BEDINGUNGEN FÜR DAS VIDEOIDENTIFIZIERUNGSVERFAHREN UND DIE AUSSTELLUNG VON KURZZEITZERTIFIKATEN

QES ONCE

SIGNICAT, S.L.U. (früher bekannt als "Electronic Identification S.L."), mit eingetragener Anschrift in der Avenida Ciudad de Barcelona 81, 4ª Planta, eingetragen im öffentlichen Handelsregister am 13. März, 2013, mit der ID-Nummer B-86681533, (im folgenden "SIGNICAT SLU"), ist ein qualifizierter Anbieter von Vertrauensdiensten, der im Einklang mit den Bestimmungen der Verordnung (EU) 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli handelt, 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionssysteme im Binnenmarkt und damit zur Aufhebung der Richtlinie 1999/93/EG sowie der technischen ETSI-Normen für die Ausstellung und Verwaltung von qualifizierten Zertifikaten, insbesondere EN 319 411-1 und EN 319 411-2, tätig ist, um die Einhaltung der rechtlichen Anforderungen und die internationale Anerkennung seiner Dienste zu erleichtern.

Andererseits der ABONNENT oder ANTRAGSTELLER, dessen Identifizierungsdaten für die Zwecke dieses Abkommens in dem verwendeten Identifizierungsdokument enthalten sind und in dem Video, das als Ergebnis des Videoidentifizierungs- und Zertifikatsausstellungsprozesses erstellt wird.

ZWECK

Zweck dieses Dokuments ist es, den Antragsteller/Abonnenten in klarer und verständlicher Form über die aktuellen *"Bedingungen für den Video-Identifizierungsprozess und die Ausstellung von Kurzzeitzertifikaten" zu* informieren und die Dienste gemäß den in diesem Dokument, in der *Erklärung zu den Zertifizierungspraktiken*, in der *eIDAS-Verordnung* und in den *gegebenenfalls anwendbaren lokalen Vorschriften* festgelegten Bedingungen zu regeln.

Dieser vorherige Identifizierungsprozess ist notwendig, um die Identität des Antragstellers/Abonnenten zu bestätigen, der bei SIGNICAT SLU die Ausstellung eines qualifizierten Zertifikats der elektronischen Signatur einer natürlichen Person von kurzer Dauer ("Zertifizierungsdienste") beantragt, ein Zertifikat, das den Bedingungen des elektronischen Zertifizierungsdienstes unterliegt, der von SIGNICAT SLU als qualifiziertem Vertrauensdiensteanbieter bereitgestellt wird (siehe unten).

Der ABONNENT erkennt an und geht davon aus, dass das Lesen und Akzeptieren dieses Dokuments durch Ankreuzen der Kästchen als einfache elektronische Unterschrift gilt.

1 DEFINITIONEN

ZERTIFIZIERUNGSBEHÖRDE (CA): vertrauenswürdige Einrichtung des Absenders und des Empfängers der Nachricht. Dieses Vertrauen beider in eine "vertrauenswürdige dritte Partei" ermöglicht es beiden, ihrerseits den von der Zertifizierungsstelle unterzeichneten Dokumenten zu vertrauen, insbesondere den Dokumenten, die jeden öffentlichen Schlüssel mit dem entsprechenden Eigentümer identifizieren und als Zertifikate bezeichnet werden. Bei der Bereitstellung des vom Abonnenten angeforderten Dienstes fungiert SIGNICAT SLU als Zertifizierungsstelle, die einen bestimmten öffentlichen Schlüssel durch die Ausstellung eines Zertifikats mit einem bestimmten Abonnenten verbindet.

REGISTRIERUNGSBEHÖRDE (REGISTRATION AUTHORITY, RA): Einrichtung, die neben anderen Funktionen den Antragsteller eines Zertifikats und gegebenenfalls die anderen mit dem Zertifikat verbundenen Umstände gemäß den Bestimmungen von Abschnitt 1.3.2 eindeutig identifiziert. Die Registrierungsstelle stellt der Zertifizierungsstelle die verifizierten Angaben des Antragstellers zur Verfügung, damit die Zertifizierungsstelle das entsprechende Zertifikat ausstellen kann. Einige oder alle Funktionen der RA können entweder direkt von SIGNICAT SLU oder von einer von SIGNICAT SLU autorisierten Stelle übernommen werden.

ELEKTRONISCHE UNTERSCHRIFTENBESCHEINIGUNG: eine elektronische Erklärung, die die Validierungsdaten einer Unterschrift mit einer natürlichen Person verbindet und zumindest den Namen oder das Pseudonym dieser Person bestätigt.

QUALIFIZIERTES ELEKTRONISCHES SIGNATURZERTIFIKAT: ein elektronisches Signaturzertifikat, das von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und die in Anhang I der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 (eIDAS-Verordnung) festgelegten Anforderungen erfüllt und die höchsten rechtlichen Garantien in Bezug auf die Identifizierung des Unterzeichners und seine eindeutige Verknüpfung mit der Signatur sowie die Integrität und Unleugbarkeit der mit der Signatur verknüpften Daten bietet.

BERICHT ZUR ZERTIFIZIERUNGSPRAXIS ("CPS"): Dies ist ein von einer Zertifizierungsstelle erstelltes Dokument, das die Erbringung von Zertifizierungsdiensten durch diese Zertifizierungsstelle in ihrer Eigenschaft als Zertifizierungsdiensteanbieter, in diesem Fall SIGNICAT SLU, beinhaltet oder regelt. Es regelt unter anderem die Verwaltung der Signaturerstellungs- und -prüfdaten und der Zertifikate, die Bedingungen für die Beantragung, Ausstellung, Verwendung, Aussetzung und Beendigung der Gültigkeit der Zertifikate.

QUALIFIZIERTE ELEKTRONISCHE SIGNATUR: eine fortgeschrittene elektronische Signatur, die mit Hilfe einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wird und auf einem qualifizierten elektronischen Signaturzertifikat beruht. Die Gültigkeit der Unterschrift ist iuris tantum, da es sich um eine qualifizierte Unterschrift handelt, die Beweislast liegt bei der Person, die die Unterschrift als gültig ablehnt.

QUALIFIZIERTER VERTRAUENSDIENSTLEISTER: Ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und von der Aufsichtsbehörde eine Qualifikation erhalten hat.

ABONNENT ODER ANTRAGSTELLER: die in der Kopfzeile angegebene natürliche Person, die die SIGNICAT SLU-Zertifizierungsdienste in Anspruch nimmt und die vor der Ausstellung des qualifizierten Zertifikats den SIGNICAT SLU-Videoidentifizierungsprozess beantragt und erfolgreich abgeschlossen hat.

2 BEDINGUNGEN FÜR DAS VIDEO-IDENTIFIZIERUNGSVERFAHREN

Der Identifizierungsprozess des Antragstellers für die von SIGNICAT SLU für die Ausstellung elektronischer Zertifikate bereitgestellten Identifizierungsdienste wird gemäß Artikel 24.1 eIDAS auf eine der folgenden Arten durchgeführt:

a) in Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person, wozu sich der Antragsteller an die SIGNICAT SLU-Büros in der Av. De la Ciudad de Barcelona, 81, 4, 28007 Madrid, da es keine beauftragten Registrierungsbehörden gibt.

