

Principes voor de verwerking van persoonsgegevens (Privacybeleid)

Versie 8.0

Datum van inwerkingtreding: 09.03.2026

Versiegeschiedenis		
Datum	Versie	Wijzigingen
9 maart 2026	8.0	• Informatie over de omvang van de dienstverlening bijgewerkt • Informatie over het afzonderlijke privacybeleid dat van toepassing is op de dienst Authentigate toegevoegd • Informatie over diensten waarbij SK als gegevensverwerker optreedt toegevoegd • Secundaire aanbieders van abonneeverificatie als bron van persoonsgegevens bijgewerkt • De lijst van verwerkte persoonsgegevens bijgewerkt • Informatie toegevoegd over de mogelijkheid om een klacht in te dienen bij de Belgische Gegevensbeschermingsautoriteit • Een rechtsgrondslag toegevoegd voor het openbaar maken van persoonsgegevens op basis van een rechtmatig belang met het oog op het voorkomen, opsporen en onderzoeken van fraude, misbruik van diensten of andere beveiligingsincidenten.
10 oktober 2022	7.0	• De lijst van verwerkte persoonsgegevens bijgewerkt en geherstructureerd • Rechtmatig belang toegevoegd als rechtsgrondslag voor de verwerking en openbaarmaking van persoonsgegevens • Secundaire aanbieders van abonneeverificatie toegevoegd als bron van persoonsgegevens • Informatie over cookies toegevoegd • Uitleg en bewoordingen verbeterd
28 september 2020	6.0	• Informatie over de MyID-portal toegevoegd • Informatie over het geografische gebied van de gegevensverwerking toegevoegd • Informatie toegevoegd over de mogelijkheid om een klacht in te dienen bij de Letse en Litouwse Gegevensbeschermingsautoriteiten • De structuur van het document bijgewerkt • De adressen van de website en het e-mailadres bijgewerkt
5 december 2019	5.0	• De lijst van 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 speciale categorieën persoonsgegevens toegevoegd • Informatie over geautomatiseerde beslissingen toegevoegd • Informatie over de bronnen van persoonsgegevens toegevoegd • De informatie over de bewaartermijn van persoonsgegevens bijgewerkt • De contactgegevens van de functionaris voor gegevensbescherming toegevoegd
10 december 2018	4.0	• De lijst van verwerkte persoonsgegevens gewijzigd • Uitleg over de rechtsgrondslagen voor de verwerking toegevoegd • Informatie over het overdragen van persoonsgegevens aan e-diensten toegevoegd
25 mei 2018	3.0	Bijgewerkt conform de vereisten van de Algemene Verordening Gegevensbescherming (hierna "AVG" genoemd), die op 25 mei 2018 in werking is getreden.
1 maart 2018	2.0	• De titel van het document gewijzigd • De inhoud en structuur herzien • De lijst van verwerkte persoonsgegevens bijgewerkt • De voorwaarden voor het wijzigen van de principes herzien • Informatie over de documentversie toegevoegd
22 december 2011	1.0	Eerste openbare versie (Principes voor de bescherming van klantgegevens)

1. Algemene informatie

Deze principes voor de bescherming van persoonsgegevens beschrijven hoe SK ID Solutions AS (hierna "SK" genoemd) als gegevensbeheerder bij het aanbieden van de diensten Smart-ID en Mobile-ID conform de toepasselijke wetgeving de bescherming van persoonsgegevens waarborgt. Deze principes gelden ook voor het levenscyclusbeheer van certificaten voor Estische ID-kaarten, digi-ID's, digi-ID's voor e-ingezetenen, verblijfsvergunningen en diplomatieke identiteitskaarten die zijn uitgegeven tot en met 14 november 2025. Het doel van deze principes is om de abonnees te informeren over relevante onderwerpen met betrekking tot de verwerking van persoonsgegevens en om de principes die SK volgt bij de verwerking van persoonsgegevens onder de aandacht te brengen.

We wijzen u erop dat de verwerking van persoonsgegevens in het kader van de dienst Authentigate wordt beschreven in een afzonderlijk privacybeleid, dat beschikbaar is op de website van SK: <https://www.skidsolutions.eu/resources/data-protection/>.

