Nutzungsbedingungen für das Produkt POSTIDENT E-Signing

1. Vertragspartner

(1) Vertragspartner des Vertrages über die Erbringung der Leistungen im Rahmen des Produktes POSTIDENT E-Signing sind Deutsche Post AG, Charles-de-Gaulle-Straße 20, 53113 Bonn, Registergericht Bonn HRB 6792, Telefon: 0228 76367660 (nachfolgend „DPAG“, die Namen der aktuell vertretungsberechtigten Personen der Deutsche Post AG können dem Impressum entnommen werden) und der Nutzer als Privatkunde.

(2) Unter dem Begriff Privatkunde (im Folgenden „Nutzer“) sind ausschließlich Verbraucher im Sinne des § 13 BGB zu verstehen. Ein Verbraucher ist eine natürliche Person, die ein Rechtsgeschäft zu Zwecken abschließt, die überwiegend weder ihrer gewerblichen noch ihrer selbstständigen beruflichen Tätigkeit zugerechnet werden können.

2. Vertragsgegenstand

Vertragsgegenstand ist die Zurverfügungstellung des Produktes POSTIDENT E-Signing, welches natürlichen Personen unter den nachfolgenden Bedingungen die Möglichkeit bietet sich über das POSTID Portal online gegenüber dem jeweiligen Auftraggeber der DPAG zu identifizieren und ein digitales Dokument online eIDAS-konform mittels einer qualifizierten elektronischen Signatur zu signieren.

3. Leistungen

(1) Für die Erstellung einer qualifizierten elektronischen Signatur wird der Nutzer mittels POSTIDENT identifiziert. Zur Identifizierung kann der Nutzer POSTIDENT durch Videoident oder durch Online-Ausweisfunktion verwenden. Alternativ kann der Auftraggeber die durch ihn erhobene Identitätsdaten des Nutzers übermitteln (Identtransfer). Anhand der Identifikationsdaten wird für den Nutzer über den Signaturservice ein einmaliges elektronisches Zertifikat ausgestellt. In diesem Zertifikat sind die übergebenen Identitätsdaten des Nutzers enthalten.

(2) Nach erfolgreicher Identifikation des Nutzers, werden die zu signierenden Dokumente digital angezeigt. Durch die Eingabe einer TAN und Bestätigung der Nutzungsbedingungen und Zertifizierungsrichtlinien (Certification Practice Statement Extrakt), gibt der Nutzer das Dokument zum Aufbringen der elektronischen Unterschrift frei. Die Erstellung der elektronischen Signatur und Integration derselben in das Dokument erfolgen vollständig automatisiert im Hintergrund.

(3) Der IT-Betrieb erfolgt in nach ISO27001 bzw. TSI Level II zertifizierten Rechenzentren. Für die Sicherheit der POSTID Plattform, der Verbindungsstrecke vom Nutzer zur POSTID Plattform, sowie für die Übertragung der Daten werden aktuelle Verschlüsselungs- und Signaturtechnologien eingesetzt. Die Daten oder ersatzweise die Nutzdaten validierenden Protokollierungsdaten werden direkt nach Erstellung integritätsgeschützt und stets verschlüsselt übertragen und gespeichert.

(4) Die im Juli 2014 verabschiedete EU-Verordnung Nr. 910/2014 (kurz eIDAS) legt den europaweit einheitlichen Rechtsrahmen und zu erfüllende Anforderungen für diverse verschiedene elektronische Dienste zur Förderung eines digitalen Binnenmarktes fest. POSTIDENT E-Signing hat sich erfolgreich als „Dienst für qualifizierte elektronische Signaturen“ qualifiziert und wurde von der zuständigen Aufsichtsbehörde Bundesnetzagentur in die Anbieterliste der Vertrauensdienste aufgenommen. Die entsprechende Konformitätsbewertungsstelle ist die Firma datenschutz cert GmbH, Konsul-Smidt-Straße 88a in 28217 Bremen. Ein Dienst für qualifizierte elektronische Signaturen ist nach der eIDAS-Verordnung ein elektronischer Dienst, der auf einem (zum Zeitpunkt ihrer Erzeugung gültigen) qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurde. Ein Zertifikat des

