ENGLISH

1. SUBJECT MATTER

The purpose of these General Terms of Use (hereinafter referred to as 'General Terms of Use') is to define the legal conditions in respect of the acquisition and use of DocuSign France subscription certificates and the corresponding obligations of DocuSign France, the registration authority (referred to as 'RA'), the customer and the subscriber. Subscriber certificates shall be supplied and administered in connection with the online service for qualified electronic signatures as provided by DocuSign France.

2. DEFINITIONS

Certificate(s): An electronic file that has confirmed the connection between a defined subscriber identity and the public key, which is connected to the private key administered by the CA.

Procedure for administering certificates: All procedures applied by the RA for issuing and administering certificates.

Certification guideline(s) (CG): The policy stipulated by an OID and published by the CA that describes the general characteristics of the certificates it supplies. A certification guideline describes the obligations and responsibilities of the CA, RA, users and the applicants for certificates and all the components that are part of the general life cycle of a certificate.

The certification guideline that is valid at the time of signing this agreement shall be used to personally identify the certificate.

The version of the CG to be used is the version that is valid on the day of initializing the service. It can be found at the following address: https://www.docusign.fr/societe/certification-policies (OID 1.3.6.1.4.1.22234.2.14.3.31). The subsequent versions of the CG shall be accessible to users on the DocuSign France website.

Certificate revocation list (CRL): The list of invalid certificates that were revoked before their expiration date. This CRL is published regularly and is digitally signed by the CA that issued the certificates in the list.

Certification authority (or CA): The authority of DocuSign France, which creates the certificates and administers the life cycle of the certificate (issuance, extension, revocation) at the request of the registration authority in accordance with the rules and practices defined in its certification guideline(s).

Customer: A legal entity who suggests an electronic document that must be signed by the subscriber. The customer is in a contractual relationship with the registration authority in order to delegate administering the verification of the subscriber identity and the signature process of the electronic document by the subscriber.

Declaration of consent: The process by which the DocuSign France receives the consent of the subscriber to:

obtain a certificate in accordance with the personal identity of the subscriber certificate;

declare consent to signing the electronic document.

The declaration of consent shall be executed between the service and the subscriber within the RA application.

RA application: The application with the name IDnow eSigning, which shall be used by the RA to verify the identity of the subscribers and to request that the service enable the subscribers to sign an electronic document.

Electronic document(s): The document in electronic form that is created by the customer and submitted with the RA application to be signed by the signatory. The electronic document may be signed by other signatories and by the customer as a legal entity.

General terms of use (GTU): The legal conditions at hand and conditions in respect of using the service. These GTU are contained in the electronic documents that must be signed by the subscriber.

Subscriber certificate (certificate) personal identity: The identity that was built using the data collected by the RA about the subscriber as well as the data defined by the RA. This identity shall be used to authenticate a natural person.

Private key: A secret mathematical key that is uniquely contained within a device and is activated remotely by the subscriber to sign electronic documents.

Evidence file(s): One of the files created, signed and assigned a time stamp by DocuSign France, which contains all relevant infor- mation associated with the authentication of the subscriber and the process of signing the electronic document. A dedicated evidence file shall be connected with each signed electronic document for the purpose of proving the validity of the electronic signature in the event of legal proceedings.

Public key: A mathematical key that shall be published and used when implementing a cryptographic protocol to verify the signature of a document.

Registration authority (or RA): The institution that is in a contractual relationship with the CA and acts on the basis of the authority transferred by the CA in accordance with the rules and practices as they have been defined in its certification guideline(s), to check the identity of the subscriber for accuracy and requesting that the service allow the subscriber to sign an electronic document. To this extent, the RA carries out the RA application.

Service: All services performed by DocuSign France in accordance with these GTU, in particular, to enable the use of the certificate and the private key associated with it, to execute the declaration of consent with legal validity and to sign the electronic document using a qualified electronic signatory.

Guideline for signing and evidence management (SPMP): The document that describes technical procedures used by the service provider for signing electronic documents by the RA and one or several subscribers in accordance with the declaration of consent, and that is used for generating and archiving evidence files during the use of the service. The SPMP and its subsequent updates can be accessed on the DocuSign France website

and form an essential part of this agreement.

Subscriber(s) (or signatory): The individual(s) who

registers/register for the RA application

process(es) the electronic document(s) for the customer

to whom the RA presents the electronic document(s) for signing and

signs/sign the electronic document(s) following his/her/their permission in accordance with the declaration of consent.

The identity of a subscriber shall be entered and confirmed beforehand by the RA as part of its responsibility as a registration authority.

URL: uniform resource locator (internet address): The address of a page or a file that is available on the internet.

3. PROCEDURE FOR THE APPLICATION OF CERTIFICATES VIA THE SERVICE

The subscriber shall be informed and expressly agrees that:

DocuSign France shall be encouraged by the customer via the RA to obtain the signature of the subscriber on the electronic document.

To this extent:

The identity of the subscriber shall be confirmed by the RA using the RA application. The procedures and technical resources of the RA have been confirmed as in conformity with ETSI 319 411-2 QCP n-qscd as well as the Geldwäschegesetz (German Money Laundering Act (GwG)). During the process of verifying the identity, the subscriber shall be connected via video conferencing to the IDnow call centre. The incoming call centre employee shall lead the subscriber through the steps of identification. These include, amongst other things, the following:

• The call centre employee takes a photograph of the subscriber. With this, amongst other things, a later facial comparison shall take place.

• The call centre employee shall check the information in the identity document (e.g. identity card number, date of birth, etc.)

• The call centre employee shall check the different security features of the identity document. For example, holographic security features shall be checked by their light reflection and a check digit validation shall take place.

• A facial comparison between the photograph on the identity document and the image taken by the subscriber to be identified shall be carried out by the call centre employee.

A private signature key shall be unambiguously assigned to the subscriber for the duration of the signature of the electronic document. The private key shall be securely created, saved and destroyed after the transaction and may be used for no other purpose than for the subscriber to sign the electronic document. Activating the private key for signing the electronic document remains the sole control of the subscriber.

Depending on the application, the subscriber shall be assigned an advanced or qualified certificate as a means for confirming that he/she is the genuine signatory of the electronic document.

It is necessary that he/she produces the declaration of consent stipulated by the service with legal effectivity to declare that he/she agrees to sign or refuses to sign the electronic document. The subscriber needs to enter a previously sent SMS (Ident-Code) within the video chat.

Optionally, the subscriber can choose a password before the declaration of consent to create an IDnow account according to the terms and conditions of IDnow. With this password and a newly issued Ident-Code, the subscriber is able to sign electronic documents at a later point in time.

Once it has been signed, the electronic document can be downloaded by the subscriber directly after the signature process at IDnow or by the customer, or it shall be transferred by IDnow or the customer to the subscriber. If the signed documents are provided by IDnow, the documents can be download from https://go.idnow.de/contract-download.

To comply with legal requirements, audio and/or video recordings of the identification process may be taken.

DocuSign France shall create and archive an evidence file connected with the signature transaction of the electronic document solely for the purpose of providing evidence of validity for the signature in the event of legal proceedings. The period of archiving shall depend on the legislation applicable to the electronic document determined by the customer. The evidence file contains:

• The version of the electronic document that was submitted to the subscriber prior to signing;

• The signed version of the electronic document;

• The time and calendar date of the transaction;

• The declaration of consent as executed between the subscriber and the service;

• The technical protocols in connection with the transaction.

4. ISSUANCE OF THE CERTIFICATE

The subscriber is responsible for examining the content of the certificate (mainly for the ‘subject’ field of the certificate that contains the full surname and first name of the aforementioned subscriber). The subscriber and the customer have eight (8) days at most after issuing the certificate to reject the content of the certificate and to submit a request for revocation to the RA. After this eight-day deadline, the certificate shall be deemed as

accepted by the user and can no longer be revoked.

5. PUBLICATION OF THE CERTIFICATE

The certificate shall be published by neither the CA nor the RA. The certificate is contained in the signed electronic document and in the evidence file associated with the electronic document.

6. VALIDITY OF THE CERTIFICATE

The certificates are valid for ten (10) days at most. The aforementioned period begins on the date the CA issues the certificate. After the time of validity of the certificate has elapsed, the signatures of the PDF documents may be verified using the checking software as issued by the customer particularly to verify that the document was electronically signed at the time of signing by a valid certificate issued by the CA.

7. CONDITIONS FOR REVOKING THE CERTIFICATE

7.1 Revocation instigated by the subscriber or customer

The subscriber and the customer can revoke the certificate by submitting a request to the CA. It can be submitted via the URL https: //www.idnow.eu/revocation. In the following events, the subscriber and the customer may submit a request for revocation:

DN information has been not correctly entered.

The certificate, which relates to the private key, has been lost or was compromised or it is suspected that it has been lost or was compromised (for example, in the event of a loss of login details and password and/or GSM).

The subscriber and the customer have eight (8) days at most after issuing the certificate to submit a request for revocation to the RA. Once this eight-day deadline has elapsed, the certificate can no longer be revoked.

The certificate shall be revoked within twenty-four (24) hours from the time of verifying the request.

7.2 Revocation instigated by the CA

In the event of the following circumstances, the certificate shall be immediately revoked by the CA:

The CA has been blocked.

The natural person or the RA neglected to observe the necessary obligations and security rules defined in the CG.

The certificate, which relates to the private key, has been lost or was compromised or it is suspected that it has been lost or was compromised.

Any other reason that shall be stated by the CA.

The subscriber concerned shall be informed about the revocation of the certificate.

7.3 Revocation at the suggestion of the RA

In the event of the following circumstances, the certificate shall be immediately revoked by the RA:

DN information has been not correctly entered;

The certificate, which relates to the private key, has been lost or was compromised or it is suspected that it has been lost or was compromised (for example, in the event of a loss of login details and password and/or GSM).

The subscriber concerned shall be informed about the revocation of the certificate.

Revocation information will always be available from the CA that publishes a CRL. In the event of the CA's end of life or the Service stopping with this CA or even in the event of a compromised CA key, a last CRL is generated and archived at DocuSign France. This CRL is published on the DocuSign France website until the TSP ends. This CRL is also published on the CRL distribution URL contained in the Certificate until the last Certificate issued by the CA expires.

8. EFFECTIVE TIME AND TERM

The General Terms of Use at hand shall be valid from the moment they are signed by the subscriber, which is associated with the time of the certificate request.

These General Terms of Use shall apply to a period that corresponds with the life cycle of the certificates issued to the subscriber and shall end at the moment the validity of the aforementioned certificates ends.

9. SUBSCRIBER OBLIGATIONS

By consenting to use this service, the subscriber shall agree to observe and be responsible for the terms of these General Terms of Use:

The verification of the certificate and the RA warning.

The use of certificates and the associated private keys in accordance with the terms of contractual term 6 above and the certifi- cation guideline.

The verification of the authenticity and accuracy of information stated in the certificate, as presented in the course of the decla- ration of consent by DocuSign France, for example.

The immediate application of a certificate revocation by the RA if this is necessary and particularly in the event of theft, disclosure, suspicion it has been compromised or the identity document used has been compromised.

10. LIABILITY

Neither DocuSign France nor the RA shall be liable for any resulting indirect or unforeseeable damages incurred by the subscriber, such as damage of a financial or economic nature, loss of revenue, business losses, loss of customers, economic difficulties, loss of earnings or loss of data, that arise from the current General Terms of Use or are a consequence thereof or are inherent in the use of the certificates issued by the CA.

Should DocuSign France be held liable, it shall be expressly agreed that DocuSign France is responsible for compensating all direct, established and immediate damage. The amount of the aforementioned compensation for the claim of a subscriber shall not exceed five (5) euros per certificate. DocuSign France shall assume no liability in the event that the subscriber has not observed the obligations provided herein.

Neither the CA nor the RA shall assume liability regarding the use of certificates or the private key associated with it and issued by the RA under conditions and for purposes not intended in the certification guideline.

As neither the CA nor the RA has knowledge of the content or the legal scope of the signed electronic documents, neither the CA nor the RA are liable on this basis.

Neither the CA nor the RA shall assume liability or responsibility for the quality of the internet connection or the consequences of delays or losses in the transfer of electronic mail, letters and documents or for delays, changes or other errors when transferring telecommunications in accordance with these General Terms of Use. Furthermore, it shall be agreed that neither the CA nor the RA shall be liable for malfunctions at the subscriber workstation if these malfunctions are the result of using the certificate in a way that does not comply with the associated documentation available. Equally, the liability of neither the CA nor the RA covers the proper functioning (failures, errors, incompatibility, etc.) of the hardware and software as well as the environment of the subscriber. Neither the CA nor the RA shall be liable or responsible for a delay in fulfilling the obligations or for non-fulfilment of the obligations that arises in connection with these General Terms of Use, if the circumstances that are the cause for this are the result of a case of force majeure as defined in the contractual term 11 listed below.

