					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P16					Dokumenta nosaukums: **Datu maskēšanas un pseidonimizācijas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un normatīvo regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1. punkts	Vispārīgās prasības risku pārvaldībai un darbības kontroles pasākumiem attiecībā uz maskēšanu un pseidonimizāciju
ISO/IEC 27002:2022	Kontroles pasākumi 8.11, 8	Vadlīnijas kontroles pasākumu ieviešanai datu maskēšanā un pseidonimizācijā
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Privātuma un konfidencialitātes kontroles pasākumi datu minimizēšanai, transformēšanai un piekļuves ierobežošanai
GDPR	4(5), 5(1)(c,f), 32. pants	Pseidonimizācijas un datu aizsardzības pasākumu tiesiskais pamats un prasības
NIS2	21(2)(c) pants	Pienākums piemērot tehniskos un organizatoriskos pasākumus, tostarp privātumu uzlabojošas tehnoloģijas (PET)
DORA	10(1), 10(2)(e) pants	IKT risku pārvaldība un konfidencialitātes kontroles pasākumi datu maskēšanai un pseidonimizācijai
COBIT 2019	DSS05.01, DSS06.06, MEA03	Pārvaldības kontroles pasākumi datu aizsardzībai, izmantojot maskēšanu, un atbilstības izvērtēšana

1. Mērķis

1.1 Šī politika nosaka organizācijas pieeju datu maskēšanas un pseidonimizācijas ieviešanai kā privātumu uzlabojošām tehnoloģijām (PET), lai samazinātu personas datu vai sensitīvu datu identificējamību un pakļautību riskam.

1.2 Tā atbalsta drošu informācijas izmantošanu testēšanā, analītikā un operacionālajā darbībā, vienlaikus nodrošinot atbilstību tiesiskajām un normatīvajām prasībām, mazinot datu aizsardzības pārkāpumu ietekmi un ievērojot datu minimizēšanas un konfidencialitātes principus.

1.3 Politika ir saskaņota ar ISO/IEC 27001:2022, atbalsta GDPR 4(5) pantā noteikto pseidonimizāciju un paredz uz risku balstītu ieviešanu atbilstoši NIST, NIS2, DORA un COBIT 2019 prasībām.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem darbiniekiem, līgumslēdzējiem, trešajām pusēm un piegādātājiem, kuriem ir piekļuve sistēmām, kas apstrādā personas datus, konfidenciālu vai sensitīvu informāciju;

2.1.2 visām datu vidēm, tostarp ražošanas, izstrādes, testēšanas un pirmsražošanas vidēm;

2.1.3 visām datu maskēšanas formām (piemēram, statiskajai, dinamiskajai, deterministiskajai maskēšanai un tokenizācijai) un pseidonimizācijas metodēm, ko izmanto privātuma risku mazināšanai;

2.1.4 visiem datu veidiem (strukturētiem vai nestrukturētiem), sistēmām (lokāli vai mākoņvidē izvietotām) un lietotnēm, kurās tiek izmantoti personas dati vai reglamentēti dati.

2.2 Piemērošanas joma ietver izmantošanu:

2.2.1 lietotņu izstrādē un QA/testēšanas vidēs;

2.2.2 analītikas vai atskaišu platformās;

2.2.3 datu apmaiņā ar trešajām pusēm vai pakalpojumu sniedzējiem;

2.2.4 rezerves kopēšanas, arhivēšanas vai atjaunošanas sistēmās.

3. Mērķi

3.1 Nodrošināt konsekventu un efektīvu maskēšanas un pseidonimizācijas piemērošanu, lai samazinātu datu izpaušanas vai neatbilstošas izmantošanas risku.

3.2 Nodrošināt, ka neprodukcijas vidēs nekad netiek izmantoti reāli dati, ja vien tie nav transformēti, izmantojot apstiprinātas PET metodes.

3.3 Saglabāt atsauču integritāti, lietojamību un formātu saglabājošas transformācijas, ja tas ir nepieciešams operacionālai konsekvencei.

3.4 Ieviest stingrus piekļuves kontroles pasākumus attiecībā uz sākotnējiem datiem, maskētajiem datiem un atkārtotas identificēšanas atslēgām.

3.5 Maskētas vai pseidonimizētas datu kopas apstrādāt kā sensitīvus datus, uz kuriem attiecas piekļuves žurnalēšana, glabāšanas kontroles pasākumi un incidentu reaģēšanas procedūras.

3.6 Validēt šo kontroles pasākumu efektivitāti, veicot nepārtrauktu testēšanu, uzraudzību un audita procedūras.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Apstiprina šo politiku un nodrošina tās ieviešanu kā daļu no plašākām IT pārvaldības un datu aizsardzības iniciatīvām.

