Datenschutzerklärung für SkIDentity Identitätsmanagement

Die ecsec GmbH fungiert als Anbieter des SkIDentity-Identitätsmanagement-Dienstes und nimmt den Schutz Ihrer privaten Daten sehr ernst. Die besondere Beachtung der Privatsphäre bei der Verarbeitung personenbezogener Daten ist uns für uns ein äußerst wichtiges Anliegen. Insbesondere werden personenbezogene Daten strikt gemäß den gesetzlichen Bestimmungen, insbesondere denen der Datenschutzgrundverordnung (DSGVO), des deutschen Bundesdatensschutzgesetzes (BDSG), des Telemediengesetzes (TMG), des Personalausweisgesetzes (PAuswG) sowie der Personalausweisverordnung (PAuswV) erhoben, verarbeitet oder genutzt.

Zweck des SkIDentity-Identitätsmanagement-Dienstes

Der SkIDentity-Identitätsmanagement-Dienst ermöglicht es dem Inhaber eines elektronischen Ausweises („Nutzer“), Einsicht in seine in dem jeweiligen Ausweis gespeicherten personenbezogenen Daten („Attribute“) zu erhalten und aus diesen Daten eine abgeleitete elektronische Identität zu bilden, die auf dem System des Nutzers abgelegt, vom Ausweisinhaber eigenverantwortlich verwaltet und bei Bedarf für einen vollständig selbstbestimmten Identitätsnachweis oder eine pseudonyme Anmeldung bei weiteren Online-Diensten genutzt werden kann.

Eine über diese Zwecke hinausgehende Verwendung der Daten erfolgt durch den SkIDentity-Identitätsmanagement-Dienst nicht.

Art der verarbeiteten personenbezogenen Daten

Der Nutzer bestimmt, welcher Ausweis im SkIDentity-Identitätsmanagement-Dienst genutzt wird. Welche Attribute genau auf dem entsprechenden Ausweis gespeichert sind und folglich in die abgeleitete elektronische Identität übertragen werden können, hängt vom konkreten Ausweistyp ab. Es existiert eine Übersicht über die grundsätzlich vom SkIDentity-Dienst unterstützten Ausweise und Attribute und dem Nutzer wird unmissverständlich angezeigt, welche Attribute konkret aus dem Ausweis bzw. der abgeleiteten elektronischen Identität ausgelesen werden bzw. wurden. Beispielhaft sind hier einige Attribute des neuen Personalausweises (nPA) gemäß § 18 Abs. 3 S. 2 PAuswG aufgeführt: Familienname; Vorname; Tag der Geburt; Ort der Geburt; Anschrift; dienste- und kartenspezifisches Kennzeichen. Die jeweils verfügbaren Attribute können auf Wunsch des Nutzers in die abgeleitete elektronische Identität übernommen werden, welche auf dem System des Nutzers abgelegt werden kann. Der Nutzer kann die abgeleiteten elektronischen Identitäten eigenverantwortlich verwalten und auf andere Systeme, wie z.B. sein persönliches Mobiltelefon, übertragen oder die abgeleitete elektronische Identität löschen. Sofern der Nutzer die vorher erstellte abgeleitete elektronische Identität bei weiteren Online-Diensten für die pseudonyme Anmeldung oder den vollständig selbstbestimmten Identitätsnachweis einsetzt, werden sogenannte Identitätsbestätigungstoken erstellt, mittels derer die Echtheit der Identitätsdaten nachgewiesen werden kann.

Wesentliche Leistungen des SkIDentity-Identitätsmanagement-Dienstes

Überblick

Der SkIDentity-Identitätsmanagement-Dienst wird dem Nutzer unter https://service.skidentity.de zur Verfügung gestellt und kann durch Klick auf das „ID-Symbol“ erreicht werden. Er umfasst folgende Leistungen:

- Übersicht über verfügbare abgeleitete elektronische Identitäten
- Erstellen einer abgeleiteten elektronischen Identität
- Einsicht in Inhalte einer abgeleiteten elektronischen Identität
- Aktivieren und Deaktivieren einer abgeleiteten elektronischen Identität
- Übertragen einer abgeleiteten elektronischen Identität in ein anderes System
- Schützen einer abgeleiteten elektronischen Identität mit einer PIN
- Löschen einer abgeleiteten elektronischen Identität
- Nutzen einer abgeleiteten elektronischen Identität bei einem anderen Online-Dienst

