



ALLGEMEINE GESCHÄFTSBEDINGUNGEN FÜR DAS
VIDEOIDENTIFIZIERUNGSVERFAHREN UND DIE
AUSSTELLUNG LANGFRISTIGER ZERTIFIKATE
QES MULTI

Dies ist eine deutsche Übersetzung der englischen Fassung der Allgemeinen Geschäftsbedingungen für das Videoidentifizierungsverfahren und die Ausstellung langfristiger Zertifikate QES MULTI, die hier abrufbar ist: <https://www.signicat.com/about/english>. Diese Allgemeinen Geschäftsbedingungen QES MULTI wurden ausschließlich zur Erleichterung für TEILNEHMER oder ANTRAGSTELLER übersetzt und haben keine Rechtswirkung. Maßgeblich ist stets die englische Fassung, die Vorrang vor der deutschen Übersetzung hat.

Einerseits SIGNICAT, S.L.U („ehemals Electronic Identification S.L.“), mit eingetragenem Sitz in Avenida Ciudad de Barcelona 81, 4ª Planta, eingetragen im Handelsregister von Madrid am 13. März 2013 unter der Identifikationsnummer B-86681533 (im Folgenden „SIGNICAT SLU“), ist ein qualifizierter Vertrauensdiensteanbieter, der gemäß den Bestimmungen der Verordnung (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG sowie gemäß den für die Ausstellung und Verwaltung qualifizierter Zertifikate geltenden technischen Normen des ETSI, insbesondere EN 319 411-1 und EN 319 411-2, handelt, um die Einhaltung der gesetzlichen Anforderungen und die internationale Anerkennung seiner Dienste zu erleichtern.

Und andererseits der ANTRAGSTELLER/TEILNEHMER, dessen Identifikationsdaten für die Zwecke dieses Vertrags in dem verwendeten Ausweisdokument sowie in dem Video angegeben sind, das im Rahmen des Verfahrens zur Videoidentifizierung und Ausstellung des Zertifikats erstellt wurde.

1. GEGENSTAND

Zweck dieses Dokuments ist es, den Antragsteller/Teilnehmer in klarer und verständlicher Weise über die vorliegenden „Allgemeinen Geschäftsbedingungen für das Verfahren zur Fernidentifizierung per unbegleitetem Video und Bedingungen des elektronischen Zertifizierungsdienstes für die Ausstellung langfristiger Zertifikate“ zu informieren und die Dienste gemäß den Bestimmungen dieses Dokuments, der Erklärung zur Zertifizierungspraxis, der eIDAS-Verordnung und der gegebenenfalls anwendbaren lokalen Gesetze zu regeln.

Dieses vorherige Identifizierungsverfahren ist erforderlich, um die Identität des Antragstellers/Teilnehmers nachzuweisen, der SIGNICAT SLU mit der Ausstellung eines qualifizierten langfristigen Zertifikats für elektronische Signaturen einer natürlichen Person beauftragt („Zertifizierungsdienste“), dessen Nutzung den nachstehend beschriebenen Bedingungen des von SIGNICAT SLU als qualifiziertem Vertrauensdiensteanbieter erbrachten elektronischen Zertifizierungsdienstes unterliegt.

Das gemäß diesen Allgemeinen Geschäftsbedingungen ausgestellte qualifizierte elektronische Zertifikat entspricht dem folgenden Zertifizierungsprofil:

- Qualifiziertes Zertifikat für natürliche Personen in der CLOUD mit QSCD, OID 1.3.6.1.4.1.55193.1.1.2. Es handelt sich um ein qualifiziertes Zertifikat, das für qualifizierte elektronische Signaturen und deren Authentifizierung gemäß der Zertifizierungsrichtlinie QCP-n-qscd, OID 0.4.0.194112.1.2, ausgestellt wird. Dieses Zertifikat wird in einer zentralisierten QSCD ausgestellt und ist ein qualifiziertes Zertifikat gemäß den Bestimmungen von Artikel 28 der Verordnung (EU) Nr. 910/2014.

Es arbeitet mit qualifizierten elektronischen Signaturerstellungseinheiten (QSCD) gemäß den Artikeln 29 und 51 der Verordnung (EU) Nr. 910/2014 und erfüllt die Bestimmungen der technischen Normen des Europäischen Instituts für Telekommunikationsnormen mit der Referenznummer ETSI EN 319 411-2. Insbesondere handelt es sich bei der QSCD um das

Hardware-Sicherheitsmodul nShield Solo XC v12.60.15 und das Entrust Signature Activation Module (SAM), Version 1.1.1, die beide nach Common Criteria EAL4+ zertifiziert und als qualifizierte elektronische Signaturerstellungseinheiten qualifiziert sind.

Es gewährleistet die Identität des Unterzeichners und seine Verbindung mit dem Teilnehmer des elektronischen Vertrauensdienstes, indem es die Erstellung der „*qualifizierten elektronischen Signatur*“ ermöglicht, d. h. der fortgeschrittenen Signatur, die auf einem qualifizierten Zertifikat beruht und mit einer qualifizierten Einheit erstellt wurde und damit für alle rechtlichen Wirkungen und Zwecke der handschriftlichen Unterschrift gleichgestellt ist, ohne dass weitere zusätzliche Voraussetzungen erfüllt werden müssen.

2. ANWENDBARE BEGRIFFSBESTIMMUNGEN

- **ZERTIFIZIERUNGSSTELLE (CA):** vertrauenswürdige Stelle des Absenders und des Empfängers der Nachricht. Dieses Vertrauen beider in einen „vertrauenswürdigen Dritten“ ermöglicht es jedem von ihnen, seinerseits den von der Zertifizierungsstelle signierten Dokumenten zu vertrauen, insbesondere den Dokumenten, die jeden öffentlichen Schlüssel seinem Inhaber zuordnen und als Zertifikate bezeichnet werden. Bei der Erbringung des vom Antragsteller/Teilnehmer beantragten Dienstes handelt SIGNICAT SLU als Zertifizierungsstelle, die einen bestimmten öffentlichen Schlüssel durch die Ausstellung eines Zertifikats einem bestimmten Antragsteller/Teilnehmer zuordnet.
- **REGISTRIERUNGSSTELLE (RA):** Stelle, die unter anderem den Antragsteller/Teilnehmer eines Zertifikats und gegebenenfalls die sonstigen mit dem Zertifikat verbundenen Umstände gemäß den Bestimmungen von Abschnitt 1.3.2. „Registrierungsstellen“ der CPS von SIGNICAT SLU eindeutig identifiziert. Die Registrierungsstelle übermittelt der Zertifizierungsstelle die überprüften Daten des Antragstellers/Teilnehmers, damit die Zertifizierungsstelle das entsprechende Zertifikat ausstellen kann. Einzelne oder alle Aufgaben der RA können entweder direkt von SIGNICAT SLU oder von einer von SIGNICAT SLU autorisierten Stelle übernommen werden.
- **ZERTIFIKAT FÜR ELEKTRONISCHE SIGNATUREN:** elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und mindestens den Namen oder das Pseudonym dieser Person bestätigt.
- **QUALIFIZIERTES ZERTIFIKAT FÜR ELEKTRONISCHE SIGNATUREN:** Zertifikat für elektronische Signaturen, das von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und die Anforderungen des Anhangs I der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 (eIDAS-Verordnung) erfüllt und die höchsten rechtlichen Garantien hinsichtlich der Identifizierung des Unterzeichners und seiner eindeutigen Verknüpfung mit der Signatur sowie der Integrität und Nichtabstreitbarkeit der mit der Signatur verknüpften Daten bietet.
- **ERKLÄRUNG ZUR ZERTIFIZIERUNGSPRAXIS („CPS“):** von einer Zertifizierungsstelle erstelltes Dokument, das die Erbringung von Zertifizierungsdiensten durch diese Zertifizierungsstelle in ihrer Eigenschaft als Zertifizierungsdiensteanbieter, in diesem Fall SIGNICAT SLU, umfasst oder regelt. Es regelt unter anderem die Verwaltung der Signaturerstellungs- und Signaturprüfdaten

und der Zertifikate sowie die Bedingungen für die Beantragung, Ausstellung, Nutzung, Aussetzung und Beendigung der Gültigkeit der Zertifikate.

