**Standard GDPR DPA**

This Data Processing Addendum ("DPA") specifies the data protection obligations of the parties, which arise from contract data processing on behalf of the Client, as stipulated in the ABBYY Terms of Service for "ABBYY FlexiCapture Cloud" Web-service available at https://flexicapture.com/terms-of-service/ (the "Terms"). It applies to all activities performed in connection with the Terms in which the staff of ABBYY or a third party acting on behalf of ABBYY may come into contact with Personal Data of the Client.

This DPA sets out the additional terms, requirements and conditions on which ABBYY will process Personal Data when providing services under the Terms. This DPA contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) ("GDPR").

All capitalized terms used herein and not otherwise defined herein shall have the meanings ascribed to such terms in the Terms.

## 1. Definitions

1.1. **"Client"** - refer to and include any person and/or any entity that is accepting the Terms.

1.2. **"Controller"** has the same meaning under the Data Protection Laws.

1.3. **"Data Protection Laws"** means any applicable law, rule, regulation, decree, statute, or other enactment, order, mandate or resolution, relating to data security, data protection and/or privacy, including, but not limited to, the General Data Protection Regulation 2016/679 ("GDPR") and all other laws implementing or supplementing the GDPR including the Germany Federal Data Protection Act 2017 ("BDSG").

1.4. **"Processing"** means processing of Personal Data as defined under the Data Protection Laws, including the storage, amendment, transfer, blocking or erasure of personal data by ABBYY acting on behalf of the Client.

1.5. **"Processor"** has the same meaning under the Data Protection Laws.

1.6. **"ABBYY"** means ABBYY Europe GmbH Landsberger Str. 300 80687 Munich, Germany.

1.7. **"Instruction"** means the written instruction, issued by Client to ABBYY, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, de-personalizing, blocking, deletion, making available). Instructions shall initially be specified in the Terms and may, from time to time thereafter, be amended, amplified or replaced by Client in separate written instructions (individual instructions).

1.8. **"Personal Data Breach" -** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.9. **"Personal Data"** means any information that is included in Uploaded Data and that relates to an identified or identifiable individual.

1.10. **"Standard Contractual Clauses" or "SCC**" - standard data protection clauses adopted by the European Commission as defined in the Article 46 of the GDPR.

1.11. **"Service Storage"** means the software and hardware used by ABBYY for Uploaded Data storage.

The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

A reference to writing or written includes faxes and email.

In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;
(b) any of the provisions of this DPA and the provisions of the Terms, the provisions of this DPA will prevail.

## 2. **Scope and Responsibility**

2.1. The Client and ABBYY acknowledge that for the purpose of the Data Protection Laws, the Client is the Controller and ABBYY is the Processor. In some circumstances, Client may be a Processor, in which case Client appoints ABBYY as Client's sub-processor, which shall not change the obligations of either Client or ABBYY under this DPA, as ABBYY will always remain a Processor with respect to the Client in such event.

2.2. Client retains control of the Personal Data and remains responsible for its compliance with its obligations under the applicable Data Protection Laws, including providing any required notices and obtaining any required consents for the lawful Processing of Personal Data made available to or otherwise transferred to ABBYY, and for the processing instructions it gives to ABBYY.

2.3. ABBYY shall process Personal Data on behalf of Client. Processing shall include such actions as may be specified in the Terms and in the scope of work. Within the scope of the Terms, Client shall be solely responsible for complying with the statutory requirements relating to the lawfulness of the data processing.

2.4. Based on this responsibility, Client shall be entitled to request that ABBYY, subject to the Data Protection Laws, rectifies, deletes, blocks and makes available Personal Data during and after the term of the Terms at Client's cost. ABBYY shall promptly comply with any of Client's request or instruction requiring the ABBYY to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorized Processing.

2.5. The provisions of this DPA shall also apply if testing or maintenance of automatic processes or of Processing equipment is performed on behalf of Client.

## 3. **ABBYY's obligations**

3.1. ABBYY shall process Personal Data only within the scope of Client's Instructions as set-out in the Terms, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which ABBYY is subject. In this case, ABBYY shall inform Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.2. ABBYY will, insofar this is possible, by appropriate technical and organizational measures, reasonably assist Client with meeting Client's compliance obligations with respect to the rights exercised by data subjects under the Data Protection Laws (particularly the Data Subject's Rights stated in Chapter 3 of the GDPR and related to Data Subject's requests), taking into account the nature of the data Processing. Taking into account the nature of Processing and any information available to ABBYY, ABBYY will further assist the Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, in particular its obligations to undertake data protection impact assessments and report to and consult

with supervisory authorities under the Data Protection Laws. In a situation where requested level of assistance will be excessive or unreasonably burdensome for ABBYY, any such assistance will be exercised at Client's cost.