Übersicht über verfügbare abgeleitete elektronische Identitäten

Nach dem Klick auf das „ID-Symbol“ wird dem Nutzer eine Übersicht über die grundsätzlich auf seinem System verfügbaren abgeleiteten elektronischen Identitäten geliefert. Ausgehend von dieser Übersicht kann der Nutzer abgeleitete elektronische Identitäten erstellen, verwalten, schützen, übertragen und schließlich wieder löschen.

Erstellung von abgeleiteten elektronischen Identitäten

Die Erstellung einer abgeleiteten elektronischen Identität umfasst den Identitätsnachweis des Nutzers gegenüber dem SkIDentity-Identitätsmanagement-Dienst, die Erstellung der abgeleiteten Identität durch den SkIDentity-Identitätsmanagement-Dienst und schließlich die Speicherung der abgeleiteten Identität im System des Nutzers.

Im Rahmen der Nutzung des neuen Personalausweises (nPA) fungiert der SkIDentity-Identitätsmanagement-Dienst als Diensteanbieter im Sinne von § 2 Abs. 3 PAuswG. Hierfür benötigt er ein Berechtigungszertifikat der Vergabestelle für Berechtigungszertifikate (VfB) beim Bundesverwaltungsamt (BVA). Das Berechtigungszertifikat ermöglicht dem SkIDentity-Identitätsmanagement-Dienst den technischen Zugriff auf die für den Geschäftszweck auch der weiteren Online-Dienste erforderlichen Daten des neuen Personalausweises. Die Kommunikation zwischen dem Nutzer und dem SkIDentity-Identitätsmanagement-Dienst erfolgt über eine Webanwendung in Verbindung mit einem geeigneten eID-Client gemäß BSI TR-03124. Für den Datenzugriff muss sich der SkIDentity-Identitätsmanagement-Dienst zunächst gegenüber dem Nutzer identifizieren. Im Anschluss kann der Nutzer über die Eingabe seiner Sicherheits-PIN die Daten freigeben, die in die abgeleitete elektronische Identität übernommen werden sollen.

Nach der Erstellung der abgeleiteten Identität durch den SkIDentity-Identitätsmanagement-Dienst wird diese im System des Nutzers gespeichert und die zwischenzeitlich im SkIDentity-Identitätsmanagement-Dienst vorhandenen Daten werden gelöscht.

Einsicht in Inhalte einer abgeleiteten elektronischen Identität

Der Benutzer kann Einsicht in die Inhalte einer abgeleiteten elektronischen Identität erhalten. Dies umfasst die Anzeige der in der abgeleiteten elektronischen Identität enthaltenen personenbezogenen Attribute sowie die Anzeige des Gültigkeitszeitraumes der abgeleiteten elektronischen Identität.

Bei der Einsicht in eine abgeleitete elektronische Identität liegen die Daten ausschließlich im lokalen System des Nutzers vor.

Aktivieren und Deaktivieren einer abgeleiteten elektronischen Identität

Eine im System des Nutzers abgelegte abgeleitete elektronische Identität kann vom Benutzer aktiviert oder deaktiviert werden. Der wesentliche Unterschied zwischen einer aktivierten oder deaktivierten abgeleiteten elektronischen Identität besteht darin, dass nur eine aktivierte abgeleitete elektronische Identität bei einem anderen Online-Dienst genutzt werden kann.

Die Aktivierung und Deaktivierung einer abgeleiteten elektronischen Identität erfolgt ausschließlich im lokalen System des Nutzers.

Übertragen einer abgeleiteten elektronischen Identität in ein anderes System

Der Nutzer kann eine in seinem System abgelegte abgeleitete elektronische Identität an ein anderes technisches System, wie z.B. sein persönliches Mobiltelefon, übertragen.

Sofern die Übertragung mit Unterstützung des SkIDentity-Identitätsmanagement-Dienstes erfolgt, werden die zwischenzeitlich dort vorhandenen Daten sofort nach der Übertragung wieder gelöscht.

