

Darbo su asmens duomenimis principai

Versija 6.0

Galioja nuo 2020.09.28

Šis dokumentas yra oficialus dokumento „Principles of processing personal data“ vertimas į lietuvių kalbą. Esant neatitikimams tarp originalaus dokumento ir vertimo, pirmenybė teikiama originalui.

Versijos ir pakeitimai		
Data	Versija	Pakeitimai
2020.09.28	6.0	• Pridėta informacija apie „myID“ portalą • Pridėta informacija apie duomenų tvarkymo geografinį regioną • Pridėta informacija apie galimybę teikti skundus priežiūros institucijoms Latvijoje ir Lietuvoje • Atnaujinta dokumento struktūra • Atnaujinti interneto puslapių ir elektroninio pašto adresai
2018.12.05	5.0	• Papildytas tvarkomų asmens duomenų sąrašas • Atnaujinta dokumento struktūra ir turinys • Pridėta informacija apie nepilnamečių asmenų duomenų tvarkymą • Pridėta informacija apie specialiųjų kategorijų asmens duomenų tvarkymą • Pridėta informacija apie automatizuotus sprendimus • Pridėta informacija apie asmens duomenų šaltinius • Atnaujinta asmens duomenų saugojimo laikotarpio informacija • Pridėti kontaktiniai duomenų apsaugos pareigūno duomenys
2018.12.10	4.0	• Papildytas tvarkomų asmens duomenų sąrašas • Pridėtas teisinio pagrindo duomenų tvarkymui paaiškinimas • Pridėta informacija apie asmens duomenų perdavimą el. paslaugoms
2018.12.25	3.0	Atnaujinta laikantis 2018 m. gegužės 25 d. įsigaliojusių Bendrojo duomenų apsaugos reglamento (toliau – BDAR) reikalavimų
2018.03.01	2.0	• Pakeistas dokumento pavadinimas • Atnaujintas turinys ir struktūra • Atnaujintas surinktų asmens duomenų sąrašas • Atnaujintos principų papildymo sąlygos • Pridėta dokumento versijos informacija
2011.12.22	1.0	Pirmoji vieša versija (Kliento duomenų apsaugos principai)

1. Bendroji informacija

Šie asmens duomenų tvarkymo principai apibrėžia, kaip „SK Solutions AS“ (toliau – SK) kaip duomenų valdytojas, užtikrina įstatymų reikalavimus atitinkančią asmens duomenų apsaugą. Šių principų tikslas yra supažindinti vartotojus su nuostatomis, kuriomis SK vadovaujasi tvarkydama asmens duomenis, taip pat suteikti vartotojams informaciją apie jų teises.

Šie principai netaikomi saugant ir tvarkant juridinių asmenų ar kitų institucijų duomenis. Asmuo, atstovaujantis juridinį asmenį ar kitas institucijas, nelaikomas fiziniu asmeniu; tai yra juridinio asmens ar kitos institucijos įgaliotasis atstovas, kurio asmens duomenims nėra taikomas BDAR.

Jei jums kiltų kokių nors klausimų dėl asmens duomenų tvarkymo, susisiekite su mumis šiais kontaktais:

Duomenų valdytojas:

„SK ID Solutions AS“

Adresas: Pärnu mnt. 141, 11314 Talinas, Estonia (Estija)

Tel.: +372 610 1880

El. paštas: info@skidsolutions.eu

Faksas: +372 610 1881

Įmonės kodas: 10747013

Duomenų apsaugos pareigūnas:

El. paštas: dpo@skidsolutions.eu

2. Apibrėžimai

Toliau pateikiame šiame dokumente naudojamų terminų ir trumpinimų apibrėžimus ir paaiškinimus.

2.1. Kas yra BDAR?

2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Tai yra tiesiogiai taikomas bendrasis reglamentas, nustatantis bendrąsias fizinių asmenų asmens duomenų apsaugos taisykles.

