

## 1 Allgemeines

Die mesoneer AG („mesoneer“) bietet den Service an, amtliche Ausweisdokumente (insbesondere Reisepässe, Identitätskarten und Führerscheine) („Ausweisdokumente“) zu verifizieren und mit dieser Person („Sie“ oder „Antragstellende Person“) abzugleichen. Diesen Service bietet mesoneer ihren Kunden, z.B. Finanzinstituten, Versicherungen, Online-Plattformen, Carsharing-Anbieter, Mietwagen-Anbieter, Betreibern von Entertainment-Plattformen und Signatur-Anbieter („Partner“), an, um gesetzliche Vorgaben zu erfüllen oder um die Sicherheit hinsichtlich der Identität der Endnutzer zu erhöhen. Dabei agiert mesoneer aufgrund von Verträgen mit den Partnern und nach deren Weisungen sowie den geltenden regulatorischen und gesetzlichen Anforderungen – die Identifikationsleistungen erbringt mesoneer namens und im Auftrag des Partners und ohne, dass Sie gegenüber mesoneer eine Zahlungsverpflichtung hätten. Für Leistungen des Partners und auch für eine allfällige Tragung der Kosten für die Identifikation gelten ausschliesslich die zwischen Ihnen und dem jeweiligen Partner vereinbarten Vertragsbedingungen. Eine direkte Vertragsbeziehung zwischen Ihnen und mesoneer besteht nicht.

mesoneer nutzt zwecks Durchführung der Identifikation die Dienstleistung der Electronic Identification, S.L. („Lösungspartner“ oder „eID“), Avenida Ciudad de Barcelona 81, 28007 Madrid, welche nach eIDAS zertifiziert ist und die Datenschutz-Grundverordnung (DSGVO) erfüllt. Neben diesen Nutzungsbedingungen sind deshalb auch das von eID herausgegebene und im Service integrierte [‘Certification Practice Statement’ \(«CPS»\)](#) sowie die Datenschutzbestimmungen von eID von Ihnen zu beachten.

Mit der Nutzung dieser Dienstleistung erklären Sie, dass Sie die vorliegenden rechtlichen Hinweise und Nutzungsbedingungen inklusive der Hinweise von eID gelesen, verstanden und anerkannt haben. Wenn Sie mit diesen Bedingungen nicht einverstanden sind, unterlassen Sie die Nutzung dieser Dienstleistung.

## 2 Funktionsweise der Videoidentifikation

Nachstehend ist die Funktionsweise des gesamten Videoidentifizierungsverfahrens beschrieben. Je nach Anwendungsfall des Partners, kommt der gesamte Prozess wie beschrieben oder auch nur Teile davon zur Anwendung.

Teil des Service ist ein Videoidentifizierungsverfahren oder ein asynchrones Videokonferenzverfahren, welches eine unbeaufsichtigte Video-Fernidentifizierung in Echtzeit erlaubt, den gesamten Registrierungsprozess einer Person aufzeichnet und die Fernvalidierung von Identitätsdokumenten mittels der Videoaufzeichnung ermöglicht.

Der Prozess besteht aus zwei Teilen, einem automatischen Modul, in dem mehrere Sicherheitskontrollen des während der Videoaufnahme vorgezeigten Dokuments durchgeführt werden, sowie einem biometrischen Gesichtsvergleich zwischen der Person, die das Dokument vorlegt, dem Benutzer, dem Foto des Benutzers und einer Lebenderkennung und einer genauen Datenextraktion.

All diese Informationen werden zur Unterstützung der Entscheidung einer menschlichen Mitarbeiterin/eines menschlichen Mitarbeiters des Lösungspartners von mesoneer verwendet, die/der später die gesamte Videoaufzeichnung asynchron überprüft und entscheidet, ob auf der Grundlage der gezeigten Beweise eine Identität zuerkannt werden kann oder nicht. Der Lösungspartner agiert hier als sog. Registrierungsbehörde (Registration Authority oder kurz RA).

Die verwendete Technologie erkennt in Echtzeit automatisch Sicherheitsmerkmale wie z.B. Muster, Abzeichen und optisch variable Elemente.

