

## 1. Präambel

Diese Allgemeinen Nutzungsbedingungen (im Folgenden „Nutzungsbedingungen“) regeln die zwischen DocuSign France SAS, und Ihnen (im Folgenden: „Signierenden“) geltenden rechtlichen Bedingungen.

## 2. Vertragsgegenstand / Definitionen

(1) Zweck des Vertrags nach diesen Nutzungsbedingungen ist es, dass DocuSign France nach Maßgabe der

Verordnung (EU) Nr 910/2014 des Europäischen Parlaments und des Rates vom 23.7.2014 über elektronische Identifizierung und Vertrauensdienste für elektronischen Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93 EG

(kurz: eIDAS-Verordnung)

für den Signierenden auf einem oder mehreren Dokumenten eine fortgeschrittene oder qualifizierte elektronische Signatur im Wege einer elektronischen Fernsignatur erstellt und im Falle einer qualifizierten elektronischen Signatur mit einem qualifizierten Zertifikat für elektronische Signaturen versieht (nachfolgend: „**der Service**“).

(2) Dabei versteht man unter einer fortgeschrittenen Signatur eine Signatur, die eindeutig dem Signierenden zugeordnet ist, die die Identifizierung des Signierenden ermöglicht und die unter Verwendung elektronischer Signaturerstellungsdaten erstellt wird, die der Signierende mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

(3) Unter einer qualifizierten elektronischen Signatur versteht man fortgeschrittene elektronische Signaturen, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und die auf einem qualifizierten Zertifikat für elektronische Signaturen beruht

(4) Ein Zertifikat für elektronische Signaturen ist eine elektronische Bescheinigung, die elektronische Daten mit einer natürlichen Person verknüpft.

(5) Als qualifizierter Vertrauensdiensteanbieter ist DocuSign France auch in der Lage, qualifizierte Zertifikate für elektronische Signaturen gemäß der eIDAS-Verordnung zu erstellen. Ebenso verfügt DocuSign France über eine qualifizierte elektronische Signaturerstellungseinheit und kann somit, sofern entsprechend beauftragt, auch qualifizierte elektronische Signaturen für den Nutzer erstellen.

(6) Der Service kann in einen, insbesondere internetbasierten, Antragsprozess eines Dritten eingebettet sein, der mit dem Signierenden einen Vertrag abschließen will (nachfolgend: „**der Vertragspartner**“). Dabei wird der Vertrag für den Service jedoch gesondert zwischen dem Signierenden und DocuSign France geschlossen.

## 3. Vertragsschluss

Der Vertrag nach diesen Nutzungsbedingungen kommt wie folgt zustande: Der Signierende gibt durch Eingabe des zuvor per SMS übermittelten Ident-Codes und Klick auf den Button mit der Aufschrift „Jetzt unterschreiben“ oder einer sinngemäß identischen Aufschrift sein Vertragsangebot hinsichtlich der Beauftragung von DocuSign France für den Service nach Maßgabe des Antragsprozesses und dieser Allgemeinen Nutzungsbedingungen ab und beauftragt DocuSign, die elektronischen Dokumente für den Signierenden zu signieren. Das Vertragsangebot des Signierenden wird ohne ausdrückliche Erklärung gegenüber dem Signierenden angenommen, wenn es nicht unverzüglich von DocuSign abgelehnt wird.

## 4. Leistungen von DocuSign France

(1) Voraussetzung für den Service ist die vorherige Identifizierung des Signierenden. Diese kann auch im Rahmen eines Antrags- oder Identifizierungsprozesses eines Dritten erfolgen.

(2) DocuSign France erstellt auf Basis des Vertrages im Rahmen eines einheitlichen Vorganges eine oder mehrere elektronische Signaturen. Nach Abschluss des Vorganges ist für die Erstellung weiterer elektronischer Signaturen erneut ein Vertrag zwischen Signierendem und DocuSign France zu schließen.