11. FORCE MAJEURE

Neither the CA nor the RA shall be liable for the non-fulfilment or delay of one or several obligations in accordance with these General Terms of Use due to a case of force majeure or unforeseen circumstances or circumstances that are beyond their reasonable control. The following shall be deemed the events of force majeure or unforeseeable circumstances: completely external strikes, extreme weather conditions, epidemics, transport blockages or blockades of supply infrastructure, earthquakes, fire, floods, water damage, official or legal limitations, legal or regulatory changes to types of marketing, disruption to telecommunications (including interceded networks) and all events in third party networks.The CA and/or the RA shall suspend the fulfilment of its obligations in the event of an incident deemed to be force majeure and shall not be liable in this matter.

12. PROTECTION OF PERSONAL DATA

The personal data collected by the subscriber and the customer during the process for administering the certificates shall be processed by the RA to:

enable the RA to authenticate and identify the subscriber as required

perform checks that are necessary for issuing and, where required, revoking certificates and

create a personal identity that shall be entered into the certificate and

authenticate the subscriber during the declaration of consent. DocuSign France agrees to observe European law in respect of protecting personal data.

Every objection to storing personal data prevents a certificate being issued. By signing the electronic document and the GTU, the subscriber agrees that the RA and/or the CA shall retain the evidence file that contains their personal data for a period of seven (7) years after Certificate expiration.

13. INTELLECTUAL PROPERTY

The subscriber acknowledges that DocuSign France retains all rights to intellectual property (patents, registered trademarks and other rights) for the elements constituting the service as well as documents, concepts, technologies, discoveries, processes, software or work associated with the certificates and the related services that shall be provided by DocuSign France, irrespective of the form, programming language, program media or the language used. These General Terms of Use shall transfer no rights to intellectual property in respect of the certificates and the related services to the subscriber.

14. INSURANCE

The CA declares that is has taken professional liability insurance in respect of the services contained herein, which shall adequately cover its obligations in accordance with these General Terms of Use.

15. PUBLICATION DATE

June 4, 2020

DEUTSCHLAND

1. GEGENSTAND

Der Zweck dieser Allgemeinen Nutzungsbedingungen (im Nachfolgenden „Allgemeine Nutzungsbedingungen“) ist es, die rechtlichen Bedingungen in Bezug auf den Erwerb und die Nutzung von DocuSign France Abonnentenzertifikaten und die entsprechenden Ver- pflichtungen von DocuSign France, der Registrierungsstelle (als „RA“ bezeichnet), des Kunden und des Abonnenten zu definieren. Abonnentenzertifikate werden im Zusammenhang mit dem Online-Dienst für qualifizierten elektronische Signaturen geliefert und verwaltet, wie er von DocuSign France angeboten wird.

2. DEFINITIONEN

Zertifikat(e): bedeutet eine elektronische Datei, die die Verbindung zwischen einer bestimmten Abonnentenidentität und dem öffent- lichen Schlüssel, der mit dem von der CA verwalteten privaten Schlüssel verbunden, ist bestätigt.

Verfahren für die Verwaltung von Zertifikaten: bedeutet alle von der RA für die Ausstellung und Verwaltung von Zertifikaten angewendeten Verfahren.

Zertifizierungsrichtlinie(n) (ZR): bedeutet das von einer OID festgelegte und durch die CA veröffentlichte Regelwerk, dass die all- gemeinen Charakteristika der Zertifikate, die sie ausliefert, beschreibt. Eine Zertifizierungsrichtlinie beschreibt die Verpflichtungen und Verantwortlichkeiten der CA, der RA, der Verwender und der Antragsteller für Zertifikate und alle die Komponenten, die der allgemeine Lebenszyklus eines Zertifikates mit sich bringt.

Für die Personenidentität des Zertifikats wird die Zertifizierungsrichtlinie, die zum Zeitpunkt der Unterzeichnung dieser Vereinbarung gültig ist, verwendet. Die anzuwendende Fassung der ZR ist die Fassung, die am Tag der Initialisierung des Dienstes Gültigkeit hat. Sie kann unter der folgenden Adresse eingesehen werden: https://www.docusign.fr/societe/certification-policies (OID 1.3.6.1.4.1.22234.2.14.3.31). Die nachfolgenden Fassungen der ZR werden für die Nutzer auf der Webseite von DocuSign France zugänglich sein.

Zertifikatssperrliste (CRL): bedeutet die Liste ungültiger Zertifikate, die vor ihrem Ablaufdatum widerrufen wurden. Die CRL wird regelmäßig veröffentlicht und durch die CA digital signiert, die die Zertifikate in der Liste ausgestellt hat.

Zertifizierungsstelle (oder CA): bedeutet die Stelle von DocuSign France, die Zertifikate erstellt und den Lebenszyklus des Zertifikats (Ausstellung, Verlängerung, Widerruf) auf Wunsch der Registrierungsstelle in Übereinstimmung mit den in deren Zertifizierungsrichtli- nie(n) definierten Regeln und Praktiken verwaltet.

Kunde: bedeutet eine Rechtspersönlichkeit, die ein elektronisches Dokument vorschlägt, das von dem Abonnenten zu signieren ist. Der Kunde steht in einer vertraglichen Beziehung mit der Registrierungsstelle, um die Verwaltung der Verifizierung der Abonnentenidentität und des Signaturvorgangs des Elektronischen Dokumentes durch den Abonnenten zu delegieren.

Einverständniserklärung: bedeutet das Verfahren, nach dem DocuSign France das Einverständnis des Abonnenten einholt, um:

Ein Zertifikat nach der **Personenidentität des Abonnentenzertifikats zu erhalten**;

das Einverständnis zur Signatur des Elektronischen Dokumentes zu erklären.

Die Einverständniserklärung wird zwischen dem Dienst und dem Abonnenten innerhalb der RA-Anwendung rechtsgültig ausgefertigt.

RA-Anwendung: bedeutet die Anwendung mit dem Namen IDnow eSigning, die von der RA verwendet wird, um die Identität der Abonnenten zu verifizieren und Anfragen an den Dienst zu stellen, um die Abonnenten in die Lage zu versetzen, ein elektronisches Dokument zu signieren.

Elektronische(s) Dokument(e): bedeutet das Dokument in elektronischer Form, das durch den Kunden erstellt wird und bei der RA-Anwendung eingereicht wird, um durch den Signatar signiert zu werden. Das elektronische Dokument kann durch andere Signatare und durch den Kunden als eine Rechtspersönlichkeit signiert werden.

Allgemeine Nutzungsbedingungen (ANB): bedeutet die vorliegenden rechtlichen Bedingungen und Bestimmungen in Bezug auf die Nutzung des Dienstes. Diese ANB sind in den elektronischen Dokumenten enthalten, die von dem Abonnenten zu signieren sind.

Abonnentenzertifikat (Zertifikat) Personenidentität: bedeutet die Identität, die unter Verwendung der von der RA erhobenen Daten des Abonnenten sowie der von der RA definierten Daten aufgebaut wurde. Diese Identität wird verwendet, um eine natürliche Person zu authentifizieren.

Privater Schlüssel: bedeutet einen geheimen mathematischen Schlüssel, der einmalig innerhalb eines Gerätes enthalten ist und ferngesteuert von dem Abonnenten aktiviert wird, um elektronische Dokumente zu signieren.

Beweisdatei(en): bedeutet eine von DocuSign France erstellte, signierte und mit Zeitstempel versehene Datei, die alle diejenigen Informationen enthält, die in Verbindung mit der Authentifizierung des Abonnenten und dem Vorgang der Signatur des elektronischen Dokumentes stehen. Mit jedem signierten elektronischen Dokument wird eine dedizierte Beweisdatei zum Zwecke des Beweises der Gültigkeit der elektronischen Signatur im Falle eines Gerichtsverfahrens verbunden.

Öffentlicher Schlüssel: bedeutet einen mathematischen Schlüssel, der öffentlich gemacht und bei der Umsetzung eines kryptogra- phischen Protokolls verwendet wird, um die Signatur eines Dokumentes zu verifizieren.

Registrierungsstelle (oder RA): bedeutet die Institution, die in einer vertraglichen Beziehung mit der CA steht und aufgrund einer durch die CA übertragenen Vollmacht in Übereinstimmung mit den Regeln und Praktiken, wie sie in ihrer(n) Zertifizierungsrichtlinie(n) definiert sind, handelt, um die Identität des Abonnenten auf ihre Richtigkeit hin zu überprüfen und Anfragen an den Dienst zu stellen, um es den Abonnenten zu ermöglichen, ein elektronisches Dokument zu signieren. In diesem Umfang führt die RA die RA-Anwendung aus.

Dienst: bedeutet alle die Dienstleistungen, die von DocuSign France nach diesen ANB erbracht werden, insbesondere, um die Nutzung des

Zertifikats und des damit verbundenen privaten Schlüssels zu ermöglichen, das Einverständnisprotokoll rechtsgültig auszufertigen und das elektronische Dokument mittels einer qualifizierten elektronischen Signatur zu signieren.

Richtlinie zur Signierung und zum Nachweismanagement (SPMP): bedeutet das Dokument, das die von dem Serviceprovider für die Signatur elektronischer Dokumente durch die RA und einen oder mehrere Abonnenten in Übereinstimmung mit der Einverständniserklärung und die für die Generierung und Archivierung der Beweisdateien während der Nutzung des Dienstes verwendeten, technischen Vorgänge beschreibt. Die SPMP und ihre nachfolgenden Aktualisierungen sind auf der Webseite von DocuSign France zugänglich und bilden einen wesentlichen Bestandteil dieser Vereinbarung.

Abonnent(en) (oder Signatar): bedeutet die Einzelperson(en), die

sich bei der RA-Anwendung anmeldet/anmelden,

für die der Kunde das/die elektronische(n) Dokument(e) ausarbeitet,

denen die RA das/die elektronische(n) Dokument(e) zur Signatur vorlegt und

die das/die elektronische(n) Dokument(e) signiert/signieren, nachdem er/sie seine/ihre Einwilligung nach Maßgabe der Einverständniserklärung gegeben hat/haben.

Die Identität eines Abonnenten wird vorab von der RA in ihrer Zuständigkeit als Registrierungsstelle eingetragen und bestätigt.

URL: Uniform Resource Locator (Internetadresse): bedeutet die Adresse einer Seite oder einer Datei, die im Internet verfügbar ist.

3. VERFAHREN FÜR DIE BEANTRAGUNG VON ZERTIFIKATEN ÜBER DEN DIENST

Der Abonnent wird darauf hingewiesen und erklärt sich ausdrücklich damit einverstanden, dass:

DocuSign France über die RA durch den Kunden aufgefordert wird, die Signatur des Abonnenten auf dem elektronischen Dokument einzuholen.

Insofern: Wird die Identität des Abonnenten durch die RA unter Verwendung der RA-Anwendung bestätigt. Die Verfahren und technischen Mittel der RA sind als konform mit ETSI 319 411-2 QCP n-qscd sowie dem Deutschen Geldwäschegesetz (GwG) bestätigt worden. Während des Prozesses der Verifizierung der Identität, wird der Abonnent mittels Video-Chat in das Callcenter von IDnow verbun- den. Der annehmende Callcenter-Mitarbeiter leitet den Abonnenten durch die Schritte der Identifizierung. Diese umfassen, unter anderem, folgendes:

• Der Callcenter-Mitarbeiter erstellt eine Lichtbildaufnahme des Abonnenten. Hiermit wird, unter anderem, ein späterer Gesichtsabgleich vorgenommen.

• Der Callcenter-Mitarbeiter überprüft Daten des Ausweisdokuments (z.B. Personalausweisnummer, Geburtsdatum, etc.).

• Der Callcenter-Mitarbeiter überprüft die verschiedenen Sicherheitsmerkmale des Ausweisdokuments. Z.B. werden hologra- fische Sicherheitsmerkmale durch deren Lichtreflektionen geprüft und es findet eine Prüfziffernvalidierung statt.

• Es wird ein Gesichtsabgleich zwischen dem Lichtbild auf dem Ausweisdokument und der gemachten Aufnahme des zu identifizierenden Abonnenten durch den Callcenter-Mitarbeiter vorgenommen.

