DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into by d.vinci HR-Systems GmbH ("Customer") and Zendesk, Inc. ("Zendesk"), each a "Party" and together the "Parties".

Customer and Zendesk have entered into the Agreement under which Customer is provided access to and use of the Services during the Subscription Term. This DPA is incorporated into and made a part of the Agreement.

SECTION 1 GLOBAL PRIVACY OBLIGATIONS OF THE PARTIES

1.1 **Ownership of Service Data.** Zendesk asserts no ownership right or interest to Service Data processed under this DPA and, between the Parties, Service Data owned by Customer remains the property of Customer.

1.2 **Personal Data.** The Parties agree that the nature, purposes, subject matter, duration of processing, categories of Personal Data or data subjects, and applicable retention periods are as described in Annex I.

1.3 **Applicable Data Protection Law.** Zendesk and Customer agree to comply with their respective obligations of Applicable Data Protection Law.

1.4 **Zendesk's Obligations.** Zendesk agrees to:

(i) process Personal Data according to Customer's documented instructions, unless otherwise permitted or required by applicable law. Zendesk will inform Customer immediately if its processing instructions infringe Applicable Data Protection Law;

(ii) not sell or share Personal Data;

(iii) ensure that all employees and contractors are fully aware of their responsibilities to protect Personal Data under this DPA and have committed to an appropriate contractual or statutory obligation of confidentiality;

(iv) notify Customer if it can no longer meet its obligations under Applicable Data Protection Law and allow Customer to take reasonable and appropriate steps to remediate unauthorized processing of Personal Data;

(v) implement and maintain appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, taking into account the likelihood and severity of risks to the privacy rights of data subjects, including the measures in Annex II;

(vi) notify Customer of a confirmed personal data breach without undue delay and within 48 hours, unless prohibited by law or government agency; take appropriate measures designed to mitigate the cause(s) of the personal data breach; and provide Customer all necessary information as required under Applicable Data Protection Law;

(vii) reasonably assist Customer with its obligation to respond to data subject requests and, if Zendesk receives a request directly from Customer's data subject, direct the data subject to Customer unless prohibited by law; and

(viii) make available commercially reasonable information and assistance to enable Customer to conduct any data protection impact assessment or supervisory authority consultation, as required by Applicable Data Protection Law.

1.5 **Customer Obligations.** Customer, as data controller, determines what Personal Data is processed by the Services. Customer is responsible for assessing Zendesk's technical and

organization measures as appropriate for the types of Personal Data Customer wishes to process by its use of the Services.

SECTION 2 USE OF SUB-PROCESSORS

2.1 **Sub-Processors.** Customer provides its general written authorization for Zendesk to use Sub-processors provided that:

(i) Zendesk remains liable to Customer for the acts or omissions of its Sub-processors with respect to their processing of Personal Data; and

(ii) each Sub-processor agrees to protect the Personal Data to standards consistent with the requirements of this DPA.

2.2 **Sub-Processor Policy Updates.** Zendesk will update the Sub-processor Policy with any newly appointed Sub-processors at least 30 days before such change. Customer may sign-up to receive email notifications of such changes.

2.3 **Sub-Processor Policy Objections.** Customer may object to any newly appointed Sub-processor on reasonable grounds relating to data protection. If Customer objects, it will inform Zendesk in writing by emailing privacy@zendesk.com within 30 days following the update to the Sub-processor Policy. In such event, the Parties will negotiate, in good faith, a solution to Customer's objection. If the Parties cannot reach resolution within 60 days of Zendesk's receipt of Customer's objection, Zendesk, in its sole discretion, will either:

(i) instruct the Sub-processor not to process Customer's Personal Data, and the DPA will continue unaffected, or

(ii) allow Customer to terminate any affected portion of the Services and provide Customer with a pro rata refund of Subscription Charges paid in advance for the affected portion of the Services not yet received as of the effective date of termination.

SECTION 3 AUDIT

3.1 **External Auditors.** Zendesk uses independent and qualified external auditors to verify the adequacy of its data protection measures and compliance with its obligations in this DPA (e.g. SOC 2 Type II or ISO 27001).

3.2 **Audit Report.** At Customer's written request, Zendesk will provide Customer with an Audit Report, subject to the confidentiality provisions of the Agreement.

3.3 **Assistance.** To the extent Customer's audit requirements under Applicable Data Protection Law are not reasonably satisfied through the Audit Report or other documentation that Zendesk makes generally available to its customers, and Customer does not otherwise have access to the relevant information, Zendesk will reasonably assist Customer.

