

Principes voor de verwerking van persoonlijke gegevens (Privacybeleid)

Versie 7.0

Geldig vanaf: 10.10.2022

Versies en veranderingen		
Datum	Versie	Veranderingen
10 Oktober 2022	7.0	• Lijst met verwerkte persoonsgegevens bijgewerkt en opnieuw gestructureerd • Legitiem belang toegevoegd als rechtsgrondslag voor het verwerken en openbaar maken van persoonsgegevens • Secundaire aanbieders van abonneeverificatie toegevoegd als bron van persoonsgegevens • Informatie over cookies toegevoegd • Uitleg en formulering verbeterd
28 september 2020	6.0	• Informatie over MyID-portaal • Toegevoegd Informatie over het geografische gebied van gegevensverwerking • Toegevoegd Informatie over de mogelijkheid om een klacht in te dienen bij de Letse en Litouwse toezichthoudende autoriteiten. • Documentstructuur • bijgewerkt Websiteadressen en e-mailadressen bijgewerkt
5 december 2019	5.0	• De lijst met verwerkte persoonsgegevens gewijzigd • De structuur en inhoud van het document bijgewerkt • Informatie over de verwerking van persoonsgegevens van minderjarigen toegevoegd • Informatie over de verwerking van bijzondere categorieën persoonsgegevens toegevoegd • Informatie over geautomatiseerde besluiten toegevoegd • Informatie over de bronnen van persoonsgegevens toegevoegd • Informatie over de bewaartermijn van persoonsgegevens bijgewerkt • De contactgegevens van de functionaris voor gegevensbescherming toegevoegd
10 december 2018	4.0	• De lijst met verwerkte persoonsgegevens gewijzigd • Uitleg toegevoegd over de rechtsgronden voor verwerking • Informatie toegevoegd over de overdracht van persoonsgegevens naar e-diensten
25 mei 2018	3.0	• Bijgewerkt volgens de vereisten van de Algemene Verordening Gegevensbescherming (hierna "GDPR" genoemd), die op 25 mei 2018 van kracht is geworden

1 maart 2018	2.0	• Titel van het document gewijzigd • Inhoud en structuur herzien • Lijst met verzamelde persoonsgegevens bijgewerkt • Voorwaarden voor het wijzigen van de principes herzien • Informatie over de versie van het document toegevoegd
22 december 2011	1.0	• Eerste openbare versie (Principes voor de bescherming van klantgegevens)

1. Algemene informatie

Deze beginselen voor de verwerking van persoonsgegevens beschrijven hoe SK ID Solutions AS (hierna "SK" genoemd) als verwerkingsverantwoordelijke de bescherming van persoonsgegevens waarborgt in overeenstemming met de toepasselijke wetgeving bij het aanbieden van de diensten Smart-ID en Mobile-ID en de certificeringsdienst voor de Estse ID-kaart, digi-ID, e-resident digi-ID, verblijfsvergunningskaart en diplomatieke identiteitskaart. Het doel van deze beginselen is om abonnees te informeren over de relevante onderwerpen met betrekking tot de verwerking van persoonsgegevens en om de beginselen te introduceren die SK volgt bij de verwerking van persoonsgegevens.

Deze beginselen hebben geen betrekking op de opslag en verwerking van gegevens van rechtspersonen of andere instellingen.

Indien u vragen heeft over de verwerking van persoonsgegevens, verzoeken wij u vriendelijk contact met ons op te nemen via de volgende contactgegevens:

Verwerkingsverantwoordelijke:

SK ID Solutions AS

Adres: Pärnu mnt 141, 11314 Tallinn, Estland

Telefoon: +372 610 1880

E-mail: info[A]skidsolutions.eu

Fax: +372 610 1881

Registratienummer: 10747013

Functionaris voor gegevensbescherming:

E-mail: dpo[A]skidsolutions.eu

2. Definities

Hieronder lichten we de definities en afkortingen toe die in deze beginselen worden gebruikt.

2.1. Wat is de AVG?

Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).

SK verwerkt persoonsgegevens in overeenstemming met de AVG en andere relevante wetgeving inzake gegevensbescherming. Houd er echter rekening mee dat SK als vertrouwensdienstverlener ook de bijzondere vereisten voor de verwerking van persoonsgegevens volgt die zijn vastgelegd in de eIDAS-verordening.

