

[Sign in](#)[Terms of Service](#)[Privacy Policy](#)[Business Agreement](#)[DMCA Policy](#)[Acceptable Use](#)

This section of the agreement only applies to [Dropbox Business](#) customers. If your organization signed a Dropbox Business or Dropbox Enterprise Agreement with Dropbox, that Agreement may be different from the terms below. Please [contact your organization's Admin](#) for details.

Dropbox Business Agreement

Posted: 14 September 2016

This Dropbox Business Agreement (the "Agreement") is between Dropbox International Unlimited Company if your organisation is based outside the United States, Canada and Mexico ("North America") or, if your organisation is based in North America, with Dropbox, Inc., a Delaware corporation (each, "Dropbox") and the organisation agreeing to these terms ("Customer"). This Agreement governs access to and use of the Dropbox Business client software and services (together, "Dropbox Business"), as well as the Beta Services that are made available to you (together, with Dropbox Business, the "Services"). By clicking "I agree", signing your contract for the Services or using the Services, you agree to this Agreement as a Customer.

To the extent that Dropbox, Inc. is, on behalf of the Customer, processing Customer Data that is subject to national laws implementing EU Data Protection Directive (95/46/EC) ("EU Data Protection Laws"), by clicking "I agree", you are also agreeing to the EU Standard Contractual Clauses with Dropbox, Inc. for the transfer of personal data to processors set forth in Schedule 1.

If you are agreeing to this Agreement and Schedule 1 (if applicable) for use of the Services by an organisation, you are agreeing on behalf of that organisation. You must have the authority to bind that organisation to these terms, otherwise you must not sign up for the Services.

1. Services.

- a. **Provision of Services.** Customer and users of Customer's Services account ("**End Users**") may access and use the Services in accordance with this Agreement.
- b. **Facilities and Data Processing.** Dropbox will use, at a minimum, industry standard technical and organisational security measures to transfer, store and process Customer Data. These measures are designed to protect the integrity of Customer Data and guard against the unauthorised or unlawful access to, use and processing of Customer Data. The Customer agrees that Dropbox may transfer, store and process Customer Data in the United States and locations other than the Customer's country. To the extent that Customer Data is subject to EU Data Protection Laws and is processed by Dropbox as a data processor acting on the Customer's behalf (as a data controller), Dropbox will use and process such Customer Data as the Customer instructs in order to provide the Services and fulfil Dropbox's obligations under the Agreement. "**Customer Data**" means Stored Data and Account Data. "**Stored Data**" means the files and structured data submitted to the Services by the Customer or End Users. "**Account Data**" means the account and contact information submitted to the Services by the Customer or End Users.
- c. **Modifications to the Services.** Dropbox may update the Services from time to time. If Dropbox changes the Services in a manner that materially reduces their functionality, Dropbox will inform Customer via the email address associated with the account.
- d. **Software.** Some Services allow Customer to download Dropbox software, which may be updated automatically. Customer may use the software only to access the Services. If any component of the software is offered under an open source licence, Dropbox will make the licence available to Customer and the provisions of that licence may expressly override some of the terms of this Agreement.
- e. **Beta Services.** Dropbox may provide features or products that we are still testing and evaluating. These products and features are identified as alpha, beta, preview, early access or evaluation (or words or phrases with similar meanings) (collectively "**Beta Services**"). Notwithstanding anything to the contrary in this Agreement or in Schedule 1, the following terms apply to all Beta Services: (a) you may use or decline to use any Beta Services; (b) Beta Services may not be supported and may be changed at any time without notice to you; (c) Beta Services may not be as reliable or available as Dropbox Business; (d) Beta Services have not been subjected to the same security measures and auditing to which Dropbox Business has been subjected; and (e) DROPBOX WILL HAVE NO LIABILITY ARISING OUT OF OR IN CONNECTION WITH BETA SERVICES - USE AT YOUR OWN RISK.