3.4 **Audit.** If Customer cannot satisfy its audit obligations under Applicable Data Protection Law through Zendesk's assistance provided in Section 3.3 and Customer has the right to conduct an audit under Applicable Data Protection Law, Customer may request such an audit by providing at least 30 days' advance written notice to privacy@zendesk.com. Such audit may be conducted no more than once annually, must be conducted during normal business hours with reasonable duration, must not interfere with Zendesk's operations, and must only be conducted at Zendesk headquarters or an agreed business office. Such audit will not involve access to any data relating to other Zendesk customers, or to secured facilities or systems in any way that would violate Zendesk's security controls or cause Zendesk to violate its confidentiality obligations to any third party. Any information generated in connection with such audit is Zendesk's Confidential

Information and will be promptly provided to Zendesk. Customer is responsible for costs and expenses relating to any audit it requests beyond the Audit Report.

SECTION 4 INTERNATIONAL DATA TRANSFERS

4.1 **International Data Transfers.** Customer acknowledges that it is necessary for the performance of the Services that Zendesk may process Service Data on a global basis in compliance with Applicable Data Protection Law. If Zendesk transfers Personal Data from an origin country to a country that has not received an adequacy decision from the origin country, the transfers will adhere to one or more of the following Transfer Mechanisms, made applicable to all Personal Data, and in the following order:

(i) a valid certification mechanism;

(ii) Binding Corporate Rules;

(iii) SCCs.

4.2 **Transfer Mechanisms.** Transfer Mechanisms, clause selections, and specific country requirements, if applicable, are detailed and incorporated by reference in Annex III.

4.3 **Data Transfer Assessment.** Customer acknowledges that it may be obligated to conduct a data transfer assessment in addition to relying on Transfer Mechanisms. Zendesk will provide reasonable assistance with this assessment upon request.

4.4 **Binding Signature.** Customer acknowledges that signature of the Agreement constitutes binding signature of the SCCs and other signature requirements stated in the Region-Specific Terms.

SECTION 5 RETURN AND DESTRUCTION OF PERSONAL DATA

Upon Customer's written request, Zendesk will make Service Data available to Customer for export or download as provided in the Agreement. Zendesk will delete Service Data in accordance with Zendesk's Service Data Deletion Policy.

SECTION 6 INNOVATION SERVICES

All Sections of this DPA apply to Innovation Services except for Section 3 (Audit), Annex II (Zendesk Technical and Organizational Security Measures - Enterprise Services), and Annex III, Sections 1 and 2 (Binding Corporate Rules and Data Privacy Framework).

SECTION 7 CONFLICTS

Unless otherwise agreed, the terms of this DPA will take precedence over any conflicting terms in the Agreement.

SECTION 8 DEFINITIONS

All terms used in this DPA will have the meanings given to them below. Where not defined in this DPA, the terms "sell", "share", "processing", "process", "processor", "controller", "data exporter", "data importer", "data subject", "personal data breach" (and similar terms), and "supervisory authority" will have the same meaning as in Applicable Data Protection Law. Any capitalized terms not otherwise defined in this DPA are as defined in the Agreement.

"Applicable Data Protection Law" means all data protection laws and regulations applicable to each party in connection with its respective processing of Personal Data under this Agreement.

"Audit Report" means a confidential summary of any such certification or audit report for Enterprise Services.

"Binding Corporate Rules" mean (a) EU Binding Corporate Rules - Processor for transfers of Personal Data subject to the GDPR, or (b) UK Binding Corporate Rules – Processor for transfers of UK Personal Data.

"Bug Bounty Program" means the terms at: https://support.zendesk.com/hc/en-us/articles/115002853607-Zendesk-Bug-Bounty-Program.

Business Resilience Webpage means https://support.zendesk.com/hc/en-us/articles/4408824212378-Business-Resilience.

"Personal Data" means any personal data relating, directly or indirectly, to an identified or identifiable natural person that is contained in Service Data.

"Status Webpage" means https://status.zendesk.com/?_ga=2.228109981.1069242886.1631551570-1973870648.1630415696.

"SCCs" mean standard contractual clauses approved by a supervisory authority as a Transfer Mechanism.

"Sub-processor" means any third-party data processor engaged by Zendesk who receives and processes Service Data in accordance with Customer's instructions (as communicated by Zendesk) and the terms of its written subcontract with Zendesk, as listed in the Sub-processor Policy.

"Sub-processor Policy" means the policy at: https://support.zendesk.com/hc/en-us/articles/4408883061530-Sub-processor-Policy.

