



S VIDEOLEGITIMATION

Datenschutzhinweise

1. PRÄAMBEL

Mit diesen Datenschutzhinweisen informieren wir, die DekaBank Deutsche Girozentrale, Große Gallusstraße 14 in 60315 Frankfurt am Main (Verantwortlicher im Sinne der Datenschutzgrundverordnung - DSGVO), welche personenbezogenen Daten wir erheben, verarbeiten und nutzen, wenn Sie das Videolegitimationsverfahren nutzen.

Die Videolegitimation selbst wird in unserem Auftrag innerhalb der Sparkassen-Finanzgruppe von der S-Markt & Mehrwert GmbH & Co. KG in Halle (Auftragsverarbeiterin) durchgeführt. Gemäß Versicherung der Auftragsverarbeiterin findet die Verarbeitung ausschließlich auf Servern innerhalb der Bundesrepublik Deutschland statt.

2. ERHOBENE DATEN UND HERKUNFT DER DATEN

Im Rahmen des Legitimationsvorganges werden folgende personenbezogenen Daten verarbeitet:

a. Identifizierungsdaten:

- Vorgangsnr.
- Anrede
- Name
- Vorname/n (alle)
- Straße
- Hausnr.
- Postleitzahl
- Ort
- Geburtsdatum
- Geburtsort
- Staatsangehörigkeit
- Mobilfunknr.
- E-Mail-Adresse

Diese Daten erhalten wir von der Sparkasse oder dem Institut, das den Depotvertrag an uns vermittelt hat.

Im Rahmen des Legitimationsvorganges werden darüber hinaus folgende Daten erfasst:

b. Kommunikationsdaten

- Ihre IP-Adresse
- Die Internetseite von der Sie zu uns gelangen
- Datum und Dauer der Nutzung unserer Internetseite

c. Legitimationsdaten

- Screenshot Ihrer Person
- Personalausweis: Screenshot der Vorder- und Rückseite
- Reisepass: Screenshot aller Seiten mit personenbezogenen Daten
- Art Ihres Legitimationsdokumentes
- Nummer Ihres Legitimationsdokumentes
- Ausstellende Behörde Ihres Legitimationsdokumentes und deren Ort
- Das Ausstellungsdatum Ihres Legitimationsdokumentes
- Das Ablaufdatum Ihres Legitimationsdokumentes
- Staatsangehörigkeit
- Audio- und Videomitschnitt des Legitimationsvorganges
- Die Ihnen auf Ihr Mobiltelefon übermittelte Transaktionsnummer (TAN)

Während der Videolegitimation werden Video- und Audioaufnahmen gemacht. Zusätzlich werden Screenshots von Sicherheitsmerkmalen des Ausweisdokuments angefertigt.

Im Zusammenhang mit der Anfertigung des Bildschirmfotos Ihrer Person bitten wir Sie, darauf zu achten, dass im Bildhintergrund keine Personen zu sehen sind.

3. EINWILLIGUNGSERKLÄRUNG ZUR GESPRÄCHSAUFZEICHNUNG UND ANFERTIGUNG EINES BILDSCHIRMFOTOS IHRER PERSON

Damit wir das Gespräch in Ton und Bild aufzeichnen und speichern können, benötigen wir Ihre Einwilligung. Vor Beginn der Videolegitimation fordern wir Sie daher auf, folgende Einwilligung abzugeben:

Ich willige hiermit in die Ton- und Videoaufzeichnung des Gesprächs und die Anfertigung von Bildschirmfotos meines Gesichtes und meines Ausweisdokumentes ein.

Wenn Sie diese Einwilligung nicht abgeben wollen, können Sie ein anderes Legitimationsverfahren nutzen, zum Beispiel eine Vor-Ort Legitimation bei der vermittelnden Sparkasse bzw. dem vermittelnden Institut.

Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Aus rechtlichen Gründen ist im Falle eines Widerrufs eine erneute Legitimation über Ihre Sparkasse bzw. das vermittelnde Institut notwendig.

