

Data Processing Agreement

October 2026

Data Processing Agreement

Background

The Controller and the Processor entered into an agreement for provision of Cloud Protection for Salesforce solution (**Solution**) that may require the Processor to process Personal Data on behalf of the Controller. This Data Processing Agreement (**DPA**) sets out the terms, requirements and conditions on which the Processor will process Personal Data when providing the Solution under the Agreement as a data processor. This applies to the extent Personal Data is processed in the Solution that is temporarily stored in the Solution's backend for encryption purposes as well as to the extent the Solution processes Personal Data in the Identity Protection feature of the Solution. This DPA contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

This DPA forms an integral part of the Agreement between Controller and Processor. The DPA shall become effective concurrently with the execution of the Agreement.

AGREED TERMS

1 Definitions and Interpretation

The following definitions and rules of interpretation apply in this DPA.

1.1 Definitions:

Affiliates: any entity that directly or indirectly controls, is controlled by, or is under common control with a Party to the Agreement.

Agreement: the order form or other agreement for the provision of the Solution which outlines the details of an order, including the scope and the fees for the Solution.

Business Purposes: the provision of the Solution as further described in the Agreement.

Controller: Client as defined in the Agreement.

Data Subject: an individual who is the subject of Personal Data.

Personal Data: any information relating to an identified or identifiable natural person that is processed by the Processor for Business Purposes under the Agreement; an identifiable natural person is one who can be identified, directly or indirectly, within the meaning of the Data Protection Legislation.

Processing, processes and process: any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process.

Processor: WithSecure Cloud Protection Oy or other Cloud Protection by WithSecure group company as defined in the Agreement.

Data Protection Legislation: all applicable data protection and privacy legislation (to the extent applicable to the Processor as a processor) in force from time to time in the region where the Solution is delivered including the General Data Protection Regulation ((EU) 2016/679); the UK GDPR; the Data Protection Act 2018; the Finnish Data Protection Act (1050/2018); the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), in each case as amended, replaced or supplemented from time to time (including by the UK Data (Use and Access) Act 2025).

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of Personal Data to third countries, adopted by the European Commission by virtue of Commission Implementing Decision (EU) 2021/914, and each as published on the European Union's webpage (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en) or any subsequent version thereof published by the European Commission or of any equivalent contractual clauses approved by it.

Services: means the Solution and other supporting services.

Sub-processor: any third party (including any Affiliate of the Processor) engaged by the Processor that processes Personal Data on behalf of the Controller in connection with the Solution.

Supervisory Authority: an independent public authority responsible for monitoring the application of the Data Protection Legislation.

- 1.2 This DPA is an integral part of the terms of the Agreement. Interpretations and defined terms set forth in the Agreement apply to the interpretation of this DPA.
- 1.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA.
- 1.4 A reference to writing or written includes email.
- 1.5 In the case of conflict or ambiguity between:
 - (a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;
 - (b) the terms of any accompanying invoice or other documents not forming part of this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail;
 - (c) any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail;
 - (d) the provisions of this DPA and the SCCs (where applicable), the SCCs will prevail.
- 1.6 Notwithstanding clause 1.5(c), any liability for breach of data protection obligations under the DPA or the Data Protection Legislation or claims made by Data Subjects shall, as between the parties, be limited in accordance with the Agreement.

2 Personal Data Types and Processing Purposes

- 2.1 The Controller and the Processor acknowledge that for the purpose of the Data Protection Legislation, the Controller is the data controller and the Processor is the data processor.
- 2.2 The Controller retains control of the Personal Data and remains responsible for its compliance obligations under Data Protection Legislation, including providing any required notices and obtaining any required consents, and for ensuring that it has a lawful basis for the processing, and for the processing instructions it gives to the Processor.
- 2.3 The subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Processor may process to fulfil the Business Purposes of the Agreement shall be outlined in Annex 1 of this DPA, the applicable privacy policy available at <https://cloudprotection.com/legal/privacy-policy/> and in the Agreement.