"Transfer Mechanism" means the framework(s) governing the international processing of Personal Data described in Annex III.

As agreed by the parties:

CUSTOMER: d.vinci HR-Systems GmbH		**ZENDESK, INC.**	
BY	DocuSigned by: Matthias Blenski 436D859AC15F415...	**BY**	Signed by: John Didday 4C0B6A53D9E6490...
NAME	Matthias Blenski	**NAME**	John Didday
TITLE	Syndikusrechtsanwalt d.vinci HR-Systems GmbH	**TITLE**	Associate General Counsel, Product & Privacy
DATE	11/19/2025	**DATE**	11/19/2025
EMAIL	matthias.blenski@dvinci.de	**EMAIL**	privacy@zendesk.com

APPROVED FOR SIGNATURE ZENDESK LEGAL DEPARTMENT

ANNEX I

Details of Processing

Data Exporter: Customer
Contact Details: Provided in the DPA signature block.
Data Exporter Role: Customer is a controller (with respect to Zendesk)

Data Importer: Zendesk, Inc.
Contact Details: Provided in the DPA signature block
Data Importer Role: Zendesk is a processor

1. **Nature and Purpose of the Processing:** Zendesk will process Personal Data as specified in the Agreement and for the purposes determined by Customer.

2. **Processing Activities:** Processing activities will include hosting and processing of Personal Data as specifically instructed by the Customer programmatically or in the Agreement.

3. **Duration of Processing and Retention:** Zendesk will process and retain Personal Data on a continuous basis for the Subscription Term. Zendesk deletes Personal Data according to the Zendesk Service Data Deletion Policy.

4. **Data Subjects:** Customer may, at its sole discretion, submit Personal Data to the Services, which may include, but is not limited to: employees (including contractors and temporary employees), relatives of employees, customers, prospective customers, service providers, business partners, vendors, End Users, advisors (all of whom are natural persons) of Customer and any natural person(s) authorized by Customer to use the Services.

5. **Categories of Personal Data:** Customer may process any category of Personal Data at its sole discretion using the Services, which may include, but is not limited to, the following categories of Personal Data: first and last name, email address, title, position, employer, contact information (company, email, phone numbers, physical address), date of birth, gender, communications (telephone recordings, voicemail, metadata), and customer service information.

6. **Special Categories of Data (if applicable):** Sensitive categories of data requiring special treatment under Applicable Data Protection Law may be included Personal Data at the discretion of Customer.

ANNEX II

Zendesk Technical and Organizational Security Measures - Enterprise Services

The technical and organizational measures to protect Service Data for Enterprise Services are contained in Zendesk's Enterprise Security Measures.

Zendesk reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections in this Annex II.

1. Information Security Program and Team: The Zendesk security program includes documented policies and standards of administrative, technical, physical and organizational safeguards, which govern the handling of Service Data in compliance with applicable law. The security program is designed to protect the confidentiality and integrity of Service Data, appropriate to the nature, scope, context and purposes of processing and the risks involved in the processing for the data subjects. Zendesk maintains a globally distributed security team on call 24/7 to respond to security alerts and events.

2. Security Certifications: Zendesk holds the following security-related certifications from independent third-party auditors: **SOC 2 Type II**, **ISO 27001:2013**, or **ISO 27018:2014**.

3. Physical Access Controls: Zendesk takes reasonable measures, such as security personnel and secured buildings, to prevent unauthorized persons from gaining physical access to Service Data and validates third parties operating data centers on Zendesk's behalf are adhering to such controls.

4. System Access Controls: Zendesk takes reasonable measures to prevent Service Data from being used without authorization. These controls vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

5. Data Access Controls: Zendesk takes reasonable measures to ensure Service Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Service Data to which they have privilege of access; and, that Service Data cannot be read, copied, modified or removed without authorization in the course of processing.

6. Transmission Controls: Zendesk takes reasonable measures to ensure the ability to check and establish which entities are transferred Service Data by means of data transmission facilities so Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport. Service Data is encrypted in transit over public networks when communicating with Zendesk user interfaces (UIs) and application programming interface (APIs) via industry standard HTTPS/TLS (TLS 1.2 or higher). Exceptions to encryption in transit may include any Third-Party Product that does not support encryption, which data controller may link to through the Enterprise Services at its election. Service Data is encrypted at rest by Zendesk's Sub-processor and managed services provider, Amazon Web Services Inc., via AES-256.

