# Data Processing Agreement
# Shared Email Templates for Outlook

**Effective date: November 18, 2022**

## Table of Contents



## 1. Introduction

This Data Processing Agreement ("**DPA**") is entered into by _____ _____("**Subscriber**") and Office Data Apps sp. z o.o. ("**Company**"), each a "**Party**" and together "the **Parties**". DPA is supplemental to, and incorporated into, the Terms of Use ("**Terms**") (https://www.ablebits.com/docs/outlook-shared-templates-terms-of-use/) between Subscriber and Company.

## 2. Definitions

"**Services**" mean collectively the Shared Email Templates web application located on https://email-templates.app/, Shared Email Templates add-in for Microsoft Outlook available from Microsoft AppSource (https://ablebits.com/go.php?to=shared-email-templates-signup&label=dpa), and Shared Email Templates backend infrastructure located on Amazon Web Services.

"**Personal Data**", "**Personal Data Breach**", "**processing**", "**process**", "**processor**", "**controller**", "**data subject**", and "**Data Subject Request**" shall have the same meaning as in the Applicable Data Protection Law and may be lowercase or capitalized herein.

"**Applicable Data Protection Law**" means, in addition to the regulations applicable to certain jurisdictions referred to in our Privacy Policy, the following data protection law(s), as applicable, including any subsequent amendments, modifications, and revisions thereto:

- 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) ("**GDPR**") and any applicable national laws implemented by European Economic Area ("**EEA**") member countries
- Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded)
- Data Protection Act 2018 (c. 12) of the United Kingdom

"**Subscriber**" means the first party named above. However, in the event Company is required to process Personal Data on the request of an Affiliate of Subscriber, such Affiliate shall also be deemed as "Subscriber". Any reference to Subscriber within this DPA, unless otherwise specified, shall include Subscriber and its Affiliates.

"**User Content**" means all content that Subscriber uploads, creates, sends, distributes, and/or posts on Services, including, but not limited to, email templates, images, graphics, files, text, document or data files, Personal Data, email messages, HTML code, personalization settings, and other information and/or content that is or may be provided to Company or entered and/or uploaded through Services.

"**Sub-processor**" means any third-party data processor engaged by Company, who receives Personal Data from Company for processing on behalf of Subscriber and in accordance with Subscriber's instructions (as communicated by Company) and the terms of the written subcontract.

"**Supervisor**" means any data protection supervisory authority as defined in the GDPR with competence over Subscriber and Company's processing of Personal Data.

—

IN WITNESS WHEREOF, the Parties hereto have executed this DPA by their duly authorized officers or representatives as of the last date of execution below ("**Effective Date**").

## 3. Purpose

Subscriber has agreed to Terms pursuant to which Subscriber is granted a license to access and use Services during the subscription term. In providing Services, Company will engage on behalf of Subscriber in the processing of Personal Data submitted to and stored within Services by Subscriber.

The terms of this DPA shall only apply to:

- Subscribers with an active subscription to Services
- Personal Data within User Content

The Parties are entering into this DPA to ensure that the processing of Subscriber's Personal Data by Company within Services is done in a manner compliant with Applicable Data Protection Law.

To the extent that any terms of Terms conflict with the substantive terms of this DPA (as they relate to the protection of Personal Data), the terms of this DPA shall take precedence.

## 4. Ownership of Personal Data

As between the Parties, all User Content processed under the terms of DPA and Terms shall remain the property of Subscriber. Under no circumstances will Company act, or be deemed to act, as a "controller" of User Content under any Applicable Data Protection Law.

## 5. Obligations of Company

The Parties agree that the subject matter and duration of processing performed by Company under this DPA, including the nature and purpose of processing, the type of Personal Data, and categories of data subjects, shall be as described in **Annex 1** of DPA.