Vertrauensdiensteanbieters (VDA) ist die elektronische Bescheinigung, dass der Signaturprüfschlüssel und damit auch der korrespondierende Signaturschlüssel einer Person zugeordnet wurde und die Identität dieser Person bestätigt werden kann. Bei der elektronischen Signatur enthält das Zertifikat den öffentlichen Schlüssel, mit dem der während der Signaturerstellung verschlüsselte Hashwert (Prüfsumme) des elektronischen Dokuments entschlüsselt und gegen einen neu erstellten Hashwert verglichen und damit die Authentizität des elektronischen Dokuments überprüft werden kann. Die elektronisch signierten Dokumente werden als Beweismittel vor Gericht anerkannt und erfüllen die mit der gesetzlichen Schriftform gleichgestellte elektronische Form. Der Inhalt der elektronisch signierten Dokumente und dessen Unversehrtheit, können von beiden Seiten nachgewiesen werden. Beiden Parteien wird ein Exemplar der elektronisch unterschriebenen Dokumente zur Verfügung gestellt. Die Zertifikatsbereitstellung erfolgt über die Firma be-ys, 46 Rue du Ressort in 63967 Clermont Ferrand Cedex 9, Frankreich.

(5) Dem Nutzer entstehen durch die Identifizierung und Signierung im Rahmen der Nutzung des Produkts POSTIDENT E-Signing keine Kosten. Durch die Nutzung des Identifizierungs- und Signaturservices der DPAG können jedoch Verbindungs- und Übertragungsentgelte anfallen, die vom Internetprovider des Nutzers erhoben werden und vom Nutzer zu tragen sind.

4. Rechte und Pflichten des Nutzers

(1) Um für den Nutzer eine qualifizierte elektronische Signatur anbieten zu können, ist der Nutzer verpflichtet sich über das POSTID Portal mittels POSTIDENT durch Videochat oder Online-Ausweisfunktion oder durch Identtransfer zu identifizieren.

(2) Der Nutzer hat im Rahmen des Identifikationsprozesses sämtliche für die Identifikation erforderlichen Daten vollständig und wahrheitsgemäß anzugeben und die geforderten Nachweise zu erbringen.

(3) Der Nutzer hat das Recht, dass eingesetzte Zertifikat für die Erstellung der qualifizierten elektronischen Signatur zu widerrufen. Eine entsprechende Funktion steht dem Nutzer im Anschluss an die Signatur online auf der Seite zum Abruf der signierten Dokumente unter *Zertifikat sperren* zur Verfügung. Durch den Widerruf wird der unterschriebene Vertrag jedoch nicht rechtlich unwirksam.

(4) Es obliegt dem Nutzer, sämtliche zur Sicherung der signierten Vertragsdokumente und der damit zusammenhängenden weiteren Daten notwendigen Maßnahmen selbst zu unternehmen. DPAG wird, abgesehen von den rechtlich vorgeschriebenen Log-Dateien zum Signaturvorgang, keine Dokumente und damit im Zusammenhang stehende Daten speichern und vorhalten.

(5) Der Nutzer ist verpflichtet, geeignete Maßnahmen zum Schutz der von ihm zur Nutzung des POSTID Portals und der vorgenannten Leistungen eingesetzten Hard- und Software (Kundensystem) zu ergreifen, um deren Sicherheit und Integrität zu gewährleisten. Hierzu zählt insbesondere der Einsatz einer aktuellen Version der Betriebssystem bzw. Browser-Software sowie eines aktuellen Virenschutzscanners.

(6) Der Nutzer hat dafür Sorge zu tragen, dass sein Mobiltelefon, auf das Benachrichtigungen im Rahmen der Identifizierung und des Signiervorgangs übermittelt werden, gegen die unbefugte Verwendung durch Dritte geschützt ist.