7. Input Controls: Zendesk takes reasonable measures to provide the ability to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed, and that any transfer of Service Data to a third-party service provider is made via a secure transmission.

8. Logical Separation: Data from different Zendesk's Customer environments is logically segregated on systems managed by Zendesk to ensure that Service Data that is collected by different controllers is segregated from one another.

9. No Backdoors: Zendesk has not built any backdoors or other methods into the Services to allow government authorities to circumvent its security measures to gain access to Service Data.

10. Data Center Architecture and Security: Zendesk hosts Service Data primarily in AWS data centers that have been certified as ISO 27001, PCI DSS Service Provider Level 1, and/or SOC2 compliant. AWS infrastructure services include backup power, HVAC systems, and fire suppression equipment to help protect servers and ultimately Customer's data. AWS on-site security includes a number of features, such as, security guards, fencing, securing feeds, intrusion detection technology, and other security measures. More details on AWS controls can be found at: https://aws.amazon.com/security.

11. Network Architecture and Security: Zendesk systems are housed in zones to commensurate with their security, depending on function, information classification, and risk. Zendesk's network security architecture consists of multiple zones with more sensitive systems, like database servers, in Zendesk's most trusted zones. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the internet and internally between the different zones of trust. Zendesk's network is protected through the use of key AWS security services, regular audits, and network intelligence technologies, which monitor and/or block known malicious traffic and network attacks. Zendesk utilizes network security scanning to provide quick identification of potentially vulnerable systems, in addition to Zendesk's extensive internal scanning and testing program. Zendesk also participates in several threat intelligence sharing programs to monitor threats posted to these threat intelligence networks and take action based on risk. Zendesk has a multi-layer approach to DDoS mitigation, utilizing network edge defenses, along with scaling and protection tools.

12. Testing, Monitoring, and Logging: Each year, Zendesk employs third-party security experts to perform a broad penetration test across the Zendesk production and corporate networks. Zendesk utilizes a Security Incident Event Management (SIEM) system, which gathers logs from important network devices and host systems. The SIEM alerts on triggers that notify the Security team based on correlated events for investigation and response. Service ingress and egress points are instrumented and monitored to detect anomalous behavior, including 24/7 system monitoring.

13. Data Hosting Location: Zendesk offers Customers an option to elect where Service Data is hosted if a Customer purchases the Data Center Location Add-On. A full description of this offering is provided at: https://support.zendesk.com/hc/en-us/articles/360053579674.

14. Availability and Continuity: Zendesk maintains a publicly available Status Webpage, which includes system availability details, scheduled maintenance, service incident history, and relevant security events. Zendesk employs service clustering and network redundancies to eliminate single points of failure. Our strict backup regime and/or Zendesk's Enhanced Disaster Recovery service offering allows us to deliver a high level of service availability, as Service Data is replicated across available zones. Zendesk's Disaster Recovery program ensures that the Zendesk Services remain available and are easily recoverable in the case of a disaster, through building a robust technical environment. Additional details are available on Zendesk's Business Resilience Webpage.

15. People Security: Zendesk performs pre-employment background checks of all employees, including education and employment verification, in accordance with applicable local laws. Employees receive

security training upon hire and annually thereafter. Employees are bound by written confidentiality agreements to maintain the confidentiality of data.

16. Vendor Management: Zendesk uses third party vendors to provide certain aspects of the Services. Zendesk completes a security risk assessment of prospective vendors.

17. Bug Bounty: Zendesk maintains a Bug Bounty Program to allow independent security researchers to report security vulnerabilities on an ongoing basis.

Zendesk Technical and Organizational Security Measures - Innovation Services

The technical and organizational measures to protect Service Data for Innovation Services are contained in Zendesk's Innovation Security Measures.

The Zendesk information security program includes documented policies or standards governing the handling of Service Data in compliance with applicable law, and administrative, technical and physical safeguards designed to protect the confidentiality and integrity of Service Data. Zendesk reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections in this Annex II.

1. Physical Access Controls: Zendesk takes reasonable measures to prevent unauthorized persons from gaining physical access to Service Data.

2. System Access Controls: Zendesk takes reasonable measures to prevent Service Data from being used without authorization.

3. Data Access Controls: Zendesk takes reasonable measures to provide that Service Data is accessible and manageable only by properly authorized staff.

4. Transmission Controls: Zendesk takes reasonable measures to ensure the ability to check and establish to which entities are transferred Service Data by means of data transmission facilities so Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls: Zendesk takes reasonable measures to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed, and that any transfer of Service Data to a third-party service provider is made via a secure transmission.