- **QUALIFIZIERTE ELEKTRONISCHE SIGNATUR:** fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht. Da es sich um eine qualifizierte Signatur handelt, gilt eine widerlegbare Vermutung (*iuris tantum*) für ihre Gültigkeit; die Beweislast trägt die Person, die die Gültigkeit der Signatur bestreitet.
- **QUALIFIZIERTER VERTRAUENSDIENSTEANBIETER:** Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Qualifikationsstatus verliehen wurde.
- **ANTRAGSTELLER/TEILNEHMER oder ANTRAGSTELLER/TEILNEHMER,** d. h. die in der Kopfzeile genannte natürliche Person, die die Zertifizierungsdienste von SIGNICAT SLU in Anspruch nimmt und die vor der Ausstellung des qualifizierten Zertifikats das Videoidentifizierungsverfahren von SIGNICAT SLU beantragt und erfolgreich abgeschlossen hat.

3. GESCHÄFTSBEDINGUNGEN DES VIDEOIDENTIFIZIERUNGSVERFAHRENS

Das Verfahren zur Identifizierung des Antragstellers/Teilnehmers für die von SIGNICAT SLU zur Ausstellung elektronischer Zertifikate erbrachten Identifizierungsdienste erfolgt gemäß Artikel 24 Absatz 1 der eIDAS-Verordnung auf eine der folgenden Arten:

- a) durch persönliche Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person; hierzu muss sich der Antragsteller/Teilnehmer in die Büros von SIGNICAT SLU in Av. de la Ciudad de Barcelona, 81, 4, 28007 Madrid begeben, da es keine delegierten Registrierungsstellen gibt;
- b) aus der Ferne unter Verwendung elektronischer Identifizierungsmittel, bei denen die Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person vor der Ausstellung des qualifizierten Zertifikats autorisiert wurde, und gemäß dem in diesem Dokument und in der Erklärung zur Zertifizierungspraxis beschriebenen Videoidentifizierungsverfahren, abrufbar unter folgendem Link: <https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>;
- c) mittels eines qualifizierten Zertifikats für elektronische Signaturen oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a oder b ausgestellt wurde;
- d) mittels anderer auf nationaler Ebene anerkannter Identifizierungsmethoden, die in Bezug auf die Verlässlichkeit eine der persönlichen Anwesenheit gleichwertige Sicherheit bieten. Die gleichwertige Sicherheit ist durch eine Konformitätsbewertungsstelle zu bestätigen.

3.1 IDENTITÄTSPRÜFUNG AUF ELEKTRONISCHEM WEG UND BESCHREIBUNG DES VIDEOIDENTIFIZIERUNGSVERFAHRENS

Das Videoidentifizierungsverfahren (im Folgenden das „Videoidentifizierungsverfahren“ oder das „Verfahren“) ist eine Methode zur Echtzeit- und unbegleiteten Fernüberprüfung der Identität per Video mittels einer von SIGNICAT SLU entwickelten und in ihrem Eigentum stehenden Anwendung (die „Anwendung“), die das gesamte Verfahren der Registrierung der Person durchführt, unterstützt und aufzeichnet und die Fernvalidierung von Ausweisdokumenten ermöglicht. Dieses Video erfasst und validiert das Ausweisdokument in Echtzeit und automatisiert (ca. 10–20 Sekunden) und wird von SIGNICAT SLU durch ihre qualifizierten menschlichen Agenten durchgeführt, die als Prüfer im Auftrag der Registrierungsstelle für die Bestätigung der Identität zuständig sind.

3.1.1 Allgemeine Informationen zum Videoidentifizierungsverfahren

Der Antragsteller/Teilnehmer greift vor Beginn der zur Identitätsprüfung erforderlichen Schritte auf die Anwendung und die Benutzeroberfläche zu **und wird aufgefordert, das vorliegende Dokument zu lesen und ihm zuzustimmen sowie seine freiwillige Einwilligung in die Verarbeitung der für die Videoidentifizierung erforderlichen biometrischen Daten zu erteilen**. Hierzu stellt SIGNICAT SLU dem Antragsteller/Teilnehmer vorab die Datenschutzerklärung zur Verfügung, die die Verarbeitung personenbezogener Daten beschreibt, die während des Verfahrens gemäß den datenschutzrechtlichen Bestimmungen erfolgt.

Erteilt der Antragsteller/Teilnehmer diese Einwilligung nicht, kann das Verfahren nicht fortgesetzt werden, und der Antragsteller/Teilnehmer muss auf eine der in Klausel 1 dieses Dokuments festgelegten alternativen Identifizierungsmethoden gemäß Artikel 24 Absatz 1 der eIDAS-Verordnung zurückgreifen.

Schließlich wird der Nutzer vor Beginn des Videoidentifizierungsverfahrens nach einer Telefonnummer gefragt, an die ein OTP gesendet wird, um die Identität des Antragstellers/Teilnehmers mit dem Gerät und der Telefonnummer zu verknüpfen, die er für die Durchführung des Verfahrens verwendet.

Nachdem der Antragsteller/Teilnehmer das Verfahren gelesen, akzeptiert und ihm zugestimmt hat, führt er die erforderliche Videoidentifizierung durch, damit SIGNICAT SLU das qualifizierte Zertifikat für natürliche Personen ausstellen kann.

Der Antragsteller/Teilnehmer wird während des Videoidentifizierungsverfahrens jederzeit per Sprache und Text geführt, und mithilfe der Anwendung wird eine automatisierte Kontrolle der Umgebungsbedingungen (Lichtverhältnisse, Netzwerk, Kameraqualität) durchgeführt, um eine optimale Aufzeichnung der Videoidentifizierung und ihrer Nachweise zu erhalten.

In diesem Sinne sind die Schritte des Verfahrens vor der Ausstellung des qualifizierten Zertifikats wie folgt:

Im ersten Schritt des Verfahrens wird der Antragsteller/Teilnehmer aufgefordert, das zu verwendende Ausweisdokument vorzuzeigen, um mittels einer speziellen Technologie einen Bildabgleich mit den Originaldokumenten durchzuführen, die Echtheit des Dokuments zu prüfen, die Datenextraktion (OCR) aus der MRZ oder anderen Teilen des Dokuments vorzunehmen und die Berechtigungsnachweise in Echtzeit abzurufen.

Daher wird die Vorderseite des vom Antragsteller/Teilnehmer während des Verfahrens verwendeten

Ausweisdokuments erfasst. Hierzu wird der Antragsteller/Teilnehmer aufgefordert, die Vorderseite seines Dokuments zu zeigen und das Bild in den angezeigten Rahmen einzupassen.

Nach Abschluss der Erfassung wird eine Bestätigungsmeldung angezeigt, und das Verfahren wird mit dem nächsten Schritt fortgesetzt.