3.3. ABBYY shall implement appropriate technical and organizational measures required pursuant to Article 32 GDPR with respect to the Personal Data, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects. Such measures shall be designed to ensure a level of security appropriate to the risk in order to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or use. Such measures hereunder shall include, but are not limited to taking reasonable steps to achieve the following:

(i) the prevention of unauthorized persons from gaining access to Personal Data Processing systems (physical access control),

(ii) the prevention of Personal Data Processing systems from being used without authorization (logical access control),

(iii) persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),

(iv) Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

(v) the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems, (entry control),

(vi) Personal Data Processed are Processed in accordance with the Instructions (control of instructions),

(vii) Persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,

(viii) Personal Data are protected against accidental destruction or loss (availability control),

(ix) Personal Data collected for different purposes can be processed separately (separation control).

A measure as referred to in lit. a) to i) above shall be in particular, but shall not be limited to, the use of appropriate encryption technology. These technical and organizational measures are listed in the

**Annex 2** to this DPA.

3.4. Contact information:

ABBYY Europe GmbH
Landsberger Str. 300, 80687 Munich, Germany
Phone: +49-89-69 33 330 Email: privacy_eu@abbyy.com
Attn. Legal Department

3.5. Client's Notification Email Address is the same address that is used by the Client for registration within the Service. "Notification Email Address" means the email address designated by Client to receive certain notifications from ABBYY relating to this DPA.

3.6. If applicable, Client shall retain title as to any carrier media provided to ABBYY as well as any copies or reproductions thereof. ABBYY shall store such media safely and protect them against unauthorized access by third parties. ABBYY shall, upon Client's request, provide to Client all information on Client's Personal Data and information. ABBYY shall be obliged to securely delete any test and scrap material based on an Instruction issued by Client on a case-by-case basis. Where Client so decides, ABBYY shall hand over such material to Client or store it on Client's behalf.

3.7. ABBYY shall provide reasonable assistance to the Client with any data protection impact assessment which the Client is required to undertake in order to Comply with Articles 35 and 36 of GDPR, in each case solely in relation to the processing of Personal Data and taking into account the nature of the Processing and information available to ABBYY and shall make available to Client on request such information as is reasonably necessary to demonstrate its compliance with this DPA and its obligations under Article 28 of GDPR and shall allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client for the purpose of demonstrating compliance by ABBYY with its obligations under Data Protection Laws in respect of the Personal Data. ABBYY may object to the deployment of a specific auditor if such auditor (i) is not subject to confidentiality regarding the results of such audit (except vis-à-vis ABBYY and Client), (ii) is a competitor of ABBYY, (iii) is affiliated with a competitor of ABBYY.

3.8. Depending on the Data Processing Location chosen by the Client (as set forth in the Terms), the Personal Data of the Client may be processed in a third country pursuant to adequate safeguards under Art. 46 GDPR including, but not limited to execution of Standard Contractual Clauses or an approved code of conduct or other appropriate safeguards (for instance EU-U.S. Privacy Shield/Swiss-U.S. Privacy Shield mechanism). In the event of using the SCC, Client hereby (itself as well as on behalf of each Controller established within the EEA or Switzerland) accedes to the SCC between ABBYY and the sub-processor. ABBYY will enforce the SCC against the sub-processor on behalf of the Client or Data Subject if a direct enforcement right is not available under Data Protection Laws. Notwithstanding the above, ABBYY Europe GmbH will always have access to Personal Data and will process Personal data.

## 4. **Client's obligations**

4.1. Client shall be separately responsible for conforming with such statutory data protection regulations including the Data Protection Laws as are applicable to it and shall ensure that the Personal Data may lawfully be processed by ABBYY under the Terms.

4.2. Client shall inform ABBYY without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during a verification of the results of such Processing or otherwise arising following the date of this DPA.

4.3. Client shall be obliged to maintain the register as defined in Article 30 of GDPR. Client shall promptly notify ABBYY of the exercise of any rights by data subjects affecting the Processing of Personal Data by ABBYY.

Client shall, upon termination or expiration of the Terms and by way of issuing an Instruction, stipulate, within a period set by ABBYY, the measures to return data carrier media or to delete stored data.

4.4. Any additional cost arising out of ABBYY's performance under Instructions outside the Terms' scope of work or otherwise not contemplated by this DPA shall be borne by Client.

5. **Audit Obligations**

ABBYY shall provide a copy of its most current security report upon Client's written request and subject to the confidentiality provisions of the Terms. If Client requires additional information beyond that which is stated in the Report, Client may contact ABBYY at privacy_eu@abbyy.com to request an on-site audit of the architecture, systems and procedures relevant to the protection of Client Personal Data that are controlled by ABBYY. Notwithstanding of the above, if an audit is excessive or unreasonably burdensome for ABBYY, then Client shall reimburse ABBYY for such excessive or unreasonably burdensome audit at ABBYY's then-current professional services rates, which shall be made available to Client upon request. Before the commencement of any such audit, Client and ABBYY will mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Client shall be responsible. Client shall promptly notify ABBYY with information regarding any non-compliance discovered during the course of an audit.

