submitted in writing within 30 days of the invoice date.

8.3 In the event of late payment, the costs of collection (including reasonable attorney's fees) and statutory interest shall be payable. If the Customer is 15 days or more in arrears with the payment of fees, Logicc may suspend access to the Platform or the provision of Services.

8.4 All amounts are exclusive of applicable value added tax or other specific taxes such as withholding tax, which shall be added to these amounts.

8.5 The Customer may only offset undisputed or legally established claims and may only base a right of retention on undisputed or legally established claims. Notwithstanding the provisions of § 354a HGB (German Commercial Code), the Customer may not assign its claims to third parties.

8.6 Logicc is entitled to adjust the contractually agreed remuneration with three months' notice of the change. A change may be made at the earliest 12 months after conclusion of the contract or after the last remuneration increase. The change shall be made in accordance with the following principles:

- Logicc may adjust the remuneration at most to the extent that the producer price index for IT services of the Federal Statistical Office has changed by at least 3% up or down since the conclusion of the contract or the last remuneration increase. Any cost reductions shall also be taken into account and offset in this change.
- If the Customer does not terminate the existing contract within four weeks of receiving the adjustment notice (special right of termination) or otherwise declares its intention to do so, the new remuneration shall be deemed agreed. When announcing the remuneration adjustment, Logicc shall specifically inform the Customer of its right of termination and the consequences of not exercising this right.

9. Warranty

9.1 Logicc warrants that the Services are materially suitable for the contractually stipulated purpose. Strict liability for initial defects pursuant to § 536a BGB (German Civil Code) is excluded.

9.2 The Customer is obliged to notify Logicc immediately in writing of any defects that occur, providing a detailed description of the problem. If the Customer fails to notify Logicc, the Services shall be deemed to have been approved. If Logicc has fraudulently concealed the defect, Logicc cannot invoke the provisions of the preceding sentences in this paragraph.

9.3 Logicc may remedy the defect by showing the Customer reasonable ways to avoid the effects of the

defect. If the subsequent performance ultimately fails after the expiry of a reasonable grace period to be set by the Customer, the Customer may terminate the contract. Logicc shall pay compensation or reimburse futile expenses due to a defect within the limits specified in these GTC. Other rights due to material defects or defects of title are excluded.

9.4 The limitation period for claims under this section is one year after performance of the Services. The reduction of the limitation period shall not apply in cases of intent or gross negligence on the part of Logicc, fraudulent concealment of the defect, personal injury, or defects of title. For defects in subsequent performance, the limitation period shall also end one year after the original performance of the Services. However, if Logicc, in agreement with the Customer, examines the existence of a defect or provides subsequent performance, the limitation period shall be suspended until Logicc informs the customer of the result of its examination or declares the subsequent performance to be completed or refuses to provide subsequent performance. The limitation period shall commence at the earliest three months after the end of the suspension.

9.5 If Logicc provides Services for troubleshooting or fault rectification without being obliged to do so, Logicc may demand reasonable remuneration. This applies in particular if a reported material defect cannot be verified or cannot be attributed to Logicc. In particular, compensation shall also be paid for the additional expense incurred by Logicc in remedying defects as a result of the Customer's failure to properly fulfill its obligations to cooperate.

9.6 If Logicc fails to perform Services outside the scope of liability for material defects and defects of title, or if Logicc commits any other breach of duty, the Customer must always notify Logicc of this in writing and grant Logicc a grace period within which Logicc is given the opportunity to perform the Services properly or to remedy the situation in some other way.

9.7 If a third party asserts claims that conflict with the exercise of the contractually granted right of use, the Customer must inform Logicc immediately in writing. The Customer will only engage in legal disputes with the third party in agreement with Logicc or authorize Logicc to conduct the dispute. This shall apply mutatis mutandis to cases in which a third party asserts claims against Logicc that are attributable to actions of the Customer or authorized users.

10. Property rights

10.1 The Customer acknowledges that, subject to the licenses granted herein, it does not obtain any ownership or other rights to the Platform or Logicc's other Services made available to the Customer. Logicc reserves all rights not expressly granted to the Customer under these GTC.

10.2 Logicc may use the Customer's name and/or logo in marketing materials and/or use the Customer's name and/or logo in any other manner agreed between the Parties.

10.3 The Customer may provide Logicc with feedback at its own discretion. In this case, Logicc may retain and freely use this feedback at its own discretion without restriction, compensation, or attribution.