Im nächsten Schritt wird die Rückseite des Dokuments erfasst. Der Antragsteller/Teilnehmer wird aufgefordert, die Rückseite seines Dokuments zu zeigen und das Bild in den angezeigten Rahmen einzupassen.

Nach Abschluss der Erfassung wird eine Bestätigungsmeldung angezeigt, und das Verfahren wird mit dem nächsten Schritt fortgesetzt.

Anschließend werden die biometrischen Daten des Antragstellers/Teilnehmers erfasst, um in einem Gesichtserkennungsverfahren auf Grundlage einer automatischen biometrischen Bewertung einen Echtzeitabgleich mit dem Bild des Ausweisdokuments durchzuführen. Hierzu wird der Antragsteller/Teilnehmer aufgefordert, sein Gesicht zu zeigen und das Bild in den auf dem Bildschirm angezeigten Rahmen einzupassen.

Nach Erfassung der biometrischen Daten wird der Antragsteller/Teilnehmer als Lebendnachweis aufgefordert, eine Gesichtsbewegung vor der Kamera auszuführen, und wenn alles korrekt ist, wird eine Konformitätsmeldung angezeigt und das Verfahren mit dem nächsten Schritt fortgesetzt.

Wenn das gesamte Verfahren erfolgreich abgeschlossen wurde, wird der Antragsteller/Teilnehmer darüber informiert, dass das Videoidentifizierungsverfahren abgeschlossen ist und dass die während des Verfahrens erzeugten Nachweise mithilfe des Prüfwerkzeugs der Registrierungsstelle zur Überprüfung des Verfahrens durch eine qualifizierte, zuvor speziell geschulte Person kontrolliert und validiert werden.

Zu diesem Zeitpunkt stellt die Anwendung die Videoidentifizierung und die dabei erzeugten Daten einem qualifizierten menschlichen Agenten zur Verfügung, der für die Überprüfung der Identität des Antragstellers/Teilnehmers des Verfahrens zuständig ist, und fordert die asynchrone Überprüfung des aufgezeichneten Videos sowie der übrigen während des Verfahrens gewonnenen Nachweise und Elemente an. Die durchschnittliche Prüfzeit eines Agenten beträgt ca. drei Minuten.

3.1.2. Sicherheitselemente des Videoidentifizierungsverfahrens und Validierung durch einen qualifizierten menschlichen Agenten

Für die asynchrone Überprüfung durch einen qualifizierten menschlichen Agenten gibt es ein auf bewährten Verfahren der EU beruhendes Sicherheitsprotokoll, das durch das dem qualifizierten menschlichen Agenten zur Verfügung gestellte Werkzeug unterstützt wird, in dem die während des Verfahrens gewonnenen Nachweise sowie die Warnhinweise oder Meldungen zu nicht gewonnenen Nachweisen angezeigt werden.

Die Aufzeichnung des Videos, die Anforderung der Überprüfung der Videoidentifizierung sowie die Entscheidung des qualifizierten Agenten werden in der Anwendung protokolliert, und auf jeden

Protokolleintrag wird ein Zeitstempel angewendet, um dessen Kohärenz und Integrität zu gewährleisten.

Das Verfahren gewährleistet somit die Nachweiskette der Überprüfung von den durch das Verfahren erhobenen Nachweisen bis zu den Protokolleinträgen, die die Identifizierung mit dem qualifizierten menschlichen Agenten der Registrierungsstelle verknüpfen. Das Ergebnis ist eine überprüfte Identität mit einer technischen Sicherheit, die einer Prüfung in physischer Anwesenheit des Antragstellers/Teilnehmers gleichwertig ist.

Sobald die Identität vom qualifizierten menschlichen Agenten positiv validiert wurde, ist die Identität des Antragstellers/Teilnehmers bestätigt, und er kann fortfahren und den elektronischen Zertifizierungsdienst von SIGNICAT SLU erhalten, der ihm die Fortsetzung des Verfahrens zur Ausstellung des qualifizierten Zertifikats für natürliche Personen und die Signatur elektronischer Dokumente ermöglicht.

Ist das Ergebnis des Verfahrens negativ, kann das Verfahren zur Ausstellung qualifizierter Zertifikate nicht fortgesetzt werden, und der Antragsteller/Teilnehmer muss sich persönlich in die Räumlichkeiten von SIGNICAT SLU begeben, um seine Identität persönlich überprüfen zu lassen.

3.2 PFLICHTEN DES ANTRAGSTELLERS/TEILNEHMERS IM ZUSAMMENHANG MIT DEM VIDEOIDENTIFIZIERUNGSVERFAHREN.

Der Antragsteller/Teilnehmer verpflichtet sich während des gesamten Verfahrens:

- den Dienst gemäß den Bestimmungen dieses Dokuments, der CPS, den gegebenenfalls anwendbaren besonderen Bedingungen sowie allen sonstigen von SIGNICAT SLU bereitgestellten Anweisungen, Handbüchern oder Verfahren zu nutzen;
- sicherzustellen, dass das während des Verfahrens verwendete Dokument ein echtes, rechtsgültiges Dokument ist und dass es darüber hinaus:
 - keine Fotokopie und keine ausgedruckte Karte ist;
 - nicht in digitalem Format (Mobiltelefon, Tablet oder Computer) vorliegt;
 - sich nicht in einer Hülle befindet;
 - nicht beschädigt und vollständig ist und alle Sicherheitsmerkmale auf dem Dokument enthalten sind;
- sicherzustellen, dass während des Verfahrens und der Aufzeichnung des Videos zur Vermeidung einer Ablehnung:
 - die Lichtverhältnisse im Video es ermöglichen, das Gesicht der identifizierten Person und das Dokument deutlich zu erkennen;
 - der Videostream konstant und ohne Unterbrechungen oder Verzögerungen ist;
 - eine lebende Person den Ausweis vorzeigt;
 - wenn eine andere Person als die zu identifizierende Person das gesamte Verfahren durchführt, die Identifizierung als nicht authentisch abgelehnt wird;

- wenn eine weitere Person im Video anwesend ist, die zu identifizierende Person aber offensichtlich nicht nötigt, die Identifizierung gültig sein kann, etwa wenn eine Person einer Person mit Behinderung bei der Identifizierung hilft;
- alle Teile der Aufnahmen des Dokuments, Vorder- und Rückseite sowie das Gesicht der Person, deutlich erkennbar sind;
- der Antragsteller/Teilnehmer nicht schläft und keine Anzeichen zeigt, die als Einfluss von Drogen oder Alkohol gedeutet werden können.

3.3 AUSSTELLUNG, ÜBERGABE UND ANNAHME DES ZERTIFIKATS

3.3.1 Zertifikatsantrag und Schlüsselerzeugung durch SIGNICAT SLU im Namen des Antragstellers/Teilnehmers.

Nach Abschluss des Videoidentifizierungsverfahrens beantragt der Antragsteller/Teilnehmer und ermächtigt SIGNICAT SLU, in seinem Namen gegebenenfalls die privaten und öffentlichen Schlüssel zu erzeugen und zu verwalten, wodurch SIGNICAT SLU das qualifizierte langfristige Zertifikat für natürliche Personen ausstellen und in seinem Namen die entsprechenden elektronischen Dokumente mit öffentlichen oder privaten Dritten signieren kann, mit denen SIGNICAT SLU bestimmte vertragliche Vereinbarungen unterhält, und zwar gemäß den Bestimmungen der Klauseln 3.3.3, 3.3.4 und 3.3.5.