2. Customer Obligations.

- a. **Compliance.** Customer is responsible for use of the Services by its End Users. Customer and its End Users must use the Services in compliance with the [Acceptable Use Policy](#). Customer will obtain from End Users any consents necessary to allow Administrators to engage in the activities described in this Agreement and to allow Dropbox to provide the Services. Customer will comply with laws and regulations applicable to Customer's use of the Services, if any.
- b. **Customer Administration of the Services.** The Customer may specify End Users as "**Administrators**" through the administrative console. Administrators may have the ability to access, disclose, restrict or remove Customer Data in or from Services accounts. Administrators may

also have the ability to monitor, restrict or terminate access to Services accounts. Dropbox's responsibilities do not extend to the internal management or administration of the Services. The Customer is responsible for: (i) maintaining the confidentiality of passwords and Administrator accounts; (ii) managing access to Administrator accounts; and (iii) ensuring that Administrators' use of the Services complies with this Agreement. The Customer acknowledges that, if the Customer purchases the Services through a reseller and delegates any of such reseller's personnel as Administrators of the Customer's Services account, such reseller may be able to control account information, including Customer Data, and access the Customer's Services account as further described above.

c. **Unauthorised Use & Access.** Customer will prevent unauthorised use of the Services by its End Users and terminate any unauthorised use of or access to the Services. The Services are not intended for End Users under the age of 13. Customer will ensure that it does not allow any person under 13 to use the Services. Customer will promptly notify Dropbox of any unauthorised use of or access to the Services.

d. **Restricted Uses.** Customer will not (i) sell, resell or lease the Services; (ii) use the Services for activities where use or failure of the Services could lead to physical damage, death or personal injury; or (iii) reverse engineer the Services, nor attempt nor assist anyone else to do so, unless this restriction is prohibited by law.

e. **Third-party Requests.**

i. **"Third-party Request"** means a request from a third party for records relating to an End User's use of the Services including information in or from an End User or Customer's Services account. Third-party Requests may include valid search warrants, court orders or subpoenas, or any other request for which there is written consent from End Users permitting a disclosure.

ii. Customer is responsible for responding to Third-party Requests via its own access to information. Customer will seek to obtain information required to respond to Third-party Requests and will contact Dropbox only if it cannot obtain such information despite diligent efforts.

iii. Dropbox will make commercially reasonable efforts, to the extent allowed by law and by the terms of the Third-party Request, to: (A) promptly notify Customer of Dropbox's receipt of a Third-party Request; (B) comply with Customer's commercially reasonable requests regarding its efforts to oppose a Third-party Request; and (C) provide Customer with information or tools required for Customer to respond to the Third-party Request (if Customer is otherwise unable to obtain the information). If Customer fails to promptly respond to any Third-party Request, Dropbox may, but will not be obligated to do so.

3. **Third-party Services.** If Customer uses any third-party service (e.g. a service that uses a Dropbox API) with the Services, (a) Dropbox will not be responsible for any act or omission of the third party, including the third party's access to or use of Customer Data and (b) Dropbox does not warrant or support any service provided by the third party.

4. **Suspension**

a. **Of End User Accounts by Dropbox.** If an End User (i) violates this Agreement or (ii) uses the Services in a manner that Dropbox reasonably believes will cause it liability, then Dropbox may request that Customer suspend or terminate the applicable End User account. If Customer fails to promptly suspend or terminate the End User account, then Dropbox may do so.

b. **Security Emergencies.** Notwithstanding anything in this Agreement, if there is a Security Emergency then Dropbox may automatically suspend use of the Services. Dropbox will make commercially reasonable efforts to narrowly tailor the suspension as needed to prevent or terminate the Security Emergency. **"Security Emergency"** means: (i) use of the Services that do or could disrupt the Services, other customers' use of the Services, or the infrastructure used to provide the Services and (ii) unauthorised third-party access to the Services.

5. **Intellectual Property Rights.**

a. **Reservation of Rights.** Except as expressly set forth herein, this Agreement does not grant (i) Dropbox any Intellectual Property Rights in Customer Data or (ii) Customer any Intellectual Property Rights in the Services or Dropbox trademarks and brand features. **"Intellectual Property Rights"** means current and future worldwide rights under patent, copyright, trade secret, trademark, moral rights and other similar rights.

b. **Limited Permission.** Customer grants Dropbox only the limited rights that are reasonably necessary for Dropbox to offer the Services (e.g. hosting Stored Data). This permission also extends to our affiliates and trusted third parties that Dropbox works with to offer the Services (e.g. payment provider used to process payment of fees).

c. **Suggestions.** Dropbox may, at its discretion and for any purpose, use, modify and incorporate into its products and services, licence and sub-licence, any feedback, comments or suggestions that Customer or End Users send Dropbox or post in Dropbox's forums without any obligation to Customer.

d. **Customer List.** Dropbox may include Customer's name in a list of Dropbox customers on the Dropbox website or in promotional materials.