2.2. Wat is de eIDAS-verordening?

Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

Als vertrouwensdienstverlener laat SK zich bij haar activiteiten en dienstverlening leiden door de eIDAS-verordening. De verordening is rechtstreeks van toepassing in de Europese Unie en bevat eisen en voorwaarden voor het verlenen van verschillende vertrouwensdiensten, met inbegrip van specifieke eisen voor de verwerking van persoonsgegevens.

2.3. Wat zijn persoonsgegevens en wat is de verwerking van persoonsgegevens?

Persoonsgegevens zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, ongeacht de vorm of het formaat waarin dergelijke gegevens bestaan. De verwerking van persoonsgegevens is elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens (incl. verzamelen, vastleggen, opslaan, wijzigen, toegang verlenen, opvragen en meedelen, enz.), ongeacht de wijze waarop de bewerkingen worden uitgevoerd of de gebruikte middelen.

2.4. Wie is een derde?

Een derde is iedere persoon (zowel rechts- als natuurlijke personen) die geen contractuele klant, werknemer of gemachtigde verwerker van SK is.

2.5. Wat is een verwerkingsverantwoordelijke?

Een verwerkingsverantwoordelijke is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan dat de doeleinden en middelen van de verwerking van persoonsgegevens vaststelt. In de context van dit document is SK de verwerkingsverantwoordelijke.

2.6. Wat is een verwerker?

Een verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan dat contractueel door SK is aangesteld om namens de verwerkingsverantwoordelijke persoonsgegevens te verwerken.

2.7. Wat is een certificaat?

Een certificaat is een digitaal gegeven dat elektronische ondertekening en identiteitsverificatie vergemakkelijkt en waarin de publieke sleutel betrekking heeft op de natuurlijke persoon die eigenaar is van het certificaat. Certificaten die ofwel elektronische identiteitsverificatie ofwel elektronische ondertekening mogelijk maken, zijn gerelateerd aan persoonsgegevens.

2.8. Wat is een e-dienst?

Een e-dienst is een informatiesysteem, applicatie of e-omgeving die gebruik maakt van door SK geleverde diensten (Mobile-ID, Smart-ID, ID-kaart) voor de authenticatie van personen of het mogelijk maken van elektronische handtekeningen.

2.9. Wat is een registratieautoriteit?

Een registratieautoriteit is een organisatie die verantwoordelijk is voor de identificatie en authenticatie van personen. Daarnaast kan een registratieautoriteit certificaataanvragen accepteren, verifiëren en/of naar SK doorsturen.

3. SK's principles on processing personal data

Privacy en de bescherming van persoonsgegevens zijn voor ons zeer belangrijk. Daarom hebben we de nodige organisatorische, fysieke en informatietechnologische beveiligingsmaatregelen getroffen om de integriteit, beschikbaarheid en vertrouwelijkheid van de gegevens te waarborgen.

We hebben de persoonsgegevens die we nodig hebben voor de dienstverlening in kaart gebracht en het doel, de omvang en de termijn waarvoor we dergelijke gegevens moeten bewaren, gespecificeerd. We hebben eisen en instructies vastgelegd voor de werknemers en gemachtigde verwerkers van SK over hoe zij persoonsgegevens op een correcte manier moeten verwerken. We verlenen alleen toegang tot persoonsgegevens aan getrainde medewerkers en gemachtigde verwerkers die een relevant antecedentenonderzoek hebben doorstaan. De werknemers en het gemachtigde personeel van SK zijn zich ervan bewust dat zij het recht hebben persoonsgegevens alleen te verwerken voor zover dat nodig is voor de uitvoering van hun taken of, zoals in het geval van gemachtigde verwerkers, voor de nakoming van de contractuele verplichtingen.

Wij bevestigen dat de verwerking van persoonsgegevens rechtmatig, eerlijk, doelgericht, minimaal, veilig en transparant is. Al onze activiteiten worden geleid door de toepasselijke EU-, Estse en andere relevante wetgeving, het beleid en de beginselen van SK, alsmede de onderhavige beginselen voor de verwerking van persoonsgegevens. Het beleid en de beginselen van SK zijn beschikbaar op de website van SK: <https://www.skidsolutions.eu/en/repository/>.