- 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 sichergestellt wurde, und in Übereinstimmung mit dem Video-Identifizierungsverfahren, auf das in diesem Dokument und im Bericht zur Zertifizierungspraxis wird, das über den folgenden Link zugänglich ist: https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

b) mittels eines qualifizierten elektronischen Signaturzertifikats oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a oder b ausgestellt wurde

c) verwendung anderer national anerkannter Identifizierungsmethoden, die eine gleichwertige Sicherheit wie die physische Anwesenheit bieten. Die Gleichwertigkeit der Sicherheit ist von einer Konformitätsbewertungsstelle zu bestätigen.

2.1 IDENTITÄTSÜBERPRÜFUNG AUF ELEKTRONISCHEM WEGE UND BESCHREIBUNG DES VIDEO-IDENTIFIZIERUNGSVERFAHRENS

Der Video-Identifizierungsprozess (im Folgenden als "Video-Identifizierungsprozess" oder "Prozess" bezeichnet) ist eine Methode der unbeaufsichtigten Video-Identitätsüberprüfung in Echtzeit, , die durch SIGNICAT SLUs proprietäre Suite von Softwarebibliotheken, REST-Anwendungsschnittstellen und Webanwendungen (die "Anwendung") bereitgestellt wird, die den gesamten Prozess der Registrierung einer Person implementiert, unterstützt und aufzeichnet und die Validierung von Identitätsdokumenten aus der Ferne per Videoaufzeichnung ermöglicht. Dieses Video validiert das Identitätsdokument in Echtzeit und auf automatisierte Weise (ca. 10-20 Sekunden), was von SIGNICAT SLU durch seine qualifizierten menschlichen Agenten durchgeführt wird, die als Verifizierungsoperatoren, die als Registrierungsbehörde fungieren, für die Akkreditierung der Identität zuständig sind.

Allgemeine Informationen über den Video-Identifizierungsprozess

Der Antragsteller öffnet die Anwendung und die Schnittstelle und wird vor der Einleitung der Maßnahmen zur Überprüfung der Identität aufgefordert, dieses Dokument zu lesen und zu akzeptieren und seine freie Zustimmung zur Verarbeitung biometrischer Daten zu erteilen, die für die Durchführung der Video-Identifizierung erforderlich sind. Zu diesem Zweck stellt SIGNICAT SLU dem Antragsteller zuvor die Datenschutzerklärung zur Verfügung, in der die Verarbeitung personenbezogener Daten während des Prozesses unter Einhaltung der Datenschutzbestimmungen beschrieben wird.

Erteilt der Antragsteller diese Zustimmung nicht, kann das Verfahren nicht fortgesetzt werden, und der Antragsteller muss gemäß Artikel 24 Absatz 1 der eIDAS-Verordnung auf eine der in Abschnitt 1 dieses Dokuments genannten Alternativen zur Identifizierung zurückgreifen.

Anschließend wird sie dem Antragsteller angezeigt:

- Eine Darstellung des zu unterzeichnenden Vertrags
- Eine Aufforderung zum Handeln, um dieses Dokument zu akzeptieren
- Eine Download-Option, die es dem Benutzer ermöglicht, das Dokument zu speichern.

Sollte der Anmelder das Dokument nicht einsehen und diese Zustimmung nicht erteilen, kann das Verfahren nicht fortgesetzt werden.

Schließlich wird der Abonnent vor Beginn des Video-Identifizierungsprozesses nach einer Telefonnummer gefragt, um ihm ein OTP zu senden.

Mit dieser OTP bestätigt der Abonnent nicht nur die vorliegenden Bedingungen, sondern genehmigt auch die Ausstellung des Zertifikats, das die Daten aus dem Video-Identifizierungsprozess gemäß Artikel 3.3.5 des vorliegenden Dokuments enthält, sowie das Vertragsdokument, das zu Beginn des Prozesses angezeigt wurde und auf das die Signaturerstellungsdaten von SIGNICAT SLU zur Erstellung einer qualifizierten elektronischen Signatur angewendet werden.

Nach Überprüfung dieses OTP wendet SIGNICAT SLU die Signaturerstellungsdaten an, wie in Abschnitt 3.4 vorgesehen und beschrieben.

Sobald der Antragsteller den Prozess gelesen, akzeptiert und seine Zustimmung gegeben hat, wird der Antragsteller die Video-Identifizierung durchführen, die notwendig ist, damit SIGNICAT SLU mit der Ausstellung des Zertifikats für qualifizierte natürliche Personen fortfahren kann.

Der Antragsteller wird während des Video-Identifizierungsprozesses jederzeit durch Sprache und Text geführt, und mit Hilfe der Anwendung wird eine automatische Kontrolle der Elemente der Umgebung (Lichtverhältnisse, Netzwerk, Qualität der Kamera) durchgeführt, um eine optimale Aufnahme der Video-Identifizierung und ihrer Beweise zu erhalten.

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

Im ersten Schritt des Verfahrens wird der Antragsteller darauf hingewiesen, dass er das zu verwendende Ausweisdokument vorlegen muss, damit ein Bildvergleich mit den Originaldokumenten mittels Mustervergleichstechnologie durchgeführt werden kann, um die Echtheit des Dokuments zu überprüfen und die Datenextraktion (OCR) der MRZ oder anderer Teile des Dokuments sowie die Möglichkeit zum Abruf der Berechtigungsnachweise in Echtzeit durchzuführen.

Daher wird die Vorderseite des Ausweises, den der Antragsteller während des Verfahrens verwendet, erfasst. Zu diesem Zweck wird der Antragsteller gebeten, die Vorderseite seines Dokuments zu zeigen und das Bild in das angezeigte Feld einzupassen.

Wenn die Erfassung abgeschlossen ist, wird eine Bestätigungsmeldung angezeigt und der nächste Teil des Prozesses wird fortgesetzt.

Der nächste Schritt besteht darin, die Rückseite des Dokuments zu erfassen. Der Antragsteller wird gebeten, die Rückseite seines Dokuments zu zeigen und das Bild in das angezeigte Feld einzupassen.

Wenn die Erfassung abgeschlossen ist, wird eine Bestätigungsmeldung angezeigt und der nächste Teil des Prozesses wird fortgesetzt.

Die biometrischen Daten des Antragstellers werden dann erfasst, um in Echtzeit einen Vergleich mit dem Bild des Ausweisdokuments für einen Gesichtserkennungsprozess auf der Grundlage einer automatischen biometrischen Auswertung durchzuführen. Zu diesem Zweck wird der Antragsteller aufgefordert, sein Gesicht zu zeigen und das Bild in das auf dem Bildschirm angezeigte Feld einzupassen.