Die Video- und Gesprächsaufzeichnung verwenden wir zur Dokumentation sowie zur Nachprüfbarkeit der Richtigkeit der Legitimation und der Erkennung und Verhinderung von Missbrauch. Den Text der Einwilligung können Sie auch unter www.deka.de/datenschutz jederzeit abrufen.

4. ZWECKBINDUNG UND SPEICHERFRISTEN

Sämtliche o. g. und im Rahmen der Videolegitimation angefallenen Daten werden von uns ausschließlich zur Identifizierung Ihrer Person nach den hierfür jeweils geltenden gesetzlichen und

bankaufsichtsrechtlichen Vorgaben verarbeitet.

Die Gesprächsaufzeichnung, die Videoaufzeichnung und das Bildschirmfoto werden, unbeschadet anderer gesetzlicher Bestimmungen, 5 Jahre nach Beendigung der Geschäftsbeziehung gelöscht. Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahres, in dem die Geschäftsbeziehung endet.

Die Mobilfunknummer wird nur für die Zusendung der TAN genutzt und unmittelbar im Anschluss gelöscht.

Die sonstigen Identifizierungsdaten und Legitimationsdaten werden unbeschadet anderer gesetzlicher Bestimmungen, 5 Jahre nach Beendigung der Geschäftsbeziehung gelöscht. Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahres, in dem die Geschäftsbeziehung endet.

Die Kommunikationsdaten werden 15 Tage nach Durchführung des Legitimationsvorgangs gelöscht.

5. RECHTSGRUNDLAGE

Rechtsgrundlage für die Verarbeitung der Identifizierungsdaten ist die Vertragserfüllung (Art. 6 Abs. 1 lit. b) DSGVO. Rechtsgrundlage für die Verarbeitung der Legitimationsdaten ist, sofern nachfolgend nicht anders genannt, unsere rechtlichen Verpflichtungen nach dem Geldwäschegesetz (Art. 6 Abs. 1 lit. c) DSGVO).

Die Video- und Gesprächsaufzeichnung und die Verarbeitung des Bildschirmfotos Ihres Gesichtes erfolgt auch auf Basis Ihrer Einwilligung.

Die Kommunikationsdaten sowie die Mobilfunknummer verarbeiten wir auf Basis unserer berechtigten Interessen (Missbrauchsbekämpfung, Nachweis ordnungsgemäßer Identifikation), ebenso das Ausstellungsdatum und Ablaufdatum Ihres

Legitimationsdokumentes, sowie Ihre Mobilfunknummer.

Erläuterungen zu den Rechtsgrundlagen finden Sie in unseren „Allgemeinen Datenschutzhinweisen“, abrufbar unter www.deka.de/datenschutz.

6. DATENEMPFÄNGER

Die im Auftrag der DekaBank erhobenen Daten werden nicht an Dritte weitergegeben, es sei denn in diesen Datenschutzhinweisen ist etwas anderes bestimmt oder wenn gesetzliche Bestimmungen dies gebieten. Unter diesen Voraussetzungen können bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung zur Weitergabe Empfänger personenbezogener Daten Öffentliche Stellen und Institutionen sein (z.B. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht, Europäische Zentralbank, Finanzbehörden, Strafverfolgungsbehörden). Bei Verdacht auf Missbrauch, insbesondere bei Verdacht einer strafbaren Handlung behalten wir uns vor, die o. g. erforderlichen Daten sowie den kompletten Gesprächsverlauf inklusive IP-Adresse weiter zu speichern und den Strafverfolgungsbehörden zu übermitteln.

Die Webseite der Videolegitimation wird für uns von der S-Markt & Mehrwert GmbH & Co. KG technisch im Rahmen einer Auftragsverarbeiterin betrieben. Die technische Umsetzung findet ausschließlich auf Servern auf dem Gebiet der Bundesrepublik Deutschland statt.