SK is gecertificeerd volgens de norm ISO/IEC 27001: 2013 "Informatietechnologie. Beveiligingstechnieken. Managementsystemen voor informatiebeveiliging." Dit is een norm die eisen stelt aan de beheerprocessen van het informatiebeveiligingssysteem van de organisatie en aan kritieke informatiebeveiligingsactiva, met inbegrip van technische, fysieke en organisatorische beveiligingsmaatregelen ter bescherming van persoonsgegevens.

4. Bronnen van persoonsgegevens

SK verkrijgt persoonsgegevens uit de volgende bronnen:

- Van de persoon zelf;
- Persoonlijke apparaten (in het geval van Smart-ID);

- Registers (bv. bevolkingsregisters);
- Aanbieders van e-diensten;
- Registratieautoriteiten, aanbieders van e-identificatie en aanbieders van secundaire authenticatie voor abonnees (bv. banken, mobiele operatoren, de Politie- en Grenswachtraad).

5. Rechtmatigheid van de verwerking van persoonsgegevens

SK verwerkt persoonsgegevens alleen op een eerlijke en rechtmatige wijze. SK bevestigt dat zij persoonsgegevens alleen voor duidelijk omschreven en legitieme doeleinden verwerkt en de verwerking van persoonsgegevens beperkt tot het minimum dat nodig is om die doeleinden te bereiken.

Wij verwerken persoonsgegevens op de volgende rechtsgronden:

- **Uitvoering van een overeenkomst:** De verwerking van persoonsgegevens voor de uitvoering van een overeenkomst betekent dat wij persoonsgegevens nodig hebben om een kwaliteitsvolle dienst te verlenen. Wij hebben vastgesteld welke persoonsgegevens SK nodig heeft om diensten te verlenen en houden de hoeveelheid verwerkte persoonsgegevens tot een minimum beperkt.
- **Voldoen aan een wettelijke verplichting:** Het voldoen aan wettelijke verplichtingen is de verwerking van persoonsgegevens die SK als dienstverlener wettelijk verplicht is uit te voeren. Wij verwerken bijvoorbeeld persoonsgegevens in antwoord op wettelijk gemotiveerde verzoeken van wetshandavingsinstanties.
- **Toestemming:** In sommige gevallen verwerken wij persoonsgegevens op basis van de toestemming van de betrokkene. Wij vragen bijvoorbeeld toestemming voor de verwerking van biometrische gegevens in het geval van het gebruik van een biometrische identificatiemethode voor het registreren van Smart-ID. Daarnaast verwerken wij op basis van toestemming persoonsgegevens in antwoord op verzoeken die persoonsgegevens bevatten. In dit geval wordt de toestemming voor de verwerking van persoonsgegevens gegeven door het verzoek naar SK te sturen.
- **Gerechtvaardigd belang:** In sommige gevallen is de verwerking van persoonsgegevens gebaseerd op een gerechtvaardigd belang. Dit betekent dat de verwerking noodzakelijk is voor een doel van SK of een derde partij dat zwaarder weegt dan de rechten van de betrokkene. Op basis van een gerechtvaardigd belang verwerken wij bijvoorbeeld bepaalde apparaatgegevens om veiligheidsredenen.

6. Welke persoonsgegevens en voor welke doeleinden verwerken wij?

SK verwerkt persoonsgegevens voor de volgende doeleinden:

- **Uitgifte en beheer van certificaten:** SK geeft Smart-ID, Mobile-ID en certificaten uit voor Estse identiteitsdocumenten zoals de ID-kaart, digi-ID, e-resident digi-ID, verblijfsvergunningskaart en diplomatieke identiteitskaart. SK zorgt ook voor het intrekken van de certificaten en, in het geval van identiteitsdocumenten, ook voor het opschorten en het beëindigen van de opschorting van de certificaten.
- **Het gebruik van de certificaten mogelijk maken:** SK maakt het gebruik van Smart-ID, Mobile-ID en Estse identiteitsdocumenten voor authenticatie en elektronische ondertekening mogelijk.
- **Afhandelen van verzoeken om persoonsgegevens:** Indien een persoon zelf of een onderzoeks- of andere autoriteit persoonsgegevens opvraagt bij SK, verwerken wij de gevraagde gegevens om het antwoord samen te stellen. De verzoeker moet een wettelijke basis hebben om de gegevens op te vragen. De verzoeken hebben betrekking op de uitgifte en het beheer van Smart-ID, Mobile-ID en certificaten van identiteitsdocumenten en/of het gebruik van de certificaten voor authenticatie en elektronische ondertekening.
- **Afhandelen van verzoeken die persoonsgegevens bevatten:** Indien een persoon een verzoek naar SK stuurt dat zijn/haar persoonsgegevens bevat, verwerkt SK de gegevens om het verzoek te behandelen en te beantwoorden.

Hierna zullen we voor elke activiteit meer in detail uitleggen wat het doel van de verwerking is, de rechtsgrond voor de verwerking en welke persoonsgegevens we verwerken.

Doel voor verwerking	Rechtsgrondslag	Welke persoonsgegevens worden of mogen worden verwerkt?
Uitgifte en onderhoud van certificaten		
Dienstverlening	Verwerking is noodzakelijk om de overeenkomst na te komen; Biometrische gegevens worden verwerkt op basis van toestemming	• Person's given name(s) and surname(s); • Persoonlijk identificatienummer en het land dat de persoonlijke identificatiecode heeft afgegeven; • Contactgegevens; • Taal van de communicatie; • Gegevens identiteitsdocument en/of een kopie van het identiteitsdocument dat is gebruikt voor het aanvragen van de certificaten; • Een aanvraagformulier voor het aanvragen van een certificaat, elektronisch ondertekend of met een handgeschreven handtekening; • Estische verblijfplaats of e-verblijfplaats; • Registratiemethode (elektronisch of in het klantenservicepunt) en/of gegevens van het klantenservicepunt; • Apparaatgegevens (alleen in geval van elektronische registratie van Smart-ID en Mobile-ID); • Gegevens certificaten; • Gegevens met betrekking tot de levenscyclus van certificaten en de handelingen die de persoon heeft verricht bij het gebruik van de dienst (opschorting van certificaten, beëindiging van opschorting, intrekking van certificaten, afgifte van PIN-

		enveloppen, verlenging van certificaten, verificatie van informatie over de geldigheid van certificaten); • SIM-kaartgegevens en mobiele operator (alleen in het geval van Mobile-ID); • Geboortedatum en Smart-ID rekeningnummer (alleen in het geval van Smart-ID); • Aanvullende informatie voor Smart-ID certificaataanvragen met de biometrische identificatiemethode: land van verblijf van de persoon, aanvullende gegevens van document gebruikt bij registratie (documenttype, land van afgifte, documentnummer, nationaliteit, geboortedatum, geslacht, vervaldatum document, gezichtsopname van de persoon, technische gegevens vereist voor verificatie van de authenticiteit van het document), video opgenomen over biometrische identificatie, aantal mislukte registratiepogingen, informatie over de geldigheid van het document uit het PRADO-register. • In het geval van Mobile-ID en Smart-ID controleren we aan de hand van het bevolkingsregister de juistheid van de naam, het persoonlijke identificatienummer, de status van de aanvrager (levend, overleden) en in het geval van minderjarigen informatie over de wettelijke voogden.
Gebruik van de certificaten voor authenticatie of elektronische ondertekening		
Dienstverlening	Verwerking is noodzakelijk om de overeenkomst na te komen	• Voorna(a)m(en) en achterna(a)m(en) van de persoon; • Persoonlijk identificatienummer, voor niet-Baltische burgers paspoortnummer of ID-kaartnummer; • IP-adres van het informatiesysteem waarin informatie over de geldigheid van het certificaat werd opgevraagd; • Telefoonnummer en communicatietaal; • IP-adres van het netwerk dat door het apparaat wordt gebruikt, apparaatgegevens, status van PIN-codes in geval van Smart-ID; • E-serviceprovider wiens dienst wordt gebruikt; • Bij gebruik van Smart-ID en Mobile-ID, de tekst die door de e-dienst naar uw apparaat wordt verzonden.
Vragen om persoonsgegevens		
Reageren op vraag	Afhankelijk van de vraag kan de rechtsgrondslag toestemming, recht of legitiem belang zijn. Merk op dat de verzoeker de persoon zelf kan zijn of een onderzoek of andere	Gegevens die door de verzoeker worden opgevraagd.

	autoriteit die een wettelijke basis heeft om de gegevens op te vragen.	
Vragen die persoonlijke gegevens bevatten		
Antwoord op vraag	Toestemming	Gegevens die in het verzoek aan SK worden doorgegeven.

