

## **Written Guarantee**

**of DZ BANK AG, Deutsche Zentral-Genossenschaftsbank, Frankfurt am Main, Germany ("DZ BANK AG") concerning the Processing of Personal Data by Legally Dependent Branches**

DZ BANK AG maintains the following legally dependent branches (hereinafter referred to as branches) outside the European Union:

Hong Kong Branch, Tower II, 9th Floor, Admiralty Centre, 18 Harcourt Road, Hong Kong, Central

New York Branch, One Vanderbilt, New York, NY 10017, USA

Singapore Branch, 50 Raffles Place #43-01, Singapore Land Tower, Singapore 048623

London Branch, 150 Cheapside, London EC2V 6ET, UK (in the event that the EU Commission's adequacy decision no longer applies)

In discharging their duties, the aforementioned also access personal data stored at DZ BANK AG in Germany. To ensure an adequate level of data protection and offer adequate guarantees for the data subjects, DZ BANK AG herewith issues the following as a unilaterally guaranteed commitment:

### **Section 1 — Ensuring an adequate level of data protection at the branches**

DZ BANK AG has, by way of binding company-internal rules, obligated its aforementioned dependent branches to observe the standard contractual clauses (Module 1 – Controller to Controller) set out in the Annex to this Declaration, in accordance with the implementing decision of the European Commission (EU) 2021/914 of 04 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).

Moreover, the aforementioned dependent branches of DZ BANK AG must, by virtue of binding company-internal guidelines, observe and uphold, without limitation, the provisions of the EU General Data Protection Regulation.

The staff who work at the dependent branches have also been obliged to observe the provisions set out in the standard contractual clauses and the provisions of the EU General Data Protection Regulation.

## **Section 2 — Binding nature vis-à-vis all data subjects**

The provisions of the standard contractual clauses are — by way of third party beneficiary rights — also binding vis-à-vis all data subjects. DZ BANK AG is responsible for handling all legal claims which are exercised.

Data subjects are entitled to compel DZ BANK AG to observe their third party beneficiary rights by lodging a complaint with a data protection supervisory authority of their choice, or by pursuing effective remedy at DZ BANK AG's competent courts of law. They may additionally contact the Data Privacy Officer of DZ BANK AG at any time.

## **Section 3 — Responsibility for infringements**

In the event of an infringement of the provisions of the standard contractual clauses by one of the aforementioned dependent branches, DZ BANK AG shall remain the competent party vis-à-vis the data subjects. In such cases, the data subjects will retain the same rights vis-à-vis DZ BANK AG as if the infringement had been committed by DZ BANK AG in Germany, as opposed to by one of the dependent branches in the third country.

The data subjects can assert claims for compensation/remedy and possibly damages against DZ BANK AG.

## **Section 4 — Verification of compliance with the standard contractual clauses**

DZ BANK AG will employ suitable measures to ensure that the sustenance of an adequate level of data security in accordance with these standard contractual clauses is verified regularly at its dependent branches outside the European Union.

Where such an inspection concludes that remedies must be implemented due to an infringement of the standard contractual clauses, DZ BANK AG will additionally take care to ensure the implementation of the necessary remedies.

## **Section 5 — Amendments to statutory regulations at the branches' registered places of business**

The Branches observe legal developments in the countries in which they are registered.

Where the respective, applicable statutory regulations are amended in such way as to potentially engender impairment of those guarantees offered by the standard contractual clauses which were declared as binding at the dependent branches outside the European Union, this information shall be passed on to DZ BANK AG. DZ BANK AG will without delay investigate the potential impact which the amended underlying legal regulations could have on ensuring an adequate level of data protection.