When providing Services to Subscriber under Terms, Company shall comply with the obligations imposed upon it under Article 28-32 of the GDPR and agrees and declares as follows:

- to process Personal Data in accordance with Subscriber's documented instructions as set out in Terms and DPA, also regarding transfers of Personal Data to a third country or an international organization in accordance with Article 28 (3)(a) of the GDPR, unless required to do otherwise by European Union or Member State Law to which Company is subject. In any such case, Company shall inform Subscriber of that legal requirement upon becoming aware of the same (except where prohibited by applicable laws);
- to ensure that all staff and management of Company are fully aware of their responsibilities to protect Personal Data in accordance with DPA and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in accordance with Article 28 (3)(b) of the GDPR;
- to implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, provided that such measures shall consider the state of the art, the costs of implementation, the nature, scope, context, and

purposes of processing and the risks involved in the processing and will include those measures described in **Annex 2**;

- to notify Subscriber in accordance with Article 33(2) of the GDPR, without undue delay, but in any event within forty-eight (48) hours, in the event of a confirmed Personal Data Breach affecting Subscriber's Personal Data and to take appropriate measures to mitigate its possible adverse effects;
- to comply with the requirements of the **Use of Sub-processors** section when engaging a Sub-processor;
- to assist Subscriber, considering the nature of the processing and insofar as it is commercially reasonable, to fulfil Subscriber's obligation to respond to requests from data subjects to exercise their rights under Applicable Data Protection Law (a "**Data Subject Request**");
- upon request, to provide Subscriber with commercially reasonable information and assistance, considering the nature of the processing and the information available to Company, to help Subscriber to conduct any data protection impact assessment, data transfer impact assessment, or Supervisor consultation Subscriber is required to conduct under Applicable Data Protection Law;
- upon termination of Subscriber's access to and use of Services, to comply with the requirements of the **Return and destruction of Personal Data** section;
- to comply with the requirements of the **Third-party certifications and audit** section to make available to Subscriber information that demonstrates Company's compliance with DPA;
- to appoint an officer who will act as a point of contact for Subscriber, coordinate, and control security compliance with DPA, including the measures detailed in **Annex 2**.

Company shall immediately inform Subscriber if, in its opinion, Subscriber's processing instructions infringe any law or regulation. In such event, Company is entitled to refuse processing of Personal Data that it believes to be in violation of any law or regulation.

## 6. Use of Sub-processors

Subscriber hereby confirms its general written authorization for Company's use of the Sub-processors (**Annex 3** to this DPA) in accordance with Article 28 of the GDPR to assist Company in providing Services and processing Personal Data, provided that such Sub-processors:

- agree to act only on Company's instructions when processing Personal Data, which instructions shall be consistent with Subscriber's processing instructions to Company;
- agree to protect Personal Data to a standard consistent with the requirements of this DPA, including implementing and maintaining appropriate technical and organizational measures to protect Personal Data they process consistent with the Sub-processor security standards described in **Annex 4** to this DPA, as applicable.

Company shall remain liable to Subscriber for the subcontracted processing services of any of its Sub-processors under this DPA. Company shall update Sub-processor Policy on its website of any Sub-processor to be appointed at least thirty (30) days prior to such change.

Subscriber may sign up to receive email notifications of any such changes to Company's website.

If Subscriber objects to the processing of its Personal Data by any newly appointed Sub-processor as described in the previous paragraph, it shall inform Company within thirty (30) days following the update of Company Sub-processor Policy. In such event, Company will either:

- instruct Sub-processor to cease the processing of Subscriber's Personal Data, in which event this DPA shall continue unaffected
- or allow Subscriber to terminate this DPA and any related services agreement with Company immediately and provide it with a pro rata reimbursement of any sums paid in advance for Services to be provided, but not yet received by Subscriber as of the effective date of termination.