## 3 Elemente des Videoidentifikationsprozesses

Der Videoidentifizierungsprozess wird auf der Grundlage der folgenden Elemente durchgeführt:

- Text- und Sprachanweisungen für die Antragstellende Person.
- Automatische Steuerung von Umgebungselementen (Beleuchtung, Netzwerk, Kameraqualitätsbedingungen), die eine optimale Aufzeichnung des Identifikationsvideos und der Beweise ermöglicht.
- Bildvergleich mit Originaldokumenten durch Mustervergleichstechnologie zur Überprüfung der Dokumentenechtheit.
- Datenextraktion (OCR) der MRZ des Dokuments und die Möglichkeit des Abrufs von Berechtigungsnachweisen in Echtzeit.

- Überprüfung, ob Vorder- und Rückseite des Dokuments (falls zutreffend) identisch sind.
- Biometrische Registrierung der Person und Vergleich in Echtzeit mit dem Bild des Ausweises
- Tool zur Überprüfung der Registrierungsbehörde, zur Überprüfung des Prozesses durch eine qualifizierte Person, die zuvor durch ein spezielles Training geschult wurde.

Sobald Sie als Antragstellende Person das Ausweisdokument auswählen, das Sie für die Durchführung des Prozesses verwenden wollen, wird eine von der Anwendung gesteuerte Streaming-Videoaufnahme erstellt, in der Sie die Vorder- und Rückseite Ihres Ausweisdokumentes für eine Identifizierung und Validierung in Echtzeit vorzeigen. Sie werden zudem aufgefordert, Ihr Gesicht zu zeigen und einzulesen, um eine automatische biometrische Erkennung zu ermöglichen.

Für die anschließende asynchrone Überprüfung durch einen menschlichen Agenten wird ein Sicherheitsprotokoll erstellt, welches die während des Prozesses erhaltene Nachweise enthält und festhält, welche Nachweise nicht oder nicht vollständig erbracht werden konnten. Der gesamte Prozess wird mit einem Zeitstempel für jeden Schritt versehen.

Der Identifizierungsprozess speichert die gesamte Verifizierungskette von der Erhebung im Zuge der Videoidentifikation bis zur anschließenden Prüfung durch die Registrierungsbehörde. Das Ergebnis ist eine verifizierte Identität mit einer technischen Sicherheit, die einer Identifikation unter Anwesenden entspricht.

## 4 Lancierung des Identifikationsprozesses

Bevor das Videoidentifizierungsverfahren gestartet wird, werden Sie in zusammengefasster Form darüber informiert, dass Sie im Begriff sind, ein Video-Fernidentifizierungsverfahren einzuleiten, dessen Ziel die Ausstellung eines Zertifikats für eine qualifizierte natürliche Person ist.

Nach dieser Information muss die Antragsstellende Person diese Bedingungen für das Videoidentifizierungsverfahren lesen und akzeptieren sowie der Verarbeitung der biometrischen Daten zustimmen, die für die Durchführung des Verfahrens erforderlich ist. Zu diesem Zweck stellt der Lösungspartner der Antragstellenden Person zuvor die Datenschutzerklärung zur Verfügung, in der die

Verarbeitung personenbezogener Daten während des Prozesses geregelt ist.

Sobald die Antragstellende Person die relevanten Bedingungen gelesen und zugestimmt hat, wird der Prozess fortgesetzt.

## 5 Identifizierung

Sie erklären sich damit einverstanden, dass (a) mesoneer respektive ihr Lösungspartner Sie nach Massgabe dieser Nutzungsbedingungen identifiziert und dabei auch eine Videoaufnahme und Standbilder erstellt werden; (b) mesoneer die von Ihnen eingegebenen und im Zuge der Identifikation erfassten Personendaten und die Ausweisdokumente für die Überprüfung der Echtheit der Ausweise an den Lösungspartner weitergibt. Die Daten bleiben in der EU und unterstehen der EU Datenschutz-Grundverordnung (DSGVO) und werden ausschliesslich zur Durchführung des Identifikationsprozesses von mesoneer und ihren Lösungspartner bearbeitet und anschliessend an den Partner, für den Ihre Identifizierung durchgeführt wird, übermittelt. Es gelten die Datenschutzrichtlinien von mesoneer und ihrem Lösungspartner, über welche Sie im Rahmen des Verfahrens informiert werden.