Tvarkydami asmens duomenis, mes užtikriname duomenų apsaugą vadovaudamiesi Bendrojo asmens duomenų apsaugos reglamentu, tačiau atkreipiame jūsų dėmesį į tai, kad kadangi esame patikimumo užtikrinimo paslaugų teikėjai, be Bendrojo reglamento taisyklių mūsų darbe tvarkant asmens duomenis, taikomi specialūs reikalavimai pagal eIDAS nutarimą.

2.2. Kas yra eIDAS reglamentas?

2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

SK, veikianti kaip patikimumo užtikrinimo paslaugų teikėjas, savo veikloje ir teikdama paslaugas laikosi eIDAS reglamento reikalavimų. Tai yra tiesiogiai taikomas Europos Sąjungos reglamentas, kuriame pateikiamos įvairių patikimumo užtikrinimo paslaugų teikimo sąlygos ir reikalavimai.

2.3. Kas yra asmens duomenys ir kas yra asmens duomenų tvarkymas?

Asmens duomenys yra bet kokie su identifiukuotu ar identifiukuojamu fiziniu asmeniu susiję duomenys, nepriklausomai nuo tokių duomenų tipo ar formato. Asmens duomenų tvarkymas - tai bet koks su asmens duomenimis vykdomas veiksmas (įskaitant surinkimą, registravimą, keitimą, prieigos suteikimą, grąžinimą, komunikavimą ir kt.) arba keletas veiksmų, nepriklausomai nuo jų pobūdžio ar tam naudojamų priemonių.

2.4. Kas yra trečioji šalis?

Trečioji šalis - tai bet kuris asmuo (fizinis arba juridinis), kuris neturi sutartinių santykių su SK, nėra SK darbuotojas ar SK įgaliotas duomenų tvarkytojas.

2.5. Kas yra duomenų valdytojas?

Duomenų valdytojas - tai fizinis arba juridinis asmuo, viešojo įstaiga, agentūra ar bet koks kitas asmuo ar asmenų grupė, apibrėžianti (-is) asmens duomenų naudojimo tikslus ir priemones. Šio dokumento kontekste duomenų valdytojas yra SK.

2.6. Kas yra įgaliotas duomenų tvarkytojas?

Įgaliotas duomenų tvarkytojas yra fizinis arba juridinis asmuo, valdžios institucija, agentūra ar bet kuri kita įstaiga, kurią SK sutarties pagrindu įgaliojo tvarkyti asmens duomenis, duomenų valdytojo vardu.

2.7. Kas yra sertifikatas?

Skaitmeniniai duomenys, suteikiantys galimybę vykdyti elektroninio parašo paslaugą ir tapatybės tikrinimą, kuriuose viešasis raktas susietas su liudijimą gavusiu fiziniu asmeniu. Sertifikatai, leidžiantys elektroniniu būdu identifiukuoti asmenį ar asmeniui pateikti elektroninį parašą, yra susiję su asmens duomenimis.

2.8. Kas yra el. paslaugos?

Elektroninė paslauga - tai informacinė sistema, programa arba elektroninė aplinka, naudojanti SK teikiamas paslaugas („Mobile-ID“, „Smart-ID“, „ID-card“) asmenų tapatybės patvirtinimui arba leidžianti pasirašyti elektroniniu parašu.

2.9. Kas yra registravimo tarnyba?

Registravimo tarnyba yra už asmenų identifikavimą ir tapatybės patvirtinimą atsakinga organizacija. Registravimo tarnyba taip pat gali priimti užklausas dėl sertifikatų, juos patikrinti ir (arba) perduoti SK.

3. SK asmens duomenų tvarkymo principai

Privatumo ir asmens duomenų apsauga mums yra labai svarbi, todėl mes ėmėmės būtinų organizacinių, fizinių ir informacinių technologijų priemonių, leidžiančių užtikrinti duomenų integralumą, prieinamumą ir konfidencialumą.