Dem Abonnenten wird für die Dauer der Signatur des elektronischen Dokumentes ein privater Signaturschlüssel eindeutig zuge- ordnet. Der private Schlüssel wird sicher erstellt, gespeichert und nach der Transaktion vernichtet und kann für keinen anderen Vorgang als für die Signatur des elektronischen Dokumentes durch den Abonnenten verwendet werden. Die Aktivierung des privaten Schlüssels zur Signatur des elektronischen

• Dokumentes bleibt, unter der alleinigen Kontrolle des Abonnenten.

Dem Abonnenten wird, je nach Antrag, ein fortgeschrittenes oder qualifiziertes Zertifikat als Mittel zur Bestätigung, dass er/sie der/die tatsächliche Signatar(in) des elektronischen Dokumentes ist, zugeordnet.

Es ist erforderlich, dass er/sie die von dem Dienst vorgelegte Einverständniserklärung rechtsgültig ausfertigt, um sich damit einverstanden zu erklären, das elektronische Dokument zu signieren oder dies zu verweigern. Der Abonnent muss hierfür während des Video-Chats einen Ident-Code eingeben welcher per SMS zugestellt wurde.

Optional kann der Abonnent vor der Einverständniserklärung ein Passwort wählen um einen IDnow-Account unter den AGB von IDnow anzulegen. Mittels des Passworts und einem weiteren verschickten Ident-Code kann der Abonnent zu einem späteren Zeitpunkt elektronische Dokumente signieren.

Nachdem es signiert ist, kann das elektronische Dokument von dem Abonnenten unmittelbar nach dem Signaturvorgang bei IDnow oder bei dem Kunden heruntergeladen werden oder es wird von IDnow oder dem Kunden an den Abonnenten übermittelt. Falls die signierten Dokumente durch IDnow zur Verfügung gestellt werden, können diese unter https://go.idnow.de/contract- download abgerufen werden.

Um gesetzlichen Anforderungen zu genügen kann es erforderlich sein, dass vom Identifizierungs-Prozess Audio und/oder Video-Aufnahmen angefertigt und gespeichert werden.

DocuSign France erstellt und archiviert eine mit der Signaturtransaktion des elektronischen Dokumentes verbundene Beweisdatei ausschließlich zum Zwecke, im Falle eines Gerichtsverfahrens in der Lage zu sein, den Beweis der Gültigkeit der Signatur zu erbringen. Die Dauer der Archivierung wird abhängig von der auf das elektronische Dokument anwendbaren Gesetzgebung durch den Kunden bestimmt. Die Beweisdatei enthält:

- die Fassung des elektronischen Dokumentes, das dem Abonnenten vor der Signatur vorgelegt wurde;
- die signierte Fassung des elektronischen Dokumentes;
- die Uhrzeit und das Kalenderdatum der Transaktion;
- die Einverständniserklärung, wie sie zwischen dem Abonnenten und dem Dienst rechtsgültig ausgefertigt wird;
- die technischen Protokolle in Verbindung mit der Transaktion.

4. AUSSTELLEN DES ZERTIFIKATS

Der Abonnent ist für die Überprüfung des Inhalts des Zertifikates verantwortlich (hauptsächlich für das „Subjekt"-Feld des Zertifikates, das den vollständigen Namen und den Vornamen des besagten Abonnenten enthält). Der Abonnent und der Kunde haben höchsten acht (8) Tage nach der Ausstellung des Zertifikates, um den Inhalt des Zertifikates zurückzuweisen und bei der RA einen Antrag auf

Widerruf einzureichen. Nach dieser Achttagesfrist wird das Zertifikat als von dem Verwender abgenommen angesehen und kann nicht mehr widerrufen werden.

5. VERÖFFENTLICHUNG DES ZERTIFIKATES

Das Zertifikat wird weder von der CA noch von der RA veröffentlicht. Das Zertifikat ist in dem signierten elektronischen Dokument und in der mit dem elektronischen Dokument verbundenen Beweisdatei enthalten.

6. GÜLTIGKEITSDAUER DES ZERTIFIKATES

Die Zertifikate sind für höchstens zehn (10) Tage gültig. Der besagte Zeitraum beginnt an dem Datum zu laufen, an dem die CA das Zertifikat ausstellt. Nach Ablauf der Gültigkeitsdauer des Zertifikates können die Signaturen von PDF-Dokumenten unter Verwendung der Überprüfungssoftware, wie sie vom Kunden angegeben ist, verifiziert werden, insbesondere um zu verifizieren, dass das Dokument zum Zeitpunkt der Signatur durch ein gültiges von der CA ausgestelltes Zertifikat elektronisch signiert wurde.

7. BEDINGUNGEN FÜR DEN WIDERRUF DES ZERTIFIKATES

7.1 Widerruf auf Veranlassung des Abonnenten oder des Kunden

Der Abonnent und der Kunde können das Zertifikat durch das Einreichen eines Antrages an die CA widerrufen. Die Einreichung erfolgt über die URL https://www.idnow.de/sperrung. In den folgenden Fällen können der Abonnent und der Kunde einen Antrag auf Widerruf einreichen:

DN-Informationen sind nicht vorschriftsmäßig ausgefüllt.

Das Zertifikat, das sich auf den privaten Schlüssel bezieht, ging verloren oder wurde kompromittiert oder es besteht der Verdacht, dass es verloren ging oder kompromittiert wurde (zum Beispiel im Fall eines Verlustes von Zugangsdaten und Passwort und/oder GSM).

Der Abonnent und der Kunde haben höchsten acht (8) Tage nach der Ausstellung des Zertifikates Zeit, um bei der RA einen Antrag auf Widerruf einzureichen. Nach dieser Achttagesfrist kann das Zertifikat nicht mehr widerrufen werden.

Das Zertifikat wird innerhalb von vierundzwanzig (24) Stunden nach dem Zeitpunkt der Verifikation des Antrags widerrufen.

7.2 Widerruf auf Veranlassung der CA

Für den Fall eines der folgenden Umstände wird das Zertifikat von der CA umgehend widerrufen:

Die CA ist gesperrt.

Die natürliche Person oder die RA versäumten es, die in der ZR definierten, notwendigen Verpflichtungen und Sicherheitsregeln einzuhalten.

Das Zertifikat, das sich auf den privaten Schlüssel bezieht, ging verloren oder wurde kompromittiert oder es besteht der Verdacht, dass es verloren ging oder kompromittiert wurde.

Jeder andere Grund, der von der CA angegeben wird.

Der betroffene Abonnent wird über den Widerruf des Zertifikates informiert.

7.3 Widerruf auf Anregung der RA

Für den Fall eines der folgenden Umstände wird das Zertifikat von der RA umgehend widerrufen:

DN-Informationen sind nicht vorschriftsmäßig ausgefüllt;

Das Zertifikat, das sich auf den privaten Schlüssel bezieht, ging verloren oder wurde kompromittiert oder es besteht der Verdacht, dass es verloren ging oder kompromittiert wurde (zum Beispiel im Fall eines Verlustes von Zugangsdaten und Passwort und/oder GSM).

Der betroffene Abonnent wird über den Widerruf des Zertifikates informiert.

Widerruf Informationen (CRL) sind immer bei der CA verfügbar, die eine CRL veröffentlicht. Im Falle des Lebensendes der CA oder beim Beenden der Dienste dieser CA oder im besonderen Falle eines kompromittierten CA-Schlüssels wird eine letzte CRL generiert und bei DocuSign France archiviert. Letztere wird bis zum Ablauf der TSP Aktivitäten auf der DocuSign France-Website publiziert und auf der im Zertifikat enthaltenen URL für die CRL veröffentlicht. Dort bleib sie abrufbar bis zum Ablauf des letzten von der CA ausgestellten Zertifikats.

8. ZEITPUNKT DES INKRAFTTRETENS UND LAUFZEIT

Die vorliegenden Allgemeinen Nutzungsbedingungen werden ab dem Zeitpunkt gültig, an dem sie durch den Abonnenten unterzeichnet werden, was mit dem Zeitpunkt der Zertifikatsanforderung einhergeht.

Diese Allgemeinen Nutzungsbedingungen finden auf einen Zeitraum Anwendung, der der Lebensdauer der für den Abonnenten ausge- stellten Zertifikate entspricht und enden mit dem Zeitpunkt des Gültigkeitsendes der besagten Zertifikate.

9. VERPFLICHTUNGEN DES ABONNENTEN

Durch das Einverständnis den Dienst zu nutzen, erklärt sich der Abonnent damit einverstanden, die Bestimmungen dieser Allgemeinen Nutzungsbedingungen einzuhalten und verantwortlich zu sein für:

Die Verifizierung des Inhalts des Zertifikates und die Warnung der RA.

Die Nutzung der Zertifikate und der damit verbundenen privaten Schlüssel in Übereinstimmung mit den Bestimmungen von Vertragsbestimmung 6 oben und der Zertifizierungsrichtlinie.

Die Verifizierung der Authentizität und Richtigkeit der in dem Zertifikat angegebenen Informationen, wie sie zum Beispiel im Verlauf der Einverständniserklärung von DocuSign France vorgelegt werden.

Die unverzügliche Beantragung eines Widerrufes des Zertifikats bei der RA wenn dies notwendig ist und dies insbesondere für den Fall eines Diebstahls, einer Offenlegung, des Verdachtes einer Kompromittierung oder einer Kompromittierung des verwendeten Ausweisdokumentes.

10. HAFTUNG

Weder DocuSign France noch die RA haften für dem Abonnenten entstandene indirekte oder nicht vorhersehbare Schäden, wie zum Beispiel Schäden finanzieller oder wirtschaftlicher Art, Ertragseinbußen, Geschäftsverluste, Verlust von Kunden, wirtschaftliche Schwie- rigkeiten, Verdienstausfälle oder den Verlust von Daten, die aus den gegenwärtigen Allgemeine Nutzungsbedingungen entstehen oder deren Folge sind oder die der Nutzung der von der CA ausgestellten Zertifikaten innewohnen.

Sollte eine Haftung von DocuSign France eingetreten sein, wird ausdrücklich vereinbart, dass DocuSign France für die Entschädigung aller direkten, bestimmten und unmittelbaren Schäden verantwortlich ist. Der Betrag der besagten Entschädigung für den Anspruch eines Abonnenten übersteigt nicht fünf (5) Euro je Zertifikat. DocuSign France übernimmt für den Fall, dass der Abonnent nicht die hierin vorgesehenen Verpflichtungen einhält, keine Haftung.

Weder die CA noch die RA übernehmen eine Haftung bezüglich der Nutzung der Zertifikate oder des damit in Zusammenhang ste- henden und von der RA ausgestellten privaten Schlüssels unter Bedingungen und für Zwecke, die nicht in der Zertifizierungsrichtlinie vorgesehen sind.

Da weder die CA noch die RA Kenntnis von dem Inhalt oder dem rechtlichen Umfang der signierten elektronischen Dokumente haben, ist weder die CA noch die RA auf dieser Grundlage haftbar.

Weder die CA noch die RA übernehmen eine Haftung oder Verantwortung für die Qualität der Internetverbindung oder die Folgen, die sich aus Verzögerungen oder Verlusten bei der Übermittlung von elektronischen Mitteilungen, Briefen und Dokumenten ergeben oder für Verzögerungen, Veränderungen oder sonstige Fehler bei der Übertragung einer Telekommunikation nach diesen Allgemeinen Nutzungsbedingungen. Des Weiteren wird vereinbart, dass weder die CA noch die RA für Fehlfunktionen der Arbeitsstation des Abon- nenten haftbar sind, wenn diese Fehlfunktionen die Folge der Nutzung des Zertifikats auf eine Art und Weise sind, die nicht die damit in Zusammenhang stehenden Dokumentation einhält. Ebenso umfasst weder die Haftung der CA noch die der RA die ordnungsgemäße Funktionsweise (Versagen, Fehler, Inkompatibilität usw.) der Hard- und Software sowie der Umgebung des Abonnenten. Weder die CA noch die RA sind für eine Verzögerung der Erfüllung von Verpflichtungen oder für die Nichterfüllung von Verpflichtungen, die in Ver- bindung mit diesen Allgemeinen Nutzungsbedingungen entstehen haftbar oder sind hierfür verantwortlich, wenn die Umstände, die diesen zugrunde liegen, die Folge eines Falles Höherer Gewalt sind, wie sie in der untenstehenden Vertragsbestimmung 11 definiert ist.