Nach der Erfassung der biometrischen Daten wird der Antragsteller als Lebensbeweis aufgefordert, eine Gesichtsbewegung vor der Kamera auszuführen, und wenn alles korrekt ist, wird eine Konformitätsmeldung angezeigt, und der nächste Teil des Prozesses wird fortgesetzt.

Wenn der gesamte Prozess erfolgreich ist, wird der Antragsteller darüber informiert, dass der Video-Identifizierungsprozess abgeschlossen ist und dass die während des Prozesses generierten Beweise mit Hilfe des Verifizierungs-Tools der Registrierungsbehörde überprüft und validiert werden, um den Prozess durch eine qualifizierte Person, die zuvor durch eine spezielle Schulung geschult wurde, zu überprüfen.

An diesem Punkt stellt die Anwendung eine Verbindung zu einem qualifizierten menschlichen Agenten her, der für die Überprüfung der Identität des Antragstellers zuständig ist und die asynchrone Überprüfung des aufgezeichneten Videos sowie der übrigen während des Prozesses gewonnenen Beweise und Elemente anfordert. Die durchschnittliche Überprüfungszeit für einen Agenten beträgt etwa drei Minuten.

Sicherheitselemente des Video-Identifizierungsprozesses und Validierung durch qualifizierte menschliche Mitarbeiter

Für die asynchrone Überprüfung durch einen qualifizierten menschlichen Beauftragten gibt es ein Sicherheitsprotokoll, das auf den bewährten Praktiken der EU basiert und durch das Tool unterstützt wird, das dem qualifizierten menschlichen Beauftragten zur Verfügung gestellt wird und in dem die während des Prozesses erhaltenen Nachweise sowie die Kennzeichnungen oder Benachrichtigungen über die nicht erhaltenen Nachweise angezeigt werden.

Die Aufzeichnung des Videos, die Anfrage zur Überprüfung der Video-Identifizierung sowie das Urteil des qualifizierten Beauftragten werden in der Anwendung nachverfolgt, und jede Aufzeichnung wird mit einem Zeitstempel versehen, um ihre Konsistenz und Integrität zu gewährleisten.

Daher gewährleistet der Prozess die Überwachungskette der Verifizierung von den durch den Prozess gesammelten Beweisen bis hin zu den Spuren, die die Identifizierung mit dem qualifizierten menschlichen Vertreter der Registrierungsbehörde verbinden. Das Ergebnis ist eine überprüfte Identität mit der gleichen technischen Sicherheit wie bei der physischen Anwesenheit des Antragstellers.

Sobald die Identität durch den qualifizierten menschlichen Agenten positiv bestätigt wurde, ist die Identität des Antragstellers akkreditiert und der Antragsteller kann weiterhin den SIGNICAT SLU-Zertifizierungsdienst in Anspruch nehmen, der es ihm ermöglicht, mit dem Prozess der Ausstellung des Zertifikats für qualifizierte natürliche Personen und der Unterzeichnung der elektronischen Dokumente fortzufahren.

Fällt das Ergebnis des Verfahrens negativ aus, kann das Verfahren zur Ausstellung qualifizierter Zertifikate nicht fortgesetzt werden, und der Antragsteller muss sich persönlich in den Räumlichkeiten von SIGNICAT SLU einfinden, um seine Identität zu überprüfen.

2.2 VERPFLICHTUNGEN DES TEILNEHMERS IN BEZUG AUF DEN VIDEOIDENTIFIZIERUNGSPROZESS

Der ABONNENT verpflichtet sich, während des gesamten Prozesses:

- Benutzen Sie den Dienst in Übereinstimmung mit den Bestimmungen dieses Dokuments, des CPS, den besonderen Bedingungen, die anwendbar sein können, und mit allen anderen Anweisungen, Handbüchern oder Verfahren, die von SIGNICAT SLU bereitgestellt werden.

  Dass es sich bei dem während des Prozesses verwendeten Dokument um ein authentisches, rechtsgültiges Dokument handelt und dass darüber hinaus:

  - Es handelt sich nicht um eine Fotokopie oder eine gedruckte Karte.
  - Sie liegt nicht in digitaler Form vor (Handy, Tablet oder Computer).
  - Es befindet sich nicht in einer Hülle.
  - Es ist nicht beschädigt und vollständig, d. h. alle Sicherheitselemente sind in dem Dokument enthalten.

- Dass während des Prozesses und der Aufzeichnung des Videos, um Ablehnung zu vermeiden:

  - Die Lichtverhältnisse im Video müssen es ermöglichen, das Gesicht der identifizierten Person und das Dokument deutlich zu erkennen.
  - Der Videostream muss konstant sein, ohne Unterbrechungen oder Verzögerungen.
  - Eine lebende Person muss den Ausweis vorzeigen.

- Wenn eine andere Person als die zu identifizierende Person den gesamten Prozess durchführt, wird die Identifizierung als unecht zurückgewiesen.
- Wenn eine andere Person in dem Video anwesend ist, die Person aber eindeutig nicht zur Identifizierung zwingt, kann die Identifizierung gültig sein, wie in dem Fall, dass eine bestimmte Person einer behinderten Person bei der Identifizierung hilft.
- Es muss möglich sein, alle Teile des Dokuments, die Vorderseite, die Rückseite und das Gesicht der Person deutlich zu erkennen.
- Der ABONNENT darf nicht schlafen oder Anzeichen zeigen, die auf Drogen- oder Alkoholeinfluss schließen lassen.

2.3 AUSSTELLUNG, LIEFERUNG UND ANNAHME DES ZERTIFIKATS

ZERTIFIZIERUNGSANFRAGE UND SCHLÜSSELGENERIERUNG DURCH SIGNICAT SLU IM NAMEN DES TEILNEHMERS

Sobald der Video-Identifizierungsprozess abgeschlossen ist, ermächtigt der ABONNENT SIGNICAT SLU, die öffentlichen und privaten Schlüssel in seinem Namen zu generieren und zu verwalten, so dass SIGNICAT SLU die Ausstellung des qualifizierten Kurzzeitzertifikats einer natürlichen Person vornehmen und in seinem Namen die elektronischen Dokumente signieren kann, die über SIGNICAT SLU oder Dritte öffentlicher oder privater Natur, mit denen SIGNICAT SLU bestimmte vertragliche Vereinbarungen unterhält, bereitgestellt werden.

WAHRHEITSGEHALT DER INFORMATIONEN

Der ABONNENT ist dafür verantwortlich, dass alle Informationen, die er SIGNICAT SLU entweder direkt oder über das bei der Ausstellung des Zertifikats verwendete Ausweisdokument zur Verfügung stellt, richtig und für den Zweck des Zertifikats vollständig sind und dass sie jederzeit auf dem neuesten Stand sind, wofür er garantiert, ein rechtmäßiges und gültiges Ausweisdokument zu verwenden, das weder vom ABONNENTEN noch von Dritten verändert und/oder modifiziert wurde.