(3) Dem Signierenden wird von DocuSign France nach der eIDAS-Verordnung nach der Identifizierung für die Dauer des Prozesses zur Erstellung einer elektronischen Signatur ein privater Signaturschlüssel eindeutig zugeordnet. Ein privater Signaturschlüssel ist ein geheimer mathematischer Schlüssel, der einmalig innerhalb einer sicheren qualifizierten elektronischen Signaturerstellungseinheit (konfigurierte Software oder Hardware zum Erstellen elektronischer Signaturen) enthalten ist und von dem Signierenden aktiviert wird, um elektronische Dokumente zu signieren. Bei einer qualifizierten elektronischen Signaturerstellungseinheit handelt es sich um eine konfigurierte Soft- oder Hardware zum Erstellen elektronischer Signaturen bei der die Anforderungen der Art. 29 in Verbindung mit Anlage II der eIDAS-Verordnung erfüllt werden. Der private Signaturschlüssel wird von DocuSign France in einer sicheren Umgebung erstellt, gespeichert und nach der Transaktion vernichtet und kann für keinen anderen Vorgang als für die Signatur der im Antragsprozess angezeigten elektronischen Dokumente und dieser Nutzungsbedingungen durch den Signierenden verwendet werden.

(4) Der Signatur des Signierenden wird ferner, je nach Antrag ein Zertifikat für elektronische Signaturen oder ein qualifiziertes Zertifikat für elektronische Signaturen zugeordnet. Damit bestätigt DocuSign France, dass die Signatur der Person zugeordnet werden kann, die sich aus der Signatur ergibt. Ein Zertifikat bedeutet dabei eine elektronische Datei, die die Verbindung zwischen der Identität des Signierenden und dem öffentlichen Schlüssel bestätigt, der mit dem von DocuSign France als Zertifizierungsstelle verwalteten privaten Schlüssel verbunden ist. Öffentlicher Schlüssel bedeutet einen mathematischen Schlüssel, der dem Vertragspartner bereitgestellt wird und bei der Umsetzung eines kryptographischen Protokolls verwendet wird, um die Signatur eines Dokumentes zu verifizieren.

(5) Wenn der Signierende den Service für die Unterzeichnung eines elektronischen Dokumentes nutzt, erstellt und archiviert DocuSign France eine mit der Signaturtransaktion des elektronischen Dokumentes verbundene Beweisdatei insbesondere zum Zwecke, um im Falle eines Gerichtsverfahrens in der Lage zu sein, den Beweis der Gültigkeit der Signatur zu erbringen. DocuSign France wird die Beweisdatei für mindestens sieben (7) Jahre aufbewahren.

Die Beweisdatei enthält:

- die Fassung des elektronischen Dokumentes, das dem Signierenden vor der Signatur vorgelegt wurde;
- die signierte Fassung des elektronischen Dokumentes;
- die Uhrzeit und das Kalenderdatum der Transaktion;

- die Vertragserklärungen des Signierenden zur Erstellung eines Zertifikats sowie zur Unterzeichnung von Dokumenten nach diesen Nutzungsbedingungen durch DocuSign France;
- die technischen Protokolle in Verbindung mit der Transaktion;
- das Ergebnis des Identifizierungsprozesses

(6) DocuSign France ist berechtigt, die Beweisdatei zusammen mit den signierten Dokumenten an den Vertragspartner zu übermitteln.

(7) Nach dem Abschluss des Signaturvorgangs können die elektronischen Dokumente von dem Signierenden entweder beim Vertragspartner oder unter <https://go.idnow.de/contract-download> heruntergeladen werden.

## **5. Pflichten des Signierenden**

(1) Der Signierende ist verpflichtet, bei der Eingabe seiner Daten, insb. seines Vornamens und seines Nachnamens zutreffende und vollständige Angaben zu machen und die Richtigkeit der Eingabe im Zertifikat im dafür vorgesehenen Prozess zu überprüfen. Vorname(n) und Nachname werden Teil des Zertifikats.