6. **Fees & Payment.**

a. **Fees.** The Customer will pay, and authorises Dropbox or the Customer's reseller to charge, using the Customer's selected payment method, for all applicable fees. Fees are non-refundable except as required by law. The Customer is responsible for providing complete and accurate billing and contact information to Dropbox or the Customer's reseller. Dropbox may suspend or terminate the Services if fees are overdue.

b. **Auto-renewals and Trials.** IF THE CUSTOMER'S ACCOUNT IS SET TO AUTO-RENEWAL OR IS IN A TRIAL PERIOD, DROPBOX (OR THE

CUSTOMER'S RESELLER) MAY CHARGE AUTOMATICALLY AT THE END OF THE TRIAL OR FOR THE RENEWAL, UNLESS THE CUSTOMER NOTIFIES DROPBOX (OR THE CUSTOMER'S RESELLER, AS APPLICABLE) THAT THE CUSTOMER WANTS TO CANCEL OR DISABLE AUTO-RENEWAL. Dropbox may revise Service rates by providing the Customer at least 30 days notice prior to the next charge.

- c. **Taxes.** The Customer is responsible for all taxes. Dropbox or the Customer's reseller will charge tax when required to do so. If the Customer is required by law to withhold any taxes, the Customer must provide Dropbox or the Customer's reseller with an official tax receipt or other appropriate documentation.
- d. **Purchase Orders.** If the Customer requires the use of a purchase order or purchase order number, the Customer (i) must provide the purchase order number at the time of purchase and (ii) agrees that any terms and conditions on a Customer purchase order will not apply to this Agreement and are null and void. If the Customer is purchasing via a reseller, any terms and conditions from the Customer's reseller or in a purchase order between the Customer and its reseller that conflict with the Dropbox Business Agreement are null and void.

7. Term & Termination.

- a. **Term.** This Agreement will remain in effect until Customer's subscription to the Services expires or terminates, or until the Agreement is terminated.
- b. **Termination for Breach.** Either Dropbox or Customer may terminate this Agreement if: (i) the other party is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written notice or (ii) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within 90 days.
- c. **Effects of Termination.** If this Agreement terminates: (i) the rights granted by Dropbox to Customer will cease immediately (except as set forth in this section); (ii) Dropbox may provide Customer access to its account at then-current fees so that Customer may export its Stored Data; and (iii) after a commercially reasonable period of time, Dropbox may delete any Stored Data relating to Customer's account. The following sections will survive expiry or termination of this Agreement: 2(e) (Third-party Requests), 5 (Intellectual Property Rights), 6 (Fees & Payment), 7(c) (Effects of Termination), 8 (Indemnification), 9 (Disclaimers), 10 (Limitation of Liability), 11 (Disputes) and 12 (Miscellaneous).

8. Indemnification.

- a. **By Customer.** Customer will indemnify, defend and hold harmless Dropbox from and against all liabilities, damages and costs (including settlement costs and reasonable attorneys' fees) arising out of any claim by a third party against Dropbox and its affiliates regarding: (i) Customer Data; (ii) Customer's use of the Services in violation of this Agreement; or (iii) End Users' use of the Services in violation of this Agreement.
- b. **By Dropbox.** Dropbox will indemnify, defend and hold harmless Customer from and against all liabilities, damages and costs (including settlement costs and reasonable attorneys' fees) arising out of any claim by a third party against Customer to the extent based on an allegation that Dropbox's technology used to provide the Services to the Customer infringes or misappropriates any copyright, trade secret, US patent or trademark right of the third party. In no event will Dropbox have any obligations or liability under this section arising from: (i) use of any Services in a modified form or in combination with materials not furnished by Dropbox and (ii) any content, information or data provided by Customer, End Users or other third parties.
- c. **Possible Infringement.** If Dropbox believes the Services infringe or may be alleged to infringe a third party's Intellectual Property Rights, Dropbox may: (i) obtain the right for Customer, at Dropbox's expense, to continue using the Services; (ii) provide a non-infringing functionally equivalent replacement; or (iii) modify the Services so that they no longer infringe. If Dropbox does not believe the options described in this section are commercially reasonable, Dropbox may suspend or terminate Customer's use of the affected Services (with a pro rata refund of pre-paid fees for the Services).
- d. **General.** The party seeking indemnification will promptly notify the other party of the claim and cooperate with the other party in defending the claim. The indemnifying party will have full control and authority over the defence, except that: (i) any settlement requiring the party seeking indemnification to admit liability requires prior written consent, not to be unreasonably withheld or delayed and (ii) the other party may join in the defence with its own counsel at its own expense. THE INDEMNITIES ABOVE ARE DROPBOX AND CUSTOMER'S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY THE OTHER PARTY OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