3.3.2 Richtigkeit der Angaben

Der ANTRAGSTELLER/TEILNEHMER ist dafür verantwortlich, dass alle SIGNICAT SLU direkt oder über das im Zertifikatsausstellungsverfahren verwendete Ausweisdokument übermittelten Angaben richtig, für den Zweck des Zertifikats vollständig und jederzeit aktuell sind; hierzu sichert er zu, ein rechtmäßiges und gültiges Ausweisdokument zu verwenden, das weder vom ANTRAGSTELLER/TEILNEHMER noch von Dritten verfälscht und/oder verändert wurde.

3.3.3 Ausstellung des Zertifikats

Für die Ausstellung des Zertifikats verwendet SIGNICAT SLU die Daten des vom Antragsteller/Teilnehmer während des Videoidentifizierungsverfahrens vorgelegten Ausweisdokuments. Diese Daten werden von SIGNICAT SLU extrahiert und nach Bestätigung durch den Antragsteller/Teilnehmer in das elektronische Zertifikat aufgenommen, um seine Identität mit diesem zu verknüpfen.

3.3.4 Erhalt der PIN

Nach Abschluss des Videoidentifizierungsverfahrens senden wir Ihnen einen PIN-Code, der mit Ihrem elektronischen Zertifikat verknüpft wird.

Diese PIN wird zum Signieren von Dokumenten gemäß Klausel 3.4 verwendet.

Der PIN-Code ist ein geheimer Code, den nur der Antragsteller/Teilnehmer kennen darf, da die alleinige Kontrolle über diese PIN die alleinige Kontrolle über das elektronische Zertifikat zum Signieren der Dokumente gewährleistet; daher darf dieser PIN-Code nur dem Nutzer bekannt sein, der ihn Dritten nicht zugänglich machen darf, da er persönlich und nicht übertragbar ist.

Verliert der Nutzer den PIN-Code oder vermutet er, dass Dritte ihn kennen könnten, muss er SIGNICAT

SLU unverzüglich benachrichtigen, damit das elektronische Zertifikat widerrufen wird.

Die Verwendung dieser PIN zum Signieren von Dokumenten gilt als Erklärung der Zustimmung des Antragstellers/Teilnehmers, an deren Inhalt gebunden zu sein.

3.3.5 Annahme der Zertifikatsausstellung und Bestätigung dieser Allgemeinen Geschäftsbedingungen.

Sobald der Antragsteller/Teilnehmer den PIN-Code erhalten hat, muss er bestätigen, dass er sich in seinem Besitz befindet.

Hierzu muss er ihn eingeben, um die Ausstellung des elektronischen Zertifikats sowie diese Allgemeinen Geschäftsbedingungen anzunehmen, die Ihnen vorab angezeigt und anschließend per E-Mail, bereits vom Antragsteller/Teilnehmer elektronisch signiert, zugesandt werden.

3.3.6 Übergabe des Zertifikats

Im Rahmen des Ausstellungsverfahrens erfolgt keine gesonderte Übergabe des Zertifikats an den Antragsteller/Teilnehmer. SIGNICAT SLU verwaltet es in ihrer Eigenschaft als qualifizierter Vertrauensdiensteanbieter, damit der Antragsteller/Teilnehmer es für die elektronische Signatur von Dokumenten verwenden kann.

3.4 SERVERSIGNATURDIENST

Nach Abschluss des Identifizierungsverfahrens und Validierung der Identität durch den Prüfer ist die Identität des Unterzeichners gewährleistet, und SIGNICAT SLU verwahrt als qualifizierter Vertrauensdiensteanbieter das elektronische Zertifikat des Nutzers sicher, damit dieser es während seiner Laufzeit zum elektronischen Signieren von Dokumenten verwenden kann.

Jedes Mal, wenn der Nutzer ein Dokument mit dem erzeugten elektronischen Zertifikat elektronisch signieren möchte, muss er den dafür vorgesehenen Bereich aufrufen, in dem er dessen Inhalt einsehen kann.

Ist er mit dem Inhalt einverstanden und möchte er sich durch seine elektronische Signatur daran binden, muss der Nutzer den Vorgang fortsetzen.

Daraufhin fordert die Plattform seinen PIN-Code an, der die alleinige Kontrolle des Nutzers über sein elektronisches Zertifikat gewährleistet.

Nach Eingabe der PIN erhält er auf seinem Mobiltelefon ein OTP, das in dem dafür vorgesehenen Feld in der Signaturumgebung einzugeben ist. Die Eingabe dieses OTP ermöglicht es SIGNICAT SLU, die Signaturerstellungsdaten des Antragstellers/Teilnehmers anzuwenden, um die elektronische Signatur des zuvor angezeigten Dokuments zu erzeugen.

SIGNICAT SLU räumt dem Antragsteller/Teilnehmer eine nicht ausschließliche und nicht übertragbare Lizenz zur Nutzung der Kopien der Software der sicheren kryptografischen Einheit von SIGNICAT SLU für den Betrieb der Signatureinheit, soweit zutreffend, sowie für die Erstellung der elektronischen

Signatur, des Zertifikats und der übrigen kryptografischen Dienste durch die Unterzeichner ein.

Nimmt eine andere Person als SIGNICAT SLU Änderungen an der bereitgestellten Software vor, erlöschen alle Gewährleistungen in Bezug auf die Software mit sofortiger Wirkung.

4. ALLGEMEINE BEDINGUNGEN DES VERTRAUENSDIENSTES

4.1 ALLGEMEINE BEDINGUNGEN DES VIDEOIDENTIFIZIERUNGSDIENSTES

- Aufbewahrungsfrist der Informationen

Alle Informationen im Zusammenhang mit dem Verfahren zur Ausstellung qualifizierter elektronischer Zertifikate für natürliche Personen, einschließlich der biometrischen Informationen, werden von SIGNICAT SLU während der Laufzeit des Vertragsverhältnisses, solange keine Löschung verlangt wird, sowie während der Verjährungsfrist möglicher Klagen oder möglicher Ansprüche seitens öffentlicher Stellen aufbewahrt.

In diesem Sinne beträgt die maximale Aufbewahrungsfrist für die relevanten Informationen im Zusammenhang mit dem Videoidentifizierungsverfahren und der Ausstellung qualifizierter Zertifikate, d. h. eine Kopie der Videoaufzeichnung, die Fotos oder Bildschirmaufnahmen des Antragstellers/Teilnehmers und des verwendeten Ausweisdokuments, das automatische Ergebnis der von der Anwendung von SIGNICAT SLU durchgeführten Prüfung sowie die Bewertung und die Anmerkungen der qualifizierten menschlichen Agenten zur Identitätsprüfung zusammen mit ihrer Entscheidung über die Genehmigung oder Ablehnung der Identifizierung, 15 Jahre ab dem Widerruf oder Ablauf des Zertifikats, sofern gesetzlich nichts anderes bestimmt ist. Nach Beendigung des Vertragsverhältnisses werden die Daten des Antragstellers/Teilnehmers gemäß den Bestimmungen der anwendbaren Vorschriften ordnungsgemäß gesperrt.

Darüber hinaus wird darauf hingewiesen, dass alle Nachweise unvollständiger Identifizierungsverfahren, die wegen des Verdachts eines Betrugsversuchs nicht abgeschlossen wurden, gemäß der hierfür festgelegten Richtlinie für einen Zeitraum von 5 Jahren ab der Durchführung des Verfahrens unter Angabe des Grundes für den Abbruch aufbewahrt werden.

- Haftungsbeschränkung im Zusammenhang mit dem Videoidentifizierungsverfahren.