## 6 Nutzungsbedingungen der Identifikationsprüfung

Als Antragstellende Person setzen Sie im Rahmen des Identifikationsprozesses ein technisches Endgerät ein (z.B. seinen PC, Tablet oder sein Smartphone), um mit Hilfe der Kamera das Ausweisdokument und sich selbst per Video aufzunehmen. Im Folgenden wird der Identifizierungsprozess mit den entsprechenden Schritten und der dazugehörigen Datenverarbeitung erläutert:

Als Antragstellende Person werden Sie in der Regel vom Partner von mesoneer auf den Identifizierungsservice aufmerksam gemacht. mesoneer benötigt für die Durchführung des Identifizierungsdienstes sowie für die allfällige Ausstellung einer elektronischen Signatur in der Regel Endnutzerdaten wie insbesondere Vor- und Nachname, Geburtsdatum, die Staatsangehörigkeit, die Art des Ausweisdokumentes und eine Mobile-Nummer.

Als Teil des Identifizierungsprozesses werden zudem Foto und Videoaufnahmen Ihres Ausweisdokumentes erstellt. Aus der Videoaufnahme werden Fotos vom Ausweisdokument und vom Gesicht der Antragstellenden Person angefertigt und miteinander abgeglichen. Aus dem

Ausweisdokument werden zudem für die Überprüfung der Identifikation Daten herausgelesen.

Im Rahmen des Identifizierungsvorganges werden zudem Daten zum verwendeten Gerät, Browser und Zugang zum Internet (z. B. Gerätetyp, Betriebssystem, IP-Adresse, Access Provider), Daten über den Besuch und Aktivitäten auf den Seiten während des Identifizierungsprozesses (wie Login mit Datum/Uhrzeit, Drücken einer «Akzeptieren»-Schaltfläche usw.) erhoben.

Die Daten der Antragstellenden Person sowie die Video- und Fotoaufnahmen der Ausweisdokumente sind nur bis zum Zeitpunkt der Übermittlung an den Partner bei mesoneer und dem Lösungspartner gespeichert. Spätestens nach 90 Tagen werden Ihre Daten auf den Servern von mesoneer und dem Lösungspartner gelöscht wenn nur eine Identifikation ohne Ausstellung einer elektronischen Signatur vorgenommen wird. Dient der Identifizierungsvorgang jedoch als Basis für ein elektronisches Zertifikat, so müssen die Daten gemäss den gesetzlichen Anforderungen weiter aufbewahrt werden und dürfen nicht gelöscht werden.

Die Daten können auch aufgrund von gesetzlichen Aufbewahrungsfristen (z.B. im Rahmen des Geldwäschereigesetzes) beim Partner während einer längeren Dauer gespeichert werden. Die Handhabung Ihrer Daten durch den Partner als Data Controller richtet sich nach den einschlägigen Datenschutzerklärungen des Partners und Ihrem Vertragsverhältnis mit dem Partner. Es gelten diesbezüglich die Bestimmungen der Datenschutzrichtlinien von mesoneer und ihrem Lösungspartner.

## 7 Ihre Verpflichtungen

Zu Ihrer eigenen Sicherheit und um sicher zu stellen, dass der Identifikationsprozess ordnungsgemäss durchgeführt werden kann, müssen Sie die folgenden Grundregeln beachten.

- (a) Verwenden Sie den Prozess und die Identifikation in Übereinstimmung mit den Bestimmungen dieses Dokuments und der darin referenzierten Dokumente (wie dem CPS).
- (b) Bitte beachten Sie, dass eine widerrechtliche, sittenwidrige und/oder potenziell schadensstiftende Nutzung der Identifikationsdienstleistung nicht erlaubt ist.
- (c) Sie sind verpflichtet, im Zuge des Identifikationsprozesses aktuelle und

wahrheitsgetreue Daten zu erfassen und keine falschen Angaben zu machen oder falsche oder manipulierte Ausweisdokumente zu verwenden. Ausserdem müssen die verwendeten Ausweisdokumente den folgenden Anforderungen genügen:

- Die verwendeten Ausweisdokumente müssen ein Lichtbild enthalten und Sicherheitsmerkmale aufweisen, die bei der Videofernidentifizierung automatisch überprüft werden können, um die Erkennung von Fälschungen und Manipulationen zu gewährleisten.
  - Beim Ausweisdokument handelt sich nicht um eine Fotokopie oder eine gedruckte Karte.
  - Das Ausweisdokument liegt nicht in einem digitalen Format vor (Handy, Tablet oder Computer).
  - Das Ausweisdokument befindet sich nicht in einer Hülle.
  - Das Ausweisdokument ist nicht beschädigt, alle Informationen und Sicherheitselemente sind vollständig vorhanden.
- (d) Während des Identifikationsprozesses und der Aufnahme des Videos sind nachfolgende Regeln zu beachten:
- Die Ausleuchtung im Video sollte eine klare Sicht auf das Gesicht der zu identifizierenden Person und auf das Dokument ermöglichen.
  - Die Videoaufnahme sollte einen konstanten Fluss haben und keine Schnitte oder Verzögerungen aufweisen.
  - Die Identifikation muss 'live' von einer Person vorgenommen werden.
  - Wenn eine andere Person als die zu identifizierende Person durch den gesamten Vorgang führt, wird die Identifizierung abgelehnt.
  - Wenn eine andere Person in die Erstellung der Videoaufnahme involviert ist, aber die zu identifizierende Person eindeutig nicht zwingt, kann die Identifizierung gültig sein (z.B., wenn eine Person einer physisch oder anderweitig beeinträchtigten Person bei der Identifizierung hilft).

- Alle Teile des erfassten Dokuments (Vorder- und Rückseite) sowie das Gesicht der Person müssen deutlich sichtbar sein.
  - Die zu identifizierende Person darf nicht schlafen oder Anzeichen zeigen, die auf Drogen- oder Alkoholeinfluss schliessen lassen.
- (e) Bitte befolgen Sie bei der Benutzung der Identifikationsdienstleistung die an Sie gerichteten Handlungsanweisungen und Vorgaben von mesoneer oder ihrem Lösungspartner.
- (f) Bitte beachten Sie, dass Sie für die Wahl der von Ihnen verwendeten Datennetze und für eine adäquate Absicherung Ihrer Endgeräte v.a. vor unberechtigten Zugriffen alleine verantwortlich bleiben (siehe nachfolgend Ziffer 8).

## **8 Risiken im Zusammenhang mit der Übermittlung von Daten im Internet und der allgemeinen Nutzung der Dienstleistung.**

Bitte beachten Sie, dass die Übermittlung Ihrer Daten via Internet erfolgt. Sie nehmen zur Kenntnis, dass mit der elektronischen Datenübermittlung Risiken verbunden sind. Die mesoneer und der Partner übernehmen für die Sicherheit Ihrer Daten während der Übermittlung keine Haftung, ebenso wenig für das ordnungsgemässe Funktionieren der durch Sie genutzten Endgeräte, Systeme und Internetverbindungen.

Auch bei allen dem neusten Stand der Technik entsprechenden Sicherheitsvorkehrungen kann sowohl auf Seiten Partner, mesoneer und auf Ihrer Seite als Antragstellende Person eine absolute Sicherheit nicht gewährleistet werden. Ihr Endgerät ist Teil des Gesamtsystems, befindet sich jedoch ausserhalb der Kontrolle des Partners und mesoneer und kann zu einer Schwachstelle des Systems werden. Trotz aller Sicherheitsmassnahmen können weder der Partner noch mesoneer eine Verantwortung für Ihre Endgeräte übernehmen. Sie nehmen insbesondere folgende Risiken zur Kenntnis:

- a.) Ungenügende Systemkenntnisse und mangelnde Sicherheitsvorkehrungen am Endgerät können einen unberechtigten Zugriff erleichtern (z. B. ungenügend geschützte Speicherung von Daten auf die Festplatte, Filetransfers, Bildschirmabstrahlung, Löschung von Log-in-Daten und Legitimationsmittel aus Datenspeichern).
- b.) Die Erstellung einer Verkehrscharakteristik der Antragstellenden Person durch den Netzwerk-

Betreiber (z. B. Internet-, SMS-Provider) kann niemand ausschliessen, d. h., dieser hat die Möglichkeit nachzuvollziehen, wann Sie mit wem in Kontakt getreten sind.

c.) Es besteht die Gefahr, dass sich ein Dritter während der Nutzung der Identifikationsdienstleistung unbemerkt Zugang zum Endgerät verschafft.

d.) Es besteht die Gefahr, dass sich bei Nutzung eines Netzwerkes (z. B. Internet-)Viren und dergleichen auf Ihrem Endgerät ausbreiten, wenn das Endgerät Kontakt mit der Aussenwelt aufnimmt.