6. Logical Separation: Data from different Zendesk's Customer environments is logically segregated on systems managed by Zendesk to ensure that Service Data that is collected by different controllers is segregated from one another.

7. Security Policies and Personnel: Zendesk has and will maintain a managed security program to identify risks and implement preventative technology, as well as technology and processes for common attack mitigation. Zendesk has, and will maintain, a full-time information security team responsible for safeguarding Zendesk's networks, systems and services, and developing and delivering training to Zendesk's employees in compliance with Zendesk's security policies.

ANNEX III

Transfer Mechanisms and Region-Specific Terms

Zendesk utilizes several transfer mechanisms governing the international transfer of Personal Data, depending upon the jurisdiction of the Personal Data that is Processed. Additional privacy-specific terms in the Region-Specific Terms are incorporated as applicable.

1. Binding Corporate Rules

Zendesk, its affiliates, and Sub-processors comply with the requirements of Zendesk's Binding Corporate Rules, which have been approved by the Irish Data Protection Commission and the UK Information Commission Office and available on Zendesk's Trust Center at: https://www.zendesk.com/trust-center/.

2. Data Privacy Framework

Zendesk has certified to participate in and comply with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") (see: https://www.dataprivacyframework.gov/s/). Zendesk commits to maintain the self-certification compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, or any replacement framework, for the Services provided under the Agreement and this DPA.

3. SCCs

(i) Zendesk also utilizes the standard contractual clauses adopted by the European Commission that are stated in the Annex to the European Commission's Implementing Decision 2021/914 of 4 June 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914 ("EU SCCs"), and the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses', available at: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf ("UK Addendum"). The parties acknowledge that the SCCs are incorporated into this DPA as if fully stated below. These links may be updated from time to time based on updates by regulatory authorities and will be updated by amendment to this DPA.

(ii) To the extent that SCCs are published and required by a supervisory authority that are not EU SCCs, the parties interpret them as completed consistent with the selections in subsection (e).

(iii) In the event of conflict or ambiguity, the terms of SCCs will take precedence over the DPA and all other terms between Zendesk and Customer.

(iv) Where the EU SCCs are recognized by a local supervisory authority as a Transfer Mechanism, they apply to all Personal Data subject to that authority and will be considered completed in the manner specified in subsection (e).

(v) **EU SCCs.** Where the EU SCCs are used as a Transfer Mechanism, they are considered completed as follows:

(a) Module 2 (Controller to Processor) will apply where Customer is a controller of Service Data and Zendesk is a processor of Service Data; Module 3 (Processor to Processor) will apply where Customer is a processor of Service Data and Zendesk is a processor of Service Data;

(b) in Clause 7, the optional docking clause will not apply;

(c) in Clause 9(a), Option 2 “General Written Authorisation” will apply, and the time period for prior notice of Sub- processor changes as stated in the “Use of Sub-processors” section of this DPA;

(d) in Clause 11, the optional language will not apply;

(e) in Clause 17, Option 1 will apply and will be governed by the laws provided in the Agreement, or by the laws of Ireland if no EEA member state law applies, or by the laws of the importer where neither apply;

(f) in Clause 18(b), disputes will be resolved before the courts in the following order of precedence: (1) as provided in the Agreement, (2) Dublin, Ireland, if no EEA member state applies, (3) Customer’s country with jurisdiction over the Customer’s headquarters, (4) Zendesk’s registered office address;

(g) in Annex I.A and I.B and Annex II of the EU SCCs are considered completed with the information listed in Annexes I and II to this DPA; and

(h) in Annex I.C of SCCs, the supervisory authority will be the authority competent with respect to the data exporter. Where the data exporter is not established in the local country but is still within the territorial scope of Applicable Data Protection Law, the competent supervisory authority will be located where the data exporter has appointed a representative, but if it has not appointed a representative, then supervisory authority of Ireland will be the competent authority.

(vi) **UK Addendum.** Where the UK Addendum applies, it will be deemed completed as follows:

(a) Table 1, is considered completed with the information stated in Annex I of this DPA, the contents of which are hereby agreed to by the Parties;

(b) Table 2, the Parties select the checkbox that reads: “Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum”, and the accompanying table are considered completed according to the Parties’ preferences outlined in this Annex;

(c) Table 3, is considered completed with the information stated in Annex I, Annex II and as stated in the “Use of Sub-processors” section of this DPA; and

(d) Table 4, the Parties agree that neither Party may terminate the UK Addendum as stated in Section 19.