Mes išanalizavome ir nustatėme asmens duomenis, kurių mums reikia paslaugoms teikti, ir apibrėžėme tokių duomenų saugojimo tikslą, apimtį ir laikotarpį. SK darbuotojams ir įgaliotiems duomenų tvarkytojams mes apibrėžėme reikalavimus ir instrukcijas, nurodančias, kaip tinkamai tvarkyti asmens duomenis. Prieiga prie asmens duomenų gali būti suteikta tik išmokytiems tinkamai su asmens duomenimis elgtis darbuotojams ir įgaliotiems atstovams, kurie sėkmingai išlaikė atitinkamą žinių patikrinimą. SK darbuotojai ir įgaliotieji darbuotojai supranta, kad tvarkyti asmens duomenis gali tik tiek, kiek būtina jų pareigoms atlikti, o įgaliotų atstovų atveju – įvykdyti sutartinius įsipareigojimus.

Patvirtiname, kad asmens duomenų tvarkymas vykdomas teisėtai, tinkamai, teisingais tikslais, minimaliai, saugiai ir skaidriai. Visa mūsų veikla vykdoma vadovaujantis galiojančiais ES ir Estijos teisės aktais, SK politika ir principais, taip pat šiais asmens duomenų tvarkymo principais. SK politika ir principai pateikiami SK svetainėje adresu : <https://www.skidsolutions.eu/en/repository/>

SK įmonė sertifikuota taikant ISO/IEC 27001: 2013 standartą – „Informacinės technologijos. Saugumo užtikrinimo metodai. Informacinės saugumo valdymo sistemos“. Šis standartas nustato organizacijos informacijos saugumo sistemos valdymo procesams ir kritiniams informacijos saugumo punkтам taikomus reikalavimus, įskaitant technines, fizines ir organizacines saugumo priemones, leidžiančias apsaugoti asmens duomenis.

4. Asmens duomenų šaltiniai

Asmens duomenis SK gauna iš šių šaltinių:

- tiesiogiai iš asmenų;
- iš asmeninių prietaisų („Smart-ID“ atveju);
- registų (pvz., gyventojų registro);
- paslaugų teikėjų;
- registruojančiųjų įstaigų ir el. identifikavimo paslaugų teikėjų (pvz., bankų, mobiliųjų tinklų operatorių, policijos ir valstybės sienos apsaugos tarnybos).

5. Asmens duomenų tvarkymo teisėtumas

Asmens duomenis SK tvarko tik sąžiningai ir teisėtai. SK patvirtina, kad asmens duomenis tvarko tik aiškiai nustatytais ir teisėtais tikslais, apsiribojant tik būtiniausiais duomenimis, kurių reikia tokiems tikslams pasiekti.

Mes tvarkome asmens duomenis šiais teisiniais pagrindais:

- **Sutarties vykdymas:** asmens duomenų tvarkymas vykdant sutartį reiškia, kad mums reikia asmens duomenų, kad galėtume teikti kokybiškas paslaugas. Mes nustatėme kokių asmens duomenų reikia SK paslaugoms teikti, ir apribojome tvarkomų asmens duomenų kiekį iki minimumo.
- **Įstatymo numatytų įpareigojimų vykdymas:** įstatymo numatytų įpareigojimų vykdymas – tai asmens duomenų, kuriuos pagal įstatymus privalome atlikti kaip paslaugų teikėjas, tvarkymas. Pavyzdžiui, asmens duomenis tvarkome atsakydami į teisėsaugos institucijų teisėtai motyvuotus prašymus.
- **Sutikimas:** remdamiesi sutikimu, mes, asmens biometrinio identifikavimo atveju, tvarkome Jūsų biometrinius duomenis (taip pat žr. 6.2 skyrių). Be to, mes tvarkome asmens duomenis atsakydami į prašymus, kuriuose yra asmens duomenų. Tokiu atveju, siūsdami prašymą SK, Jūs sutinkate, kad būtų tvarkomi Jūsų asmens duomenys.

6. Kokius asmens duomenis mes tvarkome ir kokiais tikslais?

Toliau, atkreipdami dėmesį į kiekvieną veiklos rūšį, išsamiai paaiškinsime, koks yra tvarkymo tikslas, jo teisinis pagrindas ir kokius asmens duomenis tvarkome.