In sommige gevallen kan SK optreden als gegevensverwerker in plaats van als verwerkingsverantwoordelijke. Als bijvoorbeeld in de Belgische FAS (Federale Authenticatiedienst) authenticatie via Smart-ID wordt gebruikt, verwerkt SK persoonsgegevens namens en op basis van gedocumenteerde instructies van de verwerkingsverantwoordelijke, het directoraat-generaal Vereenvoudiging & Digitalisering van de FOD BOSA. In deze context verwerkt SK als verwerker het tijdens de authenticatie uitgewisselde unieke Belgische identificatienummer en het beveiligde auditspoor. Raadpleeg hun privacybeleid voor meer informatie.

Evenzo treedt SK bij het leveren van de dienst Allkirjoitus.fi op als gegevensverwerker en verwerkt persoonsgegevens namens en in overeenstemming met de gedocumenteerde instructies van de verwerkingsverantwoordelijke, terwijl de abonnee optreedt als verwerkingsverantwoordelijke in overeenstemming met de algemene voorwaarden van SK en de servicevoorwaarden van Allkirjoitus.fi, die te vinden zijn op de website van SK: <https://www.skidsolutions.eu/resources/general-terms-of-subscriber-agreement/>. Raadpleeg het privacybeleid van de abonnee voor meer informatie.

Deze principes zijn niet van toepassing op de opslag en de verwerking van gegevens van rechtspersonen of andere instellingen.

Neem bij vragen over de verwerking van persoonsgegevens contact met ons op via onderstaande contactgegevens:

Gegevensbeheerder:

SK ID Solutions AS

Adres: Pärnu mnt 141, 11314 Tallinn, Estland

Telefoon: +372 610 1880

E-mail: [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu)

Fax: +372 610 1881

Nummer bedrijvenregister: 10747013

Functionaris voor gegevensbescherming:

E-mail: [dpo\[A\]skidsolutions.eu](mailto:dpo[A]skidsolutions.eu)

2. Definities

Hieronder lichten we de definities en afkortingen toe die in deze principes 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.

SK verwerkt persoonsgegevens in overeenstemming met de AVG en andere relevante wetgeving inzake gegevensbescherming, maar wij wijzen u erop dat SK als verlener van vertrouwensdiensten ook gebonden is aan de specifieke eisen voor de verwerking van persoonsgegevens zoals 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 verlener van vertrouwensdiensten 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, waaronder specifieke eisen voor de verwerking van persoonsgegevens.

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

Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon, ongeacht de vorm of het formaat waaruit deze gegevens bestaan. Verwerking van persoonsgegevens zijn alle handelingen of reeks handelingen die met persoonsgegevens worden uitgevoerd (waaronder het verzamelen, registreren, opslaan, wijzigen, toegang verlenen tot, opvragen en communiceren van gegevens, enz.), ongeacht de wijze waarop de handelingen worden uitgevoerd en de middelen die daarbij worden gebruikt.

2.4. Wat is een derde?

Een derde is een persoon (rechtspersoon of natuurlijke persoon) die geen contractuele klant, werknemer of gemachtigde gegevensverwerker van SK is.

2.5. Wat is een verwerkingsverantwoordelijke?

Een verwerkingsverantwoordelijke is een natuurlijke of rechtspersoon, een overheidsinstantie, een agentschap of een ander orgaan dat de doeleinden en middelen van de verwerking van persoonsgegevens bepaalt. Binnen de context van dit document is SK de verwerkingsverantwoordelijke.

2.6. Wat is een gegevensverwerker?

Een gegevensverwerker is een natuurlijke persoon of rechtspersoon, overheidsinstantie, agentschap of ander orgaan dat door SK contractueel is aangewezen om persoonsgegevens namens de

verwerkingsverantwoordelijke te verwerken. In sommige gevallen kan SK optreden als gegevensverwerker in plaats van als verwerkingsverantwoordelijke. Voorbeelden van situaties waarin SK als gegevensverwerker optreedt, worden beschreven onder Algemene informatie (zie hoofdstuk 1).

2.7. Wat is een certificaat?

Een certificaat is digitale data die elektronische ondertekening en identiteitsverificatie mogelijk maakt en waarbij de publieke sleutel betrekking heeft op de natuurlijke persoon die de eigenaar is van het certificaat. Certificaten die elektronische identiteitsverificatie of elektronische ondertekening mogelijk maken, hebben betrekking op persoonsgegevens.