(2) Der Signierende ist verpflichtet, unverzüglich die Sperrung des Zertifikats zu beantragen, insbesondere im Fall eines Diebstahls, oder des Verdachts, dass die Daten oder das verwendete Ausweisdokument von einem Nichtberechtigten verwendet wurde.

## **6. Vergütung**

Durch diesen Vertrag entstehen für den Signierenden keine Kosten mit Ausnahme der Tarife für die Internetverbindung des Signierenden.

## **7. Haftung**

(1) DocuSign France haftet im Rahmen dieses Vertrages dem Grunde nach nur für Schäden,

(a) die der DocuSign France vorsätzlich oder grob fahrlässig herbeigeführt haben bzw. die

(b) aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die durch eine Pflichtverletzung von DocuSign France entstanden sind.

(c) wenn der Schaden durch die Verletzung einer Verpflichtung von DocuSign France entstanden ist, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Signierende regelmäßig vertraut und vertrauen darf (Kardinalpflicht).

(2) DocuSign France haftet in den Fällen des Absatzes 1, Buchstaben (a) und (b) der Höhe nach unbegrenzt. Im Übrigen ist der Schadensersatzanspruch auf einen Betrag von 5 Mio. EUR begrenzt.

(3) Die Haftung von DocuSign France für leichte Fahrlässigkeit wird ausgeschlossen, soweit nicht ein Fall von Abs. 1 vorliegt.

(4) Die Haftungsregelungen in vorstehenden Absätzen gelten auch für eine persönliche Haftung der Organe, Mitarbeiter und Erfüllungsgehilfen von DocuSign France.

(5) Soweit eine Haftung nach dem Produkthaftungsgesetz aus der Übernahme einer Garantie oder wegen arglistiger Täuschung in Betracht kommt, bleibt sie von den vorstehenden Haftungsregelungen unberührt.

## **8. Schlussbestimmung**

Auf alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag (einschließlich solcher über seine Gültigkeit) findet französisches Recht Anwendung mit Ausnahme der Regelungen des UN-Kaufrechts, soweit dies nicht dazu führt, dass einem Verbraucher der Schutz durch zwingende, Verbraucher schützende Normen entzogen würde, die ihm ohne diese Regelung zustehen würden.

Für alle Streitigkeiten aus oder im Zusammenhang mit der Identifizierung des Signierenden kann die Registration Authority IDnow GmbH direkt kontaktiert werden über [support@mail.idnow.de](mailto:support@mail.idnow.de).

DocuSign France

## **Verbraucherinformationen DocuSign France**

### **Über DocuSign France**

DocuSign France ist ein qualifizierter Vertrauensdienstleister im Sinne der eIDAS-Verordnung (VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG) mit Sitz in Immeuble Central Park, 9-15 rue Maurice Mallet, 92130 Issy-les-Moulineaux, France, Tel: +33 (0) 975 181 331

### **Über den qualifizierten Vertrauensdienst**

DocuSign France betreibt den Service Cloud Signing Personal Signature CA, einen qualifizierten Vertrauensdienst im Sinne der eIDAS-Verordnung (EU-910/2014).

### **Über die Konformität mit der eIDAS-Verordnung (EU-910/2014)**

DocuSign France wurde mit dem Service Cloud Signing Personal Signature CA gemäß der einschlägigen technischen Norm ETSI EN 319 411-2 auf Konformität mit der eIDAS-Verordnung EU-910/2014 geprüft. Dem Service Cloud Signing Personal Signature CA ist die OID 1.3.6.1.4.1.22234.2.14.3.31 zugewiesen. Die Konformitätsbewertung wurde von der in Frankreich zuständigen Stelle dem LSTI, 10, Avenue Anita Conti, 35400 Saint-Malo ([www.lsti-certification.fr](http://www.lsti-certification.fr)). Die Konformitätsbewertung ist unter <https://lsti-certification.fr/index.php/en/certification/eidas/eidas-trusted-list> abrufbar. Infolge der Konformitätsbewertung ist der Service in der französischen Vertrauensliste gelistet. Dies ist abrufbar unter: <https://www.ssi.gouv.fr/en/regulation/eidas-regulation/trusted-list/>

