



DocuSign Supplemental Data Processing Addendum

## DocuSign Supplemental Data Processing Addendum Instructions

[Home](#) » [DocuSign](#) » DocuSign Supplemental Data Processing Addendum Instructions 

DocuSign Supplemental Data Processing Addendum



# DocuSign Supplemental Data Processing Addendum

## Contents

- [1 HOW TO EXECUTE THIS DPA](#)
- [2 HOW THIS DPA APPLIES](#)
- [3 SCHEDULE 1 Current Sub-Processor List](#)
- [4 SCHEDULE 2 SaaS Services Applicable to Personal Data Processing](#)
- [5 SCHEDULE 3 Details of the Processing](#)
- [6 SCHEDULE 4 Own Security Controls 3.3](#)
- [7 SCHEDULE 5 European Provisions](#)
- [8 Documents / Resources](#)
  - [8.1 References](#)
- [9 Related Posts](#)

## HOW TO EXECUTE THIS DPA

1. This Supplemental DPA consists of two parts: the main body of the Supplemental DPA, and Schedules 1, 2, 3, 4 and 5.
2. This Supplemental DPA has been pre-signed on behalf of Own.
3. To complete this Supplemental DPA, Customer must:
  - a. Complete the Customer Name and Customer Address Section.
  - b. Complete the information in the signature box and sign.
  - c. Verify that the information on Schedule 3 ("Details of the Processing") accurately reflects the subjects and categories of data to be processed.
  - d. Send the completed and signed Supplemental DPA to Own at [privacy@owndata.com](mailto:privacy@owndata.com).

Upon Own's receipt of the validly completed Supplemental DPA at this email address, this Supplemental DPA will become legally binding.

Signature of this Supplemental DPA on page 3 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses (including their Appendices) and the UK Addendum, both incorporated herein by reference.

## HOW THIS DPA APPLIES

If the Customer entity signing this Supplemental DPA is a party to the Agreement, this Supplemental DPA is an addendum to and forms part of the Agreement or Existing DPA. In such case, the Own entity that is party to the Agreement or Existing DPA is party to this DPA.

If the Customer entity signing this Supplemental DPA has executed an Order Form with Own or its Affiliate pursuant to the Agreement or Existing DPA, but is not itself a party to the Agreement or Existing DPA, this Supplemental DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Own entity that is party to such Order Form is party to this Supplemental DPA.

If the Customer entity signing this Supplemental DPA is neither a party to an Order Form nor the Agreement or Existing DPA, this Supplemental DPA is not valid and is not legally binding. Such entity should request that the Customer entity that is a party to the Agreement or Existing DPA execute this Supplemental DPA.

If the Customer entity signing the Supplemental DPA is not a party to an Order Form nor a Master Subscription Agreement or Existing DPA directly with Own, but is instead a customer indirectly via an authorized reseller of Own services, this Supplemental DPA is not valid and is not legally binding. Such entity should contact the

authorized reseller to discuss whether an amendment to its agreement with that reseller is required.

In the event of any conflict or inconsistency between this Supplemental DPA and any other agreement between Customer and Own (including, without limitation, the Agreement or Existing DPA), the terms of this Supplemental DPA shall control and prevail.

This Supplemental Data Processing Addendum, including its Schedules and Appendices, ("Supplemental DPA") forms part of the existing Data Processing Addendum identified above ("Existing DPA") between OwnBackup Inc. ("Own") and the Customer. Combined this Supplemental DPA and the Existing DPA shall form the complete data processing agreement (the "DPA") to document the parties' agreement regarding the Processing of Personal Data. If such Customer entity and Own have not entered into an Agreement, then this DPA is void and of no legal effect.

The Customer entity named above enters into this Supplemental DPA for itself and, if any of its Affiliates act as Controllers of Personal Data, on behalf of those Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the SaaS Services to Customer under the Agreement, Own may Process Personal Data on behalf of Customer. The parties agree to the following supplemental terms with respect to such Processing.

## 1. DEFINITIONS

**"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et. seq., as amended by the California Privacy Rights Act of 2020 and together with any implementing regulations.

**"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data and is deemed to also refer to a "business" as defined in the CCPA.