6. **Sub-processing**

6.1. Client agrees that ABBYY may engage ABBYY's Affiliates and third party sub-processors (collectively, "sub-processors") to Process the Personal Data on ABBYY's behalf. Client acknowledges that ABBYY's contractual obligations hereunder, or the parts of the services, will be performed by a subcontractor and consents to use of sub-processors by ABBYY as described in this Section 6 to fulfil its contractual obligations under the Terms and to provide certain services on ABBYY's behalf such as support services. The list of current sub-processors authorized by Client is provided in the Annex 1 hereof.

6.2. ABBYY undertakes to enter into a written agreement with any applicable sub-processors and such agreement will contain the same data protection obligations as set out in this DPA. ABBYY will remain responsible for its compliance with the obligations stated herein and for any acts or omissions of the sub-processors.

6.3. ABBYY may, by giving no less than thirty (30) days' notice to Client, add or make changes to the sub-processors. Client may object to the appointment of an additional sub-processor within fourteen (14) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, in which case ABBYY shall have the right to cure the objection through one of the following options (to be selected at ABBYY's sole discretion):

(a) ABBYY will cancel its plans to use the Sub-processor with regard to Personal Data or will offer an alternative to provide the Services without such Sub-processor; or
(b) ABBYY will take the corrective steps requested by Client in its objection (which remove Client's objection) and proceed to use the sub-processor with regard to Personal Data; or
(c) ABBYY may cease to provide or Client may agree not to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-processor with regard to Personal Data, subject to a mutual agreement of the parties to adjust the remuneration for the Services considering the reduced scope of the Services.

If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within 30 days after ABBYY's receipt of Client's objection, either party may terminate the Terms and Client will be entitled to a pro-rata refund for prepaid fees for Services not performed as of the date of termination.

## 7. **Data Breach**

ABBYY will without undue delay notify Client if it becomes aware of any Personal Data Breach in accordance with applicable Data Protection Laws.

Immediately following any Personal Data Breach, the parties will coordinate with each other to investigate the matter. ABBYY will reasonably co-operate with Client in Client's handling of the matter.

ABBYY will not inform any third party of any Personal Data Breach without first obtaining Client's prior written consent, except when required to do so by Data Protection Laws or any other applicable Union or Member State laws.

ABBYY will cover all reasonable expenses associated with the performance of the obligations under this Section 7 unless the matter arose from Client's specific instructions, negligence, willful default or breach of the Terms, in which case Client will cover all reasonable expenses.

ABBYY will also reimburse Client for actual reasonable expenses that Client incurs when responding to a Personal Data Breach to the extent that ABBYY caused such a Personal Data Breach, including all costs of notice and any remedy.

## 8. **Duties to Inform, Mandatory Written Form, Choice of Law, Duration**

8.1. Where Client’s Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed, ABBYY shall inform Client without undue delay. ABBYY shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Client’s sole property and area of responsibility that Personal Data is at Client’s sole disposition.

8.2. No change of or amendment to this DPA and all of its components, including any commitment issued by ABBYY, shall be valid and binding unless made in writing and unless they make express reference to being a change or amendment to these regulations. The foregoing shall also apply to the waiver of this mandatory written form.

8.3. To the extent required by applicable Data Protection Laws, this DPA shall be governed by the law of the applicable jurisdiction. In all other cases, this DPA shall be governed by the laws of the same jurisdiction stated in the Terms for governing the Terms.

8.4. The term of this DPA shall follow the term of the Terms. Upon termination or expiration of the Terms, ABBYY shall, in accordance with the Terms, delete or make available to Client for retrieval all relevant Personal Data (including copies) in ABBYY’s possession, save to the extent that ABBYY is required by any applicable Union or Member State law to retain some or all of the Personal Data. In such event, ABBYY shall extend the protections of the Terms and this DPA to such Personal Data and limit any further processing of such Personal Data to only those limited purposes that require the retention, for so long as ABBYY maintains the Personal Data.

## 9. **List of Personal Data elements and Purpose**

9.1. The purpose of the data processing by ABBYY is the provision of its services to Client. ABBYY provides for Client’s use the FlexiCapture Cloud Web-service according to the Terms.

9.2. The following types/categories of data are processed:

- Documents, images, and other files that were uploaded to the Service (to the extent that these comprise Personal Data). E.g. name, contact information.

Neither Client nor Authorized Users shall use the Service to process Special Categories of Personal Data about (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor will Client process or give instructions to process any information about criminal convictions and offences.