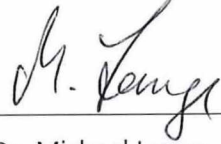
\*\*\*

Frankfurt, 30.03.2022



Ulrike Brouzi  
Member of the  
Board of Managing Directors

Frankfurt, 30.03.2022



Dr. Michael Lange  
Head of Department  
Compliance

## ANNEX

### STANDARD CONTRACTUAL CLAUSES

#### SECTION I

##### *Clause 1*

##### ***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")have agreed to these standard contractual clauses (hereinafter: "Clauses").
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### *Clause 2*

##### ***Effect and invariability of the Clauses***

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*

***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7
  - (ii) Clause 7 - Clause 7.5(e) and Clause 7.9(b)
  - (iii) Clause 10 - Clause 10(a) and (d)
  - (iv) Clause 11;
  - (v) Clause 13.1(c), (d) and (e)
  - (vi) Clause 14(e)
  - (vii) Clause 16 - Clause 16(a) and (b)
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*

***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

## **SECTION II – OBLIGATIONS OF THE PARTIES**

### *Clause 7*

#### ***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **7.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

#### **7.2 Transparency**

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 8, the data importer shall inform them, either directly or through the data exporter:
  - (i) of its identity and contact details;
  - (ii) of the categories of personal data processed;
  - (iii) of the right to obtain a copy of these Clauses;
  - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 7.7.
- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### **7.3 Accuracy and data minimisation**

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

### **7.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

### **7.5 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 11. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

## **7.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

## **7.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.



Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### **7.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

#### **7.9 Documentation and compliance**

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

### *Clause 8*

#### ***Data subject rights***

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge :
  - (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 7.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 9 (c) (i);
  - (ii) rectify inaccurate or incomplete data concerning the data subject;
  - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lay down suitable

measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

- (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

#### *Clause 9*

#### **Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 11;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 16.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 10*

***Liability***

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

*Clause 11*

***Supervision***

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

*Clause 12*

***Local laws and practices affecting compliance with the Clauses***

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its

obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16 (d) and (e) shall apply.

***Obligations of the data importer in case of access by public authorities***

**13.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 12 (e) and Clause 14 to inform the data exporter promptly where it is unable to comply with these Clauses.

**13.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 12 (e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS**

##### *Clause 14*

##### ***Non-compliance with the Clauses and termination***

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 12 (f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to

which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 15*

**Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of *Germany*.

*Clause 16*

**Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of *Germany*.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

## APPENDIX

### ANNEX I

#### A. LIST OF PARTIES

##### **Data exporter(s):**

1. Name: DZ BANK AG, Zentral-Genossenschaftsbank, Frankfurt am Main (hereinafter referred to as DZ BANK AG)

Address: Platz der Republik, 60325 Frankfurt am Main

Contact person's name, position and contact details: Data Protection Officer of DZ BANK AG, E-Mail: [datenschutz@dzbank.de](mailto:datenschutz@dzbank.de), Tel.: +49 69 744794101

Activities relevant to the data transferred under these Clauses: Activities for the processing of business operations

Signature and date:  (2022-03-30)



Role (controller/processor): Controller

##### **Data importer(s):**

1. Name: Legally Dependent Branch DZ BANK AG, Hong Kong Branch

Address: Tower II, 9th Floor, Admiralty Centre, 18 Harcourt Road, Hong Kong, Central

Contact person's name, position and contact details: Local Privacy Officer of DZ BANK AG, Hong Kong Branch, Tel.: +852 28 643 100, Telefax: +852 28 643 160, E-Mail: [hongkong@dzbank.de](mailto:hongkong@dzbank.de)

Activities relevant to the data transferred under these Clauses: Activities for the processing of business operations

Role (controller/processor): Controller

2. Name: Legally Dependent Branch DZ BANK AG, Singapore Branch

Address: 50 Raffles Place #43-01, Singapore Land Tower, Singapore 048623

Contact person's name, position and contact details: Local Privacy Officer of DZ BANK AG, Singapore Branch, Tel.: +65 6 427 8388, Telefax: +65 6 223 0082

Activities relevant to the data transferred under these Clauses: Activities for the processing of business operations

Role (controller/processor): Controller

3. Name: Legally Dependent Branch DZ BANK AG, New York Branch

Address: One Vanderbilt, New York, NY 10017, USA

Contact person's name, position and contact details: Local Privacy Officer of DZ BANK AG, New York Branch, Tel.: +1 212 745-1400, Telefax: +1 212 745-1550, E-Mail: [new.york@dzbank.de](mailto:new.york@dzbank.de)