Veiksmas	Duomenų tvarkymo tikslas	Teisinis pagrindas	Kokie asmens duomenys tvarkomi?
Sertifikatų išdavimas ir/arba aptarnavimas	Paslaugų teikimas	Tvarkymas yra būtinas sutarties vykdymo tikslais; Biometriniai asmens duomenys yra tvarkomi gavus sutikimą	1. Asmens vardas ir pavardė. 2. Asmens kodas (taip pat šalis, išdavusi asmens kodą, kai kreipiamasi dėl „Smart-ID“ sertifikato). 3. Estijos piliečių ID-1 formato dokumentams**: dokumento numeris, dokumento galiojimo laikas, dokumento tipas, el. pašto adresas svetainėje eesti.ee. 4. Sertifikato numeris. 5. Gyvenamosios vietos (rezidentavimo) Estijos Respublikoje liudijimas arba el. patvirtinimas. 6. Klientų aptarnavimo centro duomenys. 7. Duomenys, susiję su asmens veiksmais, vykdomais jam naudojantis paslaugomis (sertifikatų galiojimo sustabdymas, sustabdymo atšaukimas, sertifikatų atšaukimas, vokų su PIN kodu išdavimas, sertifikatų atnaujinimas, sertifikato galiojimo informacijos tikrinimas). 8. Asmens tapatybės dokumento, naudojamo norint gauti sertifikatą, kopija. 9. Prašymo forma, pasirašyta ranka arba elektroniniu parašu, sertifikatui gauti. 10. „Mobile-ID“ sertifikato atveju, taip pat tvarkomi šie duomenys: SIM kortelės numeris, SIM kortelės gavimo patvirtinimas, pasirašytas elektroniniu arba įprastu parašu, telefono numeris ir mobiliojo telefono operatorius (el. pašto adresas Lietuvoje naudojamo „Mobile-ID“ atveju). 11. Teikiant paraiškas dėl „Smart-ID“ liudijimo papildomai: asmens gimimo data, „Smart-ID“ paskyros numeris, telefono numeris, bendravimo kalba, prietaiso duomenys (modelis ir operacinės sistemos versija, prietaiso pavadinimas (neoficialus), IP adresas ir kiti techniniai prietaiso parametrai), el. pašto adresas, banko patvirtinimo nuoroda. Išduodant „Smart-



			ID" sertifikatą tikrinamas mums pateiktų duomenų atitikimas gyventojų registrui: Estijoje – asmens kodas, pavardė, vardas, sertifikatą išduoti prašančiojo asmens statusas (gyvas, miręs, nežinoma), papildomai nepilnamečiams – duomenys apie teisėtų globėjų egzistavimą, globos tipą, laikotarpį ir būseną; Lietuvoje – asmens kodas, pavardė, vardas, asmens duomenų būseną ir papildomai nepilnamečių pareiškėjų atveju – tėvo ir motinos asmens kodai, pavardės ir vardai. 12. Papildoma informacija „Smart-ID“ sertifikatui gauti naudojantis biometrinės identifikacijos metodu: asmens gyvenamoji šalis, papildomi dokumento, naudojamo registracijai, duomenys (dokumento tipas, dokumentą išdavusi šalis, dokumento numeris, pilietybė, gimimo data, lytis, dokumento galiojimo pabaigos data, asmens veido nuotrauka, techniniai duomenys reikalingi dokumento autentiškumui patikrinti), veido atvaizdas, gaunama biometrinės identifikacijos proceso metu, vaizdo įrašas gaunamas biometrinės identifikacijos proceso metu, nepavykusių bandymų registruotis skaičius. 13. Jei „Smart-ID“ išduodamas asmenims neturintiems asmens kodo, papildomai: paso arba asmens tapatybės kortelės numeris ir dokumentą išdavusi šalis.
--	--	--	---