Services provide links to integrations with non-Company services (e.g., Microsoft identity platform) including, without limitation, certain non-Company services which may be integrated directly into Subscriber's account or instance in Services. If Subscriber elects to enable, access, or use such non-Company services, its access and use of such non-Company services is governed solely by the terms and conditions and privacy policies of such non-Company services, and Company does not endorse and is not responsible or liable for, and makes no representations as to any aspect of such non-Company services, including, without limitation, their content, the manner in which they handle User Content (including Personal Data), or any interaction between Subscriber and the provider of such non-Company services. The providers of non-Company services shall not be deemed Sub-processors for any purpose under this DPA.

## 7. Third-party certifications and audit

Upon Subscriber's request, and subject to the confidentiality obligations, Company shall make available to Subscriber (or Subscriber's independent, third-party auditor) information regarding Company's compliance with the obligations set forth in this DPA in the form of the third-party certifications and/or audits set forth in **Annex 2.**

Subscriber may contact Company to request an audit of Company's procedures relevant to the protection of Personal Data, but only to the extent required under Applicable Data Protection Laws, and Subscriber shall not disrupt Company's business operations during the performance of such audit.

This section applies only to the extent Company is unable to demonstrate compliance with the EU SCCs (as defined hereinafter) through appropriate documentation and information on the processing activities carried out on behalf of Subscriber, considering Company's certifications and audits. By providing a notice to privacy@ablebits.com, Subscriber may ask to exercise the right to perform an audit during normal business hours at Company's premises or physical facilities for the purposes of demonstrating compliance with the EU SCCs (as defined hereinafter) and processing activities and shall be limited to data relevant to Subscriber. Company will make commercially reasonable efforts to comply with such request.

The Parties will mutually agree in advance and in good faith upon the terms of such audit, provided that:

- if the request could, in Company's reasonable opinion, create a risk for another Company Subscriber's environment, Company and Subscriber will agree on an alternative way to address the request to provide Subscriber with a similar level of assurance. For the avoidance of doubt, Subscriber acknowledges that the granting of potential access as stated in this DPA shall in no way be deemed to constitute access or potential access to User Content of other Subscribers;
- unless otherwise agreed in writing by the Parties, Subscriber shall reimburse Company for any time expended for any such on-site access at Company's then-current professional services rates, which shall be made available to Subscriber upon request.

## 8. International data exports

Subscriber acknowledges that Company and its Sub-processors may process Personal Data in countries that are outside of the EEA, United Kingdom, and Switzerland (**"European Countries"**). This will apply even where Subscriber has agreed with Company to host Personal Data in European Countries in accordance with Regional data hosting rules (**Annex 5**) if such non-European Countries processing is necessary to provide support-related or other services requested by Subscriber. If Personal Data is transferred to a country or territory outside of European Countries, then such transfer will only take place if:

- the country ensures an adequate level of data protection;
- one of the conditions listed in Article 46 of the GDPR (or its equivalent under any successor legislation) is satisfied;
- Personal Data is transferred in accordance with Company rules, which establishes appropriate security measures for such Personal Data and is legally binding on Company.

**Standard Contractual Clauses.** Where Company processes Personal Data in non-EEA countries, Company shall comply with the EU Commission's Standard Contractual Clauses (annexed to EU Commission Decision 2021/914/EU of 4 June 2021 (http://data.europa.eu/eli/dec_impl/2021/914/oj) (the "**EU SCCs**")) which shall be entered into and incorporated into this DPA by this reference and completed as follows:

- Module 2 (Controller to Processor) will apply where Subscriber is a controller of User Content and Company is a processor of User Content; Module 3 (Processor to Processor) will apply where Subscriber is a processor of User Content and Company is a processor of User Content. For each Module, where applicable:
  - in Clause 7, the optional docking clause will apply;
  - in Clause 9, Option 2 will apply, and the time for prior notice of Sub-processor changes shall be as set out in the **Use of Sub-processors** section of this DPA;
  - in Clause 11, the optional language will not apply;
  - in Clause 12, any claims brought under the EU SCCs shall be subject to the terms and conditions set forth in Terms. In no event shall any party limit its liability with respect to any data subject rights under the EU SCCs;

- in Clause 17, Option 1 will apply, will be governed by the laws of the Republic of Poland;
- in Clause 18(b), disputes shall be resolved before the courts of the Republic of Poland;
- Annex I and Annex II of the EU SCCs shall be deemed completed with the information set out in **Annex 1** and **Annex 2** to this DPA.