Qualität des Verfahrens: SIGNICAT SLU gewährleistet die ordnungsgemäße Erbringung der in diesem Dokument beschriebenen Videoidentifizierungsdienste, sofern die dem Antragsteller/Teilnehmer zur Verfügung gestellten Mittel ordnungsgemäß und gemäß den Anweisungen von SIGNICAT SLU verwendet werden.

Der Zugang zu den Videoidentifizierungsdiensten und deren Nutzung begründen keine Verpflichtung von SIGNICAT SLU, die Abwesenheit von Viren, Würmern oder sonstigen schädlichen IT-Elementen zu kontrollieren. Es obliegt dem Antragsteller/Teilnehmer als Nutzer, jederzeit über geeignete Werkzeuge zur Erkennung und Beseitigung schädlicher Computerprogramme zu verfügen. SIGNICAT SLU haftet nicht für Schäden, die während des Videoidentifizierungsverfahrens an der Computerausrüstung des Antragstellers/Teilnehmers oder Dritter entstehen.

Verfügbarkeit des Verfahrens: Der Betrieb des Videoidentifizierungsverfahrens kann von der korrekten

Konfiguration der Ausrüstung abhängen, von der aus der Nutzer auf das Videoidentifizierungsverfahren zugreift und es startet; der Nutzer muss daher die bereitgestellten Anweisungen befolgen und jederzeit die angegebenen Software- und Hardwareanforderungen erfüllen.

Ebenso muss für die Durchführung des Videoidentifizierungsverfahrens ein Internetzugang verfügbar sein. Der Betrieb des Videoidentifizierungsverfahrens kann von einer angemessenen Qualität und Geschwindigkeit der Verbindung abhängen, über die der Antragsteller/Teilnehmer auf die Anwendung zugreift; er ist allein verantwortlich für die Bereitstellung von Telekommunikationsleitungen, Internetabonnements oder -verbindungen oder sonstigen technischen Mitteln, die für den Zugriff auf seine Daten und deren Nutzung erforderlich sind.

SIGNICAT SLU haftet nicht für Schäden, die sich aus der Nichterfüllung oder mangelhaften Erfüllung der Pflichten des Antragstellers/Teilnehmers ergeben oder damit zusammenhängen, noch für die unsachgemäße Verwendung der Ergebnisse des Verfahrens und der Schlüssel, noch für mittelbare Schäden, die aus der Nutzung des Verfahrens oder der von SIGNICAT SLU bereitgestellten Informationen entstehen können.

SIGNICAT SLU haftet nicht für Ungenauigkeiten bei der Identifizierung des Antragstellers/Teilnehmers, die sich aus den von diesem während des Verfahrens gemachten Angaben ergeben.

SIGNICAT SLU haftet nicht für den ordnungsgemäßen Betrieb nicht zugelassener Anwendungen und nicht für Schäden, die dadurch entstehen, dass der Antragsteller/Teilnehmer diese Anwendungen nicht nutzen kann.

4.2 ALLGEMEINE BEDINGUNGEN DER ELEKTRONISCHEN ZERTIFIZIERUNGSDIENSTE FÜR LANGFRISTIGE ZERTIFIKATE.

- Rechtlicher Rahmen der Dienstleistung

Die Zertifizierungsdienste von SIGNICAT SLU werden technisch und betrieblich durch die Erklärung zur Zertifizierungspraxis und die Zertifizierungsrichtlinien von SIGNICAT SLU und deren spätere Aktualisierungen sowie durch ergänzende, dem ANTRAGSTELLER/TEILNEHMER zur Verfügung gestellte Unterlagen geregelt.

Diese Allgemeinen Bedingungen, die Erklärung zur Zertifizierungspraxis und die Zertifizierungsrichtlinien, soweit sie auf das ausgestellte Zertifikat anwendbar sind, bilden den rechtlichen Rahmen für das Verhältnis zwischen SIGNICAT SLU und dem ANTRAGSTELLER/TEILNEHMER, sowohl im Innenverhältnis als auch gegenüber Dritten, unbeschadet der Bestimmungen der geltenden Gesetzgebung.

Dieses Dokument enthält die wichtigsten Aspekte und Anforderungen der Rechte und Pflichten der Parteien.

Die anwendbare Erklärung zur Zertifizierungspraxis (CPS) und die spezifischen Zertifizierungsrichtlinien (CP) werden durch Verweis in dieses Dokument einbezogen. Die jeweils aktuellste Fassung der CPS ist jederzeit kostenlos in den folgenden Sprachen über den nachstehenden Link abrufbar:

Spanisch: <https://www.signicat.com/es/acerca-de/certificados-cualificados-para-firma-electronica>

Englisch: <https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>

Im Falle von Abweichungen hat die Bedeutung der in diesem Dokument enthaltenen Begriffe Vorrang vor den Festlegungen in der CPS.

- **Vertragslaufzeit**

Dieser Vertrag gilt für den Zeitraum zwischen dem Ausstellungs- und dem Ablaufdatum, die im qualifizierten Zertifikat für natürliche Personen angegeben sind, das der Antragsteller/Teilnehmer bei SIGNICAT SLU beantragt und erworben hat.

- **Pflichten zur ordnungsgemäßen Nutzung**

Der ANTRAGSTELLER/TEILNEHMER darf den von SIGNICAT SLU erbrachten Zertifizierungsdienst ausschließlich für die in der CPS zugelassenen Verwendungszwecke nutzen, die dem ANTRAGSTELLER/TEILNEHMER bekannt sind und von ihm akzeptiert wurden, indem er das Dokument gelesen und die im Verfahren vorgesehenen Auswahlkästchen angekreuzt hat.

Der ANTRAGSTELLER/TEILNEHMER verpflichtet sich, den digitalen Zertifizierungsdienst und alle sonstigen von SIGNICAT SLU bereitgestellten technischen Elemente sowie die Zertifikate gemäß diesen Allgemeinen Geschäftsbedingungen, der CPS und den gegebenenfalls anwendbaren CP, den gegebenenfalls im Handbuch aufgeführten besonderen Bedingungen sowie allen sonstigen von SIGNICAT SLU dem ANTRAGSTELLER/TEILNEHMER bereitgestellten Anweisungen oder Verfahren und unter Einhaltung aller geltenden Rechtsvorschriften zu nutzen.

Die Beauftragung des Zertifizierungsdienstes bei SIGNICAT SLU erlaubt die Nutzung des Zertifikats nur im Rahmen der offiziellen Tätigkeit des ANTRAGSTELLERS/TEILNEHMERS gemäß dem Zweck des beantragten Zertifikatstyps, d. h. des qualifizierten Zertifikats für elektronische Signaturen einer natürlichen Person mit langer Laufzeit. Nach Ausstellung des Zertifikats darf der ANTRAGSTELLER/TEILNEHMER das Zertifikat, sofern zwischen den Parteien nicht ausdrücklich etwas anderes vereinbart wurde, nicht für kommerzielle Zwecke nutzen. Als kommerzielle Nutzung des Zertifikats gilt jede Handlung, mit der der ANTRAGSTELLER/TEILNEHMER Dritten außerhalb dieses Vertrags entgeltlich oder unentgeltlich Dienste anbietet, die die Nutzung des ausgestellten Zertifikats erfordern.

- **Verbotene Vorgänge**

Die von SIGNICAT SLU erbrachten digitalen Zertifizierungsdienste sind weder dafür ausgelegt noch dafür zugelassen, als Einrichtungen zur Steuerung gefährlicher Situationen oder für Verwendungen, die fehlerfreie Abläufe erfordern, genutzt oder weiterverkauft zu werden, wie etwa für den Betrieb kerntechnischer Anlagen, von Navigations- oder Flugkommunikationssystemen, Flugverkehrskontrollsystemen oder Waffenkontrollsystemen, bei denen ein Fehler unmittelbar zum Tod führen oder Körperschäden oder schwere Umweltschäden verursachen könnte.