11. HÖHERE GEWALT

Weder die CA noch die RA ist für die Nichterfüllung oder Verzögerung einer oder mehrerer Verpflichtungen nach diesen Allgemeinen Nutzungsbedingungen aufgrund eines Falles Höherer Gewalt oder unvorhergesehener Umstände oder Umstände, die jenseits ihrer zumutbaren Kontrollen liegen, haftbar. Das Folgende wird als die Ereignisse Höherer Gewalt oder nicht vorhersehbarer Umstände ange- sehen: vollständig betriebsfremde Streiks, extreme Wetterbedingungen, Epidemien, Transportblockaden oder Blockaden der Lieferin- frastruktur, Erdbeben, Feuer, Überflutung, Wasserschäden, behördliche oder rechtliche Beschränkungen, rechtliche oder behördliche Änderungen an Formen der Vermarktung,

Unterbrechung der Telekommunikation (einschließlich vermittelter Netze) und alle Vorfälle in Netzen von Dritten. Die CA und/oder die RA setzen die Erfüllung ihrer Verpflichtungen für den Fall eines Vorfalls, der als Höhere Gewalt eingestuft wird aus und sind diesbezüglich nicht haftbar.

12. SCHUTZ PERSONENBEZOGENER DATEN

Die von dem Abonnenten und dem Kunden während der Verfahren für die Verwaltung von Zertifikaten gesammelten personenbezoge- nen Daten werden von der RA verarbeitet, um

- es dem Abonnenten zu ermöglichen von der RA nach Bedarf authentifiziert und identifiziert zu werden,
- die Überprüfungen durchzuführen, die für Ausstellung und gegebenenfalls Widerruf von Zertifikaten erforderlich sind und
- ihre Personenidentität, die in das Zertifikat eingetragen wird, zu schaffen und
- den Abonnenten während der Einverständniserklärung zu authentifizieren. DocuSign France erklärt, die europäische Gesetzge- bung im Hinblick auf den Schutz personenbezogener Daten einzuhalten.

Jeder Widerspruch gegen die Speicherung personenbezogener Daten verhindert die Ausstellung eines Zertifikates. Durch das Signie- ren des Elektronischen Dokumentes und der ANB erklärt sich der Abonnent damit einverstanden, dass die RA und/oder die CA die Beweisdatei, die seine personenbezogenen Daten enthält, für sieben (7) Jahre nach Ablauf des Zertifikats aufbewahrt.

13. GEISTIGES EIGENTUM

Der Abonnent erkennt an, dass DocuSign France alle Rechte des geistigen Eigentums (Patente, eingetragene Warenzeichen und sons- tigen Rechte) für die Elemente, aus denen der Dienst besteht, sowie die Unterlagen, Konzepte, Techniken, Erfindungen, Prozesse, die Software oder die Arbeiten, die im Zusammenhang mit den Zertifikaten und den damit in Verbindung stehenden Diensten, die von DocuSign France bereitgestellt werden, ungeachtet der Form, der Programmiersprache, des Programmmediums oder der verwendeten Sprache, behält. Diese Allgemeinen Nutzungsbedingungen übertragen keine Rechte des geistigen Eigentums hinsichtlich der Zertifikate und der damit in Zusammenhang stehenden Dienste auf den Abonnenten.

14. VERSICHERUNG

Hiermit erklärt die CA, dass sie eine Berufshaftpflichtversicherung in Bezug auf die hierin enthaltenen Dienste abgeschlossen hat, die in angemessener Art und Weise ihre Verpflichtungen nach diesen Allgemeinen Nutzungsbedingungen deckt.

15. PUBLICATIEDATUM

4. Juni 2020

FRANCAIS

1. CONTENU

L'objectif des présentes Conditions Générales (ci-après dénommées 'Conditions Générales') est de définir les conditions juridiques rela- tives à l'acquisition et l'utilisation des certificats de souscription DocuSign France ainsi que les obligations correspondantes d'DocuSign France, de l'autorité d'enregistrement (ci-après dénommée 'AE'), du client ainsi que du souscripteur. Les certificats des souscripteurs sont fournis et gérés par l'intermédiaire du service en ligne de signature électronique qualifiée d'DocuSign France.

2. DÉFINITIONS

Certificat(s) : Fichier électronique permettant de confirmer le lien entre une identité de souscripteur définie et une clef publique connectée à une clef privée gérée par l'AC.

Procédure de gestion des certificats : Toutes les procédures appliquées par l'AE relatives à la délivrance et à la gestion des certificats.

Directive(s) de certification (DC) : Politique stipulée par un OID et publiée par l'AC décrivant les caractéristiques générales du certificat fourni. Une directive de certification décrit les obligations et responsabilités de l'AC, de l'AE, des utilisateurs et des demandeurs de certificat ainsi que de tous les composants du cycle de vie global d'un certificat.

La directive de certification valide lors de la signature de cette entente est utilisée pour identifier le certificat.

La version des DC devant être utilisée correspond à la version valide le jour de l'initialisation du service. Elle est disponible à l'adresse suivante : https://www.docusign.fr/societe/certification-policies (OID 1.3.6.1.4.1.22234.2.14.3.31). Les versions ultérieures des DC sont accessibles aux utilisateurs sur le site internet d'DocuSign France.

Liste de révocation de certificat (LRC) : Liste des certificats invalides révoqués avant leur date d'expiration. La LRC est publiée régulièrement et signée numériquement par l'AC ayant délivré les certificats mentionnés dans la liste.

Autorité de certification (ou AC) : L'autorité d'DocuSign France développant les certificats et gérant le cycle de vie des certificats (assurance, extension, révocation) à la demande de l'autorité d'enregistrement conformément aux règles et pratiques définies par les directives de certification.

Client : Entité légale proposant la signature d'un document électronique par le souscripteur. Le client est impliqué dans une relation contractuelle avec l'autorité d'enregistrement permettant de déléguer la gestion du processus de vérification de l'identité du souscrip- teur ainsi que le processus de signature des documents électroniques par le souscripteur.

Déclaration de consentement : Processus selon lequel DocuSign France reçoit le consentement du souscripteur pour :

obtenir un certificat conformément à l'identité du souscripteur de certificat ;

signer des documents électroniques.

La déclaration de consentement doit être réalisée entre le service et le souscripteur dans le cadre de la demande auprès de l'AE.

Demande auprès de l'AE : Une demande sous le nom IDnow eSigning doit être utilisée par l'AE pour vérifier l'identité des souscripteurs et requérir auprès du service qu'ils soient autorisés à signer les documents électroniques.

Document(s) électronique(s) : Document au format numérique créé par le client et présenté avec la demande auprès de l'AE pour signature auprès du représentant. Le document électronique peut être signé par d'autres signataires ainsi que par le client en tant que personne juridique.

Conditions générales d'utilisation (CGU) : Conditions juridiques d'exercice et conditions d'utilisation du service. Ces CGU sont inclues dans les documents électroniques devant être signés par le souscripteur.

Identité du souscripteur du certificat : L'identité développée par les données collectées par l'AE sur le souscripteur ainsi que les données définies par l'AE. Cette identité sera utilisée pour authentifier une personne physique.

Clef privée : Clef mathématique secrète et unique contenue sur un appareil et pouvant être activée à distance par le souscripteur pour signer des documents électroniques.

Fichier(s) de preuve : L'un des fichiers créés, signés et horodatés par DocuSign France contenant toutes les informations pertinentes relatives à l'authentification du souscripteur et au processus de signature du document électronique. Un fichier de preuve dédié doit être connecté à chaque document électronique avec signature afin d'établir la validité de la signature électronique en cas de poursuites judiciaires.

Clef publique : Une clef mathématique devant être publiée et utilisée pour la mise en place d'un protocole cryptographique permettant de vérifier la signature d'un document.

Autorité d'enregistrement (ou AE) : Institution impliquée dans une relation contractuelle avec l'AC et agissant sur la base de l'au- torité transférée par l'AC conformément aux règles et pratiques définies par les directives de certification, pour vérifier avec exactitude l'identité du souscripteur et demander au service d'autoriser le souscripteur à signer un document électronique. L'AE est ainsi en charge de la demande auprès de l'AE.

Service : Tous les services réalisés par DocuSign France conformément aux CGU, notamment pour permettre l'utilisation du certificat et de la clef privée qui y est associée, l'exécution de la déclaration de consentement dans le respect de sa valeur juridique ainsi que la signature du document électronique par l'intermédiaire d'un signataire électronique qualifié.

Politique pour la signature et la gestion de preuves (PSGP) : Document décrivant les procédures techniques utilisées par le fournisseur de service pour la signature des documents électroniques entre l'AE et un ou plusieurs souscripteurs conformément à la déclaration de consentement et utilisé pour générer et archiver les fichiers de preuve au cours de l'utilisation du service. Il est possible d'accéder à la PSGP et ses actualisations

ultérieures sur le site internet d'DocuSign France, ces éléments constituant un élément essentiel du présent accord.

Souscripteur(s) (ou signataires) : Le(s) individu(s) qui

dépose(nt) une demande auprès de l'AE,

traite(nt) le(s) document(s) électronique(s) pour le client,

à qui l'AE présente le(s) document(s) électronique(s) pour signature et

est(sont) autorisé(s) à signer le(s) document(s) électronique(s) avec conformément à la déclaration de consentement.

En tant qu'autorité d'enregistrement, l'AE doit saisir et confirmer en amont l'identité du souscripteur.

URL : localisateur uniforme de ressource (adresse internet) : L'adresse d'une page ou d'un fichier disponible sur internet.

3. PROCÉDURE DE DEMANDE

DE CERTIFICAT PAR L'ENTREMISE DU
SERVICE

Le souscripteur doit être informé et accepter expressément que :

Par l'intermédiaire de l'AE, le client doit recommander DocuSign France afin que le souscripteur signe le document électronique.

Dans cette mesure :

L'AE doit confirmer l'identité du souscripteur par une demande auprès de l'AE. Les procédures et ressources techniques de l'AE ont été confirmées conformément à la norme ETSI 319 411-2 QCP n-qscd ainsi que le Geldwäschegesetz (German Money Laundering Act (GwG)). Au cours du processus de vérification de l'identité, le souscripteur doit être connecté au centre d'appels IDnow. L'employé du centre d'appels recevant la communication doit assister le souscripteur dans les étapes d'authentification. Cela inclut entre autre les étapes suivantes :

• L'employé du centre d'appels doit prendre une photographie du souscripteur. Il sera alors possible, entre autres, de réaliser ultérieurement une comparaison faciale.

• L'employé du centre d'appels doit vérifier les informations de la pièce d'identité (numéro de la carte d'identité, date de naissance, etc.).

• L'employé du centre d'appels doit vérifier les divers éléments de sécurité de la pièce d'identité. Par exemple les éléments de sécurité holographiques doivent être vérifiés sur une source lumineuse et une vérification du numéro doit être réalisée.

• L'employé du centre d'appels doit réaliser une comparaison faciale entre la photographie présentée sur la pièce d'identité et l'image prise par le souscripteur devant être identifié.

Une clef de signature privée sera assignée sans ambiguïté au souscripteur pour la durée nécessaire à la signature du document électronique. La clef de sécurité privée sera créée, sauvegardée et détruite en toute sécurité à l'issue de la transaction. Elle ne pourra être utilisée dans un but autre que pour la signature du document électronique par le souscripteur. Le souscripteur possède le contrôle exclusif de l'activation de la clef privée pour la signature du document électronique.

Selon la demande déposée, un certificat avancé ou qualifié sera assigné au souscripteur afin qu'il/elle puisse s'authentifier en tant que signataire légitime du document électronique.

Il est nécessaire qu'il/elle soit en mesure de produire la déclaration de consentement requise par le service avec la validité juridique de déclarer qu'il/elle accepte de signer ou refuse de signer le document électronique. L'abonné doit entrer un SMS envoyé préalablement (code d'identification) dans le chat vidéo.

De manière facultative, l'abonné peut choisir un mot de passe avant la déclaration de consentement afin de créer un compte IDnow selon les termes et conditions d'IDnow. Avec ce mot de passe et le code d'identification nouvellement émis, l'abonné sera par la suite en mesure de signer des documents électroniques.

Une fois signé, le document électronique pourra être téléchargé par le souscripteur immédiatement après le processus de si- gnature sur IDnow ou par le client, ou sera transféré au souscripteur par IDnow ou le client. Une fois signé, le document élec- tronique peut être téléchargé par l'abonné juste après le processus de signature par le biais d'IDnow ou du client, ou il sera transféré à l'abonné par IDnow ou le client. Si les documents signés sont fournis par IDnow, ils peuvent être téléchargés sur https://go.idnow.de/contract-download.