Nothing in the interpretations in this section is intended to conflict with either Party's rights or responsibilities under the EU SCCs and, in the event of any such conflict, the EU SCCs shall prevail.

To the extent any export from or processing of Personal Data outside the United Kingdom is subject to Applicable Data Protection Law in the United Kingdom (including UK GDPR and Data Protection Act 2018 (https://www.legislation.gov.uk/ukpga/2018/12/introduction) ("**UK Data Protection Laws**"), for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Personal Data to processors set out in the European Commission's Decision 2010/87/EU (https://eur-lex.europa.eu/eli/dec/2010/87/oj) ("**Prior SCCs**"), the Prior SCCs shall apply between Subscriber and Company on the following basis:

- Appendix I and Appendix II shall be deemed completed with the relevant information set out in **Annex 1** and **Annex 2** to this DPA;
- references in the Prior SCCs to "the law of the Member State in which the data exporter is established" shall be deemed to mean "the laws of the Republic of Poland";
- the optional illustrative indemnification clause will not apply;
- any other obligation in the Prior SCCs determined by the Member State in which the data exporter is established shall be deemed to refer to an obligation under UK Data Protection Laws. Where the Prior SCCs do not apply and the Parties are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the UK subject to completion of a UK Addendum to the EU SCCs issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 (https://www.legislation.gov.uk/ukpga/2018/12/section/119A) ("**UK Addendum**"), then the EU SCCs completed as set out above in the current paragraph of this DPA shall also apply to transfers of such Personal Data, subject to the provision that the UK Addendum shall be deemed executed between Company and Subscriber, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data. If neither the Prior SCCs nor UK Addendum with EU SCCs applies, then the Parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK Data Protection Laws without undue delay.

## 9. Obligations of Subscriber

When receiving Services under Terms, Subscriber agrees to abide by its obligations under Applicable Data Protection Law.

## 10. Return and destruction of Personal Data

Upon termination of Subscriber's access to and use of Services, Company will within twelve (12) months following such termination, at the choice of Subscriber:

- either permit Subscriber to export its User Content;
- or delete all User Content in accordance with the capabilities of Services and Article 28 (3)(g) of the GDPR.

Following such period, Company shall delete all User Content stored or processed by Company on behalf of Subscriber in accordance with Company's deletion policies and procedures. Subscriber expressly consents to such deletion.

## 11. Term

This DPA will remain in force as long as Company processes Personal Data on behalf of Subscriber under Terms.

## 12. Limitation of liability

This DPA shall be subject to the limitations of liability agreed between the Parties set forth in Terms and any reference to the liability of a Party means that Party and its Affiliates in the aggregate. For the avoidance of doubt, Subscriber acknowledges and agrees that Company's total liability for all claims from Subscriber or its Affiliates arising out of or related to Terms and DPA shall apply in aggregate for all claims under both Terms and DPA. For the avoidance of doubt, this section shall not be construed as limiting the liability of either Party with respect to claims brought by data subjects.

## 13. Miscellaneous

This DPA may not be modified except in writing and signed by both Parties. DPA may be executed in counterparts. Each Party's rights and obligations concerning assignment and delegation under this DPA shall be as described in Terms.

Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of, and be enforceable by the Parties.

This DPA, along with Terms, constitute the entire understanding between the Parties with respect to the subject matter herein and shall supersede any other arrangements, negotiations, or discussions between the Parties relating to that subject matter.