3 Processor's Rights and Obligations

- 3.1 The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Controller's written instructions. This DPA and the Agreement are the Controller's complete documented instructions at the date of the Agreement. Any additional or alternative instructions must be agreed in writing. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. The Processor must promptly notify the Controller if, in its opinion, the Controller's instruction would not comply with the Data Protection Legislation. If the Processor is required by law to process Personal Data other than on the Controller's instructions, it will inform the Controller of that legal requirement before processing, unless that law prohibits such information.
- 3.2 The Processor must promptly comply with any reasonable Controller request or instruction requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing, in each case to the extent technically feasible.
- 3.3 The Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Controller or this DPA specifically authorises the disclosure, including to Sub-processors in accordance with clause 8, or as required by law, in which case the Processor will, where legally permitted, inform the Controller before making the disclosure.
- 3.4 The Processor will reasonably assist the Controller with meeting the Controller's compliance obligations under the Data Protection Legislation, in particular Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to the Processor. Assistance that goes beyond the standard functionality of the Solution may be subject to reasonable charges.
- 3.5 The Processor shall notify the Controller if it becomes aware of any change to the Data Protection Legislation that will materially prevent the Processor from performing the Agreement.
- 3.6 The Processor may use data generated in connection with the Controller's use of the Solution to (i) analyse and improve the Solution, and (ii) for statistical purposes, provided that no individual person can be identified from the results.
- 3.7 Taking into account the nature of the processing, the Processor will assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects to exercise their rights under the Data Protection Legislation. The Processor will promptly forward to the Controller any such request it receives directly and will not respond to it, other than to refer the Data Subject to the Controller, unless instructed by the Controller or required by law.

4 Processor's Employees

- 4.1 The Processor will ensure that all employees and other personnel authorised to process the Personal Data:
- (a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;
 - (b) have received appropriate training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and
 - (c) are aware both of the Processor's duties and their personal duties under the Data Protection Legislation and this DPA.

- 4.2 The Processor will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable law on all of the Processor's employees with access to the Personal Data.

5 Security

- 5.1 The Processor must implement, having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks to the rights and freedoms of natural persons, appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data. The Processor's current measures are summarised in Annex 2. The Processor may update them from time to time provided the overall level of security is not materially reduced. The Controller is responsible for the security of its own systems and Salesforce environment, including user access and credentials.
- 5.2 The Processor shall implement measures to ensure a level of security appropriate to the risk involved, including as appropriate:
- (a) the pseudonymisation and encryption of Personal Data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident on its own systems; and
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6 Personal Data Breach

- 6.1 The Processor will notify the Controller of any Personal Data Breach affecting the Controller's Personal Data without undue delay after becoming aware of it.
- 6.2 The Processor will without undue delay notify the Controller if it becomes aware of:
- (a) any accidental, unauthorised or unlawful processing of the Personal Data in the Processor's possession or control; or
 - (b) a Personal Data Breach.
- 6.3 Following a Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Processor will reasonably co-operate with the Controller in the Controller's handling of the matter.
- 6.4 The Processor agrees that the Controller has the sole right to determine:
- (a) whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, or others, as required by law or regulation or in the Controller's discretion; and
 - (b) whether the Controller offers any type of remedy to affected Data Subjects, including the nature and extent of such remedy.
- 6.5 A notification of a Personal Data Breach under this clause will, to the extent known to the Processor, describe the nature of the breach (including the categories and approximate number of Data Subjects and Personal Data records concerned), its likely consequences, the measures taken or proposed to

address it, and a contact point for further information. Information not available at the time of notification will be provided in phases without undue further delay.

- 6.6 The Processor will not notify any Data Subject, Supervisory Authority or other third party of a Personal Data Breach affecting the Controller's Personal Data without the Controller's prior written approval, except where the Processor is required to do so by law, in which case the Processor will, where legally permitted, inform the Controller beforehand.