7. ABRUCH DER VIDEOLEGITIMATION

Kommt es zum Abbruch der Videolegitimation, so werden alle im Rahmen des Verfahrens erhobenen Daten gelöscht. Insofern Ihr Internet-Browser so konfiguriert ist, dass Formulardaten gespeichert werden, kann dies dazu führen, dass

die Eingabefelder bei der Anmeldung für einen bestimmten Zeitraum befüllt bleiben. Um dies zu vermeiden, leeren Sie bitte den Speicher Ihres Internet-Browsers.

Sofern Sie einer Aufzeichnung widersprechen, erfolgt der Abbruch des Legitimationsvorgangs sowie der Verweis an die Sparkasse und darauf, dass die Identifizierung mittels eines anderen nach Geldwäschegesetzes (GwG) zulässigen Verfahrens vorgenommen werden muss. Anschließend erfolgt die Löschung der aufgezeichneten Daten.

SICHERHEIT UND TAN

Die Videolegitimation erfolgt auf der Grundlage aktueller Sicherheitsstandards. Es findet eine komplette Verschlüsselung der Datenübermittlung statt.

Zum Nachweis, dass das Gespräch in Echtzeit geführt worden ist, erhalten Sie zum Ende des Legitimationsvorgangs eine Transaktionsnummer (TAN) an die von Ihnen auf der Startseite vorgegebene Mobiltelefonnummer.

Der Mitarbeiter wird Sie während des Gesprächs zur Eingabe der TAN im textlichen Teil des Chats auffordern. Die korrekte Eingabe der TAN ist für die rechtssichere Durchführung Ihrer Legitimation per Videolegitimation unabdingbar.

9. DATENSCHUTZBEAUFTRAGTER

Die Kontaktdaten unseres Datenschutzbeauftragten finden Sie unter www.deka.de/datenschutz.

10. IHRE RECHTE

Informationen zu Ihren Rechten nach der DSGVO finden Sie unter www.deka.de/datenschutz.

eID-SERVICE

Datenschutzinformation

1. PRÄAMBEL

Der eID-Service wird von Ihrer Sparkasse bzw. dem Verbundpartner angeboten und durch die S-Markt & Mehrwert GmbH & Co. KG durchgeführt.

Die Identifizierung erfolgt nach §18 PauswG und wird über ein mobiles und NFC-fähiges Endgerät mittels einer von der AUTHADA GmbH (siehe Punkt 7) bereitgestellten App durchgeführt.

Persönliche Daten, die Sie im Rahmen der Identitätsprüfung Ihrer Sparkasse bzw. deren Verbundpartner und beim Besuch dieser Webseite der S-Markt & Mehrwert GmbH & Co. KG mitteilen, werden gemäß den Vorgaben der EU-Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG neu) und anderen gesetzlichen Bestimmungen, die für den elektronischen Geschäftsverkehr gelten sowie nach Vorgaben der zuständigen Aufsichtsbehörden, verarbeitet.

Wenn Sie mit der beschriebenen Datenverarbeitung nicht einverstanden sind und der Verarbeitung ganz oder teilweise widersprechen, ist der eID-Service nicht nutzbar. In diesem Fall stehen Ihnen alternative Identifizierungsverfahren (z.B. Identifizierung durch den Berater in der Filiale Ihrer Sparkasse) zur Verfügung.

2. VERANTWORTLICHE STELLE

Die verantwortliche Stelle gemäß Art. 4, Abs. 7 der DSGVO für die Erhebung, Verarbeitung, Speicherung und Nutzung der personenbezogenen Daten im Zusammenhang mit dem beschriebenen Prozess ist Ihre Sparkasse.

3. ART DER DATEN

Personenbezogene Daten aus dem Ausweischip

werden im Umfang der erteilten Berechtigung nach Einwilligung des Nutzers mit Eingabe der Ausweis-PIN übertragen.