## 14. Governing law and jurisdiction

This DPA is governed by the laws of the Republic of Poland and is subject to the exclusive jurisdiction of the courts of the Republic of Poland. Notices under this DPA shall be sent in accordance with the notice provisions of Terms.

| **On behalf of Subscriber:** | **On behalf of Company:** | |
|---|---|---|
| Legal name: | Legal name: | Office Data Apps sp. z o.o. |
| Name: | Name: | Yuliya Tarasava |
| Position: | Position: | CEO |

| | | | |
|---|---|---|---|
| Address: | | Address: | Warszawska str., 109, office 5, Lomianki, 05-092, Poland |
| Email: | | Email: | privacy@ablebits.com |
| Date: | | Date: | November 18, 2022 |

# Annex 1: Details of Processing

## Nature and purpose of processing

Company will process Personal Data in the course of providing Services under Terms, which may include operation of a cloud-based backend infrastructure. Additional information about Services is available at https://www.ablebits.com/docs/#shared-email-templates-outlook. Company will process Personal Data as a Processor in accordance with Subscriber's instructions.

## Processing activities

Personal Data contained in User Content will be subject to the hosting and processing activities of providing Services.

## Duration of processing

The processing of Personal Data shall endure for the duration of the subscription term in Terms and DPA on a continuous basis.

## Data subjects

Subscriber may, at its sole discretion, submit Personal Data to Services, which may include, but is not limited to, the following categories of data subjects: employees (including contractors and temporary employees), relatives of employees, customers, consumers, prospective customers, service providers, suppliers, business partners, vendors, end-users, users of Services, advisors (all of whom are natural persons) of Subscriber, and any natural persons authorized by Subscriber to use Services.

## Categories of Personal Data

Subscriber may, at its sole discretion, transfer Personal Data to Services which may include, but is not limited to, the following categories of Personal Data: first and last name, username, email address, position, employer, contact information (company name, email address, phone number, physical address), date of birth, gender, number of users for a company account, team names, team descriptions, team members, email addresses of team members, users access permissions, and customer support service information.

## Special categories of Personal Data (if applicable)

Company does not intentionally collect or process any Special categories of Personal Data, as it is not needed for the purposes of providing Services to Subscriber. However, Special categories of Personal Data may, from time to time, be included in processing via Services where Subscriber chooses to include Special categories of Personal Data within Services.

Subscriber is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing any Special categories of Personal Data via Services.

## Retention

Company will process and retain Personal Data in accordance with the **Return and destruction of Personal Data** section of this DPA.

| | |
|---|---|
| **Data Exporter:** Subscriber | **Data Importer:** Office Data Apps sp. z o.o. |
| **Data Exporter Role:** Subscriber is Controller | **Data Importer Role:** Office Data Apps sp. z o.o. is Processor |
| **Contact Details:** Provided in DPA signature block | **Contact Details:** Provided in DPA signature block |

# Annex 2: Technical and Organizational Security Measures

Company implemented and maintains technical and organizational security measures set out in this Annex 2.

Company reserves the right to update or modify its security measures from time to time. However, any updates or modifications will not materially reduce the overall security of Services.

## Key principles

The entire IT infrastructure of Company ("**IT Infrastructure**"), including internal infrastructure—computers, local networks, access control systems, and public infrastructure located in cloud service providers—is protected from unauthorized access.

All Company employees and any third parties authorized to use IT Infrastructure, including, but not limited to, Sub-processors, must ensure that they are familiar with these security measures and must adhere to and comply with them at all times.

All User Content stored on IT Infrastructure is managed securely in compliance with all relevant parts of Applicable Data Protection Law whether now or in the future in force.

All User Content stored on IT Infrastructure is classified appropriately. All User Content so classified is handled appropriately in accordance with its classification.

All User Content stored on IT Infrastructure is protected against unauthorized access, processing, and from loss and corruption.

All breaches of security pertaining to IT Infrastructure or any User Content stored thereon are reported and subsequently investigated by the IT department.

## Organizational security measures

Company has appointed a Privacy Team ("**Privacy Team**") that is responsible for coordinating, monitoring, and improving these security measures.

