					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P16S					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 piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkts 6.1.3, punkts 8	Informācijas drošības riski un nepieciešamie kontroles pasākumi, tostarp maskēšana un pseidonimizācija
ISO/IEC 27002:2022	Kontroles pasākumi 8.11, 8.12	Vadlīnijas par maskēšanu un datu noplūdes novēršanu
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Datu aizklāšana, privātumu uzlabojošas tehnoloģijas
ES NIS2	Pants 21(2)(c)	Samērīgi tehniskie pasākumi, tostarp pseidonimizācija kā kontroles pasākums
ES DORA	Pants 10(1)	IKT risku kontroles pasākumi, tostarp datu transformācijas aizsardzības pasākumi
COBIT 2019	DSS05.01, DSS06	Datu aizsardzība, aizklāšanas un pseidonimizācijas metodes
ES VDAR	Panti 4(5), 5(1)(c), 32	Datu minimizēšana, pseidonimizācija kā tehnisks kontroles pasākums

1. Mērķis

1.1. Šī politika nosaka saistošas prasības datu maskēšanas un pseidonimizācijas izmantošanai, lai aizsargātu sensitīvus, personas un konfidenciālus datus mazos un vidējos uzņēmumos (MVU).

1.2. Šo paņēmienu izmantošana ir obligāta, ja faktiskie dati nav nepieciešami, piemēram, izstrādes, analītikas vai trešo pušu pakalpojumu sniegšanas scenārijos, tādējādi samazinot datu atklāšanas, neatbilstošas izmantošanas vai pārkāpuma risku.

1.3. Šī politika tieši atbalsta atbilstību ISO/IEC 27001:2022 sertifikācijas prasībām, kā arī Eiropas regulatīvajām prasībām, piemēram, VDAR, NIS2 direktīvai un DORA regulai.

1.4. Transformējot datus pirms to izmantošanas ārpus to sākotnējā biznesa konteksta, organizācija samazina atbildības risku un stiprina spēju pierādīt pienācīgu rūpību privātuma un drošības jomā.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visiem strukturētiem un nestrukturētiem datiem, kas klasificēti kā personas dati, konfidenciāli dati vai sensitīvi dati, neatkarīgi no tā, vai tie tiek glabāti vai apstrādāti:

2.1.1. ražošanas, testa vai izstrādes vidēs;

2.1.2. lokālajās ierīcēs, serveros vai mākoņplatformās;

2.1.3. iekšējā personāla, līgumslēdzēju vai trešo pušu pakalpojumu sniedzēju vajadzībām.

2.2. Tā attiecas arī uz visiem datu transformācijas rīkiem (maskēšana, tokenizācija, pseidonimizācija), neatkarīgi no tā, vai tie ir atvērtā pirmkoda, komerciāli vai izstrādāti organizācijas iekšienē.

2.3. Šīs politikas piemērošanas gadījumi ietver:

2.3.1. testa vai izstrādes datu kopu sagatavošanu;

2.3.2. datu eksportēšanu uz analītikas sistēmām;

2.3.3. piegādātāju vai konsultantu piekļuvi operatīvajām sistēmām;

2.3.4. datu subjektu datu minimizēšanu, lai samazinātu apstrādes risku.

3. Mērķi

3.1. Nodrošināt, ka faktiskie personas dati vai sensitīvi dati nekad netiek atklāti vidēs ar zemāku drošības līmeni, kurās tie nav būtiski nepieciešami.

3.2. Noteikt par obligātu maskēšanas vai pseidonimizācijas paņēmienu izmantošanu, ja uzdevuma izpildei faktiskie identifikatori nav noteikti nepieciešami.

3.3. Novērst nesankcionētu piekļuvi datiem vai to neatbilstošu izmantošanu, piemērojot datu transformācijas kontroles pasākumus pirms datu pārsūtīšanas vai apstrādes.

3.4. Nodrošināt, ka visi maskēšanas un pseidonimizācijas procesi ir izsekojami, auditējami un īstenoti, izmantojot apstiprinātus rīkus.

3.5. Ievērot piemērojamās tiesiskās un regulatīvās prasības attiecībā uz datu minimizēšanu, konfidencialitāti un datu transformācijas aizsardzības pasākumiem.

4. Lomas un pienākumi

4.1. Ģenerāldirektors (GM)

4.1.1. ir šīs politikas īpašnieks un to apstiprina;

4.1.2. nodrošina, ka visas struktūrvienības un pakalpojumu sniedzēji ievēro datu transformācijas prasības;

4.1.3. pārskata izņēmumus, risku izvērtējumus un datu transformācijas žurnālus;

4.1.4. pārkāpumu gadījumā koordinē juridiskās, operatīvās vai ar piegādātājiem saistītās darbības.

4.2. IT atbalsta pakalpojumu sniedzējs / iekšējā IT funkcija

4.2.1. izvēlas un pārvalda maskēšanas vai pseidonimizācijas rīkus;

4.2.2. nodrošina, ka atbilstošas datu transformācijas metodes tiek piemērotas atbilstoši datu veidam;

4.2.3. uztur transformēto datu kopu žurnālus un atslēgu pārvaldības procedūras;

4.2.4. nodrošina, ka maskēšana tiek veikta pirms datu izmantošanas testēšanā, piegādātāju vajadzībām vai analītikā.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Ikgadējā pārskatīšana

9.1.1. Ģenerāldirektoram šī politika jāpārskata vismaz reizi gadā, lai nodrošinātu, ka tā atspoguļo:

9.1.1.1. izmaiņas piemērojamajos tiesību aktos un regulējumā (piemēram, VDAR, DORA);

9.1.1.2. jaunas biznesa sistēmas vai datu apmaiņu ar trešajām pusēm;

9.1.1.3. atziņas no auditiem vai incidentiem, kas saistīti ar nemaskētu datu izmantošanu.