Schützen einer abgeleiteten elektronischen Identität mit einer PIN

Zum Schutz vor unautorisierter Einsichtnahme und missbräuchlicher Nutzung kann eine im System des Nutzers abgelegte abgeleitete elektronische Identität vom Nutzer mit einer Sicherheits-PIN versehen werden.

Der Schutz einer abgeleiteten elektronischen Identität mit einer PIN, bzw. das Entfernen des PIN-Schutzes, wird jeweils durch den Nutzer initiiert.

Sperren und löschen einer abgeleiteten elektronischen Identität

Der Nutzer kann eine elektronische Identität sperren und unwiederbringlich löschen.

Nutzen einer abgeleiteten elektronischen Identität bei einem anderen Online-Dienst

Der Nutzer kann eine auf seinem System abgelegte und aktivierte abgeleitete elektronische Identität bei anderen Online-Diensten für einen vollständig selbstbestimmten Identitätsnachweis oder eine pseudonyme Anmeldung nutzen. Hierbei wird eine Kopie der im System des Nutzers abgelegten abgeleiteten elektronischen Identität an den SkIDentity-Identitätsmanagement-Dienst übertragen, damit dieser ein Identitätsbestätigungstoken für den entsprechenden Online-Dienst erstellt, das der Nutzer zurück erhält und in einem wohlinformierten und selbstbestimmten Prozess an den entsprechenden Online-Dienst weiterleiten kann. Mit dem bereitgestellten Identitätsbestätigungstoken kann die Echtheit der Identitätsdaten nachgewiesen werden.

Sämtliche auf diese Weise nutzbaren Online-Dienste liegen außerhalb des Verantwortungsbereichs des SkIDentity-Identitätsmanagement-Dienstes. Zwar wird beim Anschluss von Online-Diensten an den SkIDentity-Identitätsmanagement-Dienst angelehnt an § 21 Abs. 2 PAuswG darauf geachtet, dass

- der dem Nutzer angezeigte Zweck des Online-Dienstes zutreffend und nicht rechtswidrig ist,
- der Zweck des Online-Dienstes nicht in der geschäftsmäßigen Übermittlung der Identitätsdaten (z.B. für Werbezwecke) besteht,

- die angefragten Daten für den angegebenen Zweck des Online-Dienstes erforderlich sind, indem nur Dienste angeschlossen werden, für die die gleichen Datenfelder erforderlich i.S.d. § 21 Abs. 2 Nr. 3 PAuswG sind, wie für das Berechtigungszertifikat, das für SkIDentity erteilt wurde,
- der Online-Dienst gemäß dem Stand der Technik geeignete technische und organisatorische Maßnahmen für den Datenschutz umgesetzt hat und
- insgesamt keine Anhaltspunkte für eine missbräuchliche Verwendung der Identitätsdaten des Nutzers durch den Online-Dienst vorliegen.

Hierfür kann allerdings seitens des SkIDentity-Identitätsmanagement-Dienstes keine Gewähr übernommen werden. Deshalb muss sich der Nutzer selbständig von der Rechtmäßigkeit des Online-Dienstes und der dortigen Einhaltung der Datenschutzvorschriften überzeugen.

Der SkIDentity-Identitätsmanagement-Dienst speichert die personenbezogenen Daten des Ausweisinhabers nicht dauerhaft, er verfolgt keine Transaktionen mit angeschlossenen Online-Diensten und erstellt keine Nutzungsprofile. Sämtliche Daten bei dem SkIDentity-Identitätsmanagement-Dienst werden umgehend gelöscht, sobald sie in die Sphäre des Nutzers, z.B. in seinen Browser, gelangt sind. IP-Adressen werden ebenfalls nicht dauerhaft gespeichert.

Der Nutzer muss vor der erstmaligen Nutzung des SkIDentity-Identitätsmanagement-Dienstes explizit das Lesen der vorliegenden Datenschutzerklärung und sein Einverständnis mit den in dieser Erklärung dargelegten Praktiken bestätigen.

Bei der Verwendung anderer Ausweise als den neuen Personalausweis sind die grundlegenden Abläufe identisch, mit dem Unterschied, dass der SkIDentity-Identitätsmanagement-Dienst hierzu kein Berechtigungszertifikat der Vergabestelle für Berechtigungszertifikate benötig und die Kommunikation möglicher Weise nicht über einen eID-Client gemäß BSI TR-03124 abgewickelt wird.