Bij authenticatie bij een e-dienst of het ondertekenen van een document worden persoonsgegevens (bv. naam en persoonlijk identificatienummer) naar de e-dienstverlener gestuurd voor het verlenen van de dienst. Dit gebeurt pas na het invoeren van de pincode. Het invoeren van de pincode wordt beschouwd als toestemming voor het verzenden van de gegevens.

6.1. Verwerking van persoonsgegevens van minderjarigen

De diensten van SK zijn beschikbaar voor gebruik door minderjarigen. Minderjarigen hebben toestemming van een ouder of voogd nodig voor de registratie van een gekwalificeerde Smart-ID, het afsluiten van een Mobile-ID-contract en aanvragen voor een ID-kaart.

Minderjarigen kunnen een niet-gekwalificeerde of een Smart-ID Basic met beperkte rechten aanvragen in het kader van een contract voor bankdiensten. Indien een ouder of wettelijke voogd een dergelijke machtiging heeft verleend via een contract voor bankdiensten, heeft een minderjarige geen afzonderlijke machtiging nodig voor een aanvraag voor een niet-gekwalificeerde Smart-ID. Meer informatie over gekwalificeerde en niet-gekwalificeerde Smart-ID vindt u op het Smart-ID portaal.

Een ouder of wettelijke voogd aanvaardt de aansprakelijkheid voor de gevolgen van het gebruik van de door SK geleverde diensten (Mobile-ID, Smart-ID, ID-kaart). Zij moeten de minderjarige ook de gebruiksvoorwaarden van de certificaten en de veiligheidseisen voor het gebruik van de dienst uitleggen.

SK verwerkt voor minderjarigen dezelfde persoonsgegevens als voor volwassenen, alsmede informatie over de toestemming van de ouder of wettelijke voogd en de band tussen het kind en de ouder/voogd (zie tabel in Hoofdstuk 6).

6.2. Verwerking van bijzondere categorieën van persoonsgegevens

Overeenkomstig de AVG mogen bijzondere categorieën van persoonsgegevens worden verwerkt op basis van de uitdrukkelijke toestemming van de persoon. Als u de biometrische identificatiemethode selecteert voor authenticatie bij de registratie van Smart-ID, zal SK u tijdens het registratieproces om uw toestemming vragen om uw biometrische persoonsgegevens te verwerken. De biometrische gegevens die worden verwerkt, zijn een gezichtsafbeelding die wordt geëxtraheerd uit een video die u van uzelf hebt opgenomen. De verwerking van de gezichtsafbeelding is noodzakelijk om u te identificeren tijdens de registratie van uw Smart-ID-account. Daarnaast kan SK vervolgccontroles uitvoeren op basis van uw biometrische gegevens om de veiligheid van uw elektronische identiteit te waarborgen en de kwaliteit van de gebruikte technische oplossing te testen.

Biometrische gegevens worden niet verwerkt in het geval van andere Smart-ID-registratiemethoden, zoals via een banklink of een filiaal, Mobile-ID, Smart-ID of ID-kaart

7. Geografisch gebied van gegevensverwerking

In de regel verwerkt SK uw persoonsgegevens binnen de Europese Unie of de Europese Economische Ruimte. Indien wij verwerkers inschakelen die buiten dit gebied gevestigd zijn, doen wij dit op basis van een adequaatheidsbesluit van de Europese Commissie (EC), ondertekenen wij standaard contractuele bedingen met de partner of treffen wij andere passende waarborgen.