**"Customer"** means the entity named above and its Affiliates.

**"Data Protection Laws and Regulations"** means all laws and regulations of the European Union and its member states, the European Economic Area and its member states, the United Kingdom, Switzerland, the United States, Canada, New Zealand, and Australia, and their respective political subdivisions, applicable to the Processing of Personal Data. These include, but are not limited to, the following, to the extent applicable: the GDPR, UK Data Protection Law, the CCPA, the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act and related regulations ("CPA"), the Utah Consumer Privacy Act ("UCPA"), and the Connecticut Act Concerning Personal Data Privacy and Online Monitoring (the "CPDPA").

**"Data Subject"** means the identified or identifiable person to whom Personal Data relates and includes **"consumer"** as defined in Data Protection Laws and Regulations. **"Europe"** means the European Union, the European Economic Area, Switzerland, and the United Kingdom. Additional provisions applicable to transfers of Personal Data from Europe are contained in Schedule 5. In the event that Schedule 5 is removed, Customer warrants that it shall not process Personal Data subject to the Data Protection Laws and Regulations of Europe.

**"GDPR"** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

**"Own Group"** means Own and its Affiliates engaged in the Processing of Personal Data.

**"Personal Data"** means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data, personal information, or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

**“Personal Data Processing Services”** means the SaaS Services listed in Schedule 2, for which Own may process Personal Data.

**“Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Processor”** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

**“Standard Contractual Clauses”** means the Annex to the European Commission’s implementing decision (EU) 2021/914 [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union and subject to required amendments for the United Kingdom and Switzerland further described in Schedule 5.

**“Sub-processor”** means any Processor engaged by Own, by a member of the Own Group or by another Sub-processor.

**“Supervisory Authority”** means a governmental or government-chartered regulatory body having binding legal authority over Customer.

**“UK Addendum”** means the United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of 21 March 2022 at <https://ico.org.uk/for-organisations/guideto-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transferagreement-and-guidance/>), completed as described in Schedule 5.

**“UK Data Protection Law”** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as may be amended from time to time by the Data Protection Laws and Regulations of the United Kingdom.

## 2. ORDER OF PRECEDENCE

a. With the exception of the Standard Contractual Clauses incorporated herein, which shall take precedence, in the event of any inconsistency between this Supplemental DPA and the Existing DPA, the terms of the Existing DPA shall prevail.

## 3. LIMITATION OF LIABILITY

a. To the extent permitted by Data Protection Laws and Regulations, each party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this Supplemental DPA, whether in contract, tort or under any other theory of liability, is subject to the “Liability Limit” clauses, and such other clauses that exclude or limit liability, of the Agreement, and any reference in such clauses to the liability of a party means the aggregate liability of that party and all of its Affiliates.

## 4. CHANGES TO TRANSFER MECHANISMS

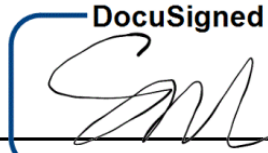
a. In the event that a current transfer mechanism relied upon by the parties for the facilitation of transfers of Personal Data to one or more countries that do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations is invalidated, amended, or replaced the parties will work in good-faith to enact such alternative transfer mechanism to enable the continued Processing of Personal Data contemplated by the Agreement. The use of such alternative transfer mechanism shall be subject to each party’s fulfilment of all legal requirements for use of such transfer mechanism.

The parties' authorized signatories have duly executed this Agreement, including all applicable Schedules, Annexes, and Appendices incorporated herein.

**OWNBACKUP INC.**

DocuSigned by:

Signed: \_\_\_\_\_

  
F58AAB0EA4A04FA...  
**Sam Gutmann**

Name: \_\_\_\_\_

Title: **Chief Executive Officer**

Date: **Sep 27, 2023**

#### List of Schedules

**Schedule 1:** Current Sub-Processor List

**Schedule 2:** SaaS Services Applicable to Personal Data Processing

**Schedule 3:** Details of the Processing

**Schedule 4:** Own Security Controls

**Schedule 5:** European Provisions

#### SCHEDULE 1 Current Sub-Processor List

Sub-Processor Name	Sub-Processor Address	Nature of Processing	Duration of Processing	Location of Processing
OwnBackup Limited	3 Aluf Kalman Magen StZ, Tel Aviv 610707 5, Israel	Customer support and maintenance	For the term of the Agreement.	Israel
Amazon Web Services, Inc.*	410 Terry Avenue North, Seattle, Washington 98109, USA	Application hosting and data storage	For the term of the Agreement.	United States, Canada, Germany, United Kingdom, or Australia
Microsoft Corporation (Azure)*	One Microsoft Way, Redmond, Washington 98052, USA	Application hosting and data storage	For the term of the Agreement.	Netherlands or United States
Elasticsearch, Inc.**	800 West El Camino Real, Suite 350, Mountain View, California 94040, USA	Indexing and search	For the term of the Agreement.	Netherlands or United States

\* Customer may choose either Amazon Web Services or Microsoft (Azure) and its desired Location of Processing during Customer's initial setup of the SaaS Services.