2.8. Wat is een e-dienst?

Een e-dienst is een informatiesysteem, applicatie of e-omgeving waarbij gebruik wordt gemaakt van diensten van SK (Mobile-ID, Smart-ID, ID-kaart) voor de authenticatie van personen of voor 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 certificaatverzoeken accepteren, verifiëren en/of naar SK verzenden.

3. De principes van SK voor de verwerking van persoonsgegevens

Privacy en de bescherming van persoonsgegevens zijn voor ons van groot belang. Daarom hebben we de noodzakelijke 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 gedurende welke we deze gegevens moeten bewaren nauwkeurig omschreven. We hebben voor de medewerkers van SK en gemachtigde gegevensverwerkers eisen en instructies opgesteld over hoe persoonsgegevens op de juiste manier verwerkt moeten worden. We verlenen uitsluitend toegang tot persoonsgegevens aan getrainde medewerkers en gemachtigde gegevensverwerkers die een relevant antecedentenonderzoek hebben doorstaan. De medewerkers en gemachtigde personen van SK zijn zich ervan bewust dat zij persoonsgegevens alleen mogen verwerken voor zover dat nodig is voor de uitvoering van hun taken of, in het geval van gemachtigde gegevensverwerkers, voor het nakomen van hun contractuele verplichtingen.

Wij onderstrepen dat de verwerking van persoonsgegevens rechtmatig, eerlijk, doelgericht, minimaal, veilig en transparant is. Al onze activiteiten zijn gebonden aan de toepasselijke Europese, Estische en andere relevante wetgeving, het beleid en de principes van SK, alsmede door de hier beschreven principes bij de verwerking van persoonsgegevens. Het beleid en de principes van SK zijn te vinden 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 standaard die eisen stelt aan de managementprocessen van het informatiebeveiligingssysteem van de organisatie en aan de kritieke

informatiebeveiligingsmiddelen ter bescherming van persoonsgegevens, waaronder technische, fysieke en organisatorische beveiligingsmaatregelen.

4. Bronnen van persoonsgegevens

SK verkrijgt persoonsgegevens uit de volgende bronnen:

- Van de persoon;
- Persoonlijke apparaten (in geval van Smart-ID);
- Registers (bijvoorbeeld bevolkingsregisters);
- E-dienstverleners;
- Registratieautoriteiten, aanbieders van elektronische identificatie en aanbieders van secundaire abonneeverificatie (bijv. banken, mobiele operators, politie, eIDAS-koppelpunt).

5. Wetmatigheid van de verwerking van persoonsgegevens

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

We verwerken persoonsgegevens op de volgende rechtsgrondslagen:

- **Uitvoering van een contract:** De verwerking van persoonsgegevens voor de uitvoering van een contract betekent dat we persoonsgegevens nodig hebben om hoogwaardige dienstverlening te kunnen waarborgen. We hebben vastgesteld welke persoonsgegevens SK nodig heeft om diensten te kunnen verlenen en houden de hoeveelheid verwerkte persoonsgegevens zo klein mogelijk.
- **Naleving van wettelijke verplichtingen:** Naleving van wettelijke verplichtingen is de verwerking van persoonsgegevens die SK als dienstverlener wettelijk verplicht is uit te voeren. We verwerken bijvoorbeeld persoonsgegevens naar aanleiding van wettelijk gemotiveerde verzoeken van wetshandavingsinstanties.
- **Toestemming:** In sommige gevallen verwerken we persoonsgegevens op basis van toestemming van de betrokkene. We vragen bijvoorbeeld toestemming voor de verwerking van biometrische gegevens als we een biometrische identificatiemethode gebruiken voor de registratie van een Smart-ID. Daarnaast verwerken we op basis van toestemming persoonsgegevens naar aanleiding van verzoeken die persoonsgegevens bevatten. In dit geval wordt de toestemming voor de verwerking van persoonsgegevens gegeven door het verzoek naar SK te sturen.
- **Rechtmatig belang:** In sommige gevallen is de verwerking van persoonsgegevens gebaseerd op een rechtmatig belang. Dit betekent dat de verwerking noodzakelijk is voor SK of een derde partij voor een doel dat voorrang heeft op de rechten van de betrokkene. Op basis van een rechtmatig belang verwerken we bijvoorbeeld bepaalde apparaatgegevens om veiligheidsredenen.