SK išduotas sertifikatas naudojamas tapatybės nustatymo arba elektroninio parašo tikslais*	Paslaugų teikimas	Tvarkymas yra būtinas sutarties vykdymo tikslais	1. Asmens vardas ir pavardė. 2. Asmens kodas, ne Baltijos šalių gyventojams – paso arba asmens tapatybės kortelės numeris. 3. Informacinės sistemos, kurioje pateiktas užklauskimas dėl sertifikato galiojimo informacijos, IP adresas. 4. Telefono numeris ir komunikavimo kalba, naudojantis „Mobile-ID“. 5. Prietaiso duomenys ir tinklo IP adresas, kai naudojama „Smart-ID“: modelis ir operacinės sistemos versija, kiti techniniai prietaiso parametrai, PIN numerių būseną. 6. Papildoma prie elektroninio parašo pridedama informacija (vaidmuo, miestas, šalis, pašto kodas, nutarimas). 7. Informacija apie kitų asmenų, pasirašiusių tą patį duomenų failą, sertifikatą (nurodyti vardai ir pavardės, asmens kodai). 8. Duomenų failo pavadinimas. 9. Duomenų failas, jei perduodamas SK naudojantis informacine sistema. 10. El. paslaugos teikėjas, kurio paslauga naudojama. 11. Naudojantis „Smart-ID“ ir „Mobile-ID“ – el. paslaugų tekstas, išsiųstas į Jūsų prietaisą.
Elektroninių parašų galiojimo patvirtinimas	Paslaugų teikimas	Tvarkymas yra būtinas sutarties vykdymo tikslais	1. Pasirašyto duomenų failo pavadinimas. 2. Duomenų failas, jei informacinės sistemos perduotas SK. 3. Pasirašiusių vardai, pavardės ir asmens kodas (sertifikato duomenys). 4. Pasirašymo laikas ir papildoma informacija (taip pat vaidmuo, miestas, šalis, pašto kodas, nutarimas). 5. El. paslaugų teikėjas, kurio paslaugomis naudojasi klientas. 6. Parašo galiojimas.
Užklauskos kuriose nurodomi asmens duomenys	Atsakymas į užklauską	Sutikimas	Apdorojamų asmens duomenų sudėtis priklauso nuo to, kokia informacija dėl konkretaus kreipimosi buvo perduota SK.

Tyrimų institucijų užklausa	Atsakymas į užklausą	Istatymas	Apdorojamų asmens duomenų sudėtis priklauso nuo to, kokios informacijos dėl konkrečios užklausa buvo prašoma iš SK.
-----------------------------	----------------------	-----------	---

* Kai mes teikiame sertifikatų galiojimo patikrinimo paslaugą kaip tarpininkas, naudodamiesi el. paslaugomis tvarkome sertifikato savininko asmens duomenis su tikslu patvirtinti asmens tapatybę, pasirašyti ir patvirtinti, jei šie sertifikatai buvo išduoti kito sertifikatus išduodančio paslaugų teikėjo.

Jei naudojate SK išduotą sertifikatą Jūsų tapatybei patvirtinti arba elektroniniam pasirašymui, mes perduodame Jūsų asmens duomenis el. paslaugoms, kad ši paslauga būtų suteikta. Asmens duomenis el. paslaugoms mes perduodame tik tuo atveju, jei turime atitinkamą Jūsų sutikimą, t. y. jei įvesdami PIN kodą Jūs inicijavote tapatybės patvirtinimo ir (arba) elektroninio parašo operaciją.

** „ID-1“ formato dokumentai yra asmens tapatybės dokumentai, atitinkantys ISO/IEC 7810 standarte nurodytus dydžių reikalavimus, tokie kaip tapatybės kortelė, gyvenamosios vietos kortelė, skaitmeninė gyventojo ID kortelė ir diplomatinė ID kortelė.