Activities relevant to the data transferred under these Clauses: Activities for the processing of business operations

Role (controller/processor): Controller

4. Name: Legally Dependent Branch DZ BANK AG, London Branch

Address: 150 Cheapside, London EC2V 6ET, UK

Contact person's name, position and contact details: Local Privacy Officer of DZ BANK AG, London Branch, Tel.: +44 20 7776 6000, Telefax: +44 20 7776 6100,

E-Mail: london@dzbank.de

Activities relevant to the data transferred under these Clauses: Activities for the processing of business operations

Role (controller/processor): Controller

## B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

*Customers, Employees, Interested Parties, Suppliers, Contact Person*

*Categories of personal data transferred*

*Employee master data, customer master data, account data, transaction data, supplier master data, communication data, system identifiers*

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*None*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

*Continually*

*Nature of the processing*

*The data is stored within the IT systems of the responsible parties and processed automatically to the extent required in accordance with the admissibility requirements according to Art. 6 GDPR and deleted after the end of retention periods.*

*Purpose(s) of the data transfer and further processing*

*Fulfillment of the functions of the branches in the individual countries on behalf of DZ BANK AG, Frankfurt*

- Processing for the purposes of the provision and intermediation of banking, financial services, risk management, prevention of money laundering and fraud as well as all activities necessary for the operation and management of a credit and financial institution*

*Establishment and execution of contractual assignments of local persons acting on behalf of the branches in compliance with applicable (local) law(s).*

*Exchange of data in connection with the initiation and processing of transactions by DZ BANK AG*

- Reading and maintenance of customer data, initiation of business, conclusion and execution of contracts*
- Transmission of data to supervisory authorities, IT system maintenance, communication, preparation of financial statements*

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

*The storage period of personal data depends on the deletion concept of the respective application.*

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

*Processors engaged by us (Art. 28 GDPR) may receive data for the above-mentioned purposes. These are companies in the categories of credit services, IT services, printing services as well as*

*sales and marketing. These companies are contractually obligated to delete the data when the contractual relationship has ended or retention periods have expired.*

### **C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 11*

*Der Hessische Beauftragte für Datenschutz und Informationsfreiheit*

## **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

### **1. Confidentiality (Article 32 (1) (b) GDPR)**

#### **1.1 Measures to control admission**

Admission control refers to measures that are suitable to prevent unauthorised individuals from accessing data processing equipment that is used to process or use personal data.

Implemented general measures:

Admission controls in data centres:

- CCTV monitoring of the data centre (24x7x365)
- Alarmed server rooms, locked at all time
- Guidelines for issuing admission credentials
- Admission is only granted to authorised employees and, where applicable, service providers and other individuals by prior appointment and following identification checks. Only a small number of selected individuals will be admitted.
- Additional card-based admission control system with recording for computing areas. Cards and/or authorisation are issued following approval by the individual's line manager.

Admissions control in offices:

- Guidelines regarding physical measures to control admission
- Card-based personalised admission control system with authorisation restricted to authorised employees
- Instructions for employees who handle admission controls
- Guidelines for accompanying visitors to buildings
- Building primarily secured by intruder alarm systems, security guard service with inspection rounds and CCTV monitoring
- Isolated areas requiring additional rights of admission with defined internal approval processes, regular review of the granted rights

#### **1.2 Measures to control access to systems**

System access control refers to measures that are suitable to prevent unauthorised individuals from accessing data processing systems.

Implemented general measures:

- Authentication information is encrypted according to the current state of technological knowledge before transmission
- Passwords, PINs and similar are masked during entry
- Computer workstations have an automatic screen lock
- User accounts are blocked following repeated failed login attempts
- Central process for password resets and logging
- Guidelines for password complexity and frequency of changes
- Encryption of hard discs in laptops and other portable data storage media

### **1.3 Measures to control access to data**

Data access control refers to measures that are suitable to ensure that those authorised to use a data processing system only have access to the data they are authorised to use, and that no unauthorised reading, copying, amendment or deletion of personal data is possible during processing, use or after saving.