6. Welke persoonsgegevens verwerken we voor welke doeleinden?

SK verwerkt persoonsgegevens voor de volgende doeleinden:

- **Uitgifte en onderhoud van certificaten:** SK verstrekt Smart-ID's, Mobile-ID's en certificaten voor Estische identiteitsdocumenten als ID-kaarten, digi-ID's, digi-ID's voor e-ingezetenen, verblijfsvergunningen en diplomatieke identiteitskaarten. SK verzorgt ook de intrekking van certificaten en in geval van identiteitsdocumenten voor de opschorting en beëindiging van de schorsing van de certificaten.

- **Mogelijk maken van het gebruik van de certificaten:** SK maakt het gebruik van Smart-ID, Mobile-ID en Estische identiteitsdocumenten voor authenticatie en elektronische ondertekening mogelijk.
- **Afhandeling van verzoeken waarin persoonsgegevens worden opgevraagd:** Als een persoon zelf of als een onderzoeks- of andere autoriteit bij SK persoonsgegevens opvraagt, verwerken wij de gevraagde gegevens om het antwoord op te stellen. De verzoeker moet een rechtsgrondslag hebben om de gegevens op te vragen. De verzoeken hebben betrekking op de uitgifte en het beheer van Smart-ID's, Mobile-ID's en certificaten van identiteitsdocumenten en/of het gebruik van de certificaten voor authenticatie en elektronische ondertekening.
- **Afhandeling van verzoeken die persoonsgegevens bevatten:** Als een persoon een verzoek naar SK stuurt dat zijn/haar persoonsgegevens bevat, verwerkt SK deze gegevens om het verzoek te behandelen en te beantwoorden.

Hieronder zullen we voor elke activiteit uitgebreider toelichten wat het doel van de verwerking is, wat de rechtsgrondslag voor de verwerking is en welke persoonsgegevens we verwerken.

Doel van de verwerking	Rechtsgrondslag	Welke persoonsgegevens worden er of kunnen er worden verwerkt?
Uitgifte en onderhoud van certificaten		
Dienstverlening	De verwerking is noodzakelijk om de overeenkomst na te komen; Biometrische gegevens worden verwerkt op basis van toestemming	• Voor- en achterna(a)m(en) van de persoon; • Persoonlijk identificatienummer en het land dat de persoonlijke identificatiecode heeft afgegeven; • Contractgegevens; • Taal van de communicatie; • Gegevens van het identiteitsdocument en/of een kopie van het identiteitsdocument dat wordt gebruikt voor het aanvragen van de certificaten; • Een aanvraagformulier voor een certificaat, elektronisch of met de hand ondertekend; • Het bestaan van een woonadres of e-woonadres in Estland; • Registratiemethode (elektronisch via de klantenservice) en/of gegevens van de klantenservice; • Gegevens over het apparaat (uitsluitend in geval van de elektronische registratie van Smart-ID's en Mobile-ID's) • Gegevens over de certificaten; • Gegevens over de levenscyclus van certificaten en de door de persoon verrichte handelingen bij het gebruik van de dienst (opschorting van certificaten, beëindiging van opschorting, intrekking van certificaten, afgifte van pinwallets, verlenging van certificaten, verificatie van informatie over de geldigheid van certificaten); • Gegevens over de simkaart en de mobiele operator (uitsluitend in geval van Mobile-ID's); • Geboortedatum en Smart-ID accountnummer (uitsluitend in geval van Smart-ID's); • Aanvullende informatie voor Smart-ID certificaataanvragen met de biometrische