## **9 Geistiges Eigentum**

Die Elemente und Inhalte, die während des gesamten Prozesses erscheinen, wie zum Beispiel Texte, Fotos, Grafiken, Bilder, Icons, Technologien, Software, Links und andere audiovisuelle oder akustische Inhalte sowie die grafische Gestaltung und die Quellcodes (im Folgenden "Inhalte"), sind geistiges Eigentum von mesoneer und/oder des Lösungspartners. An diesen Inhalten werden Ihnen bloss die Nutzungsrechte eingeräumt, die Sie benötigen, um den Identifikationsprozess gemäss diesen Bestimmungen zu absolvieren – eine Übertragung von geistigem Eigentum findet dagegen keine statt. Ebenso geschützt und vorbehalten bleiben die Marken, Handelsnamen oder anderen Kennzeichen von mesoneer, dem Leistungspartner und/oder Dritter - die Nutzung des Service vermittelt Ihnen keine Rechte an den genannten Marken, Handelsnamen und/oder anderen Kennzeichen.

## **10 Haftungsausschluss**

mesoneer und der Lösungspartner garantieren die angemessene Durchführung des in diesem Dokument beschriebenen Services, sofern Sie den Ihnen auferlegten Verpflichtungen nachkommen und auch die Anweisungen von mesoneer und/oder dem Lösungspartner befolgen.

Der Zugang und die Nutzung des Service und des Videoidentifikationsprozesses insbesondere stellt keine Verpflichtung von mesoneer und/oder dem Lösungspartner dar, das Nichtvorhandensein von Viren, Trojanern und anderer schädlicher Softwareroutine zu kontrollieren. Es liegt in jedem Fall an Ihnen als Antragstellende Person, die Verfügbarkeit geeigneter Werkzeuge für die Erkennung und Beseitigung von schädlicher Softwareroutine zu nutzen. Weder mesoneer noch der Lösungspartner haften für Schäden, die während der Benutzung des Service und der

Durchführung des Videoidentifizierungsprozesses an der ICT-Infrastruktur der Antragstellenden Person oder Dritter entstehen.

Das Funktionieren des Service und der Identifikation im Besonderen kann von der korrekten Konfiguration der von Ihnen verwendeten Geräte abhängen, wobei Sie wie dargelegt verpflichtet sind, die im Zuge des Identifizierungsprozesses an Sie gerichteten Handlungsanweisungen zu befolgen und in jedem Fall und zu jeder Zeit die Einhaltung der angegebenen Hardware- und Softwareanforderungen sicherzustellen.

Ebenso muss für die Nutzung des Service ein Internetzugang auf Ihrer Seite vorhanden sein. Das Funktionieren des Service und der Videoidentifizierungsverfahrens kann unter anderem von der angemessenen Qualität und Geschwindigkeit der von Ihnen gewählten Verbindung abhängen, über die Sie auf den Service zugreifen. Sie sind entsprechend für die Bereitstellung und die ausreichende Qualität von Telekommunikationsleitungen, Internet-Abonnements oder -Verbindungen oder anderen technischen Mitteln selber verantwortlich.

Weder mesoneer noch der Lösungspartner haften (a) für Schäden, die sich aus der Nichterfüllung oder mangelhaften Erfüllung Ihrer Verpflichtungen gemäss dieser Vereinbarung ergeben oder damit zusammenhängen; (b) für die falsche Verwendung der Ergebnisse des Services resp. des Outputs des Services und der Passwörter, noch für indirekte Schäden, die sich aus der Verwendung des Services oder der von mesoneer und/oder dem Lösungspartner gelieferten Informationen ergeben können; (c) für eventuelle Ungenauigkeiten bei der Identifizierung, die sich aus den von der Antragstellenden Person während des Prozesses gelieferten Informationen ergeben; (d) für das korrekte Funktionieren von Anwendungen und Dienstleistungen Dritter, die nicht zugelassen sind, und für Schäden, die dadurch entstehen, dass die Antragstellende Person diese Anwendungen nicht nutzen kann.

## 11 Sistierung der Nutzung

mesoneer behält sich bei der Feststellung von Sicherheitsrisiken jederzeit vor, bis zu deren Behebung die Nutzung der Identifikationsdienst-

leistung zu Ihrem Schutz oder zum Schutz aller Nutzer zu unterbrechen. Zu einer Unterbrechung Ihrer Nutzung ist mesoneer auch dann berechtigt, wenn Sie diese Nutzungsbedingungen nicht beachten sollten. Für aus diesem Unterbruch allfällig entstandenen Schaden übernimmt mesoneer keine Haftung.