7 Cross-border Transfers of Personal Data

- 7.1 The Controller authorises the Processor, as a documented instruction, to transfer Personal Data inside the EEA and the UK to an extent necessary for efficient provisioning of the Solution. Unless otherwise agreed in writing, Processor may also transfer or access personal data outside EEA. In case of transfer of personal data from European Union to destinations other than EEA countries and UK or countries which are recognized by the European Union with adequate level of legislation protecting Personal Data, Processor shall on behalf of the Controller implement proper safeguards and ensure that such transfers are subject to (i) the appropriate Module of the European Union Standard Contractual Clauses for The Transfer of Personal Data to Third Countries, version 2021 or as superseded by European Commission implementing decision ("SCC"); or (ii) other appropriate transfer mechanisms that provide an adequate level of data protection in compliance with applicable data protection legislation.
- 7.2 Where the Processor relies on the SCCs for the purposes of justifying transfer, the Processor will enter into the applicable Module of the SCCs (including completed annexes) as part of the agreement entered into by the Processor and its respective Affiliates and other Sub-processors situated in destinations other than EEA countries and UK or countries which are recognized by the European Union with adequate level of legislation protecting Personal Data.

8 Subcontractors

- 8.1 The Controller grants the Processor general written authorisation to engage Sub-processors in providing the Solution. This is done to acquire required competencies and resources for the monitoring of the Solution, to increase availability of consultants in the event of a security incident, for geo-redundancy purposes, and to minimize the network traffic lag when accessing the Solution. Processor will ensure that processing by its Sub-processors is always aligned with the purposes of the Agreement, this DPA and any additional instructions agreed to by the parties. The Processor remains fully liable to the Controller for the performance of its Sub-processors' obligations, subject to the limitations of liability in the Agreement.
- 8.2 Processor will make available, including on its website or at Controller's request, a current list of Processor's Sub-processors that process Personal Data. Processor will inform the Controller in advance of any intended addition or replacement of Sub-processors, and the Controller may object to such changes by notifying Processor thereof in writing within seven (7) days of such notice. If the Controller objects on reasonable data protection grounds and the parties cannot resolve the objection in good faith, the Controller may terminate the affected part of the Solution on written notice to the Processor.
- 8.3 Processor undertakes diligent vetting when choosing new Sub-processors. Processor's Sub-processors are bound by a written contract to data protection obligations no less protective than

those in this DPA. Processor has in place measures that are appropriate to the nature of the personal data and risks represented by the processing of personal data by its Sub-processors.

9 Term and Termination

- 9.1 This DPA will remain in full force and effect so long as:
- (a) the Agreement remains in effect; or
 - (b) the Processor retains any Personal Data related to the Agreement in its possession or control.
- 9.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Data will remain in full force and effect.
- 9.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its obligations under the Agreement, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within six (6) months, they may terminate the Agreement on written notice to the other party.

10 Data Return and Destruction

- 10.1 At the Controller's request, the Processor will give the Controller a copy of or access to all or part of the Controller's Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.
- 10.2 On termination of the Agreement for any reason or expiry of its term, the Processor will securely delete or destroy or, if directed in writing by the Controller within thirty (30) days of termination or expiry, return and not retain, all or any Personal Data related to this DPA in its possession or control, except for one copy that it may retain and use for as long as reasonably required for audit purposes only.
- 10.3 The Processor may retain any documents or materials where required to do so under any law, regulation, or government or regulatory body, provided that it continues to protect that Personal Data in accordance with this DPA and processes it only for that purpose.
- 10.4 The Processor will certify in writing that it has destroyed the Personal Data following a written request from the Controller.

11 Records

- 11.1 The Processor will keep accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Controller, as required by Article 30(2) GDPR, including approved Sub-processors, the processing purposes and the technical and organisational security measures referred to in clause 5.1.
- 11.2 The Processor will ensure that the records are sufficient to enable the Controller to verify the Processor's compliance with its obligations under this DPA and the Processor will provide the Controller with copies of the records upon request, subject to appropriate confidentiality obligations and the Processor's right to redact commercially or security-sensitive information.

- 11.3 The Controller and the Processor shall review the information listed in the Annexes to this DPA from time-to-time to confirm its current accuracy and update it when required to reflect current practices.