		identificatiemethode: het vestigingsland van de persoon, aanvullende gegevens van het bij de registratie gebruikte document (soort document, land van afgifte, documentnummer, nationaliteit, geboortedatum, geslacht, vervaldatum document, gezichtsafbeelding van de persoon, technische gegevens die nodig zijn voor de verificatie van de authenticiteit van het document), video opgenomen tijdens de biometrische identificatie, het aantal mislukte registratiepogingen, informatie uit het PRADO-register over de geldigheid van het document. • In 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 (in leven, overleden) en in geval van minderjarigen informatie over wettelijke voogden.
Gebruik van de certificaten voor authenticatie of elektronische ondertekening		
Dienstverlening	De verwerking is noodzakelijk om de overeenkomst na te komen	• Voor- en achterna(a)m(en) van de persoon; • Persoonlijk identificatienummer, voor niet-Baltische en niet-Belgische staatsburgers het nummer van het paspoort of identiteitskaart; • IP-adres van het informatiesysteem waarin de informatie over de geldigheid van het certificaat is opgevraagd; • Telefoonnummer en taal van de communicatie; • In geval van Smart-ID het IP-adres van het netwerk dat door het apparaat wordt gebruikt, apparaatgegevens en de status van pincodes; • De e-dienstverlener wiens dienst wordt gebruikt; • Bij gebruik van Smart-ID's en Mobile-ID's de tekst die de e-dienst naar uw apparaat stuurt (de gegevens worden gehasht). We wijzen u erop dat SK, indien Smart-ID-authenticatie wordt gebruikt in de Belgische FAS (Federale Authenticatiedienst), als gegevensverwerker het bij de authenticatie uitgewisselde Belgische persoonsidentificatienummer en de bijbehorende beveiligde auditgegevens verwerkt.
Verzoeken waarin persoonsgegevens worden opgevraagd		
Antwoord op de vraag	Afhankelijk van de vraag kan de rechtsgrondslag toestemming, de wet of een rechtmatig belang zijn.	Gegevens die door de aanvrager worden opgevraagd.

	Houd er rekening mee dat de aanvrager de persoon zelf kan zijn of een onderzoeksinstantie of andere autoriteit die een rechtsgrondslag heeft om de gegevens op te vragen.	
Vragen die persoonsgegevens bevatten		
Antwoord op de vraag	Toestemming	Gegevens die in het verzoek aan SK zijn overgedragen.

Bij het authenticeren bij een e-dienst of het ondertekenen van een document worden persoonsgegevens (zoals naam en persoonlijk identificatienummer) naar de e-dienstverlener verzonden om de dienst te kunnen leveren. Dit gebeurt uitsluitend nadat de pincode is ingegeven. Het ingeven van de pincode wordt opgevat als toestemming voor de verzending van de gegevens.

6.1. Verwerking van persoonsgegevens van minderjarigen

De diensten van SK kunnen door minderjarigen worden gebruikt. Minderjarigen hebben voor een gekwalificeerde Smart-ID-registratie, het afsluiten van een Mobile-ID-contract en voor ID-kaart-toepassingen toestemming van hun ouders of voogd nodig.

Minderjarigen kunnen in het kader van een contact voor bancaire diensten een niet-gekwalificeerde of beperkte Smart-ID Basic aanvragen. Als een ouder of wettelijk voogd via een contact voor bancaire diensten een dergelijke machtiging heeft verleend, heeft een minderjarige voor een niet-gekwalificeerde Smart-ID-aanvraag geen afzonderlijke machtiging nodig. Meer informatie over gekwalificeerde en niet-gekwalificeerde Smart-ID's vindt u op de Smart-ID-portal.

Een ouder of wettelijke voogd stelt zich aansprakelijk voor de gevolgen van het gebruik van de diensten van SK (Mobile-ID, Smart-ID, ID-kaart). Hij/zij moet de minderjarige ook de voorwaarden van het gebruik van certificaten en de beveiligingsvereisten voor het gebruik van de dienst uitleggen.

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

6.2. Verwerking van speciale categorieën van persoonsgegevens

Volgens de AVG mogen bijzondere categorieën van persoonsgegevens worden verwerkt op basis van de uitdrukkelijke toestemming van de betrokkene. Als u bij de Smart-ID-registratie voor authenticatie de biometrische identificatiemethode selecteert, zal SK u tijdens het registratieproces om toestemming vragen voor de verwerking van uw biometrische persoonsgegevens. De biometrische gegevens die worden verwerkt, zijn gezichtsafbeeldingen, die zijn geëxtraheerd uit een video die u van uzelf hebt opgenomen. Gezichtsherkenning is noodzakelijk om u te identificeren tijdens de registratie van een Smart-ID-account. Daarnaast kan SK aanvullende controles 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.