11. Confidentiality

11.1 The Parties undertake to treat the Confidential Information of the other Party as confidential and to use it exclusively for the purposes of performing the contract, and to protect the Confidential Information of the other Party by taking appropriate security measures with due care.

11.2 Disclosure of the other Party's Confidential Information to third parties is only permitted if this is absolutely necessary for the performance of this contract and the third party has undertaken to maintain confidentiality vis-à-vis the disclosing party or is bound to confidentiality by virtue of its profession.

Statutory disclosure obligations remain unaffected. Each Party shall ensure that the obligations of these GTC are also upheld by any third parties to whom the respective Party discloses Confidential Information of the other Party. The respective Party shall be liable for any breaches of the confidentiality obligations under this section by such third parties as if they were its own fault.

11.3 The above obligations shall not apply to information which the receiving Party can prove (i) was or is available to the public in a lawful manner that does not violate the provisions of these GTC, (ii) was already known to the receiving Party and was at its unrestricted disposal, (iii) was disclosed to the receiving Party by a third party authorized to do so, or (iv) was developed independently by the receiving Party without the use of Confidential Information from the disclosing Party.

11.4 The receiving Party undertakes to destroy completely and permanently all documents and records containing Confidential Information of the other Party immediately after termination of the contract or, in the case of electronic data, to delete them permanently. Statutory retention and archiving obligations remain unaffected by this.

11.5 After termination of the contract, all rights and obligations of the Parties with regard to the Confidential Information of the other Party shall continue to apply for a period of five years.

12. Responsibility for Customer Data

12.1 The Customer is solely responsible for all Customer Data, in particular for ensuring that its transmission and use does not violate applicable laws, including data protection laws, and/or the intellectual property rights of third parties. The Customer is obliged to check its Customer Data for viruses or other harmful components before entering it into the Platform and to use state-of-the-art antivirus programs for this purpose. The Customer indemnifies Logicc against all damages and costs imposed on Logicc or agreed to by the Customer in a settlement and resulting from such third-party claims.

12.2 The Customer grants Logicc a non-exclusive, royalty-free license to access, use, reproduce, modify, execute, display, and otherwise use Customer Data to the extent that this is reasonable or necessary for Logicc to perform or provide the Services.

12.3 Furthermore, the Customer is responsible for entering and maintaining its Customer Data. The Customer shall make a backup copy of the Customer Data at least once a week. The Customer acknowledges that Logicc has no control over the Customer Data and that Logicc acts as a mere or passive channel for the transmission and processing of Customer Data. The processing of the Customer's personal data by Logicc is governed by the DPA applicable between the Parties, which is concluded with the contract.

12.4 The Platform may, at the Customer's request, be connected via open interfaces (including the Model Context Protocol) to the Customer's user accounts in third-party systems and perform read actions and, to the extent authorized by the Customer, write actions in those systems in response to user requests ("Integrations"). The Customer is solely responsible for the selection, activation, configuration and granting of permissions. The Customer shall ensure that use complies with the terms of the third-party providers and applicable laws. Actions performed through the Integrations may be erroneous, incomplete or unintended. Clause 5.1 shall apply accordingly. Actions performed within the scope of the Integrations and permissions activated by the Customer shall be attributable to the Customer or its authorized users. The Customer shall, upon first demand, indemnify Logicc against all third-party claims asserted against Logicc in connection with an action performed through the Integrations, including reasonable costs of legal defense. This shall not apply to the extent that the claim

is based on a culpable breach of duty by Logicc. Clause 9.7 shall apply accordingly.

13. Limitation of liability

13.1 Logicc's liability is limited in accordance with the following provisions.

13.2 In the event of intent, Logicc shall be liable without limitation in accordance with the statutory provisions. The same applies to all other cases of mandatory statutory liability, such as in the event of liability for guaranteed characteristics, for injury to life, limb, or health, or under the Product Liability Act.

13.3 In the event of negligence, Logicc shall only be liable for the breach of a contractual obligation whose fulfillment is essential for the proper execution of the contract and on whose compliance the customer may regularly rely (cardinal obligation). Liability is then limited per claim to an amount equal to the fees paid in the twelve months prior to the claim and to a total of EUR 25,000 under the contractual relationship.