6.1. Nepilnamečių asmens duomenų naudojimas

SK paslaugomis gali naudotis nepilnamečiai. Nepilnamečiams reikalingas tėvų arba globėjų sutikimas kvalifikuotos „Smart-ID“ paskyros registracijai, sudarant „Mobile-ID“ sutartį ar pateikiant prašymą išduoti kortelę „ID-card“. Sutikimo užklauso funkcija yra įdiegta kvalifikuotų „Smart-ID“ prašymų registravimo sistemoje, todėl be tokio sutikimo, naudotis „Smart-ID“ paslauga nepilnamečiai negali. Biometrine „Smart-ID“ registracijos identifikacija naudotis gali tik asmenys nuo 18-os metų.

Nepilnamečiai gali teikti prašymą naudotis nekvalifikuotomis ar ribotų teisių „Smart-ID Basic“ paslaugomis, taikant bankinių paslaugų sutarties nuostatas. Jei nepilnamečio tėvai ar teisėti globėjai, naudodamiesi banko paslaugų sutartimi suteikia tokį leidimą, nepilnamečiui atskiro leidimo naudotis nekvalifikuotomis „Smart-ID“ paslaugomis nereikia. [„Smart-ID“ portale](#) rasite daugiau informacijos apie kvalifikuotas ir nekvalifikuotas „Smart-ID“ paslaugas.

Nepilnamečio tėvai arba teisėti globėjai prisiima atsakomybę už galimas pasekmes dėl naudojimosi SK teikiamomis paslaugomis („Mobile-ID“, „Smart-ID“, ID kortelė). Taip pat, nepilnamečio tėvai arba teisėti globėjai turi paaiškinti nepilnamečiui sertifikato naudojimo sąlygas ir saugumo reikalavimus, susijusius su paslaugų naudojimu.

SK tvarko tokius pačius nepilnamečių asmens duomenis, kaip ir suaugusiųjų, taip pat informaciją apie tėvų ar teisėtų globėjų sutikimą ir ryšį tarp vaiko ir tėvų / globėjų (žr. 6 skyriuje pateiktą lentelę).

6.2. Specifinio tipo asmens duomenų naudojimas

Vadovaujantis Bendrojo duomenų apsaugos reglamento nuostatomis, turint aiškų asmens sutikimą, gali būti tvarkomi specifinio tipo asmens duomenys. Jei „Smart-ID“ registracijai pasirenkamas biometrinės identifikacijos metodas, SK būtina pateikti sutikimą registracijos metu tvarkyti biometrinius asmens duomenis. Biometrinei identifikacijai naudojamas kliento veido atvaizdas, kuris paimamas iš kliento vaizdo

įrašo. Veido atvaizdas yra būtinas tapatybei patvirtinti registruojant „Smart-ID“ paskyrą. Taip pat SK, siekdama užtikrinti klientų elektroninės tapatybės saugumą ir techninių sprendimų kokybę, naudodama klientų biometrinius duomenis, gali vykdyti įvairius patikrinimus.

Jei nenorite, kad Jūsų biometriniai duomenys būtų tvarkomi, galite pasirinkti kitą registracijos metodą (internetinę bankininkystę, banko skyrių, „Mobile-ID“ ar asmens tapatybės kortelę).

7. Geografinis duomenų tvarkymo regionas

Įprastai, SK tvarko Jūsų asmens duomenis Europos Sąjungoje ar Europos ekonominėje erdvėje. Jei į paslaugų teikimą įtraukiame įgaliotus duomenų tvarkytojus, esančius ne Europos Sąjungoje ar Europos ekonominėje erdvėje, tai darome remdamiesi Europos Komisijos priimtu sprendimu dėl tinkamumo, pasirašome standartines duomenų apsaugos sąlygas su partneriu arba taikome kitas tinkamas apsaugos priemones pagal Bendrąjį duomenų apsaugos reglamentą.

8. Automatiškai priimami sprendimai

Vadovaujantis Bendrojo duomenų apsaugos reglamento nuostatomis, asmuo turi teisę reikalauti, kad sprendimai, kurie gali turėti teisinių ir (arba) materialinių pasekmių, nebūtų priimami remiantis tik automatiškai apdorojamais duomenimis. Automatiškai priimami sprendimai gali būti taikomi, jei reikia sudaryti sutartį tarp duomenų valdytojo ir asmens, jei tai leidžia įstatymai ir jei asmuo pats su tuo sutinka.