Bij andere Smart-ID-registratiemethoden, zoals koppeling met een bank of filiaal, Mobile-ID, Smart-ID of identiteitskaart, worden geen biometrische gegevens verwerkt.

7. Geografisch gebied van de gegevensverwerking

In de regel verwerkt SK uw persoonsgegevens in de Europese Unie of de Europese Economische Ruimte. Als we gemachtigde verwerkers inschakelen die zich buiten dit gebied bevinden, doen we dat op basis van een adequaatheidsbesluit van de Europese Commissie (EG), leggen we standaardcontractbepalingen met de partner vast of implementeren we andere passende waarborgen.

8. Geautomatiseerde beslissingen

Volgens de AVG heeft een persoon er recht op dat er geen beslissingen over hem of haar worden genomen die rechtsgevolgen of vergelijkbare belangrijke gevolgen voor hem of haar hebben als die uitsluitend gebaseerd zijn op geautomatiseerde verwerking. Geautomatiseerde beslissingen kunnen worden genomen indien dit noodzakelijk is voor de uitvoering van een contract tussen een verwerkingsverantwoordelijke en een persoon, mits dit wettelijk is toegestaan of met de uitdrukkelijke toestemming van die persoon.

SK neemt, indien u biometrische identificatie gebruikt voor de registratie van uw Smart-ID-account, ter identificatie met behulp van een processor geautomatiseerde beslissingen op basis van uw biometrische gegevens (gezichtsafbeelding). In dit geval zal SK u tijdens het registratieproces om uitdrukkelijke toestemming vragen. Bij andere Smart-ID-registratiemethoden, zoals koppeling met een bank of filiaal, Mobile-ID, Smart-ID of identiteitskaart, worden dergelijke geautomatiseerde beslissingen niet genomen.

SK neemt ook geautomatiseerde besluiten over de uitgifte of weigering van een certificaat op basis van gegevens uit registers en het valideert elektronische certificaataanvragen door middel van 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 om zijn/haar persoonsgegevens in te zien en te vragen om correctie, verwijdering of overdracht van de gegevens en om de verwerking te beperken.

Om bovengenoemde rechten uit te oefenen, kunt u een elektronisch ondertekend verzoek sturen naar het e-mailadres [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu). We zullen uw verzoek binnen dertig dagen beantwoorden.

We benadrukken dat het verzoek in de volgende gevallen niet kan worden gehonoreerd:

- als de identiteit van de verzoeker kan niet kan worden vastgesteld;
- als de verzoeker niet juridisch is verbonden met de gegevens;
- als dit in strijd zou zijn met de eisen in specifieke wetten;
- als dit zou in strijd zijn met de wettelijke verplichtingen van SK;
- dit de rechten en vrijheden van een andere persoon kan schaden;
- als dit de dienstverlening zou belemmeren of onmogelijk zou maken;
- als dit het werk van de wetshandhavingsinstanties zou belemmeren;

- als het technisch niet mogelijk is.

Tevens kunt u via de MyID-portal uw Mobile-ID-, Smart-ID-, ID-kaart en digi-ID-accounts en hun geschiedenis inzien. Voor ID-kaart, digi-ID en Mobile-ID kun je daar ook de geschiedenis van al uw transacties (authenticatie en ondertekening) inzien. Informatie over uw Smart-ID-accounts en de transacties die u met Smart-ID hebt uitgevoerd, vindt u op de Smart-ID-portal.

Als de verwerking van persoonsgegevens is gebaseerd op toestemming, kunt u uw toestemming te allen tijde intrekken door een verzoek in elektronisch ondertekende vorm te sturen naar 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 we u een elektronisch ondertekende klacht per e-mail te sturen naar [dpo\[A\]skidsolutions.eu](mailto:dpo[A]skidsolutions.eu). We zullen uw e-mail binnen dertig dagen beantwoorden. Als 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 (bijv. de Estische Gegevensbeschermingsautoriteit, de Letse Gegevensbeschermingsautoriteit, de Litouwse Gegevensbeschermingsautoriteit en de Belgische Gegevensbeschermingsautoriteit).