\*\* Applies only to Archive customers that choose to deploy in the Microsoft (Azure) Cloud.

#### SCHEDULE 2 SaaS Services Applicable to Personal Data Processing

- Recover for ServiceNow
- Recover for Dynamics
- Recover for Salesforce
- Governance Plus for Salesforce
- Archive
- Bring Your Own Key Management
- Accelerate

## **SCHEDULE 3 Details of the Processing**

### **Data Exporter**

**Full Legal Name:** Customer Name as specified above

**Main Address:** Customer Address as specified above

**Contact:** If not otherwise provided this shall be the primary contact on the Customer account.

**Contact Email:** If not otherwise provided this shall be the primary contact email address on the Customer account.

### **Data Importer**

**Full Legal Name:** OwnBackup Inc.

**Main Address:** 940 Sylvan Ave, Englewood Cliffs, NJ 07632, USA

**Contact:** Privacy Officer

**Contact Email:** [privacy@owndata.com](mailto:privacy@owndata.com)

### **Nature and Purpose of Processing**

Own will Process Personal Data as necessary to perform the SaaS Services pursuant to the Agreement and Orders, and as further instructed by Customer in its use of the SaaS Services.

### **Duration of Processing**

Own will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

### **Retention**

Own will retain Personal Data in the SaaS Services for the duration of the Agreement, unless otherwise agreed in writing, subject to the maximum retention period specified in the Documentation.

### **Frequency of Transfer**

As determined by Customer through their use of the SaaS Services.

### **Transfers to Sub-processor(s)**

As necessary to perform the SaaS Services pursuant to the Agreement and Orders, and as further described in Schedule 1.

### **Categories of Data Subjects**

Customer may submit Personal Data to the SaaS Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons) Customer's users authorized by Customer to use the SaaS Services

### **Type of Personal Data**

Customer may submit Personal Data to the SaaS Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Localisation data

### **Special categories of data (if appropriate)**

Customer may submit special categories of Personal Data to the SaaS Services, the extent of which is determined and controlled by Customer in its sole discretion, and which for the sake of clarity could include the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning health. See the measures in Schedule 4 for how Own protects special categories of data and other personal data.

## **SCHEDULE 4 Own Security Controls 3.3**

### **1. Introduction**

1. Own software-as-a-service applications (SaaS Services) were designed from the beginning with security in mind. The SaaS Services are architected with a variety of security controls across multiple tiers to address a range of security risks. These security controls are subject to change; however, any changes will maintain or improve the overall security posture.
2. The descriptions of controls below apply to the SaaS Service implementations on both the Amazon Web Services (AWS) and Microsoft Azure (Azure) platforms (together referred to as our Cloud Service Providers, or CSPs), except as specified in the Encryption section below. These descriptions of controls do not apply to RevCult software except as provided under "Secure Software Development" below.

### **2. Audits and Certifications**

1. The SaaS Services are certified under ISO/IEC 27001:2013 (Information Security Management System) and ISO/IEC 27701:2019 (Privacy Information Management System).

2. Own undergoes an annual SOC2 Type II audit under SSAE-18 to independently verify the effectiveness of its information security practices, policies, procedures, and operations for the following Trust Services Criteria: Security, Availability, Confidentiality, and Processing Integrity.
3. Own utilizes global CSP regions for its computing and storage for the SaaS Services. AWS and Azure are top-tier facilities with several accreditations, including SOC1 – SSAE-18, SOC2, SOC3, ISO 27001, and HIPAA.

### **3. Web Application Security Controls**

1. Customer access to the SaaS Services is only via HTTPS (TLS1.2+), establishing the encryption of the data in transit between the end-user and the application and between Own and the third-party data source (e.g., Salesforce).
2. The customer's SaaS Service administrators can provision and de-provision SaaS Service users and associated access as necessary.
3. The SaaS Services provide for role-based access controls to enable customers to manage multi-org permissions.
4. The customer's SaaS Service administrators can access audit trails including username, action, timestamp, and source IP address fields. Audit logs can be viewed and exported by the customer's SaaS Service administrator logged into the SaaS Services as well as through the SaaS Services API.
5. Access to the SaaS Services can be restricted by source IP address.
6. The SaaS Services allow customers to enable multi-factor authentication for accessing SaaS Service accounts utilizing time-based one-time passwords.
7. The SaaS Services allow customers to enable single sign-on via SAML 2.0 identity providers.
8. The SaaS Services allow customers to enable customizable password policies to help align SaaS Service passwords to corporate policies.