## 12 Änderung der Nutzungsbedingungen

mesoneer behält sich vor, diese Nutzungsbedingungen jederzeit zu ändern.

## 13 Salvatorische Klausel

Die Klauseln dieses Dokuments sind voneinander unabhängig, weshalb im Falle der Unwirksamkeit oder Nichtdurchsetzbarkeit einer Klausel die übrigen Klauseln wirksam bleiben, sofern die Parteien nicht ausdrücklich etwas anderes vereinbaren. Unwirksame oder nicht durchsetzbare Klauseln werden in guter Treu so angepasst, dass der mit dem unwirksamen oder nicht durchsetzbaren Teil angestrebte Zweck so weit wie möglich erreicht wird.

## 14 Anwendbares Recht & Forum

Auf die Leistungen der mesoneer findet ausschliesslich schweizerisches Recht Anwendung, unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11. April 1980 und unter Ausschluss des Kollisionsrechts.

Auf die Leistungen des Lösungspartners findet ausschliesslich spanisches Recht Anwendung, unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11. April 1980 und unter Ausschluss des Kollisionsrechts.

Für Streitigkeiten im Zusammenhang mit dem Service werden, soweit keine zwingenden Konsumentengerichtsstände zur Anwendung gelangen, die folgenden ausschliesslichen Gerichtsstände vereinbart: (a) für Leistungen der mesoneer, die ordentlichen Gerichte an ihrem Sitz; (b) in Bezug auf Leistungen des Lösungspartners, die ordentlichen Gerichte in Madrid.

Allgemeine Informationen zum Schutz personenbezogener Daten für den Nutzer

Grundlegende Informationen (erste Informationsebene)

<b>Verantwortlicher für die Datenverarbeitung:</b>	Electronic Identification S.L. als Vertrauensdiensteanbieterin ("eID")
<b>Zweck der Verarbeitung:</b>	(i) Verwaltung, Entwicklung, Einhaltung und Kontrolle des Vertragsverhältnisses in Bezug auf Ausstellung von elektronischen Zertifikaten, (ii) die Versendung jeglicher Art von postalischer oder elektronischer Korrespondenz im Zusammenhang mit der besagten Beziehung; (iii) die Aufnahme der Daten in die Kontakttagenden des Unternehmens, der Abteilungen und der Mitarbeiter, die dies erfordern; (iv) die korrekte wirtschaftliche, buchhalterische, steuerliche und rechnungslegende Verwaltung, die sich aus der aufrechterhaltenen Rechtsbeziehung ergibt; (v) die Verwaltung der entsprechenden Vertragsakte für die Aufbewahrung und die Pflege der Vertragsaktenhistorie; (vi) die Ausstellung und Verwaltung ihrer elektronischen Bescheinigung über die natürliche Person
<b>Rechte:</b>	Zugang, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung, Übertragbarkeit und Ablehnung einer automatisierten Entscheidungsfindung.

Erweiterte Informationen (zweite Informationsebene)

Gemäss den Bestimmungen der geltenden Gesetzgebung zum Schutz personenbezogener Daten und deren Durchführungsbestimmungen informieren wir Sie gerne über die Verarbeitung Ihrer personenbezogenen Daten (im Folgenden "Daten").

**1 Verantwortlicher für die Datenverarbeitung**

Die Daten, die Sie uns jetzt oder in Zukunft im Zusammenhang mit unserer Geschäftsbeziehung zur Verfügung stellen, werden verarbeitet von Electronic Identification S.L. (im Folgenden "eID") mit Sitz in der Avenida Ciudad de Barcelona 81- A Planta 4, 28007 Madrid, Steueridentifikationsnummer B86681533, eingetragen im Handelsregister von Madrid. Registrierungsdaten: Band: 30920, Buch: 0, Seite: 146, Abschnitt: 8, Blatt: M556508, mit Datum vom 3. April 2013. Sie gilt als für die Datenverarbeitung Verantwortliche und in ihrer Eigenschaft als Vertrauensdiensteanbieterin 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 ("eIDAS"-Verordnung), Gesetz 6/2020 vom 11. November zur Regelung bestimmter Aspekte der elektronischen Treuhanddienste und Verordnung ETD/465/2021 vom 6. Mai zur Regelung der Methoden der Videofernidentifizierung für die Ausstellung elektronischer Zertifikate.