Automatiškai sprendimus SK priima tik remiantis klientų biometriniais duomenimis (veido atvaizdas), kai „Smart-ID“ paskyros registracijai klientas pasirenka biometrinės identifikacijos metodą. Tokiu atveju, registracijos metu SK paprašys atitinkamo sutikimo. Jei klientas nesutinka, kad jo biometriniai duomenys būtų tvarkomi ir naudojami automatinio sprendimų priėmimo ir identifikavimo tikslais, jis gali rinktis kitą „Smart-ID“ paskyros registracijos metodą (internetinė bankininkystė, banko skyrius, „Mobile-ID“ ar asmens tapatybės kortelė).

Vykdydama sutartį SK automatiškai priima sprendimus dėl sertifikato išdavimo ar atsisakymo išduoti, remiantis duomenimis, gautais iš registru. Taip pat SK naudoja automatiškai priimamus sprendimus dėl elektroninių „Smart-ID“ prašymų patvirtinimo.

9. Teisė gauti informaciją ir skundų teikimas

Remiantis BDAR nuostatomis, asmuo turi teisę susipažinti su savo asmens duomenimis, reikalauti juos pakeisti, pašalinti, perduoti ir apriboti jų tvarkymą.

Norėdami susipažinti su savo asmeninius duomenis, turite pateikti prašymą SK.

Būtina sąlyga anksčiau įvardytoms teisėms gauti – besikreipiančio asmens tapatybė turi būti aiškiai identifiukuota. Todėl mes maloniai prašome jūsų atitinkamą prašymą pateikti pasirašytą elektroniniu būdu ir atsiųsti šiuo el. pašto adresu [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu). Į jūsų prašymą atsakysime per 30 kalendorinių dienų.

Pažymime, kad prašymas nebus priimtas toliau nurodytais atvejais:

1. negalima nustatyti pareiškėjo tapatybės;
2. pareiškėjas nėra teisiškai susijęs su duomenimis;
3. tai prieštarautų tam tikrų įstatymų reikalavimams;
4. tai prieštarautų SK teisiniams įsipareigojimams;
5. tai galimai pažeistų kito asmens teises ir laisves;
6. tai trukdytų tinkamai teikti paslaugas arba nutrauktų jų teikimą;
7. tai trukdytų teisėsaugos pareigūnams vykdyti savo pareigas;
8. tai techniškai neįmanoma.

Asmens duomenis, kuriuos tvarko SK, sertifikato išdavimo ir naudojimo metu, galite rasti „myID“ portale. Informacijos apie jūsų įvykdytas operacijas naudojantis „ID-card“, „Digi-ID“ arba „Mobile-ID“ galima gauti "Minu ID toimingud" portale. „Smart-ID“ portale galite rasti informaciją apie „Smart-ID“ paskyras ir veiksmus, atliktus naudojant „Smart-ID“.

Jei asmens duomenų tvarkymui asmuo duoda savo sutikimą, jis, bet kuriuo metu, tokį sutikimą gali atšaukti, toliau nurodytu el. pašto adresu pateikdamas elektroniniu būdu pasirašytą atitinkamo prašymo formą: [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu).

Jei jūsų teisės dėl asmens duomenų tvarkymo būtų pažeistos, el. pašto adresu [dpo\[A\]skidsolutions.eu](mailto:dpo[A]skidsolutions.eu) pateikite elektroniniu būdu pasirašytą skundą ir mes Jums atsakysime per 30 kalendorinių dienų. Jei SK atsakymas į skundą Jūsų netenkina, dėl savo teisių pažeidimo, galite kreiptis į Estijos, Latvijos ar Lietuvos valstybinės duomenų apsaugos inspekciją.