### **4. Encryption**

1. Own offers the following SaaS Service options for encryption of data at rest:
  1. Standard offering.
    - Data is encrypted using AES-256 server-side encryption via a key management system validated under FIPS 140-2.
    - Envelope encryption is utilized such that the master key never leaves the Hardware Security Module (HSM).
    - Encryption keys are rotated no less than every two years.
  2. Advanced Key Management (AKM) option.
    - Data is encrypted in a dedicated object storage container with a customer-provided master encryption key (CMK).
    - AKM allows for future archiving of the key and rotating it with another master encryption key.
    - The customer can revoke master encryption keys, resulting in the immediate inaccessibility of the data.
  3. Bring Your Own Key Management System (KMS) option (available on AWS only).
    - Encryption keys are created in the customer's own, separately purchased account utilizing AWS KMS.
    - The customer defines the encryption key policy that permits the customer's SaaS Service account on AWS to access the key from customer's own AWS KMS.
    - Data is encrypted in a dedicated object storage container managed by Own, and configured



to use the customer's encryption key.

- The customer may instantly revoke access to the encrypted data by revoking Own's access to the encryption key, without interacting with Own.
- Own employees have no access to the encryption keys at any time and do not access the KMS directly.
- All key usage activities are logged in the customer's KMS, including key retrieval by the dedicated object storage.

4. Encryption in transit between the SaaS Services and the third-party data source (e.g., Salesforce) utilizes HTTPS with TLS 1.2+ and OAuth 2.0.

## **5. Network**

1. The SaaS Services utilize CSP network controls to restrict network ingress and egress.
2. Stateful security groups are employed to limit network ingress and egress to authorized endpoints.
3. The SaaS Services use a multi-tier network architecture, including multiple, logically separated Amazon Virtual Private Clouds (VPCs) or Azure Virtual Networks (VNETs), leveraging private, DMZs, and untrusted zones within the CSP infrastructure.
4. In AWS, VPC S3 Endpoint restrictions are used in each region to permit access only from the authorized VPCs.

## **6. Monitoring and Auditing**

1. The SaaS Service systems and networks are monitored for security incidents, system health, network abnormalities, and availability.
2. The SaaS Services uses an intrusion detection system (IDS) to monitor network activity and alert Own of suspicious behavior.
3. The SaaS Services use web application firewalls (WAFs) for all public web services.
4. Own logs application, network, user, and operating system events to a local syslog server and a region specific SIEM. These logs are automatically analyzed and reviewed for suspicious activity and threats. Any anomalies are escalated as appropriate.
5. Own utilizes security information and event management (SIEM) systems providing continuous security analysis of the SaaS Services' networks and security environment, user anomaly alerting, command and control (C&C) attack reconnaissance, automated threat detection, and reporting of indicators of compromise (IOC). All of these capabilities are administered by Own's security and operations staff.
6. Own's incident response team monitors the [security@owndata.com](mailto:security@owndata.com) alias and responds according to the company's Incident Response Plan (IRP) when appropriate.

## **7. Isolation Between Accounts**

1. The SaaS Services use Linux sandboxing to isolate customer accounts' data during processing. This helps to ensure that any anomaly (for example, due to a security issue or a software bug) remains confined to a single Own account.
2. Tenant data access is controlled through unique IAM users with data tagging that disallows unauthorized users from accessing the tenant data.

## **8. Disaster Recovery**

1. Own uses CSP object storage to store encrypted customer data across multiple availability-zones.
2. For customer data stored on object storage, Own uses object versioning with automatic aging to support compliance with Own's disaster recovery and backup policies. For these objects, Own's systems are designed to support a recovery point objective (RPO) of 0 hours (that is, the ability to restore to any version of any object as it existed in the prior 14-day period).

3. Any required recovery of a compute instance is accomplished by rebuilding the instance based on Own's configuration management automation.
4. Own's Disaster Recovery Plan is designed to support a 4-hour recovery time objective (RTO).