8. Geautomatiseerde besluitvorming

Onder de AVG heeft een persoon het recht dat er geen besluiten over hem worden genomen die uitsluitend gebaseerd zijn op geautomatiseerde verwerking en die rechtsgevolgen voor hem hebben of hem op vergelijkbare wijze aanzienlijk treffen. Geautomatiseerde besluiten mogen worden genomen als dit noodzakelijk is voor de uitvoering van een overeenkomst tussen een verwerkingsverantwoordelijke en een persoon, als dit wettelijk is toegestaan of met de uitdrukkelijke toestemming van een persoon.

SK neemt geautomatiseerde besluiten op basis van uw biometrische gegevens (gezichtsafbeelding) met behulp van een verwerker voor identificatie, indien u de biometrische identificatiemethode gebruikt voor de registratie van een Smart-ID-account. In dit geval zal SK u tijdens het registratieproces om uw desbetreffende toestemming vragen. Dergelijke geautomatiseerde besluiten worden niet genomen in het geval van andere Smart-ID-registratiemethoden, zoals via een banklink of een filiaal, Mobile-ID, Smart-ID of ID-kaart.

SK neemt ook geautomatiseerde besluiten over de afgifte of weigering van een certificaat op basis van gegevens uit registers en valideert elektronische certificaataanvragen via een geautomatiseerd besluit.

Daarnaast nemen wij geautomatiseerde besluiten om frauduleuze activiteiten te voorkomen en op te sporen.

9. Rechten van de betrokkene

De betrokkene heeft het recht op inzage in zijn/haar persoonsgegevens en kan verzoeken om rectificatie, verwijdering, overdracht van gegevens en beperking van de verwerking.

Om de hierboven genoemde rechten uit te oefenen, kunt u een elektronisch ondertekend verzoek sturen naar het e-mailadres info@skidsolutions.eu. Wij zullen binnen 30 dagen op uw verzoek reageren.

Wij benadrukken dat aan het verzoek niet kan worden voldaan in de volgende gevallen:

- de identiteit van de aanvrager kan niet worden vastgesteld;
- de aanvrager is niet wettelijk verbonden met de gegevens;
- dit zou in strijd zijn met de eisen van bijzondere wetten;
- dit zou in strijd zijn met de wettelijke verplichtingen van SK;
- het kan de rechten en vrijheden van een andere persoon schaden;

- dit kan de verlening van de dienst of het niet verlenen van de dienst belemmeren;
- dit kan het werk van wetshandhavinginstanties belemmeren;
- het is technisch niet mogelijk.

Daarnaast kunt u op het MyID-portaal toegang krijgen tot uw Mobile-ID-, Smart-ID-, ID-kaart- en digi-ID-accounts en hun geschiedenis. Voor ID-kaart, digi-ID en Mobile-ID kunt u daar ook de geschiedenis van al uw transacties (authenticatie en ondertekening) bekijken. Informatie over uw Smart-ID-accounts en transacties die met Smart-ID zijn uitgevoerd, is te vinden op het Smart-ID-portaal.

Indien de verwerking van persoonsgegevens is gebaseerd op toestemming, kunt u uw toestemming te allen tijde intrekken door een elektronisch ondertekende aanvraag in te dienen op het e-mailadres [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu).

Mocht u van mening zijn dat uw rechten met betrekking tot de verwerking van persoonsgegevens zijn geschonden, dan verzoeken wij u een elektronisch ondertekende klacht te sturen via e-mail naar [dpo\[A\]skidsolutions.eu](mailto:dpo[A]skidsolutions.eu). Wij zullen uw e-mail binnen 30 dagen beantwoorden. Indien u van mening bent dat SK uw persoonsgegevens niet verwerkt in overeenstemming met de relevante wetgeving, kunt u een klacht indienen bij uw nationale gegevensbeschermingsautoriteit (bv. de Estse Inspectie voor gegevensbescherming, de Letse Staatsinspectie voor gegevens, de Litouwse Staatsinspectie voor gegevensbescherming).