ERTEILUNG DES ZERTIFIKATS

Für die Ausstellung des Zertifikats verwendet SIGNICAT SLU die Daten des Identitätsdokuments, die der ABONNENT während des Video-Identifizierungsprozesses angegeben hat. Diese Informationen werden von SIGNICAT SLU extrahiert und direkt in das elektronische Zertifikat aufgenommen, um die Identität des ABONNENTEN mit dem elektronischen Zertifikat zu verbinden.

AUSHÄNDIGUNG DES ZERTIFIKATS

Bei der Ausstellung des Kurzzeitzertifikats erfolgt keine konkrete Auslieferung des Zertifikats an den ABONNENTEN. SIGNICAT SLU verwaltet es in seiner Eigenschaft als qualifizierter Vertrauensdiensteanbieter, so dass der ABONNENT es für die elektronische Signatur von Dokumenten verwenden kann.

i. DIE ANNAHME DER AUSSTELLUNG DES ZERTIFIKATS UND DIE RATIFIZIERUNG DIESER BEDINGUNGEN UND KONDITIONEN.

Der ABONNENT akzeptiert mit der Eingabe seiner Telefonnummer und der Bestätigung des OTP gemäß Artikel 3.1.1 die Ausstellung des Zertifikats und die darin enthaltenen Daten aus dem Video-Identifizierungsverfahren und bestätigt die vorliegenden Allgemeinen Geschäftsbedingungen.

2.4 SERVER-SIGNATURDIENST

Nach Abschluss des Identifizierungsvorgangs, der Eingabe des OTP und der Überprüfung der Identität durch die Prüfstelle wird die Identität des Unterzeichners garantiert, und dem ABONNENTEN werden die folgenden Dokumente für die Fortsetzung der elektronischen Unterschrift vorgelegt:

Sobald der Identifizierungsprozess abgeschlossen ist und die Identität durch den Verifizierungsagenten validiert wurde, wird die Identität des Unterzeichners garantiert und SIGNICAT SLU als qualifizierter Vertrauensdiensteanbieter wendet auf das zu Beginn des Prozesses vom ABONNENTEN akzeptierte Dokument (gemäß Klausel 3.1.1) die Signaturerstellungsdaten des Benutzers/Abonnenten auf dem angezeigten und durch die Einführung des OTP akzeptierten Dokument an und gewährleistet so seine ausschließliche Kontrolle.

SIGNICAT SLU gewährt dem ABONNENTEN auf nicht ausschließlicher und nicht übertragbarer Basis eine Lizenz zur Nutzung von Kopien der kryptographischen sicheren Gerätesoftware von SIGNICAT SLU für den Betrieb der Signatureinheit, soweit anwendbar, sowie für die Erstellung der elektronischen Signatur, des Zertifikats und der übrigen kryptographischen Dienste durch die Unterzeichner.

Der ABONNENT darf Kopien der Software nur zu Archivierungs- oder Sicherungszwecken anfertigen.

Für den Fall, dass eine andere Person als SIGNICAT SLU Änderungen an der zur Verfügung gestellten Software vornimmt, werden alle Garantien in Bezug auf die Software sofort aufgehoben.

3 ALLGEMEINE BEDINGUNGEN FÜR DEN VERTRAUENSDIENSTE

3.1 ALLGEMEINE BEDINGUNGEN FÜR DEN VIDEOIDENTIFIZIERUNGSDIENST

- Aufbewahrungsfrist für Informationen

Alle Informationen im Zusammenhang mit dem Video-Identifizierungsverfahren und der Ausstellung qualifizierter elektronischer Zertifikate für natürliche Personen, einschließlich biometrischer Daten, werden von SIGNICAT SLU während der Gültigkeitsdauer des Vertragsverhältnisses aufbewahrt, solange ihre Löschung nicht verlangt wird und während der Verjährungsfrist von Klagen, die erhoben werden könnten, oder von Ansprüchen, die im Namen offizieller Stellen eingehen könnten.

Die maximale Aufbewahrungsfrist der relevanten Informationen im Zusammenhang mit dem Prozess der Video-Identifizierung und der Ausstellung von qualifizierten Zertifikaten, d.h.

eine Kopie der Videoaufzeichnung, Fotos oder Screenshots des Antragstellers und des verwendeten Identitätsdokuments, das automatische Ergebnis der von der SIGNICAT SLU-Anwendung durchgeführten Überprüfung sowie die von den qualifizierten Mitarbeitern für die Überprüfung der menschlichen Identität vorgenommene Bewertung und Beobachtungen zusammen mit ihrer Entscheidung über die Genehmigung oder Ablehnung des Ausweises, beträgt 15 Jahre ab dem Zeitpunkt der Ausstellung des Zertifikats, sofern gesetzlich nicht anders vorgeschrieben. Nach Beendigung des Vertragsverhältnisses werden die Daten des ABONNENTEN in Übereinstimmung mit den geltenden Vorschriften ordnungsgemäß gesperrt.

Darüber hinaus wird berichtet, dass alle Belege für unvollständige Identifizierungsprozesse, die wegen des Verdachts auf Betrugsversuche nicht abgeschlossen wurden, für einen Zeitraum von fünf Jahren nach Abschluss des Prozesses unter Angabe des Grundes für den Nichtabschluss gemäß der zu diesem Zweck festgelegten Politik aufbewahrt werden.

- Haftungsbeschränkung im Zusammenhang mit dem Video-Identifizierungsverfahren

Qualität des Verfahrens: SIGNICAT SLU garantiert die angemessene Leistung der in diesem Dokument beschriebenen Video-Identifizierungsdienste unter der Voraussetzung, dass die dem ABONNENTEN zur Verfügung gestellten Mittel ordnungsgemäß und in Übereinstimmung mit den Anweisungen von SIGNICAT SLU verwendet werden.

Der Zugang zu den Video-Identifizierungsdiensten und deren Nutzung verpflichten SIGNICAT SLU nicht dazu, das Nichtvorhandensein von Viren, Würmern oder anderen schädlichen Computerelementen zu kontrollieren. Es obliegt dem ABONNENTEN als Nutzer, jederzeit über angemessene Instrumente zur Erkennung und Desinfektion von schädlichen Computerprogrammen zu verfügen. SIGNICAT SLU kann nicht für Schäden haftbar gemacht werden, die während des Video-Identifizierungsprozesses am Computer des ABONNENTEN oder bei Dritten entstehen.

Verfügbarkeit des Prozesses: Das Funktionieren des Video-Identifizierungsprozesses kann von einer korrekten Konfiguration des Geräts abhängen, von dem aus der Benutzer auf den Video-Identifizierungsprozess zugreift und ihn startet. Der Benutzer muss daher die angebotenen Anweisungen befolgen und in jedem Fall sowohl die Software- als auch die Hardware-Anforderungen zu jeder Zeit spezifiziert haben.

Ebenso muss für die Durchführung des Video-Identifizierungsverfahrens ein Internetzugang vorhanden sein. Das Funktionieren des Video-Identifizierungsverfahrens kann von der angemessenen Qualität und Geschwindigkeit der Verbindung abhängen, über die der ABONNENT auf die Anwendung zugreift, wofür er allein für die Bereitstellung von Telekommunikationsleitungen, Internet-Abonnements oder -Verbindungen oder anderen technischen Mitteln verantwortlich ist, die für den Zugriff auf Ihre Daten und deren Nutzung erforderlich sind.