### **Über die maßgebliche Zertifizierungsrichtlinie**

Die Zertifizierungsrichtlinie ist das Regelwerk, das die technischen Vorgänge, insbesondere die Verfügbarkeit des Dienstes für die Signatur elektronischer Dokumente sowie die allgemeinen Charakteristika der für die Signatur verwendeten Zertifikate beschreibt. Die aktuelle Zertifizierungsrichtlinie „Certificate Policy and Public Certificate Practice Statement“ kann unter der folgenden Adresse eingesehen werden: <https://www.docusign.fr/societe/certification-policies>

### **Über die Dauer der Speicherung von Ereignisprotokollen**

Ereignisprotokolle werden für die Dauer von mindestens sieben Jahren gespeichert.

### **Über die für die Signatur verwendeten Zertifikate**

Zertifikate werden ausschließlich für elektronische Signaturen ausgestellt. Zertifikate für elektronische Signaturen haben nach der gesetzlichen Konzeption immer eine Laufzeit. Die Zertifikate für elektronischen Signaturen des Services Cloud Signing Personal Signature CA sind für den einmaligen Gebrauch vorgesehen und haben entsprechend eine kurze Laufzeit von 7 Tagen, in der das Zertifikat eingesetzt werden kann. Das Zertifikat wird von der Zertifizierungsstelle nicht veröffentlicht. Das Zertifikat ist in dem signierten elektronischen Dokument und in der mit dem elektronischen Dokument verbundenen Beweisdatei enthalten und kann daher vom Vertragspartner eingesehen und überprüft werden. Zertifikate für Signaturen können unter Verwendung einer Überprüfungssoftware, die auf Anfrage von der Zertifizierungsstelle DocuSign France bereitgestellt wird, verifiziert werden. Weitere Details ergeben sich aus der Zertifizierungsrichtlinie.

### **Über die Möglichkeit, Zertifikate zu sperren**

(1) Während der Laufzeit des Zertifikats besteht nach der gesetzlichen Konzeption für den Signierenden die Möglichkeit, ein Zertifikat mit Wirkung für die Zukunft zu sperren. Ein Zertifikat kann gesperrt werden, wenn

- Vornamen und/oder Nachnamen nicht korrekt im Zertifikat angegeben sind oder
- das Zertifikat, das sich auf den privaten Schlüssel bezieht, verloren ging oder kompromittiert wurde oder der Verdacht besteht, dass es verloren ging oder kompromittiert wurde (zum Beispiel im Fall eines Verlustes von Zugangsdaten).

(2) Die Sperrung durch den Signierenden muss über die URL <https://www.idnow.de/sperrung> beantragt werden. Das Zertifikat wird dann innerhalb von vierundzwanzig (24) Stunden nach dem Zeitpunkt der Verifikation des Antrags gesperrt.

(3) Ein Zertifikat kann unter den in (1) genannten Voraussetzungen auch durch die Zertifizierungsstelle gesperrt werden. Eine Sperrung durch die Zertifizierungsstelle kann außerdem erfolgen, wenn eine der folgenden Voraussetzungen erfüllt ist:

- Die Zertifizierungsstelle ist gesperrt.
- Die natürliche Person oder die Registrierungsstelle versäumten es, die in der Zertifizierungsrichtlinie definierten, notwendigen Verpflichtungen und Sicherheitsregeln einzuhalten.

### **Barrierefreiheit**

DocuSign France ergreift verschiedene Maßnahmen, um Nutzer mit Einschränkungen zu unterstützen. Dazu gehören die Darstellung mit hohen Kontrastwerten und weitere technische Kommunikationskanäle (z.B. Chat Funktion). Durch grundlegende Anforderungen an den Prozess (Video-Chat), gibt es jedoch bei bestimmten Einschränkungen von Nutzern (z.B. Taubheit, Blindheit) nur eingeschränkt die Möglichkeit, den Prozess zu durchlaufen.