10. Gebruik van gegevens via een gemachtigde verwerker

SK heeft het recht om, op grond van de overeenkomst, een andere persoon (d.w.z. zowel natuurlijke als rechtspersonen) te machtigen om persoonsgegevens te verwerken. Gemachtigde verwerkers zijn bijvoorbeeld partners van SK bij de uitgifte en het beheer van certificaten en het oplossen van klantproblemen. SK als verwerkingsverantwoordelijke geeft de gemachtigde verwerker de nodige instructies voor de gegevensverwerking. SK is verantwoordelijk voor de naleving door de gemachtigde verwerker van de vereisten voor de verwerking van persoonsgegevens. Een gemachtigde verwerker mag persoonsgegevens alleen verwerken voor het bereiken van het doel. SK bevestigt dat met alle gemachtigde verwerkers gegevensverwerkingsovereenkomsten zullen worden gesloten. Een lijst van de gemachtigde verwerkers van SK is [hier](#) beschikbaar.

Een e-dienst die uw persoonsgegevens opvraagt bij SK op basis van door u geïnitieerde authenticatie of elektronische ondertekening, is geen gemachtigde verwerker van SK in de zin van de AVG.

11. Openbaarmaking of mededeling van persoonsgegevens aan derden

SK maakt geen persoonsgegevens openbaar of verstrekt deze niet aan derden, behalve in de volgende gevallen:

- Een dergelijke verplichting vloeit voort uit de toepasselijke wetgeving of de op grond daarvan vastgestelde maatregelen (bv. overdracht aan een opsporingsinstantie);
- Dergelijke partijen zijn betrokken bij het verlenen van de diensten;
- De derde partij heeft een gerechtvaardigd belang om de gegevens bij SK op te vragen;

- SK heeft het recht om ten behoeve van de uitvoering van een overeenkomst of de waarborging van de uitvoering van een overeenkomst de gegevens openbaar te maken aan derden, met inbegrip van kredietinformatie- en incassobureaus en andere personen die zich bezighouden met schuldvorderingen, alsook aan juridisch adviseurs en gerechtsdeurwaarders indien de betrokkene de overeenkomst niet is nagekomen;
- De betrokkene geeft zijn/haar schriftelijke toestemming om de informatie aan andere derden openbaar te maken.

SK bevestigt dat zij persoonsgegevens alleen aan derden zal verstrekken voor zover dit noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.

SK maakt uw geldige Estse certificaten met betrekking tot identiteitsdocumenten (incl. Mobile-ID uitgegeven tot 02.07.2022) tijdens hun geldigheidsduur openbaar via de LDAP-dienst. Aanvullende informatie over de LDAP-dienst is [hier](#) beschikbaar.

12. Bewaartermijn van persoonsgegevens

SK verwerkt persoonsgegevens alleen zolang als nodig is voor de vervulling van de doeleinden waarvoor de persoonsgegevens zijn verzameld of voor de vervulling van de verplichtingen die voortvloeien uit de toepasselijke wetgeving. Houd er rekening mee dat wij ons voor het verlenen van vertrouwensdiensten laten leiden door de eIDAS-verordening en de Estse Wet op elektronische identificatie en vertrouwensdiensten voor elektronische transacties voor de opslag van persoonsgegevens.

SK is verplicht om bewijsmateriaal dat is gebruikt om u te identificeren tijdens de uitgifte van certificaten ten minste 10 jaar na het verstrijken van het certificaat te bewaren, en logboeken met betrekking tot de procedures die zijn uitgevoerd tijdens het verlenen van vertrouwensdiensten ten minste 10 jaar te bewaren om, indien nodig, misbruik van uw identiteit en de juistheid van de handelingen van SK bij het verlenen van diensten te kunnen bewijzen. Het bewaren van gegevens en bewijsmateriaal is wettelijk verplicht en wordt gecontroleerd door onafhankelijke auditors en toezichthoudende organen.

13. Cookies

SK gebruikt cookies op haar websites. Cookies worden gebruikt op basis van het cookiebeleid van de websites, dat beschikbaar is op de [website van SK](#).

14. Wijziging van de beginselen voor de verwerking van persoonsgegevens

SK heeft het recht om deze beginselen voor de verwerking van persoonsgegevens eenzijdig te wijzigen in overeenstemming met de eisen die zijn vastgelegd in de toepasselijke wetgeving. De wijzigingen zullen op de [website van SK](#) worden gepubliceerd en treden onmiddellijk in werking.