SIGNICAT SLU haftet nicht für Schäden, die sich aus der Nichterfüllung oder der mangelhaften Erfüllung der Verpflichtungen des Abonnenten ergeben oder damit zusammenhängen, noch für die falsche Verwendung der Ergebnisse des Prozesses und der Schlüssel, noch für indirekte Schäden, die sich aus der Verwendung des Prozesses oder der von SIGNICAT SLU bereitgestellten Informationen ergeben können.

SIGNICAT SLU kann nicht für Ungenauigkeiten bei der Identifizierung des ABONNENTEN verantwortlich gemacht werden, die sich aus den vom ABONNENTEN während des Prozesses bereitgestellten Informationen ergeben.

SIGNICAT SLU haftet nicht für den korrekten Betrieb mit nicht genehmigten Anwendungen und für Schäden, die dadurch entstehen, dass der ABONNENT die besagten Anwendungen nicht nutzen kann.

3.2 ALLGEMEINE BEDINGUNGEN FÜR DEN VIDEOIDENTIFIZIERUNGSDIENST

- Rechtlicher Rahmen für die Erbringung der Dienstleistung

Die SIGNICAT SLU-Zertifizierungsdienste werden in technischer und betrieblicher Hinsicht durch die Erklärung zu den Zertifizierungspraktiken und die SIGNICAT SLU-Zertifizierungsrichtlinien und ihre späteren Aktualisierungen sowie durch ergänzende Unterlagen geregelt, die dem ABONNENTEN zur Verfügung gestellt werden und von denen er erklärt, dass er sie zum Zeitpunkt der Unterzeichnung dieses Vertrags kennt.

Daher bilden die vorliegenden allgemeinen Bedingungen, die Erklärung zu den Zertifizierungspraktiken und die Zertifizierungsrichtlinien, sofern sie auf das ausgestellte Zertifikat anwendbar sind, den rechtlichen Rahmen, der die Beziehungen zwischen SIGNICAT SLU und dem ABONNENTEN sowohl intern als auch gegenüber Dritten regelt, unbeschadet der Bestimmungen der geltenden Rechtsvorschriften.

Das vorliegende Dokument enthält daher die wichtigsten Aspekte und Anforderungen an die Rechte und Pflichten der Parteien.

Die Erklärung zur Zertifizierungspraxis (Certification Practice Statement, CPS) und die spezifischen Zertifizierungsrichtlinien (Specific Certification Policies, CP) werden durch Verweis in dieses Dokument aufgenommen. Die zuletzt aktualisierte Fassung der CPS ist jederzeit und kostenlos in den folgenden Sprachen über den unten angegebenen Link zugänglich:

- **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 Widersprüchen ist die Bedeutung der in diesem Dokument enthaltenen Begriffe gegenüber den im CPS enthaltenen Begriffen maßgebend.

- Dauer des Vertrags

Dieser Vertrag gilt für die Dauer der Ausstellung und des Ablaufs, die in dem vom Abonnenten bei SIGNICAT SLU beantragten und abgeschlossenen Zertifikat für qualifizierte Einzelpersonen angegeben sind.

- Verpflichtungen zur ordnungsgemäßen Verwendung

Der ABONNENT darf den von SIGNICAT SLU bereitgestellten Zertifizierungsdienst ausschließlich für die im CPS genehmigten Verwendungszwecke nutzen, die dem ABONNENTEN bekannt sind und von ihm akzeptiert werden, nachdem er das Dokument gelesen und die im Prozess enthaltenen Auswahlmöglichkeiten angekreuzt hat.

Der ABONNENT ist verpflichtet, den digitalen Zertifizierungsdienst und jedes andere von SIGNICAT SLU gelieferte technische Element sowie die Zertifikate in Übereinstimmung mit den vorliegenden Bedingungen, dem DPC und den ggf. anwendbaren PCs, den besonderen Bedingungen im Handbuch, soweit anwendbar, und mit jeder anderen Anweisung oder Prozedur, die SIGNICAT SLU dem ABONNENTEN zur Verfügung stellt, sowie in Übereinstimmung mit den ggf. geltenden gesetzlichen Bestimmungen zu nutzen.

Die Beauftragung des Zertifizierungsdienstes mit SIGNICAT SLU erlaubt nur die Verwendung des Zertifikats im Rahmen der offiziellen Tätigkeit des ABONNENTEN, entsprechend dem Zweck des beantragten Zertifikatstyps, d.h. des qualifizierten Zertifikats der elektronischen Signatur einer natürlichen Person von kurzer Dauer. Nach der Ausstellung des Zertifikats darf der ABONNENT das Zertifikat nicht zu kommerziellen Zwecken verwenden, es sei denn, die Parteien haben ausdrücklich etwas anderes vereinbart. Unter kommerzieller Nutzung des Zertifikats ist jede Handlung zu verstehen, mit der der ABONNENT Dritten außerhalb dieses Vertrags entgeltliche oder unentgeltliche Dienste anbietet, die die Nutzung des ausgestellten Zertifikats erfordern.

- Verbotene Transaktionen

Die von SIGNICAT SLU erbrachten digitalen Zertifizierungsdienste sind nicht für die Verwendung oder den Weiterverkauf als Ausrüstungen zur Steuerung von Gefahrensituationen oder für Verwendungszwecke, die fehlerfreie Handlungen erfordern, wie z. B. der Betrieb von Nuklearanlagen, Navigationssystemen oder Luftkommunikation, Flugverkehrskontrollsystemen oder Waffenkontrollsystemen, bei denen ein Fehler unmittelbar zum Tod führen oder zu körperlichen Schäden oder schweren Umweltschäden führen könnte, konzipiert oder zugelassen.

- Pflichten und Verantwortlichkeiten von SIGNICAT SLU

b. In Bezug auf die Erbringung der Dienstleistung als Registrierungsbehörde

SIGNICAT SLU verpflichtet sich, die Daten des Zertifikats und dessen anschließende Ausstellung an den ABONNENTEN zu registrieren, wofür es die von ihm als notwendig erachteten Kontrollen hinsichtlich der Identität und anderer persönlicher und ergänzender Informationen der ABONNENTEN und gegebenenfalls der Unterzeichner selbst durchführen muss.

Diese Überprüfungen müssen die vom ABONNENTEN über den Antragsteller vorgelegten Nachweise und, falls SIGNICAT SLU dies für erforderlich hält, alle anderen vom ABONNENTEN vorgelegten relevanten Dokumente und Informationen umfassen.

Stellt SIGNICAT SLU Fehler in den Daten fest, die in den Zertifikaten enthalten sein müssen oder die diese Daten rechtfertigen, kann SIGNICAT SLU die von ihr als notwendig erachteten Änderungen vornehmen, bevor das Zertifikat ausgestellt wird, oder den Ausstellungsprozess aussetzen und den entsprechenden Vorfall mit dem ABONNENTEN regeln.