#### **9. Vulnerability Management**

1. Own performs periodic web application vulnerability assessments, static code analysis, and external dynamic assessments as part of its continuous monitoring program to help ensure application security controls are properly applied and operating effectively.
2. On a semi-annual basis, Own hires independent third-party penetration testers to perform both network and web vulnerability assessments. The scope of these external audits includes compliance against the Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities ([www.owasp.org](http://www.owasp.org)).
3. Vulnerability assessment results are incorporated into the Own software development lifecycle (SDLC) to remediate identified vulnerabilities. Specific vulnerabilities are prioritized and entered into the Own internal ticket system for tracking through resolution.

#### **10. Incident Response**

1. In the event of a potential security breach, the Own Incident Response Team will perform an assessment of the situation and develop appropriate mitigation strategies. If a potential breach is confirmed, Own will immediately act to mitigate the breach and preserve forensic evidence, and will notify impacted customers' primary points of contact without undue delay to brief them on the situation and provide resolution status updates.

#### **11. Secure Software Development**

1. Own employs secure development practices for Own and RevCult software applications throughout the software development life cycle. These practices include static code analysis, Salesforce security review for RevCult applications and for Own applications installed in customers' Salesforce instances, peer review of code changes, restricting source code repository access based on the principle of least privilege, and logging source code repository access and changes.

#### **12. Dedicated Security Team**

1. Own has a dedicated security team with over 100 years of combined multi-faceted information security experience. Additionally, the team members maintain a number of industry-recognized certifications, including but not limited to CISM, CISSP, and ISO 27001 Lead Auditors.

#### **13. Privacy and Data Protection**

1. Own provides native support for data subject access requests, such as the right to erasure (right to be forgotten) and anonymization, to support compliance with data privacy regulations, including the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA). Own also provides a Data Processing Addendum to address privacy and data protection laws, including legal requirements for international data transfers.

#### **14. Background Checks**

1. Own performs a panel of background checks, including criminal background checks, of its personnel who may have access to customers' data, based on the employee's jurisdictions of residence during the prior seven years, subject to applicable law.

#### **15. Insurance**

Own maintains, at minimum, the following insurance coverage: (a) workers' compensation insurance in accordance with all applicable law; (b) automobile liability insurance for non-owned and hired vehicles, with a combined single limit of \$1,000,000; (c) commercial general liability (public liability) insurance with single limit

coverage of \$1,000,000 per occurrence and \$2,000,000 general aggregate coverage; (d) errors and omissions (professional indemnity) insurance with a limit of \$20,000,000 per event and \$20,000,000 aggregate, including primary and excess layers, and including cyber liability, technology and professional services, technology products, data and network security, breach response, regulatory defense and penalties, cyber extortion and data recovery liabilities; and (e) employee dishonesty/crime insurance with coverage of \$5,000,000. Own will furnish to Customer evidence of such insurance upon request.

## **SCHEDULE 5 European Provisions**

This schedule shall only apply to transfers of Personal Data (including onward transfers) from Europe that, in the absence of the application of these provisions, would cause either Customer or Own to breach applicable Data Protection Laws and Regulations.

### **1. Transfer Mechanism for Data Transfers.**

**a)** The Standard Contractual Clauses apply to any transfers of Personal Data under this Supplemental DPA from Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of such territories, to the extent such transfers are subject to such Data Protection Laws and Regulations. Own enters into the Standard Contractual Clauses as data importer. The additional terms in this Schedule also apply to such data transfers.

### **2. Transfers Subject to the Standard Contractual Clauses.**

**a)** Customers Covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Schedule apply to (i) Customer, to the extent Customer is subject to the Data Protection Laws and Regulations of Europe and, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses and this Schedule, such entities are “data exporters.”

**b)** Modules. The Parties agree that where optional modules may be applied within the Standard Contractual Clauses, that only those labelled “MODULE TWO: Transfer controller to processor” shall be applied.

**c)** Instructions. The Parties agree that Customer’s use of the Personal Data Processing Services in accordance with the Agreement and the Existing DPA are deemed to be instructions by Customer to process Personal Data for the purposes of Clause 8.1 of the Standard Contractual Clauses.


**d)** Appointment of New Sub-processors and List of Current Sub-processors. Pursuant to OPTION 2 to Clause 9(a) of the Standard Contractual Clauses, Customer agrees that Own may engage new Sub processors as described in the Existing DPA and that Own’s Affiliates may be retained as Sub-processors, and Own and Own’s Affiliates may engage third-party Sub-processors in connection with the provision of the Data Processing Services. The current list of Sub-processors as attached as Schedule 1.