12 Audit

- 12.1 During the validity of the Agreement, the Controller is permitted to audit Processor's processes that are involved in processing Personal Data on behalf of the Controller. Any such audit shall be carried out via independent third party auditors reasonably acceptable to Processor and no more frequently than once every twelve (12) months. Before requesting an audit, the Controller will first review the Processor's then-current third-party certifications or audit reports (such as ISO/IEC 27001), which the Processor will make available on request.
- 12.2 Any audit shall be conducted during regular business hours at Processor's facilities or remotely and shall not unreasonably interfere with Processor's business activities. The Controller shall give at least thirty (30) days' written notice prior to the audit. The Controller or the auditor shall further provide an audit plan (containing scope, high level targets and methods of the audit) in advance to Processor to make relevant assets available for such audit. The auditor shall conduct its work with due process and shall be bound by a written confidentiality undertaking. Processor shall provide the auditor with such cooperation as well as visibility to documents/records and access to staff used in the performance of the Solution as is reasonably necessary for an effective and efficient execution of the audit that does not impose undue strain on Processor, and also subject to Processor's right to refuse visibility to commercially or technically sensitive information, personal data, information regarding its customers or information that would be unlawful to disclose. Further, Processor has the right of rejection to such portions of the plan that could potentially endanger Processor's obligations to third parties or disrupt systems servicing also other parties than the Controller.
- 12.3 Controller will bear all of the costs of audit (including but not limited to costs of the auditor and costs arising from availability of requested Processor's personnel). The Controller shall be liable for any and all damages caused by itself, or its third party auditor, when conducting the audit.

13 Warranties

- 13.1 The Processor warrants that:
- (a) it has taken reasonable steps, as set out in clauses 4.1, 4.2 and 8.3, to ensure that its employees, subcontractors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and appropriately trained in the Data Protection Legislation relating to the Personal Data;
 - (b) it will process the Personal Data in compliance with the Data Protection Legislation applicable to it as a processor and will require its Sub-processors to comply with the obligations set out in clause 8.3;
 - (c) it will take appropriate technical and organisational measures designed to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data.
- 13.2 The Controller warrants that the Processor's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Controller will comply with the Data Protection Legislation. The Controller further warrants that it is authorised to give instructions and to enter into this DPA on behalf of any Affiliates or other controllers on whose behalf Personal Data is processed.

14 Notice

14.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to:

For the Controller: For notices under this DPA, the designated contact person shall be as defined in the Agreement. In the absence of such definition in the Agreement, the general contact person specified in the Agreement shall apply.

For the Processor: legal@cloudprotection.com *with a copy sent to:* Head of Legal, WithSecure Cloud Protection Oy, Välimerenkatu 1, 00180 Helsinki, Finland.

14.2 Clause 14.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This Data Processing Agreement has been entered into on the date of the Agreement.

Annex 1 Details of Processing

The subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Processor may process and transfer personal data to fulfil the Business Purposes of the Agreement shall be outlined in the applicable privacy policy available at <https://cloudprotection.com/> and/or the Agreement.

Further details here:

Nature: Accessing and analyzing personal data in order to facilitate the performance of the Solution.

Types of personal data: Personal data found in the metadata of the files and URLs scanned. In the Identity Protection feature, the email address and related breach data in encrypted format.

Purpose of processing: In order to scan the content for potential malware and to identify breaches.

Duration of processing: During the scanning of the content and deletion near-instantaneously after the analysis, the processing activity will be undertaken during the term of the agreement.

Subprocessors: Cloud Protection uses WithSecure Corporation to provide backend technology for the Solution and Amazon Web Services for data hosting in the Solution. In the Identity Protection feature, the breach data is checked using a Cloud Protection-vetted third-party data source.

Annex 2 Technical and Organizational Measures

Processor has implemented technical and organisational security measures within its organisation that are appropriate to prevent unauthorized access, modification, destruction or loss, unauthorized transmission or other unlawful processing or misuse of personal data and make available information necessary to demonstrate compliance with the data protection obligations to the Client. Processor commits to following the requirements of the ISO 27001 Certified Information Security Management System (ISMS) and producing a ISAE 3000 Type 2 Security Assurance report annually and shall provide a copy of such documentation upon the Client's written request.