Privacy Team conducts regular training for Company employees on data protection regulations and also informs employees about possible consequences of non-compliance. These training sessions are conducted using anonymized data.

Privacy Team maintains a record of security incidents which include the date and time of the incident, the consequences of the breach, and measures implemented to avoid similar situations in the future. They verify and monitor logs against irregularities and suspicious activity on Services.

Company makes regular backup copies of User Content and Services settings and configurations. All backups are automatically created by Amazon Web Services and stored on Amazon. We have processes in place which ensure that access to backup copies is

restricted to the necessary minimum, that backups may not be used outside of Amazon Web Services environment, and that no data can be restored without the authorization of senior management.

## IT Infrastructure Security Measures

### Physical access to Company facilities

Company on-premises IT Infrastructure is located in secured, climate-controlled rooms which are securely locked.

Only identified and authorized employees may access Company facilities. Unauthorized visitors may not access these facilities.

Company facilities are constantly security monitored to prevent unauthorized access. Visitors may only access a designated space of facilities where no data is processed.

All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by Company are always transported securely and handled with care.

### Physical access to cloud datacenters

User Content is processed within Amazon and Microsoft datacenters. Access to these datacenters is restricted only to identified Amazon or Microsoft staff members. Company employees may not physically access these datacenters.

### Data access controls

All IT Infrastructure (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) are protected with a secure password or passcode, or such other form of secure log-in system as the IT department may deem appropriate and approve.

Only a small, selected group of IT department employees may grant, alter, or cancel access privileges to Company facilities and IT Infrastructure. The scope of access rights granted to employees is limited strictly to assets necessary to perform their functions.

Company maintains a record of employees authorized to access Company facilities and IT Infrastructure. Company has implemented a system of controls to make sure that no one can stop working for Company without having their authentication credentials deactivated and all access rights revoked. Additionally, Company conducts regular (at least once every 6 months) audits to make sure that authentication credentials that have not been used are deactivated. Deactivated or expired identifiers are not granted to other or new employees. All passwords are strong and reliable. They are changed at least every 90 days, different from the previous password, not obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.), and created by individual users.

All IT Infrastructure with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) is protected with a password protected screensaver that will activate after 5 minutes of inactivity.

Company monitors IT Infrastructure against all attempts of unauthorized access and use of expired or invalid credentials.

Company has procedures in place to ensure that no User Content may be printed or copied to portable media without the prior permission of Company. Employees are prohibited from using unauthorized portable media on Company premises.

Only authorized devices may use Company networks. Company has controls in place to ensure that unauthorized devices cannot be used within the Company network.

User Content is encrypted in transit over public networks when communicating with Services via industry standard HTTPS/TLS (TLS 1.2 or higher).

### Software security measures

All software in use on IT Infrastructure (including, but not limited to, operating systems, individual software applications, and firmware) are kept up-to-date and all relevant software updates, patches, fixes, and other intermediate releases are applied.

Where any security flaw is identified in any software, that flaw is fixed immediately, or the software may be withdrawn from IT Infrastructure until such time as the security flaw can be effectively remedied.

No Company employees may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT department. Any software must be approved by the IT department and may only be installed where that installation poses no security risk to IT Infrastructure and where the installation would not breach any license agreements to which that software may be subject.

IT Infrastructure (including all computers and servers) is protected with suitable anti-virus, firewall, and other suitable internet security software.

IT Infrastructure is subject to a full system scan with anti-virus software at least once a week.

Company employees are permitted to transfer files using only pre-approved by the IT department cloud storage services. All files downloaded from any cloud storage services are scanned for viruses during the download process.

Any files being sent to third parties outside Company, whether by email, on physical media, or by other means (e.g., shared cloud storage services) are scanned for viruses before being sent or as part of the sending process.

## Security measures when developing and providing Services

Company maintains developer guidelines and policies which ensure that User Content processing principles such as Privacy by Design and Privacy by Default are observed while developing and providing Services.