### **Datenschutz**

DocuSign France erhält für die Ausstellung der Signatur die folgenden Daten:

- die Fassung des elektronischen Dokumentes, das dem Signierenden vor der Signatur vorgelegt wurde;
- Personenbezogene Daten aus dem Ausweisdokument des Signierenden
- Mobilnummer des Signierenden
- Email des Signierenden
- IP Adresse des Signierenden
- Aufnahme des Gesichts des Signierenden im Identifizierungsprozess

Diese Daten werden während des Identifizierungsprozess aufgenommen nach den Vorgaben der eIDAS-Verordnung zum Zweck der Ausstellung eines fortgeschrittenen oder qualifizierten Zertifikates. Nur eine begrenzte Gruppe von autorisierten Mitarbeitern haben Zugriff auf die erhobenen personenbezogenen Daten zum Zweck der Beweisverwaltung. Falls der Signierende den Signaturvorgang abbricht, wird kein Zertifikat ausgestellt und insofern auch keine Dokumente unterschrieben.

Der Widerspruch zur Verarbeitung der Daten des Signierenden ist gekoppelt an das Recht den Identifizierungsvorgang und / oder den Signaturvorgang abzubrechen. Falls Fehler in den Daten (Vor- / Nachnamen, Mobilnummer, Emailadresse) festgestellt werden, hat der Signierende das Recht den Vorgang während der Signatur abzubrechen. Zusätzlich hat der Signierende die Möglichkeit zur Sperrung des Zertifikates wie in diesen Nutzungsbedingungen beschrieben.

Die personenbezogenen Daten werden erhoben auf Basis Artikel 6 (1) (b) GDPR für den Zweck (a) der Identifizierung des Signierenden, (b) zur Ausstellung des Zertifikates (c), Authentifizierung des Signierenden während der Unterschrift und (d) falls eine Sperrung eines Zertifikates beantragt wird.

Die personenbezogenen Daten des Signierenden werden in Übereinstimmung der anwendbaren Europäischen Regularien erhoben und verarbeitet. Der Signierende hat das Recht die erhobenen Daten einzusehen und gegebenenfalls zu korrigieren oder der Verarbeitung zu widersprechen. Dieses Recht ist gekoppelt an die Möglichkeit zur Sperrung des Zertifikates wie in diesen Nutzungsbedingungen beschrieben und/oder an die Möglichkeit den Identifizierungsprozess abzubrechen.

Nachdem ein Zertifikat ausgestellt wurde können die personenbezogenen Daten nicht mehr verändert oder gelöscht werden, da diese nach der eIDAS-Verordnung als Beweismittel vorgehalten werden müssen. Die personenbezogenen Daten werden nach den Anforderungen der eIDAS-Verordnung für ein Minimum von 7 Jahren gespeichert.

Auskunftsanfragen nach 2016/679 European Regulation (GDPR) müssen an Data Privacy Officer DocuSign France, 9-15 Rue Maurice Mallet, 92130 Issy-les-Moulineaux, France, cil@docusign.com gestellt werden. Der Signierende hat ebenfalls das Recht sich an die verantwortliche französische Datenschutzbehörde zu wenden.

## 1. Preamble

These General Terms of Use (hereinafter "Terms of Use") shall govern the legal conditions that apply between DocuSign France and you (hereinafter: "the Signatory").