- **Pflichten und Verantwortlichkeiten von SIGNICAT SLU**

a) In Bezug auf die Erbringung des Dienstes als Registrierungsstelle.

SIGNICAT SLU verpflichtet sich, die Zertifikatsdaten zu registrieren und das Zertifikat anschließend für den ANTRAGSTELLER/TEILNEHMER auszustellen, wofür sie die von ihr für erforderlich gehaltenen Prüfungen hinsichtlich der Identität und der sonstigen persönlichen und ergänzenden Angaben des ANTRAGSTELLERS/TEILNEHMERS und gegebenenfalls der Unterzeichner selbst durchführen muss.

Diese Prüfungen müssen die vom ANTRAGSTELLER/TEILNEHMER vorgelegten Nachweisunterlagen und, sofern SIGNICAT SLU dies für erforderlich hält, alle sonstigen relevanten vom ANTRAGSTELLER/TEILNEHMER vorgelegten Dokumente und Informationen umfassen.

Stellt SIGNICAT SLU Fehler in den Daten fest, die in die Zertifikate aufzunehmen sind oder diese Daten belegen, kann sie vor der Ausstellung des Zertifikats die von ihr für erforderlich gehaltenen Änderungen vornehmen oder das Ausstellungsverfahren aussetzen und den entsprechenden Vorfall mit dem ANTRAGSTELLER/TEILNEHMER klären.

Berichtigt SIGNICAT SLU die Daten, ohne den entsprechenden Vorfall zuvor mit dem ANTRAGSTELLER/TEILNEHMER geklärt zu haben, muss sie dem ANTRAGSTELLER/TEILNEHMER die letztlich zertifizierten Daten mitteilen.

SIGNICAT SLU behält sich das Recht vor, das Zertifikat nicht auszustellen, wenn die vorgelegten Nachweisunterlagen für die korrekte Identifizierung und Authentifizierung des ANTRAGSTELLERS/TEILNEHMERS nicht ausreichen oder wenn das vor der Ausstellung des Zertifikats durchgeführte Videoidentifizierungsverfahren von SIGNICAT SLU nicht als gültig bestätigt wurde.

Die vorstehenden Pflichten ruhen, wenn der ANTRAGSTELLER/TEILNEHMER als Registrierungsstelle tätig ist und über die technischen Elemente zur Schlüsselerzeugung und Zertifikatsausstellung verfügt.

b) In Bezug auf die Erbringung des Zertifizierungsdienstes.

SIGNICAT SLU verpflichtet sich, die Pflichten aus dem Gesetz 6/2020 vom 11. November zur Regelung bestimmter Aspekte elektronischer Vertrauensdienste einzuhalten, insbesondere:

- a) Zertifikate gemäß den Anweisungen des ANTRAGSTELLERS/TEILNEHMERS in den Fällen und aus den Gründen, die in der CPS von SIGNICAT SLU beschrieben sind, auszustellen, zu übergeben, zu verwalten, auszusetzen, zu widerrufen und zu erneuern.
- b) Die Dienste mit geeigneten technischen und materiellen Mitteln und mit Personal zu erbringen, das die in der CPS festgelegten Anforderungen an Qualifikation und einschlägige Erfahrung erfüllt.
- c) Die Dienstqualitätsniveaus gemäß den Festlegungen der CPS in technischer, betrieblicher und sicherheitsbezogener Hinsicht einzuhalten.
- d) Den Status der Zertifikate gemäß den Festlegungen der CPS für die verschiedenen Zertifikatsprüfdienste Dritten mitzuteilen, die dies verlangen.

e) Qualität des Verfahrens: SIGNICAT SLU gewährleistet die ordnungsgemäße Erbringung der in diesem Dokument beschriebenen Zertifizierungsdienste, sofern die dem ANTRAGSTELLER/TEILNEHMER zur Verfügung gestellten Mittel ordnungsgemäß und gemäß den Anweisungen von SIGNICAT SLU verwendet werden.

Der Zugang zu den Zertifizierungsdiensten und deren Nutzung begründen keine Verpflichtung von SIGNICAT SLU, die Abwesenheit von Viren, Würmern oder sonstigen schädlichen IT-Elementen zu kontrollieren. Es obliegt dem ANTRAGSTELLER/TEILNEHMER als Nutzer, jederzeit über geeignete Werkzeuge zur Erkennung und Beseitigung schädlicher Computerprogramme zu verfügen. SIGNICAT SLU haftet nicht für Schäden, die während des Videoidentifizierungsverfahrens an der Computerausrüstung des ANTRAGSTELLERS/TEILNEHMERS oder Dritter entstehen.

f) Verfügbarkeit des Verfahrens: Der Betrieb des Zertifizierungsverfahrens kann von der korrekten Konfiguration der Ausrüstung abhängen, von der aus der Nutzer auf das Videoidentifizierungsverfahren zugreift und es startet; der Nutzer muss daher die bereitgestellten Anweisungen befolgen und jederzeit die angegebenen Software- und Hardwareanforderungen erfüllen.

Ebenso muss für die Durchführung des Videoidentifizierungsverfahrens ein Internetzugang verfügbar sein. Der Betrieb des Videoidentifizierungsverfahrens kann von einer angemessenen Qualität und Geschwindigkeit der Verbindung abhängen, über die der ANTRAGSTELLER/TEILNEHMER auf die Anwendung zugreift; er ist allein verantwortlich für die Bereitstellung von Telekommunikationsleitungen, Internetabonnements oder -verbindungen oder sonstigen technischen Mitteln, die für den Zugriff auf seine Daten und deren Nutzung erforderlich sind.

- **Als Zertifizierungsdiensteanbieter.**

SIGNICAT SLU ist verpflichtet:

a) wahrheitsgemäße Informationen gemäß dem Gesetz 6/2020 vom 11. November zur Regelung bestimmter Aspekte elektronischer Vertrauensdienste und der Verordnung (EU) Nr. 910/2014 zu veröffentlichen.

b) die Signaturerstellungsdaten weder selbst noch durch Dritte zu speichern oder zu kopieren, außer im Fall ihrer Verwaltung im Namen des Inhabers zum Zweck der Anwendung der privaten Schlüssel zur Signaturerstellung gemäß den Anweisungen des ANTRAGSTELLERS/TEILNEHMERS über das OTP-System, das SIGNICAT SLU dem ANTRAGSTELLER/TEILNEHMER für die Signatur elektronischer Dokumente zur Verfügung stellt. In diesem Fall werden vertrauenswürdige Systeme und Produkte einschließlich sicherer elektronischer Kommunikationskanäle verwendet und geeignete technische und organisatorische Verfahren und Mechanismen angewandt, um sicherzustellen, dass die Umgebung vertrauenswürdig ist und unter der alleinigen Kontrolle des Zertifikatsinhabers genutzt wird. Darüber hinaus sind die Signaturerstellungsdaten vor Veränderung, Zerstörung oder unbefugtem Zugriff zu sichern und zu schützen und ihre ständige Verfügbarkeit zu gewährleisten.

c) einen öffentlich zugänglichen Abfragedienst zum Gültigkeits- oder Widerrufsstatus der ausgestellten Zertifikate anzubieten.

d) die folgenden zusätzlichen Pflichten zu erfüllen:

1. Der Zeitraum, in dem die Informationen über die erbrachten Dienste gemäß Artikel 24 Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 aufzubewahren sind, beträgt 15 Jahre ab dem Ablauf des Zertifikats oder dem Ende des erbrachten Dienstes. Werden qualifizierte Zertifikate für elektronische Siegel oder für die Website-Authentifizierung an juristische Personen ausgestellt, zeichnen die Vertrauensdiensteanbieter außerdem die Informationen auf, die es ermöglichen, die Identität der natürlichen Person festzustellen, der diese Zertifikate übergeben wurden, um sie in Gerichts- oder Verwaltungsverfahren identifizieren zu können.
2. Abschluss einer Haftpflichtversicherung mit einer Mindestdeckungssumme von 1.500.000 Euro, sofern der Anbieter nicht dem öffentlichen Sektor angehört. Werden mehr als einer der in der Verordnung (EU) Nr. 910/2014 vorgesehenen qualifizierten Dienste erbracht, erhöht sich der Betrag für jede zusätzliche Dienstart um 500.000 Euro. Diese Sicherheit kann ganz oder teilweise durch eine Bankbürgschaft oder eine Kautionsversicherung ersetzt werden, sodass die Summe der versicherten Beträge den Bestimmungen des vorstehenden Absatzes entspricht. Die Beträge sowie die in den beiden vorstehenden Absätzen festgelegten Versicherungs- und Sicherungsmittel können durch königliches Dekret geändert werden.
3. im Falle der Einstellung ihrer Tätigkeit als qualifizierter Vertrauensdiensteanbieter die Kunden, für die sie die Dienste erbringt, sowie die Aufsichtsstelle mindestens zwei Monate vor der tatsächlichen Einstellung der Tätigkeit auf einem Weg zu benachrichtigen, der, soweit möglich, die tatsächliche Zustellung und den Empfang nachweist. Der Beendigungsplan des Diensteanbieters kann die Übertragung der Kunden, nachdem das Fehlen eines Widerspruchs festgestellt wurde, auf einen anderen qualifizierten Anbieter vorsehen, der alle Informationen über die bis dahin erbrachten Dienste aufbewahren kann. Ebenso unterrichtet sie die Aufsichtsstelle über alle sonstigen relevanten Umstände, die die Fortführung ihrer Tätigkeit verhindern könnten. Insbesondere muss sie über die Eröffnung eines gegen sie gerichteten Insolvenzverfahrens informieren, sobald sie davon Kenntnis erlangt.
4. den Konformitätsbewertungsbericht gemäß Artikel 20 Absatz 1 der Verordnung (EU) Nr. 910/2014 dem Ministerium für Wirtschaft und digitale Transformation zu übermitteln. Die Nichterfüllung dieser Pflicht führt, nachdem der Diensteanbieter zur Abstellung des genannten Verstoßes aufgefordert wurde, zum Entzug des Qualifikationsstatus des Anbieters und des von ihm erbrachten Dienstes sowie zu seiner Streichung aus der in Artikel 22 der genannten Verordnung vorgesehenen Vertrauensliste.

e) SIGNICAT SLU übernimmt gegenüber Dritten die volle Verantwortung für die Handlungen der Personen oder anderen Diensteanbieter, denen sie die Ausführung einzelner oder aller für die Erbringung elektronischer Vertrauensdienste erforderlichen Aufgaben überträgt, einschließlich der Identitätsprüfungen vor der Ausstellung eines qualifizierten Zertifikats.

- **GEWÄHRLEISTUNGEN FÜR ZERTIFIZIERUNGSDIENSTE**

Gewährleistung von SIGNICAT SLU für elektronische Zertifizierungsdienste.

SIGNICAT SLU gewährleistet, dass der private Schlüssel der Zertifizierungsstelle, der zur Ausstellung von Zertifikaten verwendet wird, nicht kompromittiert wurde, sofern nicht über das Zertifizierungsverzeichnis gemäß der CPS etwas anderes mitgeteilt wurde.

SIGNICAT SLU gewährleistet dem ANTRAGSTELLER/TEILNEHMER zum Zeitpunkt der Ausstellung des Zertifikats lediglich, dass:

- a) die Zertifikate gegebenenfalls im Sinne des Gesetzes 6/2020 vom 11. November zur Regelung bestimmter Aspekte elektronischer Vertrauensdienste qualifiziert sind;
- b) SIGNICAT SLU weder falsche noch fehlerhafte Angaben in den in einem Zertifikat enthaltenen Informationen verursacht oder eingefügt noch es unterlassen hat, notwendige vom ANTRAGSTELLER/TEILNEHMER bereitgestellte und geprüfte Informationen aufzunehmen;
- c) alle Zertifikate die in der CPS und den CP von SIGNICAT SLU festgelegten formalen und inhaltlichen Anforderungen erfüllen;
- d) SIGNICAT SLU die in der CPS beschriebenen Verfahren eingehalten hat.

SIGNICAT SLU wendet angemessene Sorgfalt an, um sicherzustellen, dass jedes im Rahmen ihrer Dienste gelieferte Produkt frei von Computerviren, Würmern und sonstigem unzulässigem Code ist, und ist verpflichtet, den ANTRAGSTELLER/TEILNEHMER über jeden später in einem Produkt entdeckten Virus, Wurm oder sonstigen unzulässigen Code zu informieren.

- **GEWÄHRLEISTUNGSAUSSCHLÜSSE**

SIGNICAT SLU übernimmt keine Gewährleistung für Software, die vom ANTRAGSTELLER/TEILNEHMER des Zertifikats, vom Unterzeichner oder von einer anderen Person verwendet wird, um eine von SIGNICAT SLU ausgestellte digitale Signatur oder ein digitales Zertifikat zu erzeugen, zu prüfen oder anderweitig zu verwenden, es sei denn, es liegt eine gegenteilige schriftliche Erklärung von SIGNICAT SLU vor.

- **HAFTUNGSBESCHRÄNKUNGEN ALS ANBIETER ELEKTRONISCHER VERTRAUENSDIENSTE.**

SIGNICAT SLU haftet, soweit dies im Rahmen des anwendbaren Rechts zulässig ist, nicht für Schäden und Verluste, die der Person, für die sie ihre Dienste erbracht hat, oder gutgläubigen Dritten entstehen, wenn diese in einem der in der Verordnung (EU) Nr. 910/2014 vorgesehenen Fälle oder in den folgenden Fällen eintreten:

- a) Unterlassene Übermittlung wahrheitsgemäßer, vollständiger und genauer Informationen an den Vertrauensdiensteanbieter für die Erbringung des Vertrauensdienstes, insbesondere zu den Daten, die in das elektronische Zertifikat aufzunehmen sind oder für dessen Ausstellung, Erlöschen oder die Aussetzung seiner Gültigkeit erforderlich sind, sofern deren Unrichtigkeit vom Diensteanbieter trotz gebotener Sorgfalt nicht erkannt wurde.
- b) Unterlassene unverzügliche Mitteilung an SIGNICAT SLU über jede Änderung der Umstände, die die Erbringung des Vertrauensdienstes betreffen, insbesondere der im elektronischen Zertifikat wiedergegebenen Umstände.
- c) Fahrlässigkeit bei der Aufbewahrung der Signaturerstellungs- oder Website-Authentifizierungsdaten, bei der Sicherstellung ihrer Vertraulichkeit und beim Schutz vor

jedem Zugriff auf diese oder jeder Offenlegung dieser Daten oder gegebenenfalls der Mittel, die den Zugriff darauf ermöglichen.

d) Unterlassene Beantragung der Aussetzung oder des Widerrufs des elektronischen Zertifikats bei Zweifeln an der Wahrung der Vertraulichkeit der Signaturerstellungs-, Siegel- oder Website-Authentifizierungsdaten oder gegebenenfalls der Mittel, die den Zugriff darauf ermöglichen.

e) Verwendung der Signaturerstellungs-, Siegel- oder Website-Authentifizierungsdaten nach Ablauf der Gültigkeitsdauer des elektronischen Zertifikats oder nachdem der Vertrauensdiensteanbieter Ihnen das Erlöschen oder die Aussetzung seiner Gültigkeit mitgeteilt hat.