Company regularly checks Services codes for errors and releases patches in timely manner.

Company maintains documentation that describes the architecture and functionality of Services and demonstrates User Content processing principles.

## Annex 3: Sub-processors for Services

Subscriber, as Controller, hereby confirms its general written authorization for Company's use of Sub-processors to assist Company in providing Services and processing User Content.

A list of Sub-processors is published at:
https://www.ablebits.com/docs/outlook-shared-templates-sub-processors/

The parties' authorized signatories have executed this DPA including Annexes as set forth below.

| **On behalf of Subscriber:** | **On behalf of Company:** | |
|---|---|---|
| Legal name: | Legal name: | Office Data Apps sp. z o.o. |
| Name: | Name: | Yuliya Tarasava |
| Position: | Position: | CEO |
| Address: | Address: | Warszawska str., 109, office 5, Lomianki, 05-092, Poland |
| Email: | Email: | privacy@ablebits.com |
| Date: | Date: | November 18, 2022 |

# Annex 4: Sub-processor Security Standards

Our Sub-processors, when processing User Content on behalf of Subscriber, shall implement and maintain the following technical and organizational security measures for the processing of such User Content as described below.

## Data protection

Our Sub-processors will take reasonable measures to ensure that User Content is secured to protect against accidental destruction or loss. Our Sub-processors shall ensure that, when hosted by Sub-processor, backups are completed on a regular basis, are secured and encrypted, to ensure that User Content is protected.

## Data access controls

Our Sub-processors will take reasonable measures to ensure that User Content is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to access User Content only have access to User Content to which they have privilege of access and that User Content cannot be read, copied, modified, or removed without authorization in the course of processing. Sub-processors will implement and maintain an access policy under which access to their system environment, data processing systems, User Content, and other data is restricted to authorized personnel only.

## Physical access controls

Our Sub-processors will take reasonable measures, such as security personnel and secured buildings, to prevent unauthorized persons from gaining physical access to User Content.

## Transmission controls

Our Sub-processors will take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of User Content by means of data transmission facilities is envisaged so User Content cannot be read, copied, modified, or removed without authorization during electronic transmission.

## Logical separation

Our Sub-processors will logically segregate User Content from the data of other parties on their systems to ensure that User Content may be processed separately.

## Annex 5: Regional Data Hosting Rules

In order to meet the needs of Services' Subscribers around the globe, Company has developed regional data hosting rules.

Services allow Subscribers to host their User Content in selected regions: the United States (US) or the European Countries (EU).

The following regions are currently available:

| Region in Services | AWS region code | Location |
|---|---|---|
| US Region 1 | us-east-1 | US East (Northern Virginia) |
| EU Region 1 (Under construction) | eu-central-1 | Europe (Frankfurt, Germany) |

The list of available regions will expand depending on Subscribers' requests.

Company's obligation to host User Content in a particular region only applies to certain subscription plans, as described below.

| Subscription plan | Available regions |
|---|---|
| Free trial | US Region 1 only |
| Business | All regions |
| Enterprise | All regions |
| Mail Merge | All regions |

Subscriber acknowledges that Company and its Sub-Processors may process User Content in countries outside the selected region if such processing is necessary to provide support-related or other services requested by Subscriber pursuant to the DPA.

Subscription billing data may be transferred by payment service provider outside of the selected region.

If Subscriber has an existing account prior to the date Subscriber purchases applicable subscription plans and selects the region, Company may be required to transfer existing User Content to the selected location. To complete this step, Company will make a copy of Subscriber's User Content to ensure that all relevant User Content has been successfully transferred to the selected location in its entirety. Upon completion and confirmation of the migration process, the copy of Subscriber's User Content will be removed from the original location.

Any data transmitted through links to external resources available within Services (for example, Ablebits.com, Microsoft.com, etc.) may leave the selected region after Subscriber clicks on these links.