Afin de se conformer aux exigences légales, des enregistrements audio et/ou vidéo du processus d'identification peuvent être réalisés.

DocuSign France créera et archivera un fichier de preuve connecté à la transaction de signature du document électronique uniquement en vue de servir de preuve de la validité de la signature en cas de poursuites judiciaires. La période d'archivage est fonction de la législation applicable au document électronique déterminée par le client. Le fichier de preuve contient :

• La version du document électronique soumise au souscripteur avant signature ;

• La version signée du document électronique ;

• L'heure et la date de la transaction ;

• La déclaration de consentement conclue entre le souscripteur et le service ;

• Les protocoles techniques en rapport avec la transaction.

4. DÉLIVRANCE DU CERTIFICAT

Le souscripteur est responsable de la vérification du contenu du certificat (en particulier concernant le champ 'sujet' du certificat contenant le prénom et nom complets du souscripteur susmentionné). Le souscripteur et le client disposent d'un délai maximum de huit (8) jours à partir de la date de délivrance du certificat pour rejeter le contenu du certificat et déposer une demande de révocation auprès de l'AE. Passé ce délai de huit jours, le certificat sera réputé accepté par l'utilisateur et ne pourra plus être révoqué.

5. PUBLICATION DU CERTIFICAT

L'AC et l'AE ne peuvent publier le certificat. Le certificat est inclus dans le document électronique avec signature ainsi que dans le fichier de preuve associé au document électronique.

6. VALIDITÉ DU CERTIFICAT

Les certificats sont valides sur une période maximale de dix (10) jours. La période susmentionnée débute à la date de délivrance du certificat par l'AC. Une fois la période de validité du certificat écoulée, les signatures des documents PDF peuvent être vérifiées avec les logiciels de vérification publiés par le client, notamment pour vérifier que les documents ont été signés électroniquement avec un certificat valide délivré par l'AC au moment de la signature.

7. CONDITIONS DE RÉVOCATION DU CERTIFICAT

7.1 Révocation à l'initiative du souscripteur ou du client

Le souscripteur et le client peuvent révoquer le certificat en soumettant une demande auprès de l'AC. Cette demande peut être soumise via l'URL https://www.idnow.io/revocation. Dans les cas suivants, le souscripteur et le client peuvent déposer une demande de révocation :

Les informations de ND sont incorrectes.

Le certificat, lié à la clef privée, a été perdu ou compromis ou est suspecté d'avoir été perdu ou compromis (par exemple, lors de la perte de l'identifiant et du mot de passe et/ou du GSM).

Le souscripteur et le client disposent d'un délai maximal de huit (8) jours après la délivrance du certificat pour déposer une demande de révocation auprès de l'AE. Passé ce délai de huit jours, le certificat ne pourra plus être révoqué.

Le certificat sera révoqué sous vingt-quatre (24) heures à compter du moment où la demande sera prise en charge.

7.2 Révocation à l'initiative de l'AC

Dans les circonstances suivantes, le certificat sera révoqué par l'AC avec effet immédiat :

L'AC a été bloquée.

La personne physique ou l'AE n'ont pas respecté les conditions contractuelles et règles de sécurité telles que définies dans les DC.

Le certificat, lié à la clef privée, a été perdu ou compromis ou est suspecté d'avoir été perdu ou compromis.

Toute autre raison signalée par l'AC.

Le souscripteur concerné sera informé de la révocation du certificat.

7.3 Révocation suggérée par l'AE

Dans les circonstances suivantes, le certificat sera révoqué par l'AC avec effet immédiat :

Les informations de ND sont incorrectes.

Le certificat, lié à la clef privée, a été perdu ou compromis ou est suspecté d'avoir été perdu ou compromis (par exemple, lors de la perte de l'identifiant et du mot de passe et/ou du GSM).

Le souscripteur concerné sera informé de la révocation du certificat.

Les informations de révocation seront toujours disponibles auprès de l'AC qui publie une CRL. En cas de fin de vie de l'AC ou d'arrêt du Service avec cette AC ou y compris en cas de compromission de clé d'AC, une dernière CRL est générée et archivée chez DocuSign France. Cette dernière CRL est publiée sur le site internet de DocuSign France jusqu'à expiration du TSP et sur l'URL de distribution de la CRL, contenue dans le Certificat, jusqu'à expiration du dernier Certificat émis par l'AC.

8. CONDITIONS ET PÉRIODE DE VALIDITÉ

Les présentes Conditions Générales sont considérées comme étant valides à partir du moment où elles ont été signées par le souscrip- teur, ce qui est considéré comme étant le moment de référence de demande de certificat.

Les présentes Conditions Générales sont applicables sur la période correspondant au cycle de vie des certificats délivrés au souscripteur et expirent lorsque la validité des certificats susmentionnés arrive à terme.

9. OBLIGATIONS DU SOUSCRIPTEUR

En acceptant d'utiliser ce service, le souscripteur accepte de respecter les modalités les présentes Conditions Générales :

Vérification du certificat et des notifications de l'AE.

Utilisation des certificats et des clefs privées associées conformément aux termes de la condition contractuelle n°6 ci-dessus ainsi qu'aux directives de certification.

La vérification de l'authenticité et de l'exactitude de l'information stipulée dans le certificat telles que présentées par DocuSign France dans la déclaration de consentement par exemple.

Si nécessaire, l'application immédiate de la révocation d'un certificat par l'AE, notamment en cas de vol, divulgation ou suspicion de compromission ou dans l'éventualité où la pièce d'identité utilisée aurait été compromise.

10. RESPONSABILITÉ

DocuSign France et l'AE ne peuvent être tenus responsables des préjudices exceptionnels ou indirects encourus par le souscripteur, tels que des dommages de nature financière ou économique, perte de revenus, pertes commerciales, perte de clientèle, difficultés économiques, perte de salaires ou de données pouvant résulter des présentes Conditions Générales, par voie de conséquence ou inhérents à l'utilisation des certificats délivrés par l'AC.

Dans l'éventualité où DocuSign France serait reconnu responsable, ce dernier convient expressément d'indemniser tous les dommages directs, avérés et immédiats. Le montant de l'indemnité susmentionnée suite à la réclamation d'un souscripteur ne peut excéder cinq (5) euros par certificat. DocuSign France se dégage de toute responsabilité dans l'éventualité où un souscripteur ne respecterait pas les présentes obligations. L'AC et l'AE ne peuvent être tenues responsables de l'utilisation des certificats ou de la clef privée associée délivrée par l'AE dans des conditions et à des fins non prévues par la directive de certification.

L'AC et l'AE n'ayant pas connaissance du contenu ni du cadre légal des documents électroniques avec signature, l'AC et l'AE ne peuvent de fait être tenues responsables.

L'AC et l'AE n'assument aucune responsabilité relative à la qualité de la connexion internet ou aux conséquences d'un retard ou de perte concernant les transferts de courriers, lettres ou documents électroniques ou pour le retard, les modifications ou toute autre erreur dans le transfert des télécommunications conformément aux présentes Conditions Générales. Par ailleurs, il est convenu que l'AC et l'AE ne peuvent être tenues responsables du dysfonctionnement du poste de travail du souscripteur si ce dysfonctionnement résulte de l'utilisation du certificat dans un cadre ne respectant pas la documentation associée disponible. De la même manière, la responsabilité de l'AC et ne l'AE ne peut être engagée concernant le fonctionnement (défaillance, erreurs, incompatibilité, etc.) du matériel, du logiciel ainsi que de l'environnement utilisés par le souscripteur. L'AC et l'AE ne peuvent être tenues responsables d'un éventuel retard dans l'exécution des obligations ou le manquement aux obligations liées aux présentes Conditions Générales, si les circonstances résultant de cette situation sont dues à un cas de force majeure tel que décrit aux termes de la condition contractuelle n°11 énoncée ci-dessous.

11. CAS DE FORCE MAJEURE

L'AC et l'AE ne peuvent être tenues responsables du manquement ou du retard dans l'exécution d'une ou de plusieurs obligations confor- mément aux présentes Conditions Générales en cas de force majeure, de circonstances exceptionnelles ou échappant à tout contrôle. Les situations mentionnées ci-après constituent des cas de force majeure ou circonstances exceptionnelles : grèves entièrement ex- térieures, conditions climatiques extrêmes, épidémie, interruption des transports ou blocage de l'infrastructure d'approvisionnement, tremblements de terre, incendies, inondations, dégâts des eaux, restrictions officielles ou juridiques, modifications réglementaires ou juridiques des pratiques commerciales, interruption des télécommunications (incluant les réseaux) et tout événement sur un réseau tiers. L'AC et l'AE suspendront l'exécution de leurs obligations dans l'éventualité d'un incident résultant d'un cas de force majeure et ne pourront en être tenues responsables.

12. PROTECTION DES DONNÉES PERSONNELLES

Les données personnelles collectées par le souscripteur et le client au cours du processus de gestion des certificats seront traitées par l'AE pour :

permettre à l'AE d'authentifier et d'identifier le souscripteur si nécessaire,

de réaliser les vérifications nécessaires pour la délivrance ou le cas échéant la révocation des certificats et

de créer une identité propre au certificat et

d'authentifier le souscripteur lors de la déclaration de consentement. DocuSign France accepte de respecter la législation euro- péenne relative à la protection des données personnelles.

Toute objection au stockage des données personnelles empêche la délivrance d'un certificat. En signant le document électronique et les CGU, le souscripteur accepte que l'AE et/ou l'AC conserve(nt) un fichier de preuve contenant ses données personnelles sur une période de sept (7) ans après expiration du certificat.

13. PROPRIÉTÉ INTELLECTUELLE

Le souscripteur accepte qu'DocuSign France conserve tous les droits de propriété intellectuelle (brevets, marques déposées et autres droits) relatifs aux éléments constitutifs du service comme les documents, concepts, technologies, découvertes, procédures, logiciels ou travaux associés aux

certificats ainsi qu'aux services connexes devant être fournis par DocuSign France, indépendamment de la forme, langage de programmation, langue ou programme utilisé. Les présentes Conditions Générales n'entraînent aucun transfert de droits de propriété intellectuelle relatif aux certificats ainsi qu'aux services connexes pour le souscripteur.

14. ASSURANCE

L'AC déclare avoir souscrit une assurance responsabilité professionnelle relative aux services mentionnés ici, couvrant adéquatement ses obligations conformément aux présentes Conditions Générales.

15. DATE DE PUBLICATION

4 Juin 2020

ESPAÑOL

1. OBJETO DEL CONTRATO

El objeto de estas condiciones generales de uso (en adelante, “Condiciones generales de uso”) es el de definir las condiciones legales relacionadas con la adquisición y el uso de certificados de abonado DocuSign France y las obligaciones correspondientes de DocuSign France, de la autoridad registradora (denominada RA, por sus siglas en inglés, “Registration Authority”), del cliente y del abonado. Los certificados de abonado se emitirán junto con el servicio online para firmas electrónicas calificada y administrados tal y como DocuSign France lo ofrece.

2. DEFINICIONES

Certificado(s): se trata de un archivo electrónico que confirma la conexión de la identidad de un abonado en concreto con una clave pública que va emparejada a una clave privada administrada por la CA (autoridad de certificación, por sus siglas en inglés, “Certification Authority”).

Procedimiento para la administración de certificados: son todos los procesos empleados por una RA para la emisión y adminis- tración de certificados.

Directrices de certificación (DC): es el código fijado por una OID y publicado por la CA que describe las características generales de los certificados. Una directriz de certificación describe las obligaciones y responsabilidades de la CA, de la RA, del usuario y del solicitante de certificados y de todos aquellos componentes que se derivan del ciclo de vida de un certificado. Para la identidad personal del certificado se aplicará la directriz de certificación que esté vigente en el momento de la firma del presente contrato. La versión de las DC que se aplicará será la versión que esté vigente el día en que se inicie el servicio. Se podrá leer en la siguiente dirección:https: //www.docusign.fr/societe/certification-policies (OID 1.3.6.1.4.1.22234.2.14.3.31). Las posteriores versiones del DC estarán disponibles para los usuarios en la página web de DocuSign France.

Lista de bloqueo de certificados (CRL): es la lista de los certificados no válidos que se revocaron antes de alcanzar su fecha de caducidad. Esta lista se publicará con regularidad y será firmada de forma digital por la CA que haya emitido los certificados de la lista.

Autoridad de certificación (CA): es la instancia de DocuSign France que provee los certificados y que administra el ciclo de duración de los mismos (emisión, prolongación, revocación) de acuerdo con lo que la autoridad de registro desee y en cumplimiento con las reglas definidas por sus directrices de certificación y otras prácticas.