9.2. Starpposma pārskatīšana

9.2.1. Pārskatīšana jāveic arī, ja:

9.2.1.1. tiek ieviestas jaunas lietotnes vai platformas, kas apstrādā sensitīvus datus;

9.2.1.2. būtisks incidents atklāj trūkumus esošajos datu transformācijas kontroles pasākumos;

9.2.1.3. klasifikācijas līmeņu izmaiņas ietekmē datu apstrādes procedūras.

9.3. Versiju kontrole un izmaiņu pārvaldība

9.3.1. Visi politikas grozījumi:

9.3.1.1. jāapstiprina GM un jādokumentē izmaiņu žurnālā;

9.3.1.2. skaidri jāpaziņo ietekmētajiem darbiniekiem un pakalpojumu sniedzējiem;

9.3.1.3. droši jāarhivē, ierobežojot piekļuvi novecojušajām versijām.

10. Saistītās politikas un sasaiste

10.1. Šī politika jāpiemēro kopā ar šādām MVU politikām, lai nodrošinātu konsekventu un saistošu sensitīvu datu aizsardzību:

10.1.1. P13S – Datu klasificēšanas un marķēšanas politika: nosaka klasifikācijas līmeņus (piemēram, “konfidenciāli – personas dati”), pēc kuriem nosaka, kad jāpiemēro maskēšana vai pseidonimizācija. Šī politika nosaka datu transformācijas prasības atbilstoši datu sensitivitātes līmenim.

10.1.2. P14S – Datu glabāšanas un likvidēšanas politika: nodrošina, ka transformētās datu kopas, tostarp rezerves kopijas, kas satur maskētus vai pseidonimizētus datus, tiek glabātas un likvidētas atbilstoši piemērojamajām prasībām, tostarp dzēšot sasaistes atslēgas, kad tās vairs nav nepieciešamas.

10.1.3. P17S – Datu aizsardzības un privātuma politika: saskaņo datu transformācijas praksi ar plašākiem privātuma pienākumiem, tostarp VDAR prasībām par datu minimizēšanu un pseidonimizācijas izmantošanu kā aizsardzības pasākumu personas datu apstrādē.

10.1.4. P30S – Incidentu pārvaldības politika: aptver ziņošanas un eskalācijas kārtību nesankcionētas datu izpaušanas gadījumā, tostarp maskētu vai pseidonimizētu datu neatbilstošu izmantošanu vai atgriezenisku atjaunošanu.

10.1.5. P2S – Pārvaldības lomu un atbildības politika: nosaka vispārējo pārskatatbildību par politikas ieviešanu, riska pieņemšanu un izņēmumu apstiprināšanu, galvenokārt ģenerāldirektoram.

10.2. Šīs politikas veido integrētu datu aizsardzības ietvaru, nodrošinot, ka maskēšanas un pseidonimizācijas pasākumi atbalsta ISO 27001 sertifikāciju un atbilstību vairākām regulatīvajām prasībām.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. Punkts 6.1.3: nosaka informācijas drošības risku apstrādi, tostarp datu atklāšanas riska mazināšanu, izmantojot datu transformācijas paņēmienus.

11.1.2. Punkts 8.1: nosaka tādu kontroles pasākumu ieviešanu, kas nepieciešami drošības mērķu sasniegšanai, tostarp pseidonimizāciju un maskēšanu.

11.2. ISO/IEC 27002

11.2.1. Kontroles pasākums 8.11: sniedz vadlīnijas sensitīvu datu maskēšanai testa un izstrādes sistēmās.

11.2.2. Kontroles pasākums 8.12: nosaka pieeju datu noplūdes novēršanai, izmantojot kontrolētu transformāciju un piekļuves praksi.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: nodrošina informācijas konfidencialitāti, izmantojot datu aizklāšanu.

11.3.2. SC-28: aizsargā informāciju glabāšanā un lietošanā.

11.3.3. PT-2/PT-3: veicina privātumu uzlabojošu tehnoloģiju, tostarp pseidonimizācijas, izmantošanu PII apstrādes laikā.

11.4. ES VDAR

11.4.1. Pants 4(5): definē pseidonimizāciju un nosaka kontroles pasākumus sasaistes atslēgām un identifikatoriem.

11.4.2. Pants 5(1)(c): atbalsta datu minimizēšanas principu īstenošanu, izmantojot maskēšanu.

11.4.3. Pants 32: atzīst pseidonimizāciju par tehnisku kontroles pasākumu, kas samazina privātuma riskus.

11.5. ES NIS2 direktīva

11.5.1. Pants 21(2)(c): nosaka samērīgus tehniskos pasākumus datu drošības riska mazināšanai, tostarp pseidonimizāciju kā daļu no risku kontroles pasākumiem.

11.6. ES DORA regula

11.6.1. Pants 10(1): nosaka ar IKT saistītus risku kontroles pasākumus, kas ietver datu transformācijas aizsardzības pasākumus darbības nepārtrauktībai un konfidencialitātei ārpakalpojumu izmantošanas un sistēmu izstrādes laikā.

11.7. COBIT 2019

11.7.1. DSS05.01: nosaka informācijas aktīvu aizsardzību, tostarp transformāciju, ja tā ir iespējama.

11.7.2. DSS06.06: paredz atbilstošu aizklāšanas un pseidonimizācijas paņēmienu izmantošanu, lai ierobežotu datu atklāšanu vidēs ar zemāku uzticamības līmeni.