**2 Legitimation**

Die Rechtsgrundlage für die Verarbeitung ist die Erfüllung des Vertrags, an dem Sie als Nutzer beteiligt sind.

**3 Zweck**

Als Vertrauensdiensteanbieter verarbeitet eID Ihre Daten von eID, um ein elektronisches Zertifikat für eine natürliche Person auszustellen und zu verwalten sowie Ihnen die Authentifizierung in bestimmten Systemen mittels elektronischer Unterschrift zu ermöglichen; und um unsere Beziehung zu pflegen, zu entwickeln und zu kontrollieren, was die Bearbeitung

Ihrer Anfragen oder Ersuchen um Informationen oder Unterlagen einschliesst.

Alle vom Antragsteller zur Verfügung gestellten Daten werden zur Überprüfung der Identität und zur Ausstellung elektronischer Zertifikate sowie zu deren Verwaltung während ihres gesamten Lebenszyklus verwendet. Mit der Annahme der Richtlinie und der Erklärung zu den Zertifizierungspraktiken erklärt sich der Antragsteller mit der Verarbeitung seiner personenbezogenen Daten zu den angegebenen Zwecken einverstanden.

Die Zwecke der Verarbeitung sind insbesondere: (i) Verwaltung, Entwicklung, Einhaltung und Kontrolle des Vertragsverhältnisses in Bezug auf Ausstellung von elektronischen Zertifikaten, (ii) die Versendung jeglicher Art von postalischer oder elektronischer Korrespondenz im Zusammenhang mit der besagten Beziehung; (iii) die Aufnahme der Daten in die Kontakttagenden des Unternehmens, der Abteilungen und der Mitarbeiter, die dies erfordern; (iv) die korrekte wirtschaftliche, buchhalterische, steuerliche und rechnungslegende Verwaltung, die sich aus der aufrechterhaltenen Rechtsbeziehung ergibt; (v) die Verwaltung der entsprechenden Vertragsakte für die Aufbewahrung und die Pflege der Vertragsaktenhistorie; (vi) die Ausstellung und Verwaltung ihrer elektronischen Bescheinigung über die natürliche Person

## 4 Kategorie der personenbezogenen Daten

Zu den Kategorien personenbezogener Daten, die von eID für die Bereitstellung vertrauenswürdiger elektronischer Dienste gehören unter anderem Identifizierungsdaten (Name, Vorname und Identitätsdaten), Kontaktdaten (Postanschrift, Email und Telefon)

Alle vom Nutzer bereitgestellten Daten werden für die Bereitstellung elektronischer Vertrauensdienste sowie für die Verwaltung der ausgestellten Zertifikate während ihres gesamten Lebenszyklus verwendet.

## 5 Dauer der Datenspeicherung

Die Daten werden für die Dauer des Vertragsverhältnisses aufbewahrt, solange ihre Löschung nicht verlangt wird, sowie für die Dauer der Verjährung eventueller Klagen oder Ansprüche von

Behörden im Zusammenhang mit diesem Vertrag und nach dessen Beendigung. In jedem Fall beträgt die maximale Aufbewahrungsfrist 15 Jahre ab dem Datum der Ausstellung des elektronischen Zertifikats, sofern gesetzlich nichts anderes vorgesehen ist. Nach Beendigung unserer Beziehung werden Ihre Daten gemäss den geltenden Vorschriften ordnungsgemäss gesperrt.

## 6 Adressaten

Die Daten werden an folgende Empfänger weitergeleitet: (i) Richter, Gerichte und Strafverfolgungsbehörden zur Erfüllung von Anforderungen, rechtlichen Verpflichtungen oder im Rahmen von Gerichtsverfahren; (ii) Bankinstitute zur Verwaltung von Einzügen und Zahlungen; (iii) Steuerbehörde zur Erfüllung von steuerlichen Verpflichtungen; (iv) Finanzprüfer zur Erfüllung von finanziellen Verpflichtungen; (v) Notare, falls das Dokument notariell beglaubigt wird; und (vi) sonstige Dritte, an die die Übermittlung aufgrund der jeweils geltenden Vorschriften zu Kontroll-, Registrierungs- und Prüfzwecken erfolgen muss, wie z. B. die zuständigen staatlichen Stellen.