Cliente: es una persona jurídica que propone un documento electrónico que el abonado deberá firmar. El cliente tendrá una relación contractual con la autoridad de registro y delegará la gestión de la verificación de la identidad del abonado y el procedimiento de la firma del documento electrónico mediante el abonado.

Consentimiento: es el proceso mediante el cual DocuSign France recoge el consentimiento del abonado para: recibir un certificado de acuerdo con la identidad de la persona del certificado del abonado, aclarar el consentimiento para la firma del documento electrónico. Se emitirá una copia legal del consentimiento entre el servicio y el abonado durante el transcurso de la aplicación de la RA.

Aplicación de la RA: es la aplicación con el nombre IDknow eSigning, que emplea la RA para verificar la identidad del abonado y enviar solicitudes que llevarán al abonado a poder firmar un documento con una firma electrónica.

Documento(s) electrónico(s): es un documento en forma electrónica que crea el cliente y que se genera en la aplicación de la RA para que el signatario lo pueda firmar. El documento electrónico podrá ser firmado por otros signatarios y por el cliente como persona jurídica

Condiciones generales de uso (CGU): son las condiciones y disposiciones legales vigentes en relación al uso del servicio. Estas están presentes en los documentos electrónicos que habrán de ser firmados por los abonados.

Identidad personal del certificado abonado: se trata de la identidad del abonado que se ha generado mediante la aplicación de los datos obtenidos por la RA, así como los datos definidos por la RA. Se emplea esta identidad para identificar a una persona natural.

Clave privada: es una clave matemática secreta que se encuentra una única vez en un dispositivo y que se activa a distancia por parte del abonado para firmar un documento electrónico.

Archivo de prueba: es un archivo generado, firmado y provisto de un sello con fecha por parte de DocuSign France que contiene todas las informaciones necesarias relacionadas con la identificación del abonado y con el proceso de firma del documento electrónico. Se vinculará un archivo de prueba a cada documento electrónico firmado para servir de prueba en caso de que tuviera lugar un proceso judicial.

Clave pública: es una clave matemática que se publica y se aplica durante la puesta en marcha del protocolo de encriptamiento para verificar la firma de un documento.

Autoridad de registro (o RA): es una institución que tiene una relación contractual con la CA y que actúa de acuerdo a un poder notarial otorgado por la CA y conforme a las reglas y prácticas que fueron definidas en sus directrices de certificación para verificar la identidad del abonado. Esta autoridad hace la solicitud para que el abonado pueda firmar el documento electrónico. Por extensión, la RA pondrá en funcionamiento su aplicación.

Servicio: se trata de todos los servicios que llevará a cabo DocuSign France de acuerdo con estas CGU, en particular, aquel que permitirá usar el certificado y su clave privada, la entrega del consentimiento de forma legal y firmar el documento electrónico con una firma electrónica cualificada.

Directriz para la firma y la administración del documento de prueba (SPMP): es el documento que describe todos los procesos técnicos empleados durante el uso del servicio por el cual se utiliza una firma electrónica para firmar un documento por parte de la RA o de uno o varios abonados y se genera y almacena un archivo de prueba. Se podrá acceder a los SPMP y a sus siguientes actualizaciones en la página de DocuSign France. Estos forman una parte fundamental de este acuerdo.

Abonado(s) (o signatarios): se trata de la personas

que se dan de alta en la aplicación de la RA,

para la que el cliente prepara los documentos electrónicos,

a la que se le presenta los documentos electrónicos y

que los firma después de haber dado su consentimiento de acuerdo con las normas.

La RA, en calidad de autoridad de registro, registra y confirma la identidad de un abonado antes de comenzar el proceso.

URL: Uniform Resource Locator (dirección de internet): es la dirección de una página o un archivo que está disponible en internet.

3. PROCEDIMIENTO PARA LA OBTENCIÓN DE CERTIFICADOS CON EL SERVICIO

Se informará al abonado sobre lo siguiente y este dará su acuerdo expreso con respecto a los puntos citados a continuación:

DocuSign France habrá de solicitar al cliente mediante la RA la firma del abonado en el documento electrónico.

En este sentido:

Se confirmará la identidad del abonado mediante la RA y su aplicación. El procedimiento y los medios técnicos de la RA han sido validados de acuerdo con ETSI 319 411-2 QCP n-qscd, así como con la Ley alemana contra el blanqueo de capitales (Deutscher Geldwäschegesetzt, GwG). Durante el proceso de verificación de la identidad, el abonado será conectado con el servicio técnico de IDnow. El empleado de dicho servicio técnico que atienda la llamada mostrará al abonado los pasos a seguir para la identificación.

Los pasos serán los siguientes:

El empleado del servicio técnico realizará una fotografía del abonado. Más tarde utilizará esta foto, entre otras cosas, para hacer un cotejo del rostro.

Dicho empleado comprobará los datos del carnet de identidad (por ejemplo: el número de identificación, la fecha de nacimiento, etc.).

El empleado comprobará que los diferentes elementos de seguridad están en orden, por ejemplo: verificará la validez de las marcas holográficas mediante sus reflejos de luz y validará el código de control.

Se hará una comparación entre la fotografía del carnet de identidad y la foto tomada para la identificación del abonado por parte del empleado del servicio técnico.

El abonado recibirá una clave privada inequívoca que valdrá durante todo el proceso de firma electrónica del documento. Esta clave se generará de forma segura, se archivará y se eliminará después de la transacción y el abonado no podrá utilizarla para otro proceso que no sea el de firmar un documento electrónico. La activación de la clave privada para la firma de un documento electrónico dependerá única y exclusivamente del abonado.

Por cada solicitud, el abonado recibirá un certificado avanzado o cualificado como medio de confirmación de que él es la persona a la que pertenece dicha firma electrónica del documento.

Es necesario que él proporcione el consentimiento legal otorgado por el servicio para declarar que está o no de acuerdo con la firma del documento electrónico. El usuario debe ingresar en el videochat la información (código Ident) de un SMS que habrá recibido previamente.

De acuerdo a los términos y condiciones de IDnow, el usuario tiene la opción de elegir una contraseña antes de la declaración de consentimiento para crear una cuenta en IDnow. Con esta contraseña y el código Ident que acaba de recibir, el usuario podrá firmar documentos electrónicos más adelante.

Después de haberlo firmado, el abonado podrá descargar de forma inmediata el documento bien en IDnow, bien mediante el cliente o bien IDnow se lo enviará al abonado. Una vez firmado el documento electrónico, tanto el usuario como el cliente pueden pueden descargarlo directamente tras el proceso de firma en IDnow. De no ser así, IDnow o el cliente se lo transferirán al usuario. En caso de que IDnow proporcione los documentos firmados, estos pueden descargarse desde https://go.idnow.de/contract- download.

A fin de cumplir con los requisitos legales, es posible que se realicen grabaciones de audio o vídeo durante el proceso de identi- ficación.

DocuSign France crea y archiva el archivo de prueba vinculado a la firma del documento electrónico con el fin exclusivo de que en caso de un litigio, este archivo dará prueba de la validez de la firma. El tiempo que este archivo de prueba quedará archivado dependerá de la legislación aplicable al documento electrónico por el cliente. El archivo de prueba contiene:

- la versión del documento electrónico que el abonado recibió antes de firmarlo;
- la versión firmada del documento electrónico;
- la hora y la fecha de la transacción;
- el consentimiento, tal y como se formalizó entre el abonado y el servicio;
- el protocolo técnico de la transacción.

4. EMISIÓN DEL CERTIFICADO

El abonado será responsable de comprobar el contenido del certificado (sobre todo el campo de “sujeto” del certificado en el que se encuentran el

nombre y los apellidos de dicho abonado). El abonado y el cliente tendrán un máximo de ocho (8) días después de haberse emitido el certificado para cancelar el contenido del certificado y revocar la solicitud en la RA. Pasado el plazo de ocho días se entenderá que el certificado ha sido aceptado por la persona que lo va a usar y no podrá ser cancelado.

5. PUBLICACIÓN DEL CERTIFICADO

El certificado no será publicado ni por la CA, ni por la RA. El certificado se incluirá con el documento con firma electrónica y en el archivo de prueba generado en el mismo.

6. PERÍODO DE VIGENCIA DEL CERTIFICADO

Los certificados tendrán un período de vigencia de diez (10) días. Dicho período comienza en la fecha en la que la CA emite el certificado. Pasado este período de vigencia del certificado se podrán verificar las firmas de los PDF utilizando el software de comprobación que fue entregado por el cliente. Sobre todo, para verificar que el documento fue firmado electrónicamente mediante un certificado válido otorgado por la CA en el momento en que el abonado lo firmó.

7. CONDICIONES PARA LA REVOCACIÓN DEL CERTIFICADO

7.1 Revocación por parte del abonado o del cliente

El abonado y el cliente podrán revocar el certificado entregando la solicitud de cancelación a la CA. Habrá de cancelarse a través de la URL https://www.idnow.io/revocation. El abonado y el cliente podrán solicitar la cancelación en los siguientes casos:

- Las informaciones DN no cumplen los requisitos legales.
- El certificado vinculado a la clave privada se ha perdido, podría comprometer a la persona o existe la sospecha de que se haya perdido o haya comprometido a dicha persona (por ejemplo, en caso de pérdida de los datos de acceso y de la contraseña o GSM).

El abonado y el cliente tienen máximo ocho (8) días después de haber recibido el certificado para entregar a la RA la revocación. Pasados estos ocho días el certificado no podrá cancelarse.

El certificado será cancelado en un plazo de veinticuatro (24) horas después de haber sido verificada la solicitud de cancelación.

7.2 Revocación por parte de la CA

Si se diera uno de los siguientes casos, la CA podrá cancelar el certificado de forma inmediata:

- La CA está bloqueada.
- La persona natural o la RA descuidan las obligaciones necesarias y las reglas de seguridad definidas en las DR.
- El certificado vinculado a la clave privada se ha perdido o ha comprometido a la persona o existe la sospecha de que se haya perdido o que haya comprometido a una persona.
- Cualquier otro motivo que la CA alegue.

Se informará al abonado afectado sobre la cancelación del certificado.

7.3 Revocación por iniciativa de la RA

Si se diera uno de los casos siguientes, la RA revocará el certificado de forma inmediata:

- La información DN no ha sido completada de acuerdo con las instrucciones.
- El certificado vinculado a la clave privada se ha perdido, ha comprometido a la persona o existe la sospecha de que se haya perdido o que haya comprometido a una persona (por ejemplo, en caso de pérdida de los datos de acceso y la contraseña o GSM).

Se informará al abonado de la cancelación del certificado.

La información de revocación siempre será publicada por la CA que publica una CRL. En caso de que la CA finalice su vida útil o la clave de CA e comprometta, la CA genera una última CRL y esta CRL se archiva en DocuSign France. Esta última CRL se publica en el sitio web de DocuSign France hasta que caduque el TSP y en la URL de distribución de la CRL contenida en el certificado hasta que caduque el último certificado emitido por la CA.

8. ENTRADA EN VIGOR Y VIGENCIA

Las condiciones de uso presentes entrarán en vigor en el momento en que el abonado las firme. Dicho momento coincide con aquel en que se solicita el certificado. Estas condiciones de uso serán vigentes durante el período de vigencia del certificado y dejarán de serlo en el momento en que el certificado no sea válido.

9. OBLIGACIONES DEL ABONADO

Con su consentimiento para que se produzca el servicio, el abonado se declara conforme con lo establecido por estas condiciones de uso generales y se hace responsable de:

La verificación del contenido del certificado y las advertencias de la RA.

El uso del certificado y de la clave privada vinculada a este, de acuerdo con lo establecido en el punto 6 de este contrato y con las directrices de certificación.

La comprobación de la autenticidad y precisión de la información del certificado, como se presenta, por ejemplo, en el consenti- miento de DocuSign France.

La solicitud de cancelación inmediata del certificado por parte de RA en caso necesario y sobre todo en caso de robo, divulgación, sospecha de peligro o de que se vaya a poner en peligro la información del carnet de identidad utilizado.

10. RESPONSABILIDAD

Ni DocuSign France, ni la RA son responsables de los daños indirectos o no previsibles que sufra el abonado. Daños imprevisibles como, por ejemplo, de tipo financiero o económico, pérdida de beneficios, pérdida del volumen de negocio, pérdida de clientes, problemas económicos, pérdida de ganancias o de datos que puedan derivarse de las presentes condiciones generales de uso o que sean causas de estas o inherentes al uso de los certificados expedidos por la CA.