Folgende Daten werden erhoben, verarbeitet und gespeichert:

a. Personenbezogene Daten und Adressdaten

- Anrede
- Doktorgrad
- Name
- Vorname(n)
- Ggf. Geburtsname
- Geburtsdatum
- Geburtsort
- Staatsangehörigkeit
- Straße & Hausnr.
- PLZ
- Ort
- Wohnland
- E-Mail
- Mobilfunknr.

b. Ausweisdaten

- Dokumententyp
- Ausweisnr.
- Ausstellungsdatum
- Gültig-Bis-Datum
- Ausstellende Behörde
- Dienste- und kartenspezifisches Kennzeichen/Pseudonym

c. Legitimationsdaten bzw. -dateien

- Ggf. angefertigtes Foto der Vorderseite Ihres Legitimationsdokumentes
- Ggf. angefertigtes Foto der Rückseite Ihres Legitimationsdokumentes
- Ergebnis-PDF mit erhobenen Daten und ggf. aufgenommenen Fotos

d. Protokolldateien

Die Art und Version der Anwendungsumgebung (Android-Version, mobiles Endgerät, usw.) des Nutzers. Diese Daten übermitteln die AUTHADA App an die AUTHADA GmbH, um z.B. die App kontinuierlich zu verbessern und Fehler im Verarbeitungsprozess zu identifizieren. Die Nutzung der Daten erfolgt ausschließlich für den genannten Zweck.

Die AUTHADA nutzt das Analyse-Tool Matomo, um Fehler zu erkennen und die App ständig zu verbessern. Darüber hinaus unterstützt das Tool die AUTHADA GmbH, das Nutzer-Verhalten in der App nachzuvollziehen, indem es Nutzungsbericht anonymisiert anfertigt. Diese Daten werden auf dem Server der AUTHADA GmbH in Deutschland gespeichert. Das Analyse-Tool ist so konfiguriert, dass lediglich Daten zur Nutzung der AUTHADA App, zum genutzten Endgerät und dessen Standort gesammelt werden. Die mögliche Übertragung von personenbezogenen Daten wurde durch AUTHADA deaktiviert (wiederkehrende Besuche) bzw. die Daten so anonymisiert (User-ID und IP-Adresse), dass kein Rückschluss auf eine Person vorgenommen werden kann.

Mit der weiteren Nutzung der AUTHADA App stimmen die Nutzer diesem Analyse-Verfahren zu.

Die AUTHADA nutzt das Analyse-Tool Sentry, um ein mögliches Fehlverhalten beim Absturz der App auswerten zu können. Nach einem Absturz wird ein Report erstellt, der die betroffenen Codestellen und die Geräteinformationen an AUTHADA versendet. Diese Daten werden auf dem Server der AUTHADA GmbH in Deutschland gespeichert. Es werden keine personenbezogenen Daten übermittelt. Die mögliche Übertragung von personenbezogenen Daten wurde durch AUTHADA deaktiviert (wiederkehrende

Besuche) bzw. die Daten so anonymisiert (User-ID und IP-Adresse), dass kein Rückschluss auf eine Person vorgenommen werden kann.

Mit der weiteren Nutzung der AUTHADA App stimmen die Nutzer diesem Analyse-Verfahren zu.

4. ZWECKBINDUNG

Sämtliche o. g. und im Rahmen des eID-Service angefallenen personenbezogenen Daten werden im Auftrag Ihrer Sparkasse bzw. deren Verbundpartner ausschließlich zur Identifizierung Ihrer Person nach den hierfür jeweils geltenden gesetzlichen und bankaufsichtsrechtlichen Vorgaben verwendet (erhoben, verarbeitet und genutzt). Zu den Verwendungszwecken sind die Sparkassen bzw. deren Verbundpartner aufgrund diverser gesetzlichen Anforderungen (z.B. Kreditwesengesetz, Geldwäschegesetz, Wertpapierhandelsgesetz, Steuergesetze) sowie aufgrund sparkassenaufsichtsrechtlichen Vorgaben (z.B. der Europäischen Zentralbank, der Europäischen Sparkassenaufsicht, der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht) verpflichtet. Die Verarbeitung erfolgt deshalb aufgrund gesetzlicher Vorgaben (Art. 6 Abs.1 Buchst. c DSGVO) und darüber hinaus nur, soweit von Sie eine Einwilligung zur Datenverarbeitung erteilt haben (Art. 6 Abs. 1 Buchst. a DSGVO). Soweit in dieser Datenschutzerklärung nichts anderes genannt ist, werden die Daten nicht an Dritte weitergegeben, es sei denn, es besteht eine gesetzliche Pflicht hierzu. Bei Verdacht auf Missbrauch, insbesondere bei Verdacht einer strafbaren Handlung behalten wir uns vor, die o. g. erforderlichen Daten inklusive IP-Adresse dauerhaft zu speichern und den Strafverfolgungsbehörden zu übermitteln. Die Mitarbeiter der S-Markt & Mehrwert GmbH & Co. KG sind zur Verschwiegenheit und dem Bank- und Datengeheimnis verpflichtet.