Für den Fall, dass SIGNICAT SLU die Daten korrigiert, ohne den entsprechenden Vorfall vorher mit dem ABONNENTEN zu regeln, muss SIGNICAT SLU dem ABONNENTEN die endgültig zertifizierten Daten mitteilen.

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

Die oben genannten Verpflichtungen werden ausgesetzt, wenn der ABONNENT als Registrierungsstelle fungiert und über die technischen Elemente verfügt, die für die Erzeugung von Schlüsseln, die Ausstellung von Zertifikaten und die Aufzeichnung von Unternehmenssignaturgeräten erforderlich sind.

c. Im Zusammenhang mit der Bereitstellung des digitalen Zertifizierungsdienstes

SIGNICAT SLU verpflichtet sich zur Einhaltung der im Gesetz 6/2020 vom 11. November festgelegten Verpflichtungen, das bestimmte Aspekte der elektronischen Vertrauensdienste regelt, und insbesondere zur:

a) Ausstellung, Aushändigung, Verwaltung, Aussetzung, Widerruf und Erneuerung von Zertifikaten gemäß den vom ABONNENTEN erteilten Anweisungen in den Fällen und aus den Gründen, die im SIGNICAT SLU CPS beschrieben sind.

b) Dienstleistungen mit den geeigneten technischen und materiellen Mitteln und mit Personal auszuführen, das die im CPS festgelegten Qualifikations- und einschlägigen Erfahrungsbedingungen erfüllt.

c) Einhaltung der Dienstqualitätsniveaus in Übereinstimmung mit den im CPS festgelegten technischen, betrieblichen und sicherheitstechnischen Aspekten.

d) Übermittelung des Status der Zertifikate an Dritte auf Verlangen gemäß den im CPS für die verschiedenen Zertifikatsüberprüfungsdienste festgelegten Bestimmungen.

e) Qualität des Verfahrens: SIGNICAT SLU garantiert die angemessene Durchführung der in diesem Dokument beschriebenen Zertifizierungsdienste, sofern die dem ABONNENTEN zur Verfügung gestellten Mittel ordnungsgemäß und in Übereinstimmung mit den Anweisungen von SIGNICAT SLU verwendet werden.

f) Der Zugang zu den Zertifizierungsdiensten und deren Nutzung implizieren keine Verpflichtung seitens SIGNICAT SLU, die Abwesenheit von Viren, Würmern oder anderen schädlichen Computerelementen zu kontrollieren. Es obliegt dem ABONNENTEN als Benutzer, jederzeit über angemessene Instrumente zur Erkennung und Desinfektion von schädlichen Computerprogrammen zu verfügen. SIGNICAT SLU kann nicht für Schäden verantwortlich gemacht werden, die während des Video-Identifizierungsprozesses an der Computerausrüstung des ABONNENTEN oder an Dritten entstehen.

g) Verfügbarkeit des Prozesses: Das Funktionieren des Zertifizierungsprozesses kann von einer korrekten Konfiguration des Geräts abhängen, von dem aus der Benutzer auf den Video-Identifizierungsprozess zugreift und ihn startet. Der Benutzer muss daher die angebotenen Anweisungen befolgen und in jedem Fall sowohl die Software- als auch die Hardware-Anforderungen zu jeder Zeit spezifiziert haben.

h) Ebenso muss für die Durchführung des Video-Identifizierungsverfahrens ein Internetzugang vorhanden sein. Das Funktionieren des Video-Identifizierungsverfahrens kann von der angemessenen Qualität und Geschwindigkeit der Verbindung abhängen, über die der ABONNENT auf die Anwendung zugreift, wofür er allein für die Bereitstellung von Telekommunikationsleitungen, Internet-Abonnements oder -Verbindungen oder anderen technischen Mitteln verantwortlich ist, die für den Zugriff auf Ihre Daten und deren Nutzung erforderlich sind.

- Als Anbieter von Zertifizierungsdiensten

SIGNICAT SLU soll:

a) Wahrheitsgemäße Informationen gemäß dem Gesetz 6/2020 vom 11. November, das bestimmte Aspekte elektronischer Vertrauensdienste regelt, und der Verordnung (EU) 910/2014 veröffentlichen.

b) Daten der Signaturerstellung, des Siegels oder der Website-Authentifizierung der natürlichen oder juristischen Person, für die sie ihre Dienste erbracht haben, weder selbst noch durch Dritte aufzubewahren oder zu kopieren, es sei denn, sie werden im Auftrag des Inhabers zum Zweck der Anwendung der privaten Schlüssel für die Signaturerstellung verwaltet, wie vom ABONNENTEN über das OTP-System angegeben, das SIGNICAT SLU dem ABONNENTEN für die Unterzeichnung elektronischer Dokumente zur Verfügung stellt. In diesem Fall werden sie zuverlässige Systeme und Produkte verwenden, einschließlich sicherer elektronischer Kommunikationskanäle, und es werden geeignete technische und organisatorische Verfahren und Mechanismen angewandt, um sicherzustellen, dass die Umgebung zuverlässig ist und unter der ausschließlichen Kontrolle des Zertifikatsinhabers verwendet wird. Darüber hinaus müssen sie die Signatur-, Siegel- oder Authentifizierungserstellungsdaten der Website sichern und vor jeglicher Veränderung, Zerstörung oder unberechtigtem Zugriff schützen sowie ihre ständige Verfügbarkeit gewährleisten.

c) Einen öffentlich zugänglichen Konsultationsdienstes über den Status der Gültigkeit oder des Widerrufs der ausgestellten Zertifikate anbieten.

d) Folgende zusätzliche Verpflichtungen erfüllen:

1. Der Zeitraum, in dem sie die Informationen über die erbrachten Dienstleistungen gemäß Artikel 24.2.h) der Verordnung (EU) 910/2014 aufbewahren müssen, beträgt 15 Jahre nach Ablauf des Zertifikats oder dem Ende der ausgeliehenen Dienstleistung. Falls qualifizierte Zertifikate für elektronische Siegel oder Website-Authentifizierung an juristische Personen ausgestellt werden, zeichnen die Vertrauensdiensteanbieter auch die Informationen auf, die es ermöglichen, die Identität der natürlichen Person zu bestimmen, der die genannten Zertifikate ausgehändigt wurden, um sie in Gerichts- oder Verwaltungsverfahren zu identifizieren.

2. Abschluss einer Haftpflichtversicherung mit einer Mindesthöhe von 1.500.000 Euro ab, es sei denn, der Anbieter gehört zum öffentlichen Sektor. Wenn Sie mehr als eine qualifizierte Dienstleistung erbringen, als in der Verordnung (EU) Nr. 910/2014 vorgesehen ist, wird für jede zusätzliche Art von Dienstleistung ein zusätzlicher Betrag von 500.000 Euro erhoben. Die vorgenannte Bürgschaft kann ganz oder teilweise durch eine Bürgschaft in Form einer Bankgarantie oder einer Kautionsversicherung ersetzt werden, so dass die Summe der Versicherungssummen mit den Bestimmungen des vorherigen Absatzes übereinstimmt. Die in den beiden vorangegangenen Absätzen festgelegten Beträge und die Art der Versicherung und Garantie können durch königlichen Erlass geändert werden.