## 2. Subject matter of the contract / definitions

- (1) The purpose of the contract pursuant to the present Terms of Use is that DocuSign France shall, in accordance with Regulation (EU) No. 910/2014 of the European Parliament and the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (for short: eIDAS Regulation), create an advanced or qualified electronic signature for the Signatory on one or more documents by means of an electronic remote signature and, in the event of a qualified electronic signature, provide the Signatory with a qualified certificate for electronic signatures (hereinafter: "**the Service**")
- (2) An advanced signature is a signature that is unambiguously assigned to the Signatory, allows the identification of the Signatory and is created using electronic signature creation data that is under the sole control of the Signatory with a high degree of trust.
- (3) A qualified signature is an advanced electronic signature that has been created by a qualified electronic signature creation unit and that is based on a qualified certificate for electronic signatures.
- (4) A certificate for electronic signatures is an electronic certificate that connects electronic data to a natural person.
- (5) As a qualified trust services provider, DocuSign France is also able to create qualified certificates for electronic signatures in accordance with the eIDAS Regulation. DocuSign France also has a qualified electronic signature creation unit and can thus create qualified electronic signatures for the user if instructed accordingly.
- (6) The Service can be embedded in a primarily internet-based request procedure of a third party which wishes to conclude a contract with the Signatory (hereinafter: "**the Contractual Partner**"). The contract for the Service shall, however, be concluded separately between the Signatory and DocuSign France.

## 3. Conclusion of the contract

The contract pursuant to the present Terms and Conditions shall enter into force as follows: by entering the ident code that has previously been sent by text message and by clicking on the "sign now" button or a button with a correspondingly identical label, the Signatory shall submit its contract proposal with respect to commissioning DocuSign France for the Service in accordance with the request procedure and the present General Terms and Conditions and shall commission DocuSign to sign electronic documents for the Signatory. The Signatory's contract proposal shall be accepted without an explicit declaration to the Signatory, unless it is rejected by DocuSign immediately.

## 4. Services of DocuSign France

- (1) The prerequisite for the Service is the prior identification of the Signatory. This can also take place within the framework of a request procedure or identification process of a third party.
- (2) DocuSign France shall create one or more electronic signatures on the basis of the contract within a uniform process. After the completion of the process, a contract between the Signatory and DocuSign France must be concluded for the creation of further electronic signatures.
- (3) After the identification, the Signatory shall be unambiguously assigned a private signature key by DocuSign France, in accordance with the eIDAS Regulation, for the duration of the process relating the creation of an electronic signature. A private signature key is a secret mathematical key that is contained as a one-off within a secure qualified electronic signature creation unit (configured software or hardware for the creation of electronic signatures) and is activated by the Signatory to sign documents. A qualified electronic signature creation unit is configured software or hardware for the creation of electronic signatures, in which the requirements of Art. 29, in conjunction with Appendix II, of the eIDAS Regulation are satisfied. The private signature key shall be created by DocuSign France in a secure environment, stored and destroyed after the transaction and cannot be used for any other process than for the signature of the electronic documents indicated in the request procedure and of the present Terms of Use by the Signatory.
- (4) The signature of the Signatory shall also be assigned a certificate for electronic signatures or a qualified certificate for electronic signatures, depending on the request. With this, DocuSign France confirms that the signature can be assigned to the person who is identified by the signature. A certificate is an electronic file that confirms the link between the identity of the Signatory and the public key which is connected to the private key administered by DocuSign France as the certification authority. A public key is a mathematical key that is provided to the Contractual Partner and used for the implementation of a cryptographic protocol to verify the document.
- (5) If the Signatory uses the Service to sign an electronic document, DocuSign France shall create and archive an evidence file linked to the signature transaction of the electronic document especially for the purpose so that it is able to provide evidence of the validity of the signature in the event of court proceedings. DocuSign France shall store the evidence file for at least seven (7) years.

The evidence file shall contain:

- the version of the electronic document that was presented to the Signatory prior to the signature;
- the signed version of the electronic document;
- the time and date of the transaction;
- the contractual declarations of the signatory regarding the creation of a certificate and the signing of documents by DocuSign France in accordance with the present Terms of Use;
- the technical protocols connected to the transaction;
- the result of the identification process

(6) DocuSign France shall be entitled to send the evidence file to the Contractual Partner, along with the signed documents.