Si DocuSign France tuviera que asumir alguna responsabilidad, se pactará de forma expresa que DocuSign France asumirá la respon- sabilidad de indemnización de todos los daños directos, concretos e inmediatos. El derecho del abonado al importe de indemnización no sobrepasará los cinco (5) euros por certificado. DocuSign France no asume ninguna responsabilidad en caso de que el abonado no cumpliera con sus obligaciones. Ni la CA, ni la RA asumirán responsabilidades en relación al uso de los certificados o de las claves privadas otorgadas por la RA que no cumplan las condiciones y los propósitos dispuestos en la directriz de certificación.

Ya que ni la CA, ni la RA están informadas del contenido o del alcance legal de los documentos firmados electrónicamente, no podrán incurrir en responsabilidad alguna. Ni la CA, ni la RA asumen responsabilidad alguna por la calidad de la conexión a internet o por las consecuencias derivadas del retraso o pérdida en la conexión de notificaciones, cartas o documentos electrónicos. Tampoco se harán responsables de los retrasos, cambios o demás errores generados en la transmisión de las telecomunicaciones de acuerdo con estas condiciones generales de uso. Además, se acuerda que ni la CA, ni la RA serán responsables del mal funcionamiento del lugar de trabajo del abonado, si este mal funcionamiento conllevara un uso del certificado no conforme a la documentación relacionada con el mismo. Tampoco será responsabilidad, ni de la CA, ni de la RA, el funcionamiento correcto (errores, incompatibilidad. . . etc.) del hardware o software, así como del entorno del abonado. Ni la CA, ni la RA serán responsables de un retraso de las obligaciones o de su no cumplimiento relacionadas con las condiciones generales. Tampoco serán responsables cuando las consecuencias derivadas sean de fuerza mayor, tal y como queda estipulado en el punto 11 siguiente.

11. FUERZA MAYOR

Ni la CA, ni la RA serán responsables en caso de no cumplimiento o retraso de una o varias de las obligaciones, de acuerdo con estas condiciones generales de uso debido a causas de fuerza mayor o situaciones imprevisibles que queden fuera de su alcance exigible. Se contemplan como casos de fuerza mayor los puntos siguientes: huelga total ajena al servicio, condiciones climáticas extremas, epidemias, bloqueos del transporte o bloqueos en la infraestructura de distribución, terremotos, incendios, inundaciones, daños causados por agua, limitaciones dictadas por las instituciones o la legalidad, modificaciones legales o de las instituciones sobre la comercialización, la interrupción de las telecomunicaciones (únicamente los proveedores de redes) y todo lo que ocurra con las redes de terceros. En caso de que tenga lugar una situación de fuerza mayor, la CA o la RA renuncian al cumplimiento de sus obligaciones y no se las podrá hacer responsables de ello.

12. PROTECCIÓN DE DATOS PERSONALES

Los datos personales recogidos por el abonado y el cliente durante el proceso de administración de los certificados serán gestionados por la RA para :

hacer posible que el abonado pueda ser identificado por la RA en caso de necesidad,

para llevar a cabo las comprobaciones necesarias para la emisión de certificados y llegado el caso, su revocación,

para la identidad personal que quedará registrada en el certificado y

para la identificación del abonado durante la transmisión de su consentimiento. DocuSign France declara su cumplimiento con la legislación europea en materia de protección de datos.

Toda contradicción al almacenamiento de datos personales impedirá la emisión de un certificado. Mediante la firma del documento electrónico y de las CGU, el abonado expresa su conformidad con que la RA o la CA conserven el archivo de prueba con sus datos personales durante siete (7) años después de la expiración del certificado.

13. PROPIEDAD INTELECTUAL

El abonado reconoce que DocuSign France se reserve todos los derechos de la propiedad intelectual (patentes, marcas comerciales registradas y demás derechos) para elaborar todos los elementos que integren sus servicios, así como los documentos, conceptos, técnicas, invenciones, procesos, software o demás tareas que estén relacionados con los certificados o los servicios vinculados a los mismos, sin importar la forma, la lengua de programación, el medio del programa o idioma utilizados. Estas condiciones generales de uso no otorgan al abonado derecho alguno de propiedad intelectual de cara a los certificados, ni a los servicios relacionados con los mismos.

14. SEGURO

Por la presente, la CA declara que está cubierta por un seguro de responsabilidad civil profesional que, de acuerdo a los servicios aquí enumerados, cubre sus obligaciones de forma razonable y apropiada como así lo establecen estas condiciones generales de uso.

15. FECHA DE PUBLICACIÓN

4 de junio de 2020

ITALIANO

1. OGGETTO

Lo scopo delle presenti condizioni generali di utilizzo (in seguito ("condizioni generali di utilizzo") è, quello di definire le condizioni giuridiche relative all'acquisizione e all'utilizzo dei certificati di abbonamento DocuSign France, nonché i corrispondenti obblighi da parte di DocuSign France, dell'autorità di registrazione (qui di seguito "RA"), del cliente e dell'abbonato. I certificati di abbonamento vengono consegnati e gestiti tramite il servizio online offerto da DocuSign France, grazie al rilascio di firme digitali qualificata.

2. DEFINIZIONI

Certificato (i): indica un documento elettronico che conferma il collegamento tra una data identità dell'abbonato e la chiave pubblica collegata alla chiave privata gestita dall'autorità di certificazione (CA).

Procedura per la gestione dei certificati: indica tutte le procedure utilizzate dalla RA per il rilascio e la gestione dei certificati.

Norma(e) di certificazione (ZR): indica il corpo di norme stabilito da un OID e pubblicato attraverso la CA, che descrive le caratteristi- che generali dei certificati che rilascia. Una norma di certificazione descrive gli obblighi e le responsabilità della CA, della RA, dell'utente e del richiedente per i certificati e tutti i componenti che il generale ciclo di vita di un certificato comporta. Per l'identità personale del certificato viene utilizzata la norma di certificazione valida al momento della sottoscrizione del presente accordo. La versione da utilizzare della ZR è la stessa che ha validità nel giorno di inizializzazione del servizio. Può essere consultata al seguente indirizzo: https://www.docusign.fr/societe/certification-policies (OID 1.3.6.1.4.1.22234.2.14.3.31). Le successive versioni della ZR verranno rese accessibili agli utenti del sito web di DocuSign France.

Lista di revoca dei certificati (CRL): indica la lista dei certificati non validi, revocati prima della loro data di scadenza. La CRL viene resa pubblica regolarmente e siglata in formato digitale dalla CA che ha emesso i certificati nella lista.

Autorità di certificazione (o CA): indica l'ente di DocuSign France che emette i certificati e che gestisce il ciclo di vita del certificato (emissione, prolungamento, revoca) a richiesta dell'autorità di registrazione, conformemente alle regole e alle pratiche definite nelle ZR.

Cliente: indica una personalità giuridica che propone un documento elettronico che deve essere firmato dall'abbonato. Il cliente è in un rapporto contrattuale con l'autorità di registrazione, per delegare la gestione della verifica dell'identità dell'abbonato e del processo di firma del documento elettronico.

Atto di assenso: indica la procedura secondo la quale DocuSign France ottiene l'assenso dell'abbonato per:

Ottenere un certificato secondo l'identità personale del certificato di abbonamento;

Dichiarare l'assenso alla firma del documento elettronico.

L'atto di assenso viene redatto in modo giuridicamente valido tra il servizio e l'abbonato entro l'applicazione RA.

Applicazione RA: indica l'applicazione con il nome IDnow eSigning utilizzata dalla RA al fine di verificare l'identità dell'abbonato e presentare richieste al servizio, affinché gli abbonati siano in condizione di siglare un documento elettronico.

Documento (i) elettronico (i): indica il documento in forma elettronica che viene emesso da parte del cliente e viene presentato presso l'applicazione RA per essere siglato dal firmatario. Il documento elettronico può essere firmato da altri firmatari e dal cliente quale personalità giuridica.

Condizioni generali di utilizzo (ANB): indicano le condizioni legali esistenti e le disposizioni in materia di utilizzo del servizio.

Queste ANB sono contenute nei documenti elettronici che gli abbonati sono tenuti a firmare.

Identità personale del certificato di abbonamento (certificato): indica l'identità costituita attraverso l'uso dei dati dell'abbonato raccolti dalla RA e dei dati definiti dalla RA. Questa identità viene utilizzata per autenticare una persona fisica.

Chiave privata: indica una chiave segreta matematica contenuta una volta sola in un apparecchio e attivata in modo telecomandato dall'abbonato per firmare i documenti elettronici.

File probatorio: indica un file che DocuSign France ha emesso, firmato e fornito di marca temporale, che contiene tutte le informazioni connesse con l'autenticazione dell'abbonato e la procedura di firma del documento elettronico. A ciascun documento elettronico firmato è collegato un file probatorio dedicato, allo scopo di comprovare la validità della firma elettronica in caso di procedimento giudiziario.

Chiave pubblica: indica una chiave matematica destinata a essere resa pubblica e utilizzata per l'attuazione di un protocollo critto- grafico, al fine di verificare la firma di un documento.

Autorità di registrazione (RA): indica l'istituzione in rapporto contrattuale con la CA e che – alla luce di una procura conferita dalla CA – agisce in osservanza delle regole e delle pratiche definite nella(e) sua(e) norma(e) di certificazione al fine di verificare la correttezza dell'identità dell'abbonato e di presentare delle richieste al servizio, al fine di permettere agli abbonati di firmare un documento elettronico. La RA esegue l'applicazione RA in questa estensione.

Servizio: indica tutte le prestazioni di servizio che vengono erogate da DocuSign France secondo queste ANB, in particolare per consentire l'utilizzo del certificato e della chiave privata a esso collegata, per redigere il protocollo di assenso in modo legalmente valido e per firmare il documento elettronico per mezzo di una firma elettronica qualificata.

Norma per la firma e la gestione probatoria (SPMP): indica il documento che descrive i processi tecnici impiegati dal fornitore di servizi per la firma dei documenti elettronici da parte della RA e di uno o più abbonati in conformità con l'atto di assenso e per la generazione e l'archiviazione dei file probatori durante l'utilizzo del servizio. La SPMP e i suoi successivi aggiornamenti sono accessibili al sito web DocuSign France e

costituiscono parte integrante importante di questo accordo.

Abbonato(i) (o firmatario): indica la(e) persona(e) singola(e)

che si registra(registrano) nell'applicazione RA,

per la quale (le quali) il cliente elabora il documento elettronico (i documenti elettronici),

alla quale (alle quali) la RA presenta il documento elettronico (i documenti elettronici) per la firma e

che firma(firmano) il documento elettronico (i documenti elettronici) dopo che ha manifestato il proprio assenso conformemente all'atto di assenso.

L'identità di un abbonato viene registrata e confermata previamente dalla RA nella sua competenza di autorità di registrazione.

URL: Uniform Resource Locator (indirizzo internet): indica l'indirizzo di una pagina o di un file disponibile in internet.

3. PROCEDURA PER LA RICHIESTA DI CERTIFICATI TRAMITE IL SERVIZIO

L'abbonato è avvisato di quanto segue e si dichiara espressamente d'accordo che:

DocuSign France venga esortata attraverso la RA da parte del cliente a ottenere la firma dell'abbonato sul documento elettronico.

A tale riguardo:

L'identità dell'abbonato viene confermata dalla RA utilizzando l'applicazione RA. La procedura e i mezzi tecnici della RA sono stati confermati quali conformi alla specifica ETSI 319 411-2 QCP n-qscd e alla legge tedesca contro il riciclo di denaro (GwG). Durante il processo di verifica dell'identità, l'abbonato viene collegato con il call center di IDnow. Il centralinista del call center che riceve la chiamata guida l'abbonato attraverso i passi dell'identificazione. Questi comprendono, tra l'altro, quanto segue:

• Il centralinista scatta una fototessera dell'abbonato. Con questa viene eseguito, tra l'altro, un successivo confronto del volto.

• Il centralinista del call center verifica i dati del documento d'identità (per esempio n° della carta d'identità, data di nascita, ecc.).

• Il centralinista del call center controlla le diverse caratteristiche di sicurezza del documento d'identità. Ad esempio, le caratteristiche di sicurezza olografiche vengono controllate attraverso la loro riflessione della luce e avviene una convalida delle cifre di controllo.

• Viene eseguito un confronto del viso tra la fototessera sul documento d'identità e la fototessera dall'abbonato da identificare scattata dal centralinista del call center.