3. Im Falle der Beendigung seiner Tätigkeit als qualifizierter vertrauensdienstleister die Kunden, für die er die Dienste erbringt, und die Aufsichtsbehörde mindestens zwei Monate vor der tatsächlichen Beendigung der Tätigkeit zu benachrichtigen, und zwar auf eine Weise, die eine wirksame Zustellung und einen wirksamen Empfang gewährleistet, wann immer dies möglich ist. Der Plan des Dienstleisters zur Beendigung der Tätigkeit kann die Übergabe der Klienten an einen anderen qualifizierten Dienstleister vorsehen, sobald nachgewiesen ist, dass kein Widerspruch vorliegt, wobei dieser alle Informationen über die erbrachten Dienstleistungen bis dahin aufbewahren kann. Ebenso unterrichtet er die Aufsichtsbehörde über jeden anderen relevanten Umstand, der die Fortsetzung seiner Tätigkeit verhindern könnte. Insbesondere muss er über die Eröffnung eines gegen ihn laufenden Insolvenzverfahrens informieren, sobald er davon Kenntnis erlangt.

4. Übermittlung des Konformitätsbewertungsberichts an das Ministerium für Wirtschaft und digitale Transformation unter den in Artikel 20.1 der Verordnung (EU) 910/2014 vorgesehenen Bedingungen. Die Nichteinhaltung dieser Verpflichtung führt zum Entzug der Qualifikation des Anbieters und der von ihm erbrachten Dienstleistung sowie zu seiner Streichung von der in Artikel 22 der genannten Verordnung vorgesehenen Vertrauensliste, nachdem der Anbieter aufgefordert wurde, den genannten Verstoß abzustellen.

e) SIGNICAT SLU übernimmt gegenüber Dritten die gesamte Verantwortung für die Handlungen der Personen oder anderen Diensteanbieter, denen sie die Ausführung einzelner oder aller für

die Erbringung elektronischer Vertrauensdienste erforderlichen Funktionen übertragen, einschließlich der Identitätsüberprüfung vor der Ausstellung eines qualifizierten Zertifikats.

- GARANTIEN FÜR ZERTIFIZIERUNGSDIENSTE

SIGNICAT SLU-Garantie für digitale Zertifizierungsdienste

SIGNICAT SLU garantiert, dass der private Schlüssel der Zertifizierungsstelle, der für die Ausstellung von Zertifikaten verwendet wird, nicht kompromittiert wurde, es sei denn, die Zertifizierungsstelle hat in Übereinstimmung mit dem CPS etwas anderes mitgeteilt.

SIGNICAT SLU garantiert dem ABONNENTEN zum Zeitpunkt der Ausstellung des Zertifikats nur, dass:

a) Gegebenenfalls werden die Zertifikate qualifiziert und funktionieren in einer sicheren Signaturerstellungseinheit gemäß den Bestimmungen des Gesetzes 6/2020 vom 11. November, das bestimmte Aspekte der elektronischen Vertrauensdienste regelt.

b) SIGNICAT SLU weder falsche oder fehlerhafte Angaben in die Informationen auf den Bescheinigungen aufgenommen hat, noch es versäumt hat, die vom ABONNENTEN zur Verfügung gestellten und überprüften Informationen aufzunehmen.

c) Alle Zertifikate erfüllen die formalen und inhaltlichen Anforderungen der SIGNICAT SLU CPS und PC.

d) SIGNICAT SLU hat den im CPS beschriebenen Verfahren entsprochen.

SIGNICAT SLU wendet angemessene Sorgfalt an, um sicherzustellen, dass jedes Produkt, das im Rahmen der Erbringung seiner Dienstleistungen geliefert wird, frei von Computerviren, Würmern und anderen illegalen Codes ist, und ist verpflichtet, den ABONNENTEN über jeden Virus, Wurm oder anderen illegalen Code, der später in einem Produkt entdeckt wird, zu informieren.

- AUSSCHLUSS VON GARANTIEN

SIGNICAT SLU übernimmt keine Garantie für Software, die vom ABONNENTEN oder dem Unterzeichner oder einer anderen Person verwendet wird, um eine digitale Signatur oder ein digitales Zertifikat, das von SIGNICAT SLU ausgestellt wurde, zu erzeugen, zu überprüfen oder anderweitig zu verwenden, es sei denn, es liegt eine gegenteilige schriftliche Erklärung von SIGNICAT SLU vor.

- HAFTUNGSBESCHRÄNKUNGEN ALS ANBIETER VON ELEKTRONISCHEN VERTRAUENSDIENSTEN

SIGNICAT SLU haftet im Rahmen des geltenden Rechts nicht für Schäden und Verluste, die der Person, für die es seine Dienste erbracht hat, oder Dritten in gutem Glauben zugefügt werden, wenn dies in einem der in der Verordnung (EU) 910/2014 vorgesehenen Fälle oder in den folgenden Fällen geschieht:

a) Das Versäumnis, dem Vertrauensdiensteanbieter wahrheitsgemäße, vollständige und genaue Informationen für die Erbringung des Vertrauensdienstes zu übermitteln, insbesondere über die Daten, die in das elektronische Zertifikat aufgenommen werden müssen oder die für seine

Ausstellung oder für das Erlöschen oder die Aussetzung seiner Gültigkeit erforderlich sind, wenn der Diensteanbieter die Unrichtigkeit dieser Informationen nicht mit der gebotenen Sorgfalt festgestellt hat.

b) Das Fehlen einer unverzüglichen Mitteilung an SIGNICAT SLU über jede Änderung der Umstände, die sich auf die Erbringung des Vertrauensdienstes auswirken, insbesondere derjenigen, die sich in der elektronischen Bescheinigung widerspiegeln.

c) Nachlässigkeit bei der Aufbewahrung der Signatur, des Siegels oder der Authentifizierungsdaten der Website, bei der Sicherstellung ihrer Vertraulichkeit und beim Schutz jedes Zugangs oder jeder Offenlegung dieser Daten oder gegebenenfalls der Mittel, die den Zugang zu ihnen ermöglichen.

d) Nicht die Aussetzung oder den Widerruf des elektronischen Zertifikats zu beantragen, wenn Zweifel an der Wahrung der Vertraulichkeit der Signatur, des Siegels oder der Website-Authentifizierungsdaten oder gegebenenfalls der Mittel, die den Zugang zu diesen Daten ermöglichen, bestehen.

e) Die Signatur-, Siegel- oder Authentifizierungserstellungsdaten der Website zu verwenden, wenn die Gültigkeitsdauer des elektronischen Zertifikats abgelaufen ist oder der Vertrauensdiensteanbieter Sie über die Beendigung oder Aussetzung der Gültigkeit benachrichtigt.