13.4 In the event of slight negligence, liability for indirect damage and consequential damage, in particular for lost profits, is excluded.

13.5 The above exclusions and limitations of liability apply to the same extent in favor of Logicc's organs, legal representatives, employees, and other vicarious agents.

13.6 The above exclusions and limitations of liability apply to all claims, regardless of their legal basis, in particular those arising from impossibility, delay, defective or incorrect delivery, infringement of third-party property rights, other breaches of contract, breach of duties during contract negotiations, and tort. They also apply to any indemnification obligations of Logicc.

13.7 A limitation period of one year applies to all claims against Logicc for damages or reimbursement of futile expenses in the case of contractual and non-contractual liability. The limitation period begins at the time specified in § 199 (1) BGB (German Civil Code). It expires at the latest five years after the claim arises. The above provisions of this paragraph do not apply to liability for intent or gross negligence or for personal injury or under the Product Liability Act. The deviating limitation period for claims due to material defects and defects of title remains unaffected by the provisions of this paragraph.

14. Term and termination

14.1 Unless otherwise specified in the order confirmation, the Term for use of the Platform is one month from the Effective Date. Thereafter, it shall be automatically extended for a further month unless terminated by either Party at the end of the initial Term or an extension period.

14.2 The Customer cannot terminate the commissioning of consulting Services by giving notice. The contract for the use of the Platform may be terminated by the Customer with 14 days' notice to the end of the month if the specifications of the AI applications available via the Platform change in such a way that continuation of the contract appears unreasonable for the Customer in view of the circumstances. In this case, the Customer shall only owe remuneration on a pro rata basis for the Term up to the date of termination.

14.3 The Parties' rights to terminate for good cause remain unaffected. Good cause shall be deemed to exist in particular if (i) the Customer fails to make due payments within 15 days of the due date; (ii) the Customer fails to fulfill another material obligation imposed on it under the contract under these GTC and this failure is not remedied within a period of 30 days; or (iii) the Customer files for insolvency, a third party files for insolvency against the Customer, proceedings for the granting of legal remedies under insolvency laws are initiated, the appointment of an insolvency administrator is requested, or

insolvency proceedings are initiated.

14.4 One-time payments for the use of the Platform will not be refunded in the event of termination. Remuneration and reimbursement of costs relating to services rendered up to the effective date of termination must be paid.

14.5 Termination with regard to consulting Services does not generally result in termination of the contract for other Services, in particular for the use of the Platform.

14.6 The deletion of Customer Data after the end of the Term is governed in its entirety (including for non-personal data) by the provisions of the DPA.

15. Final provisions

15.1 Each Party shall bear its own costs incurred in connection with the conclusion and execution of the contract, unless expressly agreed otherwise in these GTC.

15.2 These GTC fully reflect the agreements between the Parties with regard to the subject matter of the contract; no verbal or other ancillary agreements have been made. Unless expressly agreed otherwise in these GTC, all previous agreements between the parties regarding the subject matter of the contract are completely replaced by these GTC.

15.3 Logicc is entitled to change the services and these GTC if this is necessary to take into account developments that were not foreseeable at the time of conclusion of the contract, in particular changes in technical or legal conditions. Logicc will take the legitimate interests of the Customer into account in doing so. Changes will be communicated to the Customer in advance by email. If the Customer does not object within four weeks of receiving the notification, the changes shall be deemed accepted with effect for the future. If the Customer objects, Logicc shall be entitled to terminate the contract extraordinarily if Logicc has pointed out the effect of silence and the right of termination in the notification.

15.4 Neither Party is entitled to transfer the contract or rights or obligations arising therefrom to a third party without the prior written consent of the other Party.

15.5 The contract under these GTC is subject to the law of the Federal Republic of Germany, excluding the conflict of law rules of international private law. The applicability of the UN Convention on Contracts for the International Sale of Goods (CISG) is excluded.

15.6 The exclusive place of jurisdiction for all disputes arising from or in connection with the contract under these GTC is Hamburg, unless the law mandatorily prescribes otherwise.

15.7 Should any provision of these GTC be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions of these GTC. The same shall apply if and to the extent that it transpires that the contract contains a loophole under these GTC. In place of the invalid or unenforceable provision or to fill the loophole, an appropriate provision shall be deemed to have been agreed 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 these GTC, had they considered this point.

Data Processing Agreement (DPA)

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)

Place of processing: EU

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.