9. **Disclaimers.** THE SERVICES ARE PROVIDED "AS IS". TO THE FULLEST EXTENT PERMITTED BY LAW, EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, NEITHER CUSTOMER NOR DROPBOX AND ITS AFFILIATES, SUPPLIERS AND DISTRIBUTORS MAKE ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE OR NON-INFRINGEMENT. CUSTOMER IS RESPONSIBLE FOR MAINTAINING AND BACKING UP ANY STORED DATA.

10. Limitation of Liability.

- a. **Limitation on Indirect Liability.** TO THE FULLEST EXTENT PERMITTED BY LAW, EXCEPT FOR DROPBOX OR CUSTOMER'S INDEMNIFICATION OBLIGATIONS, NEITHER CUSTOMER NOR DROPBOX AND ITS AFFILIATES, SUPPLIERS AND DISTRIBUTORS WILL BE LIABLE UNDER THIS AGREEMENT FOR (I) INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES, OR (II) LOSS OF USE, DATA, BUSINESS, REVENUES OR PROFITS (IN EACH CASE WHETHER DIRECT OR INDIRECT), EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE.
- b. **Limitation on Amount of Liability.** TO THE FULLEST EXTENT PERMITTED BY LAW, DROPBOX'S AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL NOT EXCEED THE LESSER OF \$100,000 OR THE AMOUNT PAID BY THE CUSTOMER FOR THE SERVICES HEREUNDER DURING

THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY.

1. Disputes.

- a. **Informal Resolution.** Dropbox wants to address your concerns without resorting to a formal legal case. Before filing a claim, each party agrees to try to resolve the dispute by contacting the other party through the notice procedures in section 12(e). If a dispute is not resolved within 30 days of notice, Customer or Dropbox may bring a formal proceeding.
- b. **Agreement to Arbitrate.** Customer and Dropbox agree to resolve any claims relating to this Agreement or the Services through final and binding arbitration, except as set forth below. The [American Arbitration Association](#) (AAA) will administer the arbitration under its Commercial Arbitration Rules. The arbitration will be held in San Francisco (CA), or any other location both parties agree to in writing.
- c. **Exception to Agreement to Arbitrate.** Either party may bring a lawsuit in the federal or state courts of San Francisco County, California solely for injunctive relief to stop unauthorised use or abuse of the Services or infringement of Intellectual Property Rights without first engaging in the informal dispute notice process described above. Both Customer and Dropbox consent to venue and personal jurisdiction there.
- d. **NO CLASS ACTIONS.** Customer may only resolve disputes with Dropbox on an individual basis and will not bring a claim in a class, consolidated or representative action. Class arbitrations, class actions, private attorney general actions and consolidation with other arbitrations are not allowed.