SIGNICAT SLU kann auch nicht für Schäden haftbar gemacht werden, wenn der Empfänger fahrlässig handelt.

Es wird davon ausgegangen, dass der Empfänger fahrlässig handelt, wenn er die Aussetzung oder den Verlust der Gültigkeit des elektronischen Zertifikats nicht berücksichtigt oder die elektronische Signatur oder das Siegel nicht überprüft.

SIGNICAT SLU haftet nicht für Schäden im Falle der Unrichtigkeit der in der elektronischen Bescheinigung enthaltenen Daten, wenn diese durch ein öffentliches oder amtliches Dokument beglaubigt oder in einem öffentlichen Register eingetragen wurden, wenn dies erforderlich ist.

- TEILNEHMERHAFTUNG

Der ABONNENT muss sich gegenüber jeder Person für die Verletzung seiner Pflichten verantworten, insbesondere in Bezug auf die Identifizierungstätigkeit oder gegebenenfalls gegenüber der Registrierungsbehörde gemäß den vorliegenden Bestimmungen und Bedingungen.

Der ABONNENT ist für alle elektronischen Mitteilungen verantwortlich, die durch eine mit seinem privaten Schlüssel erzeugte digitale Signatur authentifiziert werden, wenn das Zertifikat durch die von SIGNICAT SLU festgelegten Mechanismen und Bedingungen gültig überprüft wurde.

Solange die in Artikel 5 dieses Dokuments vorgesehene Mitteilung nicht erfolgt ist, bleibt die Verantwortung für die unbefugte und/oder unsachgemäße Verwendung der Zertifikate beim ABONNENTEN.

- EIGNUNG VON PRODUKTEN, DIE EINE IDENTIFIZIERUNG, EINE ELEKTRONISCHE SIGNATUR ODER EINE VERSCHLÜSSELUNG VERWENDEN

SIGNICAT SLU haftet nicht für die Angemessenheit der auf dem Markt vorhandenen Produkte und Dienstleistungen im Zusammenhang mit digitaler Zertifizierung, Identifizierung, elektronischer Signatur oder Verschlüsselung, die in den Computeranwendungen des ABONNENTEN verwendet werden, es sei denn, SIGNICAT SLU stellt sie zur Verfügung. In diesem Fall gelten für die Parteien die entsprechenden Benutzungsbedingungen.

- EIGENTUM AN ZERTIFIKATEN UND SIGNIERGERÄT

Die gelieferten Zertifikate und Signiergeräte bleiben Eigentum des ABONNENTEN.

- BEENDIGUNG

Die Kündigung erfolgt in den folgenden Fällen:

a) Aufgrund eines Verstoßes der anderen Partei gegen eine ihrer Verpflichtungen, wenn dieser Verstoß nicht behoben wurde:

b) Innerhalb von dreißig Tagen nach Erhalt der Mitteilung durch die Partei, die ihren Verpflichtungen nicht nachgekommen ist.

c) Unverzüglich, wenn die Verletzung die Sicherheit der Dienste gefährdet.

d) Aufgrund des Zusammentreffens anderer Gründe für eine vorzeitige Auflösung, die in den geltenden Rechtsvorschriften und insbesondere in den geltenden Rechtsvorschriften über die digitale Zertifizierung elektronischer Signaturen festgelegt sind.

- VERTRAULICHKEITSRICHTLINIEN

SIGNICAT SLU kann keine vertraulichen Informationen über Zertifikate offenlegen und kann auch nicht dazu gezwungen werden, diese offenzulegen, ohne dass ein spezieller vorheriger Antrag gestellt wurde:

a) Von der Person, gegenüber der SIGNICAT SLU zur Geheimhaltung der Informationen verpflichtet ist, oder

b) Einer gerichtlichen, behördlichen oder einer anderen möglichen Anordnung nach geltendem Recht.

Der ABONNENT akzeptiert jedoch, dass bestimmte persönliche und sonstige Informationen, die in der Zertifikatsanforderung angegeben werden, in seine Zertifikate und in den Mechanismus zur Überprüfung des Zertifikatsstatus aufgenommen werden und dass die genannten Informationen nicht zwingend als vertraulich gelten.

- ERSTATTUNGSPOLITIK

SIGNICAT SLU erstattet in keinem Fall die Kosten für den Zertifizierungsdienst.

- AUFBEWAHRUNGSFRIST FÜR INFORMATIONEN

Alle Informationen, die sich auf den Prozess der Ausstellung qualifizierter elektronischer Zertifikate für natürliche Personen beziehen, einschließlich des vom ABONNENTEN ordnungsgemäß abgeschlossenen Vertrags und der während des Ausstellungsvorgangs erstellten Protokolle, werden von SIGNICAT SLU während der Gültigkeitsdauer des Vertragsverhältnisses aufbewahrt, solange ihre Löschung nicht verlangt wird und während der Verjährungsfrist der Klagen, die erhoben werden könnten, oder der Forderungen, die im Namen offizieller Stellen eingehen könnten.

In diesem Sinne beträgt die maximale Aufbewahrungsfrist der relevanten Informationen im Zusammenhang mit dem Prozess der Video-Identifizierung und der Ausstellung von qualifizierten Zertifikaten 15 Jahre ab dem Zeitpunkt der Ausstellung des Zertifikats, es sei denn, das Gesetz sieht etwas anderes vor. Nach Beendigung des Vertragsverhältnisses werden die Daten des ABONNENTEN gemäß den Bestimmungen der geltenden Vorschriften ordnungsgemäß gesperrt.

4 ALLGEMEINE BESTIMMUNGEN

4.1 ORT DER ERBRINGUNG DER TÄTIGKEIT

Erfüllungsort für die Verpflichtungen von SIGNICAT SLU in Bezug auf digitale Zertifizierungsdienste und ggf. Software-Nutzungslizenzen ist die Dienstadresse von SIGNICAT SLU.

4.2 ABTRENNBARKEIT DER BESTIMMUNGEN UND BEDINGUNGEN.

Die Klauseln dieses Dokuments sind voneinander unabhängig, weshalb im Falle der Ungültigkeit oder Undurchsetzbarkeit einer Klausel die übrigen Klauseln weiterhin gelten, sofern die Parteien nicht ausdrücklich etwas anderes vereinbart haben.

4.3 GELTENDEN VORSCHRIFTEN UND DER ZUSTÄNDIGEN GERICHTSBARKEIT.

Die Beziehungen zu SIGNICAT SLU unterliegen den Bestimmungen der Verordnung (EU) 910/2014 eIDAS, dem spanischen Recht und insbesondere den Bestimmungen, die sich aus der Compliance-Politik von SIGNICAT SLU ergeben.

Zuständig ist die im Gesetz 1/2000 vom 7. Januar 2000 über den Zivilprozess angegebene Gerichtsbarkeit, es sei denn, der ABONNENT wird als Verbraucher angesehen; in diesem Fall unterwirft sich SIGNICAT SLU der Gerichtsbarkeit, die ihm rechtlich zusteht.