Sicherheit

Die ecsec GmbH setzt dem Stand der Technik entprechende technische und organisatorische Sicherheitsmaßnahmen ein, um den SkIDentity-Identitätsmanagement-Dienst und die darin verwalteten personenbezogenen Daten gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Beispielsweise sind sämtliche Kommunikationskanäle zwischen dem System des Nutzers und dem SkIDentity-Identitätsmanagement-Dienst 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.

Speicherung von Daten im System des Nutzers

Der SkIDentity-Identitätsmanagement-Dienst speichert die abgeleiteten elektronischen Identitäten im lokalen System des Nutzers, so dass nur der Nutzer bzw. Personen mit lokalem Zugriff auf das System des Nutzers und der SkIDentity-Identitätsmanagement-Dienst aber nicht auch weitere Online-Dienste auf diese Daten zugreifen können. Sofern der Zugriff auf das System des Nutzers nicht anderweitig kontrolliert wird, wird der Schutz der abgeleiteten elektronischen Identität durch eine entsprechende Sicherheits-PIN empfohlen.

Protokolldaten

Im SkIDentity-Identitätsmanagement-Dienst werden zur Aufrechterhaltung des technischen Betriebs verschiedene technische Protokolldaten erzeugt. Hierbei werden grundsätzlich keine personenbezogenen Daten erfasst.

Links zu anderen Websites

Das unter http://skidentity.de verfügbare Online-Angebot des SkIDentity-Projektes enthält Links zu anderen Websites. Diese Webseiten unterliegen der Haftung der jeweiligen Seitenbetreiber. Bei Verknüpfung der externen Links waren keine Rechtsverstöße ersichtlich. Auf die aktuelle und künftige Gestaltung der verlinkten Seite hat der Anbieter keinen Einfluss. Die permanente Überprüfung der externen Links ist für den Anbieter ohne konkrete Hinweise auf Rechtsverstöße nicht zumutbar. Bei Bekanntwerden von Rechtsverstößen werden die betroffenen externen Links unverzüglich gelöscht.

Rechte des Betroffenen

Der Nutzer kann die Einwilligung in die Verarbeitung seiner Daten durch den SkIDentity-Identitätsmanagement-Dienst, die durch die Ausstellung der abgelegten abgeleiteten elektronischen Identität und die Speicherung im lokalen System des Benutzers protokolliert wird, jederzeit widerrufen, indem er wie oben erläutert die abgeleitete elektronische Identität löscht. Der Nutzer hat das Recht, Auskunft über Art und Umfang der zu seiner Person gespeicherten Daten, die Herkunft der Daten und die an den SkIDentity-Identitätsmanagement-Dienst angeschlossenen Online-Dienste, die im Rahmen des vollständig selbstbestimmten Identitätsnachweises als potenzielle Empfänger der Daten auftreten können, zu erhalten und die strukturierte Bereitstellung seiner Daten anzufordern. Diese Informationen stehen dem Nutzer über die regulären Verwaltungsfunktionen des SkIDentity-Identitätsmanagement-Dienstes bzw. über das ergänzende Online-Angebot unter http://skidentity.de zur Verfügung. Für weiter gehende Anfragen kann der Nutzer die unter „Verantwortliche Stelle“ aufgeführten Kontaktdaten nutzen.

Verantwortliche Stelle

Verantwortliche Stelle gemäß Art. 4 Nr. 7 DSGVO für den SkIDentity-Identitätsmanagement-Dienst ist die

ecsec GmbH
Sudetenstrasse 16
96247 Michelau
http://www.ecsec.de ,

vertreten durch die Geschäftsführer Tina Hühnlein und Dr. Detlef Hühnlein. Weitere Informationen finden sich im Impressum der ecsec GmbH.

Datenschutzaufsichtsbehörde

Die zuständige Datenschutzaufsichtsbehörde gemäß Art. 51 DSGVO für den SkIDentity-Identitätsmanagement-Dienst ist das

Landesamt für Datenschutzaufsicht

Promenade 27
91522 Ansbach
http://www.lda.bayern.de/ .