2. Miscellaneous.

- a. **Terms Modification.** Dropbox may revise this Agreement from time to time and the most current version will always be posted on the Dropbox Business website. If a revision, in Dropbox's sole discretion, is material, Dropbox will notify Customer (by, for example, sending an email to the email address associated with the applicable account). Other revisions may be posted to Dropbox's blog or terms page, and Customer is responsible for checking such postings regularly. By continuing to access or use the Services after revisions become effective, Customer agrees to be bound by the revised Agreement. If Customer does not agree to the revised Agreement terms, Customer may terminate the Services within 30 days of receiving notice of the change.
- b. **Entire Agreement.** This Agreement, including the Customer's invoice and order form with Dropbox (if applicable), constitutes the entire agreement between the Customer and Dropbox with respect to the subject matter of this Agreement, and supersedes and replaces any prior or contemporaneous understandings and agreements, whether written or oral, with respect to the subject matter of this Agreement. If there is a conflict between the documents that make up this Agreement, the documents will control in the following order: the Dropbox invoice, the Dropbox order form, the Agreement.
- c. **Governing Law.** THE AGREEMENT WILL BE GOVERNED BY CALIFORNIA LAW EXCEPT FOR ITS CONFLICTS OF LAWS PRINCIPLES.
- d. **Severability.** Unenforceable provisions will be modified to reflect the parties' intention and only to the extent necessary to make them enforceable, and the remaining provisions of the Agreement will remain in full effect.
- e. **Notice.** Notices must be sent via first class post, airmail or overnight courier and are deemed given when received. Notices to Customer may also be sent to the applicable account email address and are deemed given when sent. Notices to Dropbox must be sent to Dropbox, Inc., P.O. Box 77767, San Francisco, CA 94107, with a copy to the Legal Department.
- f. **Waiver.** A waiver of any default is not a waiver of any subsequent default.
- g. **Assignment.** Customer may not assign or transfer this Agreement or any rights or obligations under this Agreement without the written consent of Dropbox. Dropbox may not assign this Agreement without providing notice to Customer, except Dropbox may assign this Agreement or any rights or obligations under this Agreement to an affiliate or in connection with a merger, acquisition, corporate reorganisation or sale of all or substantially all of its assets without providing notice. Any other attempt to transfer or assign is void.
- h. **No Agency.** Dropbox and Customer are not legal partners or agents, but are independent contractors.
- i. **Force Majeure.** Except for payment obligations, neither Dropbox nor Customer will be liable for inadequate performance to the extent caused by a condition that was beyond the party's reasonable control (for example, natural disaster, act of war or terrorism, riot, labour condition, governmental action and Internet disturbance).
- j. **No Third-party Beneficiaries.** There are no third-party beneficiaries to this Agreement. Without limiting this section, a Customer's End Users are not third-party beneficiaries to Customer's rights under this Agreement.
- k. **Export Restrictions.** The export and re-export of Customer Data via the Services may be controlled by the United States Export Administration Regulations or other applicable export restrictions or embargo. The Services may not be used in Cuba, Iran, North Korea, Sudan or Syria, or any country that is subject to an embargo by the United States and Customer must not use the Services in violation of any export restriction or embargo by the United States or any other applicable jurisdiction. In addition, Customer must ensure that the Services are not provided to persons on the United States Table of Denial Orders, the Entity List or the List of Specially Designated Nationals.

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: **The Customer that is a party to the Dropbox Business Agreement with Dropbox International Unlimited Company**
(the data **exporter**)

And

Name of the data importing organisation: **Dropbox, Inc.**
Address: 333 Brannan Street, San Francisco, CA 94107, USA
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in [Appendix 1](#).

Clause 1
Definitions

For the purposes of the Clauses:

- a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;
- b. 'the data exporter' means the controller who transfers the personal data;
- c. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d. 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written sub-contract;
- e. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f. 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and, in particular, the special categories of personal data where applicable, are specified in Appendix 1, which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

- 1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e) and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- 2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- 3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be

limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 **Obligations of the data exporter**

The data exporter agrees and warrants:

- a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in [Appendix 2](#) of this contract;
- d. that, after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e. that it will ensure compliance with the security measures;
- f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before or as soon as possible after the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g. to forward any notifications received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services, which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j. that it will ensure compliance with Clause 4(a) to (i).

Clause 5 **Obligations of the data importer²**

The data importer agrees and warrants:

- a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to promptly inform the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that, in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- d. that it will promptly notify the data exporter about:
 - i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - ii. any accidental or unauthorised access, and
 - iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e. to deal promptly and properly with all enquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

- f. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses, which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2, which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- i. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- j. to send a copy of any sub-processor agreement it concludes under the Clauses promptly to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.
The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that, if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - a. to refer the dispute to mediation by an independent person or, where applicable, by the supervisory authority;
 - b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall inform the data exporter promptly about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case, the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business-related issues where required, as long as they do not contradict the Clause.

Clause 11 Sub-processing

1. The data importer shall not sub-contract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer sub-contracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor, which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses³. Where the sub-processor fails to fulfil its data protection obligations under such written agreement, the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent, and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that, upon termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all of the personal data transferred and the copies thereof to the data exporter or shall destroy all of the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will no longer actively process the personal data transferred.
2. The data importer and the sub-processor warrant that, upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Additional Provisions

Capitalised terms used in Sections A to C and the Appendices but not defined in the Clauses shall have the meaning provided in the Dropbox Business Agreement between the data exporter and Dropbox International Unlimited Company.