4.2 Galvenais informācijas drošības vadītājs (CISO) / IDPS vadītājs

4.2.1 Pārrauga ieviešanu un nepārtrauktu atbilstību.

4.2.2 Nodrošina atbilstību ISO/IEC 27001 6.1.3. punktam (risku apstrāde) un 8.1. punktam (darbības kontrole).

4.2.3 Pārskata audita žurnālus un validē kontroles pasākumu efektivitāti.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā vai agrāk, ja notiek:

9.1.1 normatīvā regulējuma izmaiņas, kas ietekmē maskēšanu vai pseidonimizāciju;

9.1.2 jaunu IT sistēmu ieviešana, kurās tiek apstrādāti sensitīvi dati;

9.1.3 būtiskas izmaiņas organizācijas datu klasificēšanas shēmā;

9.1.4 audita konstatējumi, kas norāda uz kontroles pasākumu nepilnībām;

9.1.5 jaunu apdraudējumu vai maskēšanas tehnoloģiju rašanās.

9.2 IDPS vadītājs vada pārskatīšanu, konsultējoties ar datu aizsardzības speciālistu, datu īpašniekiem, IT drošību un Juridisko un atbilstības funkciju. Atjauninājumi jāpārvalda versiju kontroles ietvaros, tie jāapstiprina izpildvadības līmenī un par tiem jāpaziņo visām skartajām iesaistītajām pusēm.

10. Saistītās politikas un sasaiste

10.1 P13 - Datu klasificēšanas un marķēšanas politika. Lēmumi par maskēšanu un pseidonimizāciju ir tieši atkarīgi no P13 noteiktās datu lauku klasifikācijas un sensitivitātes līmeņiem.

10.2 P14 - Datu glabāšanas un likvidēšanas politika. Transformētās datu kopas jāglabā un jālikvidē saskaņā ar P14 dzīves cikla prasībām, nodrošinot, ka maskēti un pseidonimizēti dati tiek apstrādāti kā sensitīvi.

10.3 P17 - Datu aizsardzības un privātuma politika. Tā nosaka privātuma principus un normatīvo pamatu pseidonimizācijas piemērošanai kā atbilstošai apstrādes darbībai saskaņā ar GDPR un līdzīgiem tiesību aktiem.

10.4 P22 - Žurnalēšanas un uzraudzības politika. Tā nodrošina centralizētu maskēšanas un pseidonimizācijas notikumu auditēšanu un brīdināšanu saskaņā ar strukturētiem drošības uzraudzības protokoliem.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 6.1.3. punkts - Risku apstrādes plāns: nosaka maskēšanu un pseidonimizāciju kā risku apstrādes mehānismus sensitīvu datu identificējamības samazināšanai nebūtiskās apstrādes vidēs.

11.1.2 8.1. punkts - Operacionālā plānošana un kontrole: nosaka tehniskos un procesu kontroles pasākumus drošai datu transformēšanai apstrādes, glabāšanas vai pārsūtīšanas laikā.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroles pasākumi 8.11, 8: vadlīnijas datu maskēšanai un pseidonimizācijai, lai mazinātu atkārtotas identificēšanas un datu noplūdes risku.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - PII aizsardzība: privātumu uzlabojošu tehnoloģiju, piemēram, maskēšanas un pseidonimizācijas, ieviešana.

11.3.2 PT-2, PT-3: PII apstrādes minimizēšana un drošība - transformēšana, lai samazinātu identificējamību un nodrošinātu piekļuves kontroli.

11.3.3 SC-12, SC-28, SC-30: datu konfidencialitāte un integritāte - konfidencialitātes un aizklāšanas kontroles pasākumi glabāšanai, pārraidei un izmantošanai.

11.4 GDPR (2016/679)

11.4.1 4(5) pants: pseidonimizācijas formālā definīcija.

11.4.2 32. pants: apstrādes drošība - organizatoriskie un tehniskie pasākumi pseidonimizācijai.

11.4.3 5(1)(c,f) pants: datu minimizēšana un konfidencialitāte, izmantojot pseidonimizāciju un maskēšanu.

11.5 NIS2 direktīva (2022/2555)

11.5.1 21(2)(c) pants: nosaka PET, piemēram, maskēšanu un pseidonimizāciju, kā drošības pasākumus.

11.6 DORA (2022/2554)

11.6.1 10(1) pants: IKT risku pārvaldības ietvars ietver maskēšanas un pseidonimizācijas kontroles pasākumus.

11.6.2 10(2)(e) pants: nosaka pienākumu izmantot transformācijas tehnoloģijas personas un finanšu datu aizsardzībai.

11.7 COBIT 2019

11.7.1 DSS05.01: informācijas aktīvu aizsardzība - prasības maskēšanai un pseidonimizācijai.

11.7.2 DSS06.06: droša testēšana un analītika - maskēšana vidēs ārpus ražošanas vides.
11.7.3 MEA03: atbilstības uzraudzība maskēšanas un pseidonimizācijas efektivitātei.