**e)** Sub-processor Agreements. The parties agree that data transfers to Sub-processors may rely on a transfer mechanism other than the Standard Contractual Clauses (for example, binding corporate rules), and that Own’s agreements with such Sub-processors may therefore not incorporate or mirror the Standard Contractual Clauses, notwithstanding anything to the contrary in clause 9(b) of the Standard Contractual Clauses. However, any such agreement with a Sub-processor shall contain data protection obligations not less protective than those in this Supplemental DPA regarding protection of Customer Data, to the extent applicable to the services provided by such Sub-processor. Copies of the Sub-processor agreements that must be provided by Own to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses will be provided by Own only upon the written request of Customer and may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Own beforehand.

- f) Audits and Certifications.** The parties agree that the audits described in Clause 8.9 and Clause 13(b) of the Standard Contractual Clauses shall be carried out in accordance with the terms of the Existing DPA.
- g) Erasure of Data.** The parties agree that the erasure or return of data contemplated by Clause 8.5 or Clause 16(d) of the Standard Contractual Clauses shall be done in accordance with the terms of the Existing DPA and any certification of deletion shall be provided by Own only upon Customer's request.
- h) Third-Party Beneficiaries.** The parties agree that based on the nature of the SaaS Services, Customer shall provide all assistance required to allow Own to meet its obligations to data subjects under Clause 3 of the Standard Contractual Clauses.
- i) Impact Assessment.** In accordance with Clause 14 of the Standard Contractual Clauses the parties have conducted an analysis, in the context of the specific circumstances of the transfer, of the laws and practices of the destination country, as well as the specific supplemental contractual, organizational, and technical safeguards that apply, and, based on information reasonably known to them at the time, have determined that the laws and practices of the destination country do not prevent the parties from fulfilling each party's obligations under the Standard Contractual Clauses.
- j) Governing Law and Forum.** The parties agree, with respect to OPTION 2 to Clause 17, that in the event that the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, the Standard Contractual Clauses shall be governed by the law of Ireland. In accordance with Clause 18, disputes associated with the Standard Contractual Clauses shall be resolved by the courts specified in the Agreement, unless such court is not located in an EU Member State, in which case the forum for such disputes shall be the courts of Ireland.
- k) Annexes.** For purposes of execution of the Standard Contractual Clauses, Schedule 3: Details of the Processing shall be incorporated as ANNEX IA and IB, Schedule 4: Own Security Controls (which may be updated from time to time at <https://www.owndata.com/trust/>) shall be incorporated as ANNEX II, and Schedule 1: Current Sub Processor List (as may be updated from time-to-time at <https://www.owndata.com/legal/sub-p/>) shall be incorporated as ANNEX III.
- l) Interpretation.** The terms of this Schedule are intended to clarify and not to modify the Standard Contractual Clauses. In the event of any conflict or inconsistency between the body of this Schedule and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
- 3. Provisions Applicable to Transfers from Switzerland** The parties agree that for purposes of the applicability of the Standard Contractual Clauses to facilitate transfers of Personal Data from Switzerland the following additional provisions shall apply: (i) Any references to Regulation (EU) 2016/679 shall be interpreted to reference the corresponding provisions of the Swiss Federal Act on Data Protection and other data protection laws of Switzerland ("Swiss Data Protection Laws"), (ii) Any references to "Member State" or "EU Member State" or "EU" shall be interpreted to reference Switzerland, and (iii) Any references to Supervisory Authority, shall interpreted to refer to the Swiss Federal Data Protection and Information Commissioner.
- 4. a) Table 1:** The parties, their details, and their contacts are those set forth in Schedule 3.
- b) Table 2:** the "Approved EU Standard Contractual Clauses" shall be the Standard Contractual Clauses as set forth in this Schedule 5.
- c) Table 3:** Annexes I(A), I(B), and II are completed as set forth in section 2(k) of this Schedule 5.
- d) Table 4:** Own may exercise the optional early termination right described in Section 19 of the UK Addendum.



## Documents / Resources

	<a href="#">DocuSign Supplemental Data Processing Addendum</a> [pdf] Instructions Supplemental Data Processing Addendum, Data Processing Addendum, Processing Addendum, Addendum
--	--

## References

-  [OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation](#)
-  [OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation](#)
-  [Trust - Security & Privacy - Own](#)
- [User Manual](#)