All'abbonato viene associata univocamente una chiave di firma privata per tutta la durata della firma del documento elettronico. La chiave privata viene generata in maniera sicura, salvata e distrutta dopo la transazione e non è utilizzabile per nessun altro processo diverso dalla firma del documento elettronico da parte dell'abbonato. L'attivazione della chiave privata per la firma del documento elettronico rimane esclusivamente sotto il controllo dell'abbonato.

All'abbonato, a seconda della richiesta, viene associato un certificato avanzato o qualificato quale mezzo di conferma che egli è l'effettivo firmatario del documento elettronico. È necessario che firmi in modo legalmente valido l'atto di assenso fornito dal servizio, per accettare o rifiutare di firmare il documento elettronico. Il firmatario deve inserire all'interno della video chat l'SMS che gli è stato inviato in precedenza (codice d'identificazione).

In via opzionale, il firmatario può scegliere una password prima della dichiarazione di consenso per creare un account IDnow così come da Termini e Condizioni di IDnow. Con questa password e l' Codice d'identificazione di nuova emissione, il firmatario potrà firmare documenti elettronici in un secondo momento.

Dopo che è stato firmato, il documento elettronico può essere scaricato dall'abbonato immediatamente dopo la procedura di firma presso IDnow o presso il cliente essere trasmesso da IDnow o dal cliente all'abbonato. Una volta firmato, il documento elettronico può essere scaricato direttamente dal firmatario dopo la procedura di firma presso IDnow o dal cliente, o, ancora, verrà inviato da IDnow o dal cliente al sottoscrittore. Se i documenti firmati vengono forniti da ID now, possono essere scaricati all'indirizzo https://go.idnow.de/contract-download.

Al fine di ottemperare ai requisiti di legge, la procedura di identificazione può essere registrata in audio e/o in video.

DocuSign France genera e archivia un file probatorio connesso alla transazione di firma del documento elettronico, esclusivamente allo scopo di essere in grado di produrre la prova della validità della firma nell'eventualità di procedimenti giudiziari. La durata dell'archiviazione sarà definita dal cliente in base alla legislazione applicabile al documento elettronico. Il file probatorio contiene:

• La stesura del documento elettronico presentata all'abbonato prima della firma;

• La stesura firmata del documento elettronico;

• L'ora e la data di calendario della transazione;

• L'atto di assenso, come firmato in modo giuridicamente valido tra l'abbonato e il servizio;

• I protocolli tecnici collegati la transazione.

4. RILASCIO DEL CERTIFICATO

L'utente è responsabile della verifica del contenuto del certificato (principalmente per il campo "Soggetto" del certificato, che contiene cognome e nome completi del suddetto abbonato). L'abbonato e il cliente hanno al massimo otto (8) giorni dopo il rilascio del certificato per respingere il contenuto del certificato e per inoltrare una richiesta di revoca alla RA. Trascorso questo termine di otto giorni, il certificato verrà considerato accettato dall'utilizzatore e non potrà più essere revocato.

5. PUBBLICAZIONE DEL CERTIFICATO

Il certificato non viene reso pubblico né dalla CA né dalla RA. Il certificato è contenuto nel documento elettronico firmato e nel file probatorio connesso al documento elettronico.

6. DURATA DI VALIDITÀ DEL CERTIFICATO

I certificati sono validi per un massimo di dieci (10) giorni. Il suddetto lasso di tempo inizia a decorrere dalla data nella quale la CA rilascia il certificato. Dopo lo scadere della durata di validità del certificato, le firme dei documenti PDF possono essere verificate, utilizzando il software di verifica, come indicato dal cliente, in particolare per verificare che il documento, al momento della firma, sia stato firmato elettronicamente per mezzo di un certificato valido rilasciato dalla CA.

7. CONDIZIONI PER LA REVOCA DEL CERTIFICATO

7.1 Revoca su iniziativa dell'abbonato o del cliente

L'abbonato e il cliente possono revocare il certificato presentando una richiesta alla CA. La presentazione avviene tramite l'URL https://www.idnow.io/revocation. L'abbonato e il cliente possono inoltrare una richiesta di revoca nei seguenti casi:

Le informazioni DN non sono state compilate conformemente alla norma.

Il certificato riferito alla chiave privata è andato perso è stato compromesso o sussiste il sospetto che sia andato perso o sia stato compromesso (ad esempio in caso di perdita di dati di accesso e password e/o GSM).

L'abbonato e il cliente hanno al massimo otto (8) giorni di tempo dal rilascio del certificato per presentare una richiesta di revoca presso la RA. Trascorso questo termine di otto giorni, il certificato non può più essere revocato.

Il certificato viene revocato entro ventiquattro (24) ore dal momento della verifica della richiesta.

7.2 Revoca su iniziativa della CA

Il certificato viene revocato dalla immediatamente dalla CA al verificarsi di una delle circostanze seguenti:

La CA è disabilitata.

La persona fisica o la RA hanno mancato di osservare gli obblighi e le regole di sicurezza necessari definiti nella ZR.

Il certificato riferito alla chiave privata è andato perso o è stato compromesso o sussiste il sospetto che sia andato perso o sia stato compromesso.

Qualsiasi altro motivo indicato dalla CA.

L'abbonato interessato viene informato della revoca del certificato.

7.3 Revoca su indicazione della RA

Il certificato viene revocato dalla immediatamente dalla RA al verificarsi di una delle circostanze seguenti:

Le informazioni DN non sono state compilate conformemente alla norma;

Il certificato riferito alla chiave privata è andato perso o è stato compromesso o sussiste il sospetto che sia andato perso o sia stato compromesso (ad esempio in caso di perdita di dati di accesso e password e/o GSM).

L'abbonato interessato viene informato della revoca del certificato.

Le informazioni sulla revoca saranno sempre disponibili presso CA che pubblica un CRL. In caso di fine vita dell CA o di arresto del servizio con questo CA o anche in caso di una chiave CA compromessa, un ultimo CRL viene generato e archiviato presso DocuSign France. Quest'ultimo CRL è pubblicato sul sito web di DocuSign France fino alla scadenza del TSP e sull'URL di distribuzione del CRL contenuto nel certificato fino alla scadenza dell'ultimo certificato rilasciato dall'autorità competente.

8. MOMENTO DI ENTRATA IN VIGORE E DURATA

Le presenti condizioni generali di utilizzo hanno efficacia dal momento in cui esse vengono sottoscritte dall'abbonato, associato al mo- mento della richiesta del certificato. Queste condizioni generali di utilizzo trovano applicazione per un periodo di tempo corrispondente alla durata dei certificati rilasciati per l'abbonato e cessano al momento della fine della validità di detti certificati.

9. OBBLIGHI DELL'ABBONATO

Tramite l'assenso all'utilizzo del servizio, l'abbonato accetta di rispettare le disposizioni delle presenti condizioni generali di utilizzo e di essere

responsabile:

Della verifica del contenuto del certificato e dell'avviso della RA.

Dell'utilizzo dei certificati e della chiave privata a essi connessa in conformità alle disposizioni della clausola contrattuale 6 precedente e della norma di certificazione.

Della verifica dell'autenticità e della correttezza delle informazioni indicate nel certificato, come presentate ad esempio nell'am- bito dell'atto di assenso di DocuSign France.

Dell'immediata richiesta, se necessario, di una revoca del certificato presso la RA, in particolare in caso di furto, rivelazione, sospetto di compromissione o compromissione del documento d'identità utilizzato.

10. RESPONSABILITÀ

Né DocuSign France né la RA sono responsabili per i danni indiretti o non prevedibili originatisi per l'utente – come ad esempio i danni di natura finanziaria o economica, perdite di guadagno, perdita d'affari, perdita di clienti, difficoltà economiche, mancanza di profitto o perdita di dati – derivanti dalle attuali condizioni generali di utilizzo o conseguenti alle stesse o insiti nell'utilizzo del certificato rilasciato dalla CA.

Qualora sopravvenga una responsabilità di DocuSign France, si concorda espressamente che DocuSign France è responsabile per il risarcimento di tutti i danni diretti, definiti e immediati. L'importo del suddetto indennizzo per il diritto di un abbonato non superare i cinque (5) euro per certificato. DocuSign France non si assume nessuna responsabilità nel caso in cui l'abbonato non rispetti gli obblighi qui previsti.

Né la CA né la RA si assumono una responsabilità relativamente all'utilizzo dei certificati o della chiave privata connessa a essi e rilasciata dalla RA.
in condizioni e per finalità non previste nella norma di certificazione.

Poiché né la CA né la RA hanno conoscenza del contenuto o della portata giuridica dei documenti elettronici firmati, né la CA né la RA sono responsabili su questo fondamento. Né la CA né la RA si assumono una responsabilità per la qualità della connessione a internet o per le conseguenze derivanti da ritardi o perdite nella trasmissione di comunicazioni elettroniche, lettere e documenti o per rallentamenti, variazioni o altri errori nella trasmissione di una telecomunicazione ai sensi delle presenti condizioni generali di utilizzo. Si concorda inoltre che né la CA né la RA non sono responsabili per malfunzionamenti della stazione di lavoro dell'abbonato, se questi malfunzionamenti sono la conseguenza dell'utilizzo del certificato in modalità non rispettose della documentazione a esso correlata. Allo stesso modo, né la responsabilità della CA né quella della RA comprende la modalità di funzionamento regolare (guasti, errori, incompatibilità, ecc.) dell'hardware e del software e l'ambiente dell'abbonato. Né la CA né la RA sono responsabili per un ritardo nell'adempimento di obblighi o per l'inadempimento di obblighi derivanti dalle presenti condizioni generali di utilizzo né sono responsabili di ciò se le circostanze alla base di ciò sono conseguenza di un caso di forza maggiore, come definito nella sottostante clausola 11.

11. FORZA MAGGIORE

Né la CA né la RA sono responsabili per l'inadempimento o il ritardo di uno o più obblighi ai sensi le presenti condizioni generali di utilizzo a causa di in un caso di forza maggiore o di circostanze imprevedibili o di circostanze che si trovano al di là del loro ragionevole controllo. I seguenti casi sono valutati come eventi di forza maggiore o circostanze imprevedibili: scioperi totali estranei all'azienda, condizioni atmosferiche estreme, epidemie, blocco dei trasporti, blocco delle infrastrutture di fornitura, terremoti, incendi, inondazioni, danni dovuti all'acqua, limitazioni burocratiche o legali, modifiche burocratiche o legali alle forme di commercializzazione, interruzione delle telecomunicazioni (incluse le reti comunicanti) e tutti gli avvenimenti in reti di terzi. La CA e/o la RA sospendono l'adempimento dei loro obblighi per il caso di un evento classificabile quale forza maggiore e non sono responsabili rispetto a esso.

12. PROTEZIONE DEI DATI PERSONALI

I dati personali raccolti dall'abbonato e dal cliente durante la procedura per la gestione dei certificati vengono elaborati dalla RA per

consentire all'abbonato di essere autentificato e identificato secondo necessità dalla RA,

condurre le verifiche necessarie per il rilascio ed eventualmente la revoca dei certificati e

creare l'identità personale che viene registrata nel certificato e

autenticare l'abbonato durante l'atto di assenso.

DocuSign France dichiara di osservare la legislazione europea in riferimento al trattamento dei dati personali. Ogni obiezione contro il salvataggio dei dati personali impedisce il rilascio di un certificato. Mediante la firma del documento elettronico e delle ANB, l'abbonato accetta che la RA e/o la CA conservino il file probatorio, che contiene i suoi dati personali, per sette (7) anni dopo la scadenza del certificato.

13. PROPRIETÀ INTELLETTUALE

L'abbonato riconosce che DocuSign France conserva tutti i diritti della proprietà intellettuale (brevetti, marchi registrati e diritti partico- lari) per gli elementi di cui si compone il servizio, oltre che per i documenti, i concetti, le tecniche, le scoperte, i processi, i software o i lavori correlati ai certificati e i servizi a essi correlati messi a disposizione da DocuSign France, indipendentemente dalla forma, dal lin- guaggio di programmazione, dal mezzo di programmazione o la lingua utilizzata. Queste condizioni generali di utilizzo non trasferiscono all'abbonato nessun diritto di proprietà intellettuale per quanto concerne i certificati e i servizi a essi correlati.

14. ASSICURAZIONE

Con la presente la CA dichiara di aver stipulato un'assicurazione per la responsabilità relativa ai servizi qui contenuti che copre in maniera adeguata i suoi obblighi derivanti dalle presenti condizioni generali di utilizzo.

15. DATA DI PUBBLICAZIONE

4 giugno 2020