SIGNICAT SLU haftet ferner nicht für Schäden, wenn der Empfänger fahrlässig handelt.

Der Empfänger handelt insbesondere dann fahrlässig, wenn er die Aussetzung oder den Verlust der Gültigkeit des elektronischen Zertifikats nicht berücksichtigt oder wenn er die elektronische Signatur oder das elektronische Siegel nicht prüft.

SIGNICAT SLU haftet nicht für Schäden aufgrund unrichtiger Daten im elektronischen Zertifikat, wenn diese durch eine öffentliche oder amtliche Urkunde nachgewiesen oder, sofern erforderlich, in einem öffentlichen Register eingetragen wurden.

- HAFTUNG DES ANTRAGSTELLERS/TEILNEHMERS

Der ANTRAGSTELLER/TEILNEHMER haftet gegenüber jeder Person für die Verletzung seiner Pflichten, insbesondere im Hinblick auf die Identifizierungstätigkeit oder gegebenenfalls die Tätigkeit als Registrierungsstelle, gemäß diesen Allgemeinen Geschäftsbedingungen.

Der ANTRAGSTELLER/TEILNEHMER ist für alle elektronischen Kommunikationen verantwortlich, die mittels einer mit seinem privaten Schlüssel erzeugten digitalen Signatur authentifiziert wurden, sofern das Zertifikat über die von SIGNICAT SLU festgelegten Mechanismen und Bedingungen gültig geprüft wurde.

Solange die in diesem Dokument vorgesehene Benachrichtigung nicht erfolgt ist, trägt der ANTRAGSTELLER/TEILNEHMER jede Haftung, die sich aus der unbefugten und/oder missbräuchlichen Nutzung der Zertifikate ergeben kann.

- EIGNUNG VON PRODUKTEN, DIE IDENTIFIZIERUNG, ELEKTRONISCHE SIGNATUR ODER VERSCHLÜSSELUNG NUTZEN

SIGNICAT SLU haftet nicht für die Eignung der auf dem Markt vorhandenen Produkte und Dienste im Zusammenhang mit digitaler Zertifizierung, Identifizierung, elektronischer Signatur oder Verschlüsselung, die in den Computeranwendungen des ANTRAGSTELLERS/TEILNEHMERS verwendet werden, es sei denn, SIGNICAT SLU stellt sie bereit. In diesem Fall unterliegen die Parteien den entsprechenden Nutzungsbedingungen.

- EIGENTUM AN DEN ZERTIFIKATEN

Die bereitgestellten Zertifikate bleiben Eigentum des ANTRAGSTELLERS/TEILNEHMERS.

- **BEENDIGUNG**

Die Beendigung erfolgt in den folgenden Fällen:

- a) Bei Verletzung einer ihrer Pflichten durch die andere Partei, sofern dieser Verstoß nicht behoben wurde:
- b) innerhalb von dreißig Tagen nach Eingang der Mitteilung der Partei, die ihre Pflichten nicht verletzt hat;
- c) mit sofortiger Wirkung, wenn der Verstoß die Sicherheit der Dienste gefährdet.
- d) Bei Vorliegen eines sonstigen Grundes für eine vorzeitige Beendigung, der in der geltenden Gesetzgebung und insbesondere in der geltenden Gesetzgebung über elektronische Signaturen und digitale Zertifizierung vorgesehen ist.

- **VERTRAULICHKEITSRICHTLINIE**

SIGNICAT SLU darf vertrauliche Informationen über Zertifikate ohne ausdrückliches vorheriges Ersuchen der folgenden Stellen nicht offenlegen und kann nicht zu ihrer Offenlegung gezwungen werden:

- a) der Person, hinsichtlich derer SIGNICAT SLU zur Vertraulichkeit der Informationen verpflichtet ist, oder
- b) einer gerichtlichen, behördlichen oder sonstigen nach geltendem Recht vorgesehenen Anordnung.

Der ANTRAGSTELLER/TEILNEHMER erklärt sich jedoch damit einverstanden, dass bestimmte personenbezogene und sonstige Informationen, die im Zertifikatsantrag angegeben wurden, in seine Zertifikate und in den Mechanismus zur Prüfung des Zertifikatsstatus aufgenommen werden und dass diese Informationen kraft gesetzlicher Vorschrift nicht als vertraulich gelten.

- **ERSTATTUNGSRICHTLINIE**

SIGNICAT SLU erstattet die Kosten des Zertifizierungsdienstes in keinem Fall.

- **AUFBEWAHRUNGSFRIST DER INFORMATIONEN**

Alle Informationen im Zusammenhang mit dem Verfahren zur Ausstellung qualifizierter elektronischer Zertifikate für natürliche Personen, einschließlich des vom ANTRAGSTELLER/TEILNEHMER ordnungsgemäß abgeschlossenen Vertrags und der während des gesamten Ausstellungsvorgangs erzeugten Protokolle, werden von SIGNICAT SLU während der Laufzeit des Vertragsverhältnisses, solange keine Löschung verlangt wird, sowie während der Verjährungsfrist möglicher Klagen oder möglicher Ansprüche seitens öffentlicher Stellen aufbewahrt.

In diesem Sinne beträgt die maximale Aufbewahrungsfrist für die relevanten Informationen im Zusammenhang mit dem Verfahren zur Ausstellung qualifizierter Zertifikate 15 Jahre ab dem Widerruf oder Ablauf des Zertifikats, sofern gesetzlich nichts anderes bestimmt ist. Nach Beendigung des Vertragsverhältnisses werden die Daten des ANTRAGSTELLERS/TEILNEHMERS gemäß den Bestimmungen der anwendbaren Vorschriften ordnungsgemäß gesperrt.

5. GEMEINSAME BESTIMMUNGEN

5.1. ERFÜLLUNGORT

Erfüllungsort für die Pflichten von SIGNICAT SLU in Bezug auf digitale Zertifizierungsdienste und gegebenenfalls Softwarenutzungslizenzen ist der eingetragene Sitz von SIGNICAT SLU.

5.2. SALVATORISCHE KLAUSEL

Die Klauseln dieses Dokuments sind voneinander unabhängig; sollte eine Klausel für ungültig oder nicht durchsetzbar erachtet werden, bleiben die übrigen Klauseln daher anwendbar, sofern die Parteien nicht ausdrücklich etwas anderes vereinbart haben.

5.3. ANWENDBARES RECHT UND GERICHTSSTAND.

Die Beziehungen zu SIGNICAT SLU unterliegen den Bestimmungen der Verordnung (EU) Nr. 910/2014 (eIDAS), spanischem Recht und insbesondere allen Bestimmungen, die sich aus ihrer Compliance-Richtlinie ergeben.

Zuständig ist das Gericht, das im Gesetz 1/2000 vom 7. Januar über den Zivilprozess bestimmt ist, außer wenn der ANTRAGSTELLER/TEILNEHMER als Verbraucher gilt; in diesem Fall unterwirft sich SIGNICAT SLU der gesetzlich zuständigen Gerichtsbarkeit.