Die personenbezogenen Daten der Nutzer können infolge der Einsichtnahme in die Sperrlisten oder an Dritte, die Informationen über die Gültigkeit und die Gültigkeit der Zertifikate benötigen, übermittelt und/oder weitergegeben werden.

Darüber hinaus können die Daten Dritten sowohl in Spanien als auch in der Europäischen Union zur Verfügung gestellt werden, um Dienstleistungen für unser Unternehmen zu erbringen (z. B. Daten-Hosting oder Unterstützung bei der Identifizierung), und zwar im Rahmen eines Datenverarbeitungsvertrags, in dem die entsprechenden Schutzmassnahmen gemäss den Bestimmungen der Gesetzgebung zum Schutz personenbezogener Daten garantiert werden, sowie mit der Verpflichtung zur Rückgabe und/oder Vernichtung nach Beendigung der Dienstleistung.

## 7 Internationale Datenübermittlung

Eine internationale Datenübermittlung ist nicht vorgesehen.

## 8 Rechte

Die betroffene Person kann ihr Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung, Übertragbarkeit und Verweigerung automatisierter Einzelentscheidungen ausüben, indem sie einen Antrag an die folgende Email-Adresse sendet: [legal@electronicid.eu](mailto:legal@electronicid.eu), oder an die Postanschrift: Avenida Ciudad de Barcelona 81- A Planta 4, 28007, Madrid; dabei ist anzugeben, welches Recht sie ausüben möchte. Die betroffene Person wird darüber informiert, dass sie das Recht hat, in Spanien eine Beschwerde bei der spanischen Datenschutzbehörde ([www.aepd.es](http://www.aepd.es)) oder an ihre zuständige Aufsichtsbehörde gerichtet werden. einzureichen und bei dieser Stelle Informationen und Schutz hinsichtlich der Ausübung ihrer Rechte beantragen kann.

Sie können die spezifischen Zustimmungen, die wir in dieser Klausel verlangen, auf die oben angegebene Weise und jederzeit widerrufen, ohne Rückwirkung und unter den gesetzlich vorgesehenen Bedingungen.

Alle von uns angeforderten Informationen sind obligatorisch, so dass die Nichtbereitstellung einer dieser Informationen die Erbringung der von uns angebotenen Dienstleistungen unmöglich machen kann. Die von eID angebotenen elektronischen Signaturdienste können nur durchgeführt werden, wenn der Antragsteller alle abgefragten Daten wahrheitsgemäss und ohne falsche Angaben beantwortet.

Die Daten, die Sie uns zur Verfügung stellen, müssen zu dem Zeitpunkt, zu dem Sie uns die Informationen zur Verfügung stellen, korrekt und aktuell sein, und Sie garantieren daher ihre Authentizität und Wahrhaftigkeit. Ausserdem bitten wir Sie, uns jede Änderung Ihrer Daten schnell und sorgfältig mitzuteilen, damit wir unsere Datei ständig auf dem neuesten Stand halten können und keine Fehler in Bezug auf Ihre Daten auftreten.

## 9 Volljährigkeit

Unsere Dienstleistungen sowie die Waren, die wir im Zusammenhang mit den eTrust-Diensten über unsere Plattform anbieten, dürfen nur von volljährigen Personen genutzt werden. Zu diesem Zweck versichern Sie, dass die von Ihnen gemachten

Angaben zu Ihrem Geburtsdatum der Wahrheit entsprechen. Jegliche Haftung für eID, die durch eine falsche Altersangabe entsteht, wird vom Nutzer eingefordert.

## 10 Vertraulichkeit und Sicherheitsmassnahmen

Abschliessend möchten wir Sie darüber informieren, dass eID Ihre Daten jederzeit streng vertraulich und in Übereinstimmung mit den oben ausdrücklich genannten Verwendungszwecken behandeln wird. Ebenso informieren wir Sie darüber, dass eID die notwendigen technischen und organisatorischen Massnahmen ergriffen hat, um die Sicherheit Ihrer Daten zu gewährleisten und deren Änderung, Verlust, Verarbeitung oder unbefugten Zugriff zu verhindern, unter Berücksichtigung des Stands der Technik, der Art der gespeicherten Daten und der Risiken, denen sie ausgesetzt sind, und in Übereinstimmung mit den Bestimmungen des geltenden Datenschutzgesetzes.