Kommt es zum Abbruch des Prozesses werden die bis dahin erhobenen Daten nach Wegfall des Zwecks gelöscht. Insofern Ihr Internet-Browser so konfiguriert ist, dass Formulardaten gespeichert werden, kann dies dazu führen, dass die Eingabefelder bei der Anmeldung für einen bestimmten Zeitraum befüllt bleiben. Um dies zu vermeiden, leeren Sie bitte den Speicher Ihres Internet-Browsers.

5. EINWILLIGUNG

Soweit Sie für die beschriebene Datenverarbeitung eine Einwilligung erteilt haben, kann diese Einwilligung jederzeit widerrufen werden. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

6. LÖSCHUNG IHRER DATEN

Die im Rahmen der Identifizierung erhobenen Daten und Fotos des Ausweisdokuments werden direkt nach der Übermittlung an die S-Markt & Mehrwert GmbH & Co. KG von den Servern der AUTHADA GmbH gelöscht. Die bei der S-Markt & Mehrwert erhobenen Daten werden nach Erreichen des Zwecks und Übergabe an die betreffende Sparkasse bzw. deren Verbundpartner in den Systemen der S-Markt & Mehrwert gelöscht. Die betreffende Sparkasse speichert die Daten gemäß gesetzlichen Vorgaben.

7. WEITERGABE UND HOSTING

Soweit im Rahmen des Vertragsabschlusses und der Vertragserfüllung notwendig, geben wir die Daten an die jeweiligen Vertragspartner (Sparkassen bzw. deren Verbundpartner) zur Erfüllung der unter 3. genannten Zweckbestimmungen weiter.

Zur technischen Umsetzung des eID-Service koope-

rieren wir mit dem Systemanbieter AUTHADA GmbH, Julius-Reiber-Straße 15a, 64293 Darmstadt. Die AUTHADA GmbH erfüllt alle Anforderungen an den Datenschutz und die Datensicherheit. Die technische Umsetzung findet ausschließlich auf Servern auf dem Gebiet der Bundesrepublik Deutschland statt. Details zum Datenschutz im Rahmen der Dienstleistung von AUTHADA finden Sie unter <https://authada.de/app-privacy> bzw. im Rahmen der Identifizierungsdienstleistung in der AUTHADA App.

8. SICHERHEIT

Der eID-Service erfolgt auf der Grundlage aktueller Sicherheitsstandards¹. Es werden dem Stand der Technik entsprechende technische und organisatorische Sicherheitsmaßnahmen eingesetzt, um den eID-Service und die darin verarbeiteten personenbezogenen Daten gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Beispielsweise sind sämtliche Kommunikationskanäle zwischen dem Ausweischip und der S-Markt & Mehrwert GmbH & Co. KG entsprechend dem Stand der Technik mit sicherheitstechnisch geeigneten Transport Layer Security (TLS) Mechanismen geschützt. Außerdem werden die eingesetzten Sicherheitsmaßnahmen entsprechend der technologischen Entwicklung fortlaufend überwacht und verbessert.

9. DATENSCHUTZRECHTE

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DSGVO).

¹ "Sicherer IT-Betrieb"

Bei Fragen zur Verarbeitung Ihrer persönlichen Daten wenden Sie sich bitte an den Datenschutzbeauftragten Ihrer Sparkasse bzw. des Verbundpartners.