Terms of Use for the POSTIDENT E-Signing product

1. Parties to the Agreement

(1) The Parties to the Agreement for the provision of services as part of the POSTIDENT E-Signing product are Deutsche Post AG, Charles-de-Gaulle-Strasse 20, 53113 Bonn, Germany; Registration Court: Bonn HRB 6792, phone: +49(0) 228 76367660 (hereafter referred to as “DPAG”; the names of the current authorised representatives of Deutsche Post AG can be found in the legal information) and the users as private customers.

(2) The term “private customer” (hereinafter referred to as the “User”) refers exclusively to consumers as defined in Section 13 of the German Civil Code (BGB – Bürgerliches Gesetzbuch). A consumer is a natural person who completes a legal transaction for purposes that are largely not attributable to either their commercial or self-employed activity.

2. Subject of the Agreement

The Subject of the Agreement is the provision of the POSTIDENT E-Signing product, which enables natural persons under the following conditions to identify themselves online via the POSTID Portal to the respective customer of DPAG and to sign a digital document online using a qualified electronic signature in compliance with eIDAS.

3. Services

(1) To create a qualified electronic signature, the User is identified using POSTIDENT. For identification, the User may use POSTIDENT via Videoident or eID function. Alternatively, the customer may transfer the User’s identity information it has collected (Identtransfer). Based on the identification information, the User is issued with a unique electronic certificate via the signature service. This certificate contains the User’s transmitted identity information.

(2) Once the User has successfully been identified, the documents that are to be digitally signed are displayed. By entering a TAN and consenting to the Terms of Use and Certification Practice Statement Extract, the User approves the document to be signed electronically. The electronic signature is created and integrated into the document in a fully automated manner in the background.

(3) The IT operations take place in data centres certified in accordance with ISO27001 or TSI Level II. To ensure the security of the POSTID platform, up-to-date encryption and signature technologies are used for the connection path from the User to the POSTID platform, as well as for the transmission of data. The data or alternatively the log data validating the usage data are transmitted and stored in an integrity-protected form directly after creation in and encrypted at all times.

(4) EU Regulation No 910/2014 (eIDAS for short), ratified in July 2014, lays down Europe’s standardised legal framework and the requirements to be met for various different electronic services with a view to promoting an internal digital market. POSTIDENT E-Signing has successfully qualified as a “Service for qualified electronic signatures” and was added to the list of trust service providers of the responsible supervisory authority, the German Federal Network Agency (*Bundesnetzagentur*). The corresponding conformity assessment body is the company datenschutz cert GmbH, Konsul-Smidt-Strasse 88a in 28217 Bremen, Germany. The eIDAS Regulation states that a service for qualified electronic signatures is an electronic service based on a qualified certificate (valid from the time of its creation) and created using a secure signature creation device (SSCD). A certificate of a trust service provider (TSP) is the electronic certification that the signature verification key and thus the corresponding signature key was allocated to a person and that this person’s identity can be confirmed. In the electronic

signature, the certificate contains the official key with which the encrypted hash value (checksum) of the electronic document encrypts the electronic document during the creation of the signature and against which a new hash value can be compared, thereby enabling the authenticity of the electronic document to be checked. The electronically signed documents are admissible as evidence in court and meet the requirements for an electronic form of equal status to the legal written form. The contents of the electronically signed documents and their integrity can be verified by both sides. Both Parties are provided with a copy of the electronically signed documents. The certificate is issued by the company be-ys, 46 Rue du Ressort in 63967 Clermont Ferrand Cedex 9, France.

(5) Identification and signing in the course of using the POSTIDENT E-Signing product do not incur any costs on the part of the User. Using DPAG's identification and signature service may, however, incur connection and transmission fees levied by the User's internet service provider and which must be borne by the User.

4. Rights and obligations of the User

(1) In order to be able to provide the User with a qualified electronic signature, the User must identify themselves via the POSTID Portal using POSTIDENT via video chat or the eID function or via Identtransfer.

(2) The User must provide all the data required for identification during the identification process completely and truthfully; the User must also provide the requested evidence.

(3) The User has the right to revoke the certificate used to create the qualified electronic signature. The User gains access to a corresponding function after issuing a signature online on the page for revoking the signed documents under *Block certificate* (*Zertifikat sperren*). Revocation, however, will not render the signed contract legally invalid.

(4) It is the User's responsibility to take all necessary measures to keep the signed contractual documents and the additional associated data secure. DPAG will not save or store any documents or associated data, aside from the legally required log files relating to the signing process.

(5) The User is obliged to take appropriate measures to protect the hardware and software (customer system) that he/she deploys for using the POSTID Portal and aforementioned services, in order to ensure their security and integrity. This includes, in particular, the use of the latest version of the operating system or browser software as well as an up-to-date virus protection scanner.

(6) The User shall ensure that the mobile phone to which messages are sent in connection with the identification and signing process is protected against unauthorised use by third parties.

(7) Various document platforms (such as Adobe Reader) have verification mechanisms that can verify the validity of certificates in use. If the electronically signed document is opened with Adobe Reader for example, then once the certificate has been checked, a green tick appears at the top of the screen, confirming the validity of the digital signature. Information about the digital signature in the document and the document's change history can also displayed in the "Signatures" window. Here you can also find information about the time the document was signed as well as details about its trustworthiness and about the signatory.

5. Rights and Obligations of DPAG

(1) DPAG shall provide the services in accordance with these Terms of Use.

(2) If the User or a third party attributable to him/her culpably violates statutory requirements or these Terms of Use, DPAG shall be entitled to terminate the services and stop the process for issuing an electronic certificate.

6. Liability

(1) DPAG bears liability for its services as a qualified trust service in accordance with Article 13 of Regulation (EU) No. 910/2014 (eIDAS Regulation) in conjunction with Section 6 of the German Trust Services Act (*Vertrauensdienstegesetz*). The amount of liability is based on Article 24 (2)(c) of the Regulation in conjunction with Section 10 of the Trust Services Act. The amount of liability shall therefore amount to a maximum of €250,000 for each individual instance of an event that gives rise to liability within the meaning of Section 10 of the Trust Services Act, but no more than €2.5 million per year.

(2) Regarding damage unrelated to qualified trust services as per Regulation (EU) No 910/2014 (eIDAS Regulation), DPAG shall be liable in the case of the violation of material contractual obligations (known as cardinal obligations) for all culpable conduct on the part of its statutory agents, executives or other vicarious agents. Cardinal obligations are duties, the fulfilment of which make due performance of this Agreement possible in the first place and in regards to which the Parties to this Agreement may regularly expect compliance. Liability for negligence is excluded in all other respects.

(3) DPAG cannot be held liable in any way for damage caused as a consequence of service downtime or delays in the provision of services based on unforeseeable events for which DPAG, its legal representatives or its vicarious agents cannot be held responsible (“force majeure”). Events that are considered the result of force majeure include in particular war, civil unrest, forces of nature, fire, attacks of sabotage by third parties (for example through computer viruses), power outages, directives of governmental agencies, lawful industrial action within the company and failures of or service limitations on communication networks or gateways of other operators.

(4) The aforementioned exclusions and limitations of liability shall not apply to damage due to intentional or gross negligence or arising from harm to life, limb or health, the assumption of a warranty respecting a particular condition or any wilful concealment of defects by the contractor, nor to product liability claims.