(7) After the completion of the signature process, the electronic documents may be downloaded by the Signatory either from the Contractual Partner or at <https://go.idnow.de/contract-download>.

#### **5. Obligations of the Signatory**

(1) The Signatory is obliged to provide complete and accurate information when entering his data, especially his name and his surname, and to check the accuracy of the entry in the certificate in the process provided for this. The forename(s) and surname shall become part of the certificate.

(2) The Signatory shall be obliged to apply for the certificate to be revoked, especially in the event of theft or a suspicion that the data or the ID document used have been used by an unauthorised person.

#### **6. Remuneration**

No costs shall arise for the Signatory as a result of the present contract, with the exception of the tariffs for the Signatory's internet connection.

#### **7. Liability**

(1) Within the framework of this contract, DocuSign France shall essentially be liable for

(a) damages that DocuSign France caused through wilful intent or gross negligence or

(b) damages resulting loss of life, physical injury or damage to health caused by an infringement of an obligation by DocuSign France.

(c) damages caused by the infringement of an obligation by DocuSign France where the fulfilment of this obligation makes the proper execution of the contract possible in the first place and the Signatory regularly relies and may rely upon compliance with this obligation (cardinal obligation).

(2) DocuSign France shall have unlimited liability in the cases referred to in (1) (a) and (b). Claims to compensation shall be limited to an amount of 5 million euros.

(3) The liability of DocuSign France for slight negligence shall be ruled out, unless a case referred to in (1) is present.

(4) The liability regulations in the above paragraphs shall also apply to a personal liability of the bodies, employees and vicarious agents of DocuSign France.

(5) If a liability in accordance with the German Product Liability Act comes into question as a result of the assumption of a warranty or because of fraudulent misrepresentation, it shall remain unaffected by the above liability regulations.

#### **8. Final provisions**

French law shall apply to all disputes arising from or in connection with the present Contract (including disputes relating to its validity), to the exclusion of the provisions of the UN Convention on Contracts for the International Sale of Goods, unless this leads to the withdrawal of the protection by mandatory consumer protection standards to which a consumer would otherwise be entitled.

For all disputes arising from or in connection with the identification of the Signatory, the registration authority IDnow GmbH can be contacted directly at [support@mail.idnow.de](mailto:support@mail.idnow.de).

DocuSign France

## **DocuSign France consumer information**

### **About DocuSign France**

DocuSign France is a qualified trust service provider in terms of the eIDAS Regulation (REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 23rd July 2014 electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) with its registered place of business in Immeuble Central Park, 9-15 rue Maurice Mallet, 92130 Issy-les-Moulineaux , France, Tel: +33 (0) 975 181 331

### **About the qualified trust service**

DocuSign France runs the service Cloud Signing Personal Signature CA, a qualified trust service in terms of the eIDAS Regulation (EU 910/2014)

### **About conformity with the eIDAS Regulation (EU 910/2014)**

DocuSign France was checked for conformity with the eIDAS Regulation EU 910/2014 in accordance with the relevant technical standard ETSI EN 319 411-2. The OID 1.3.6.1.4.1.22234.2.14.3.31 shall be assigned to the service Cloud Signing Personal Signature CA. The conformity assessment was performed by the competent authority in France, LSTI, 10, Avenue Anita Conti, 35400 Saint-Malo ([www.lsti-certification.fr](http://www.lsti-certification.fr)). The conformity assessment can be accessed at <https://lsti-certification.fr/index.php/en/certification/eidas/eidas-trusted-list>. As a result of the conformity assessment, the service is listed in the French trusted list. This can be accessed at: <https://www.ssi.gouv.fr/en/regulation/eidas-regulation/trusted-list/>

### **About the decisive certification guidelines**

The certification guidelines are the set of rules that describe the technical processes, especially the availability of the service for the signature of electronic documents and the general characteristics of the certificates used for the signature. The current certification guidelines "Certificate Policy and Public Certificate Practice Statement" can be viewed at the following address: <https://www.docusign.fr/societe/certification-policies>