(7) Diverse Dokument-Plattformen (wie z.B. Adobe Reader) besitzen Prüfmechanismen, die die Gültigkeit eines eingesetzten Zertifikats prüfen. Wird das elektronisch unterschriebene Dokument, z.B. mit dem Adobe Reader geöffnet, erscheint nach der Prüfung des Zertifikats ein grünes Häkchen oben im Screen, welches die Gültigkeit des digitalen Signatur wiedergibt. Zudem können im Fenster „Signaturen“ Informationen zur digitalen Signatur im Dokument und die Änderungshistorie des Dokuments angezeigt werden. Hier finden Sie außer-

dem Informationen zum Signierzeitpunkt des Dokuments und Details zur Vertrauenswürdigkeit und zum Unterzeichner.

5. Rechte und Pflichten der DPAG

(1) Die DPAG stellt die Leistungen gemäß diesen Nutzungsbedingungen zur Verfügung.

(2) Bei einem schuldhaften Verstoß gegen gesetzliche Vorschriften oder diese Nutzungsbedingungen durch den Nutzer oder einen ihm zurechenbaren Dritten ist DPAG berechtigt, ihre Leistungen einzustellen und den Prozess zur Ausstellung eines elektronischen Zertifikates zu beenden.

6. Haftung

(1) Die DPAG haftet für ihre Leistungen als qualifizierter Vertrauensdienst gemäß Artikel 13 der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) in Verbindung mit § 6 des Vertrauensdienstgesetzes. Die Haftungssumme richtet sich nach Artikel 24 Absatz (2) c der Verordnung in Verbindung mit § 10 des Vertrauensdienstgesetz. Damit beträgt die Haftungssumme maximal 250.000 € für jedes auf den Einzelfall bezogene haftungsauslösende Ereignis im Sinne des § 10 Vertrauensdienstegesetz, maximal jedoch 2.5 Mio. € pro Jahr.

(2) Für Schäden, die nicht im Zusammenhang mit einem qualifizierte Vertrauensdienste auf Basis der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) stehen, haftet die DPAG im Fall der Verletzung wesentlicher Vertragspflichten (sog. Kardinalpflichten) für jedes schuldhafte Verhalten seiner gesetzlichen Vertreter, leitenden Angestellten oder sonstigen Erfüllungsgehilfen. Kardinalpflichten sind solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung dieses Vertrages überhaupt erst ermöglicht und auf deren Einhaltung die Vertragspartner regelmäßig vertrauen dürfen. Darüber hinaus ist die Haftung für einfache Fahrlässigkeit ausgeschlossen.

(3) DPAG haftet keinesfalls für Schäden infolge von Leistungsausfällen und Leistungsverzögerungen aufgrund unvorhersehbarer, von der DPAG, ihren gesetzlichen Vertretern oder ihren Erfüllungsgehilfen nicht zu vertretender Ereignisse (höhere Gewalt). Als Ereignisse höherer Gewalt gelten insbesondere Krieg, Unruhen, Naturgewalten, Feuer, Sabotageangriffe durch Dritte (wie z. B. mit Computerviren), Stromausfälle, behördliche Anordnungen, rechtmäßige unternehmensinterne Arbeitskampfmaßnahmen und der Ausfall oder eine Leistungsbeschränkung von Kommunikationsnetzen und Gateways anderer Betreiber.

(4) Die vorgenannten Haftungsausschlüsse und -beschränkungen gelten nicht für Schäden, die auf Vorsatz oder Grober Fahrlässigkeit beruhen oder die aus der Verletzung des Lebens, des Körpers oder der Gesundheit, der Übernahme einer Beschaffenheitsgarantie oder einem arglistigen Verschweigen von Mängeln durch den Auftragnehmer resultieren, sowie im Fall von Produkthaftungsansprüchen.