10. Duomenų naudojimas per įgaliotąjį duomenų tvarkytoją

Remiantis sutarties nuostatomis SK turi teisę įgalioti kitą asmenį (juridinį arba fizinį) tvarkyti asmens duomenis. Įgaliotieji duomenų tvarkytojai gali būti SK partneriai, išduodantys sertifikatus, aptarnaujantys klientus ir padedantys klientams išspręsti iškilusius nesklandumus. SK, kaip duomenų valdytojas, įgaliotajam duomenų tvarkytojui teikia būtinus nurodymus dėl duomenų tvarkymo. SK yra atsakinga už įgaliotųjų duomenų tvarkytojų atitikimą asmens duomenų tvarkymo reikalavimams. Įgaliotasis duomenų tvarkytojas asmens duomenis gali tvarkyti tik konkrečiam ir leistinam tikslui pasiekti. SK patvirtina, kad

konfidencialios informacijos apsaugos ir duomenų apsaugos sutartys pasirašomos su visais įgaliotaisiais duomenų tvarkytojais. SK įgaliojimų duomenų tvarkytojų sąrašas pateiktas [čia](#).

Remiantis BDAR nuostatomis, dėl jūsų inicijuoto tapatybės patvirtinimo ar elektroninio parašo pateikimo, jūsų asmens duomenų iš SK reikalaujanti el. paslauga nėra SK įgaliojasis duomenų tvarkytojas.

11. Asmens duomenų atskleidimas arba perdavimas trečiosioms šalims

SK neatskleidžia ir neperduoda asmens duomenų trečiosioms šalims, išskyrus toliau nurodytus atvejus:

1. Iškilus pareigai dėl atitinkamų teisės aktų ar jų pagrindu taikomų priemonių (pavyzdžiui, duomenis perduodant tiriančiajai institucijai).
2. Asmenims, susijusiems su paslaugų teikimu.
3. SK turi teisę, siekiant įvykdyti sutarties įsipareigojimus, atskleisti asmens duomenis trečiosioms šalims, įskaitant kredito informacijos ir skolų išieškojimo įmones ir kitus asmenis, administruojančius skolų bylas, įskaitant advokatus ir antstolius, jei asmuo nevykdo sutarties įsipareigojimų.
4. Susijęs asmuo pateikia raštišką sutikimą atskleisti informaciją trečiosioms šalims.

SK patvirtina, kad asmens duomenis trečiosioms šalims atskleidžia tik tiek, kiek tai būtina atitinkamiems asmens duomenų tvarkymo tikslams pasiekti.

SK atskleidžia su asmens dokumentais (įskaitant „Mobile-ID“) susijusių galiojančių estiškų sertifikatų duomenis, jų galiojimo laikotarpiu, naudojantis LDAP paslauga. Papildomą informaciją apie LDAP paslaugą rasite [čia](#).

12. Asmens duomenų saugojimo laikotarpis

SK tvarko asmens duomenis tik tiek laiko, kiek tai būtina, siekiant tikslų, dėl kurių asmens duomenys renkami arba vykdant įsipareigojimus, atsirandančius dėl galiojančių teisės aktų reikalavimų. Pažymime, kad teikdami patikimumo užtikrinimo paslaugas, mes vadovaujamės eIDAS reglamentu ir Estijos elektroninio identifikavimo ir elektroninių operacijų patikimumo užtikrinimo paslaugų akto nuostatomis dėl asmens duomenų saugojimo. SK privalo saugoti asmens duomenis mažiausiai 10 metų po to, kai baigia galioti sertifikatas, kad prireikus, būtų galima įrodyti bet kokius piktnaudžiavimo asmens tapatybe atvejus ir įrodyti SK veiksmų, teikiant paslaugas, teisėtumą. Duomenis ir įrodymus saugoti numato įstatymai ir atitiktis šiam reikalavimui tikrinimą vykdo nepriklausomi auditoriai ir priežiūros institucijos.

13. Asmens duomenų tvarkymo principų papildymai

SK turi teisę vienašališkai keisti šiuos asmens duomenų tvarkymo principus, laikydamosi galiojančių teisės aktų reikalavimų. Pakeitimai skelbiami [SK tinklapyje](#) ir įsigalioja iš karto po paskelbimo.