### **About the period of storage for event protocols**

Event protocols shall be stored for a period of at least seven years

### **About the certificates used for the signature**

Certificates shall be issued exclusively for electronic signatures. In accordance with the statutory concept, certificates for electronic signatures shall always have a term. The certificates for electronic signatures of the service Cloud Signing Personal Signature CA are intended for one-off use and accordingly shall have a short term of 7 days, in which the certificate can be used. The certificate shall not be published by the certification authority. The certificate shall be contained in the signed electronic document and in the evidence file connected with the electronic document and may, therefore, be viewed and checked by the Contractual Partner. Certificates for signatures can be verified using verification software that is made available to DocuSign France by the certification authority upon request. Further details can be found in the certification guidelines.

### **About the possibility of revoking certificates**

(1) During the term of the certificate, the Signatory shall have the option of revoking a certificate with effect for the future in accordance with the statutory concept. A certificate may be revoked if

- forenames and/or surnames are not provided correctly in the certificate or
- the certificate that relates to the private key is missing or has been compromised or there is a suspicion that it is missing or has been compromised (for example in the event of the loss of access data).

(2) The revocation by the Signatory must be requested via the URL <https://www.idnow.de/sperrung>. The certificate shall then be revoked within twenty four (24) hours of the time of the verification of the request.

(3) A certificate may also be revoked by the certification authority under the conditions specified in (1). A revocation by the certification authority may also take place if one of the following conditions is met:

- the certification authority is closed.
- the natural person or the registration authority have neglected to observe the necessary obligations and security rules defined in the certification guidelines.

### **Accessibility**

DocuSign France shall take various measures to support users with disabilities. These shall include a presentation with high contrast values and other technical communication channels (e.g. chat function). Due to underlying requirements with regard to the process (video chat), users with certain disabilities (e.g. deafness, blindness) shall only be able to go through the process to a limited extent.

### **Data privacy**

DocuSign France shall receive the following data for the issuance of the signature:

- the version of the electronic document that was presented to the Signatory prior to the signature
- personal data from the ID document of the Signatory
- the mobile phone number of the Signatory
- the e-mail address of the Signatory
- the IP address of the Signatory
- a photograph of the face of the Signatory in the identification process

This data shall be collected during the identification process, in accordance with the provisions of the eIDAS Regulation, for the purpose of the issuance of an advanced or qualified certificate. Only a restricted group of authorised employees shall have access to the collected personal data for the purpose of the management of the evidence. If the Signatory aborts the signature process, no signature shall be issued and no documents shall be signed.

The objection to the processing of the Signatory's data shall be connected to the right to abort the identification process and / or the signature process. If errors are identified in the data (forenames / surnames, mobile number, e-mail address), the Signatory shall have the right to abort the process during the signature. The Signatory shall also have the option of revoking the certificate as described in the present Terms of Use.

The personal data shall be collected on the basis of Article 6 (1) (b) GDPR for the purpose of (a) the identification of the Signatory, (b) the issuance of the certificate, (c) the authentication of the Signatory during the signature and (d) if a revocation of a certificate is requested.

The personal data of the Signatory shall be collected and processed in accordance with the applicable European regulations. The Signatory shall have the right to view the collected data and, if applicable, to correct it or to object to the process. This right is connected to the possibility of revoking the certificate as described in the present Terms of Use and/or to the possibility of aborting the identification process.

After a certificate has been issued, the personal data can no longer be changed or deleted, as it has to be kept as evidence in accordance with the eIDAS Regulation. The personal data shall be stored for a minimum of 7 years in accordance with the requirements of the eIDAS Regulation.

Requests for access in accordance with European Regulation 2016/679 (GDPR) must be made to Data Privacy Office, DocuSign France, 9-15 Rue Maurice Mallet, 92130 Issy-les-Moulineaux, France, cil@docusign.com. The Signatory shall also have the right to contact the responsible French data protection authority.