Implemented general measures:

- Authorisations are issued according to the minimal principle and via documented authorisation processes
- Implemented authorisations are subject to regular checks (recertification)
- The implementation of user authorisations is separate from the approval process

### **1.4 Measures to control separation**

Separation control refers to measures that are suitable to ensure that data recorded for different purposes is processed separately.

Implemented general measures:

- Observance of the principles of orderly data processing. The contractually agreed and legally required data security measures are guaranteed.
- Separation of data recorded for different purposes by means of saving in physically or logically separate databases and/or systems.

## **2. Integrity (Article 32 (1) (b) GDPR)**

### **2.1 Measures for disclosure control**

Disclosure control refers to measures that are suitable to ensure that personal data is not read, copied, amended or deleted by unauthorised individuals during electronic transmission, during transportation or when saved to data storage media, and to make it possible to check and determine where the transmission of personal data by data transmission organisations is provided for.

Implemented general measures:

- General internet network security through firewalls, virus filters and internet access restricted to proxy servers.
- Internal network via dedicated connections, where necessary as a VPN.
- Central administrative interface control for writing to USB and CD/DVD writers pursuant to the authorisation process
- Setting of archiving and deletion periods/deadlines for personal data
- Binding process for the destruction or decommissioning of data storage media, including deletion or destruction by a service provider
- Access-secured storage of backup and archive data carriers
- Documentation of all data transmission interfaces
- Exchange of sensitive data via dedicated or encrypted lines
- TLS encryption of e-mails sent via server connections.

## **2.2 Measures for entry control**

Entry control refers to measures that are suitable to ensure that it can subsequently be checked and determined whether personal data was entered into, amended in, or deleted from data processing systems, and if so by whom.

Implemented general measures:

- Use of personalised user identification where possible
- Principle that only employees allocated to the respective task in the organizational structure may use personal data
- Logging of all changes in the user management system
- Logging of access to systems and applications
- Employees are obliged to maintain confidentiality when processing personal data

## **3. Availability and resilience (Article 32 (1) (b) and (c) GDPR)**

Availability control refers to measures that are suitable to ensure that personal data is protected from accidental destruction or loss.

Implemented general measures:

- Securing of IT operations using two geographically separate, failure-proof data centres with mirrored data storage, an uninterrupted power supply and respective redundant network connection.
- Full backup and recovery concept with daily backups and disaster-proof storage of backup data storage media in geographically separate data centres.
- Data archiving pursuant to the legal and regulatory requirements with redundant data storage at two separate locations where special admission controls are in place, and regular checks of the readability of archived data.

- Expert use of protective measures such as virus scanners, firewalls and SPAM filters according to detailed use concepts
- Regular assessment and drills regarding the relevant failure scenarios

#### **4. Process for regular testing, assessment and evaluation (Article 32 (1) (d) GDPR, Article 25 (1) GDPR)**

Implemented general measures:

- The contractor has appointed an operational data protection officer and ensures their appropriate inclusion in the relevant operational processes by means of the data protection organisation.
- Regular assessment by internal audit.
- Employees are informed of and trained with regard to data protection and compliance with the obligation to maintain confidentiality. Organisational data protection measures are in place.
- There is a process for the regular assessment of protection requirements with regard to the personal data, including appropriate protective measures.
- Deletions can be carried out in the systems used for processing (deletability).
- Only the data required according to the client's specifications is processed.
- The contracts with another contractor pursuant to Article 28 (4) GDPR (processing of personal data carried out on behalf of a controller) include the required details and agreements.
- Contracts with another contractor include detailed information about the type and scope of the contracted processing and use of personal data on behalf of the client
- Contracts with another contractor include detailed information about purpose limitation with regard to personal data processed on behalf of the client.
- Careful selection and controls of another contractor.

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

*The controller shall ensure in its (sub-)contractual relationships that sufficient guarantees are provided to ensure the processing with appropriate technical and organisational measures in accordance with the requirements of the GDPR.*