A. Security audit. The data importer maintains ISO/IEC 27001:2013 and ISO/IEC 27018:2014 certifications, which are issued by an independent third-party auditor. The data importer will continue to undergo regular ISO/IEC 27001:2013 and ISO/IEC 27018 audits necessary for maintaining such certifications for the Services during the Term. The data importer also regularly undergoes Service Organization Control 2 (SOC 2) Type II audits. Subject to the data importer's confidentiality obligations, and no more than once a year, the data importer will provide the data exporter with a copy of the SOC 2 Type II Report upon written request. The data importer will make new SOC 2 reports available as they are completed, subject to the data importer's confidentiality requirements. The data importer regularly reviews its third-party sub-service organisations, which undergo Standards for Attestation Engagements No.16 (SSAE 16) / International Standard on Assurance Engagements No.3402 (ISAE 3402) Service Organization Control 1 (SOC 1) Type II or Service Organization Control 2 (SOC 2) Type II audits that evaluate the design and effectiveness of their security policies, procedures and controls.

The data exporter agrees that the data importer's obligations set forth in this Section A fully satisfy the audit rights under Clause 5(f) and Clause 12 (2) of the Clauses.

B. Sub-processing. The data importer may engage other companies to provide limited parts of the Services (including support services) on the data importer's behalf, and the data exporter consents to the data importer sub-contracting the processing of personal data to such sub-processors as described in the Clauses. The data importer will ensure that any sub-processor will only access and use personal data to provide the Services as set forth in a written agreement between the data importer and the sub-processor. The data exporter acknowledges that any requirements applicable to the data importer under the Clauses in respect of agreements with sub-processors shall be satisfied in full provided that the sub-processing agreement between the data importer and the sub-processor provides at least the level of data protection required under the Dropbox Business Agreement.

C. Liability. The Clauses shall be subject to the limitations and exclusions of liability contained in the "Limitation of Liability" section of the Dropbox Business Agreement, such that the total liability of the data importer and Dropbox International Unlimited Company, in aggregate, shall not exceed the limitations set out in the Dropbox Business Agreement. For the avoidance of doubt, the data exporter shall not be entitled to recover from both the data importer and Dropbox International Unlimited Company in respect of the same loss.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The Customer of the Dropbox Business Agreement with Dropbox International Unlimited Company.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Dropbox, Inc., a global provider of cloud services for individuals and businesses. Dropbox, Inc. and its affiliates provide a website, software and mobile applications that allow people to store files, synchronise files across multiple devices and collaborate with others. Dropbox, Inc.'s service may also be accessed by Application Programming Interfaces (APIs).

Data subjects

The personal data transferred concerns the following categories of data subjects (please specify):

The data exporter and data exporter's affiliates' end users including employees, consultants and contractors of the data exporter, as well as any individuals collaborating or sharing with these end users using the services provided by the data importer.

Categories of data

The personal data transferred concerns the following categories of data (please specify):

End user-identifying information and organisation data (both online and offline) as well as documents, images and other content or data in electronic form stored or transmitted by end users via the data importer's services.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The data importer or its sub-processors will use and process personal data, and the data exporter instructs the data importer to use and process personal data in order to provide the Services under the Dropbox Business Agreement.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data privacy contact

The data privacy officer of the data importer can be reached at privacy@dropbox.com

Security measures

The data importer has implemented and will maintain appropriate administrative, technical and physical safeguards to protect personal data as further described in the Dropbox Business security white paper (available as of the effective date at: https://www.dropbox.com/.../Security_Whitepaper.pdf) and additionally set forth below. The data importer may update these security measures from time to time, with the most recent version available at the above URL (or other URL as communicated by the data importer), provided however that the data importer will notify the data exporter if the data importer updates the security measures in a manner that materially diminishes the administrative, technical or physical security features described therein or in this Appendix 2.