10. Gebruik van data via een gemachtigde gegevensverwerker

SK heeft op grond van het contract het recht om een andere persoon (zowel natuurlijke als rechtspersonen) te machtigen om persoonsgegevens te verwerken. Gemachtigde gegevensverwerkers zijn bijvoorbeeld partners van SK bij het uitgeven en onderhouden van certificaten en het oplossen van problemen van klanten. Als verwerkingsverantwoordelijke verstrekt SK de gemachtigde verwerker de noodzakelijke instructies voor de gegevensverwerking. SK is er verantwoordelijk voor dat de gemachtigde gegevensverwerker de vereisten voor de verwerking van persoonsgegevens naleeft. Een gemachtigde gegevensverwerker mag persoonsgegevens uitsluitend verwerken om het beoogde doel te bereiken. SK onderstreept dat met alle gemachtigde gegevensverwerkers overeenkomsten voor gegevensverwerking zullen worden gesloten. Een lijst van door SK gemachtigde gegevensverwerkers is [hier](#) te vinden.

Een e-dienst die uw persoonsgegevens bij SK opvraagt op basis van authenticatie of een op uw initiatief geplaatste elektronische handtekening, is geen gemachtigde verwerker van SK in de zin van de AVG.

11. Ontsluiting of communicatie van persoonsgegevens aan derden

SK ontsluit of verstrekt geen persoonsgegevens aan derden, tenzij er sprake is van een van de volgende gevallen:

- Een dergelijke verplichting vloeit voort uit de toepasselijke wetgeving of op basis daarvan genomen maatregelen (bijvoorbeeld doorgifte aan een onderzoeksinstantie);
- Zulke partijen zijn betrokken bij het leveren van de diensten;
- De derde partij heeft een rechtmatig belang om de gegevens bij SK op te vragen;
- Met het oog op het voorkomen, opsporen en onderzoeken van fraude, misbruik van diensten of andere beveiligingsincidenten, waarbij SK of een andere partij een rechtmatig belang heeft bij een dergelijke verwerking;
- Met het oog op de uitvoering van een contract of het waarborgen van de nakoming van het contract heeft SK het recht de gegevens te ontsluiten voor derden, waaronder kredietinformatiebureaus, incassobureaus en andere personen die zich bezighouden met de afhandeling van vorderingen,

alsmede aan juridische adviseurs en deurwaarders indien de betrokkene het contract niet is nagekomen;

- De betrokkene geeft schriftelijke toestemming voor de ontsluiting voor andere derden.

SK onderstreept dat het persoonsgegevens uitsluitend voor derden ontsluit voor zover dat noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.

SK ontsluit via de LDAP-service uw geldige Estische certificaten met betrekking tot identiteitsbewijzen (inclusief Mobile-ID's uitgegeven tot 02-07-2022) gedurende de periode dat deze geldig zijn. Aanvullende informatie over de LDAP-service is [hier](#) te vinden.

12. Opslagtermijn van persoonsgegevens

SK verwerkt persoonsgegevens uitsluitend zolang dat noodzakelijk is voor het bereiken van de doeleinden waarvoor de persoonsgegevens zijn verzameld of voor het nakomen van de verplichtingen die voortvloeien uit de toepasselijke wetgeving. We wijzen u erop dat we ons bij het leveren van vertrouwensdiensten bij de opslag van persoonsgegevens laten leiden door de eIDAS-verordening en de Estische wet op de elektronische identificatie en vertrouwensdiensten voor elektronische transacties.

SK is verplicht om bewijsmateriaal dat het heeft gebruikt om u te identificeren bij de uitgifte van certificaten minstens 10 jaar na het verstrijken van het certificaat te bewaren en logboeken met betrekking tot de procedures die zijn uitgevoerd tijdens de verlening van vertrouwensdiensten minstens 10 jaar te bewaren teneinde zo nodig misbruik van uw identiteit en de juistheid van de activiteiten van SK bij de verlening van zijn diensten aan te kunnen tonen. Het bewaren van gegevens en bewijsmateriaal is wettelijk verplicht en wordt gecontroleerd door onafhankelijke auditors en toezichthoudende organen.

13. Cookies

SK gebruikt cookies op zijn websites. Cookies worden gebruikt op bases van het Cookiebeleid van de website, dat te vinden is op [de website van SK](#).

14. Wijziging van de principes voor de verwerking van persoonsgegevens

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