Client is liable for any Personal Data that is provided or otherwise made available to ABBYY in excess of the categories of data described above ("Excess Data"). ABBYY's obligations under the Terms of this DPA shall not apply to any such Excess Data.

The Categories of data subjects comprise:

- Client
- Client's Employees
- Authorized Users
- Other data subjects about whom Personal Data was provided by the Client/Authorized Users as a part of Uploaded Data

9.3. Types of the data processing operations:

- Recognition
- Conversion
- Extraction

## Annex 1

1. **Sub-processors**

Client acknowledges that ABBYY's contractual obligations hereunder, or the parts of the deliverables defined below, will be performed by sub-processors:

1) If you have chosen Service Storage Location in the EU or Australia
   a) Microsoft Ireland Operations Ltd.
   Carmenhall Road, Sandyford, Dublin 18, Ireland
   b) Mongo DB, Inc
   229 West 43rd St. New York NY 10036 United States
2) If you have chosen Service Storage Location in the USA
   a) ABBYY USA Software House Inc., 890 Hillview Court, Suite 300, Milpitas, California 95035, USA.
   b) Microsoft Corporation One Microsoft Way Redmond, Washington 98052, USA
   c) Mongo DB, Inc
   229 West 43rd St. New York NY 10036 United States

# Annex 2

1. **Technical and organizational measures**

ABBYY and the Client agree that the technical and organizational measures are an integral and an effective part of this DPA. This applies subject to the provision that these technical and organizational measures may be adopted to the newest developments from time to time. ABBYY will inform without any further delay the Client about any changes of its security guidelines.

General practices. ABBYY has implemented and will maintain for the Services appropriate technical and organizational measures, internal controls, and information security measures as provided by Data Protection Laws (including pursuant to Article 32 of GDPR) to protect Personal Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. Client is wholly responsible for implementing and maintaining security within any interface and Client's Services\Application provided by Client, or on Client's behalf.

a. **Service.** For the Service, ABBYY has implemented and will maintain the following:
   1) Security roles and responsibilities. ABBYY personnel authorized to Process the Personal Data are subject to confidentiality obligations.
   2) Asset handling. ABBYY restricts access to Personal Data. ABBYY imposes restrictions on printing Personal Data and has procedures for disposing of printed materials that contain Personal Data.
   3) Logging and Reporting. ABBYY will use logging and reporting systems allowing to check whether data have been entered, changed, or removed (deleted).

b. **Human resources security.**
   1) Security training.

      ABBYY informs its personnel about relevant security procedures and their respective roles. ABBYY also informs its personnel of possible consequences of breaching the security rules and procedures. ABBYY will only use anonymous data in training.
   2) Physical access to facilities. ABBYY limits access to facilities where information systems that Process Personal Data are located.
   3) Protection from disruptions. ABBYY uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.
   4) Component disposal. ABBYY uses industry standard processes to delete Personal Data when it is no longer needed.

c. **Communications and operations management.**
   1) Data recovery procedures. The Service includes replication features that facilitate recovery of Personal Data in the event a particular machine or cluster fails.
   2) On an ongoing basis, ABBYY maintains multiple copies of Personal Data from which Personal Data can be recovered. ABBYY does not preserve state or data within a virtual machine, which will be restored to its original state.
   3) ABBYY has anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks.

d. **Domain: access control.**

1) ABBYY maintains a record of security privileges of individuals having access to Personal Data.
2) ABBYY maintains and updates a record of personnel authorized to access ABBYY systems that contain Personal Data.
3) ABBYY identifies those personnel who may grant, alter or cancel authorized access to data and resources.
4) Technical support personnel are only permitted to have access to Personal Data when needed.
5) ABBYY restricts access to Personal Data to only those individuals who require such access to perform their job function.
6) ABBYY uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, ABBYY requires that the passwords are renewed regularly. Where authentication mechanisms are based on passwords, ABBYY requires the password to be at least eight characters long. ABBYY ensures that de-activated or expired identifiers are not granted to other individuals.

e. **Audits and job control.**

1) ABBYY will select Subcontractors according to the standards of confidentiality set forth in this DPA.
2) ABBYY will monitor by way of regular reviews the performance and fulfillment of this DPA.
3) ABBYY will make available to Client all information necessary to demonstrate compliance with Data Protection Laws (including the obligations laid down in Article 28 of GDPR) and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client. Client audit will be limited in time to a maximum of 5 business days and scope as reasonably agreed in advance between the Parties. Reasonable advance notice of at least thirty days is required, unless Data Protection Laws requires earlier audit. Client and ABBYY will each bear their own expenses for conducting the audit. However, in case of excessive or unreasonably burdensome audit, Client should reimburse ABBYY for any such audit in accordance with Section 5 of this DPA.