1. Service security

1.1 Dropbox architecture. The data importer's service is designed with multiple layers of protection, covering data transfer, encryption, network configuration and application-level controls that are distributed across a scalable, secure infrastructure. End users of the data importer's service can access files and folders at any time from the desktop, web and mobile clients. All of these clients connect to secure services to provide access to files, allow file sharing with others, and update linked devices when files are added, changed or deleted. The service can be utilised and accessed via a number of interfaces. Each has security settings and features that process and protect the data whilst ensuring ease of access.

1.2 Reliability. The data importer's service is developed with multiple layers of redundancy to guard against data loss and ensure availability.

1.3 Encryption. To protect the data in transit between the data exporter and the data importer, the data importer uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data at rest is encrypted using 256-bit AES encryption. The data importer's encryption key management infrastructure is designed with operational, technical and procedural security controls with very limited direct access to keys. Encryption key generation, exchange and storage are distributed for decentralised processing.

1.4 User management features. End users of the data importer's service have the ability to restore lost files and recover previous versions of files, ensuring that changes to those files can be tracked and retrieved. The data importer's service allows for the use of a two-step authentication procedure, which adds an extra layer of protection.

1.5 Data centres. The data importer's corporate and production systems are housed at third-party sub-service organisation data centres located in the United States. The data importer reviews all sub-service organisation data centre Service Organization Control (SOC) 1 and/or SOC 2 reports at least annually to ensure sufficient security controls.

2. Information security.

2.1 Policies. The data importer has established a thorough set of security policies covering areas of information security, physical security, incident response, logical access, physical production access, change management and support. These policies are reviewed and approved at least annually. The data importer personnel are notified of updates to these policies and are provided security training.

2.2 Personnel policy and access. The data importer's internal policies require onboarding procedures that include background checks (as allowed by local laws), security policy acknowledgement, communication of updates to security policy and non-disclosure agreements. All personnel access is removed promptly when an employee or contractor leaves the company. The data importer employs technical access controls and internal policies to prohibit employees or contractors from arbitrarily accessing file data and to restrict access to metadata and other information about end users' accounts. In order to protect end user privacy and security, only a small number of employees or contractors have access to the environment where end user files are stored. A record of access request, justification and approval is kept by management, and access is granted by appropriate individuals.

2.3 Network security. The data importer maintains network security and monitoring techniques that are designed to provide multiple layers of protection and defence. The data importer employs industry-standard protection techniques, including firewalls, network security monitoring and intrusion detection systems to ensure that only eligible traffic is able to reach the data importer's infrastructure.

2.4 Change management. The data importer ensures that security-related changes have been authorised prior to implementation into the production environments. Source code changes are initiated by developers that would like to make an enhancement to a data importer application or service. Changes to the data importer's infrastructure are restricted to authorised personnel only. Changes to the application level of the services are required to go through automated quality assurance ("QA") testing procedures to verify that security requirements are met. Successful completion of QA procedures leads to implementation of the change.

2.5 Compliance. The data importer, its data centre providers and its managed service provider undergo regular security audits performed by an independent third party. The data importer will continue to participate in regular ISO/IEC 27001:2013 and ISO/IEC 27018:2014 audits. The data importer also reviews SOC 1 and/or SOC 2 reports for all sub-service organisations. In the event that a sub-service organisation's SOC 1 and/or SOC 2 report is unavailable, the data importer performs security site visits to verify that applicable physical, environmental and operational security controls satisfy control criteria and contractual requirements. The data importer evaluates additional certifications and compliance attestations, as made available to the data importer by the sub-service providers, on an ongoing basis.

3. Physical security

3.1 Infrastructure. Physical access to sub-service organisation facilities where production systems reside are restricted to personnel authorised by the data importer, as required to perform their job function. Any individuals requiring additional access to production environment facilities are granted that access through explicit approval by appropriate management.

3.2 Office. The data importer maintains a physical security team that is responsible for enforcing a physical security policy and overseeing the security of the data importer's corporate offices. Access to areas containing corporate services is restricted to authorised personnel via elevated roles granted through the badge access system.

Footnotes

- Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone. [↩](#)
- Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax reporting requirements or anti-money-laundering reporting requirements. [↩](#)

3. This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision. [↩](#)

Dropbox	About us	Support	Community	English (United States)
Install	Dropbox Blog	Help Center	Referrals	
Mobile	About	Contact us	Forum	
Pricing	Branding	Copyright	Twitter	
Business	News	Cookies	Facebook	
Enterprise	Jobs	Privacy & Terms	Developers	
Tour				