					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P16S					Dokumendi pealkiri: **Andmete maskeerimise ja pseudonüümimise poliitika – VKE**						
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:						
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 6.1.3, punkt 8	Infoturberiskid ja vajalikud kontrollimeetmed, sh maskeerimine ja pseudonüümimine
ISO/IEC 27002:2022	Kontrollimeetmed 8.11, 8.12	Suunised maskeerimise ja andmelekkete vältimise kohta
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Andmete hägustamine, privaatsust suurendavad tehnoloogiad
EL NIS2	Artikkel 21(2)(c)	Proportsionaalsed tehnilised meetmed, sh pseudonüümimine kontrollimeetmena
EL DORA	Artikkel 10(1)	IKT-riskide kontrollimeetmed, sh andmete teisendamise kaitsemeetmed
COBIT 2019	DSS05.01, DSS06	Andmekaitse, hägustamise ja pseudonüümimise meetodid
EL isikuandmete kaitse üldmäärus (GDPR)	Artiklid 4(5), 5(1)(c), 32	Andmete minimeerimine, pseudonüümimine tehnilise kontrollimeetmena

1. Eesmärk

1.1. Käesolev poliitika kehtestab siduvad nõuded andmete maskeerimise ja pseudonüümimise kasutamiseks, et kaitsta väikeses ja keskmise suurusega ettevõttes (VKE) tundlikke, isiku- ja konfidentsiaalseid andmeid.

1.2. Nende meetodite kasutamine on kohustuslik juhtudel, kui tegelikke andmeid ei ole vaja, näiteks arenduses, analüütikas või kolmandate isikute teenuste kasutamisel, et vähendada andmete avalikustamise, väärkasutuse või rikkumise riski.

1.3. Käesolev poliitika toetab otseselt vastavust standardi ISO/IEC 27001:2022 sertifitseerimisnõuetele ning Euroopa õigusaktidele, sealhulgas GDPR-ile, NIS2 direktiivile ja DORA määrusele.

1.4. Andmete teisendamine enne nende kasutamist väljaspool algset ärikonteksti vähendab organisatsiooni vastutust ning tugevdab suutlikkust tõendada andmekaitse- ja infoturbekontrollide rakendamist.

2. Kohaldamisala

2.1. Käesolev poliitika kohaldub kõigile struktureeritud ja struktureerimata andmetele, mis on klassifitseeritud isikuandmeteks, konfidentsiaalseteks või tundlikeks andmeteks ning mida säilitatakse või töödeldakse:

2.1.1. tootmiskeskkonnas, testkeskkonnas või arenduskeskkonnas;

2.1.2. kohalikes seadmetes, serverites või pilveplatvormidel;

2.1.3. sisepersonali, töövõtjate või kolmandatest isikutest teenuseosutajate poolt.

2.2. Poliitika hõlmab ka kõiki andmete teisendamise tööriistu (maskeerimine, tokeniseerimine, pseudonüümimine), sõltumata sellest, kas need on avatud lähtekoodiga, kommertslikud või ettevõttesiseselt arendatud.

2.3. Käesoleva poliitika kohased kasutusjuhud hõlmavad muu hulgas järgmist:

2.3.1. test- või arendusandmestike ettevalmistamine;

2.3.2. andmete eksport analüütikasüsteemidesse;

2.3.3. tarnija või konsultandi juurdepääs tööks kasutatavatele süsteemidele;

2.3.4. andmesubjektiga seotud andmete minimeerimine töötlemisriski vähendamiseks.

3. Eesmärgid

3.1. Tagada, et tegelikud isiku- või tundlikud andmed ei satuks kunagi madalama turbetasemega keskkondadesse, kus need ei ole hädavajalikud.

3.2. Nõuda maskeerimise või pseudonüümimise kasutamist juhtudel, kui ülesande täitmiseks ei ole tegelikud identifikaatorid rangelt vajalikud.

3.3. Tõkestada andmete loata juurdepääs või väärkasutus, rakendades andmete teisendamise kontrollimeetmeid enne andmete edastamist või töötlemist.

3.4. Tagada, et kõik maskeerimise ja pseudonüümimise protsessid on jälgitavad, auditeeritavad ja rakendatud heakskiidetud tööriistade abil.

3.5. Tagada vastavus kohaldatavatele õiguslikele ja regulatiivsetele nõuetele, mis eeldavad andmete minimeerimist, konfidentsiaalsust ja andmete teisendamise kaitsemeetmeid.

4. Rollid ja vastutused

4.1. Tegevjuht

4.1.1. vastutab käesoleva poliitika eest ja kiidab selle heaks;

4.1.2. tagab, et kõik üksused ja teenuseosutajad täidavad andmete teisendamise nõudeid;

4.1.3. vaatab läbi erandid, riskihindamised ja andmete teisendamise logid;

4.1.4. koordineerib rikkumiste korral õiguslikke, operatiivseid ja tarnijatega seotud tegevusi.

4.2. Väline IT-teenuseosutaja / sisemine IT

4.2.1. valib ja haldab maskeerimise või pseudonüümimise tööriistu;

4.2.2. tagab, et andmetüübi alusel rakendatakse sobivaid andmete teisendamise meetodeid;

4.2.3. haldab teisendatud andmestike logisid ja võtmehalduse protseduure;

4.2.4. tagab, et maskeerimine toimub enne testimist, tarnijale edastamist või analüütikas kasutamist.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Iga-aastane läbivaatamine

9.1.1. Tegevjuht peab käesoleva poliitika läbi vaatama vähemalt kord aastas, et tagada selle vastavus järgmisele:

9.1.1.1. kohaldatavate õigusaktide ajakohastused (nt GDPR, DORA);

9.1.1.2. uued ärisüsteemid või andmevahetused kolmandate isikutega;

9.1.1.3. auditite või intsidentide tagasiside, mis on seotud maskeerimata andmete kasutamisega.

9.2. Vahepealsed läbivaatamised

9.2.1. Läbivaatamine tuleb teha ka siis, kui:

9.2.1.1. kasutusele võetakse uusi rakendusi või platvorme, mis töötlevad tundlikke andmeid;

9.2.1.2. oluline intsident toob esile puudused kehtivates andmete teisendamise kontrollimeetmetes;

9.2.1.3. muudatused klassifikatsioonitasemetes mõjutavad andmekäitluse protseduure.

9.3. Versioonihaldus ja muudatuste juhtimine

9.3.1. Kõik poliitikamuudatused peavad olema:

9.3.1.1. tegevjuhi poolt heaks kiidetud ja dokumenteeritud muudatuste logis;

9.3.1.2. selgelt edastatud mõjutatud töötajatele ja teenuseosutajatele;

9.3.1.3. turvaliselt arhiveeritud nii, et aegunud versioonidele on juurdepääs piiratud.

10. Seotud poliitikad ja seosed

10.1. Tundlike andmete järjepideva ja siduva kaitse tagamiseks tuleb käesolevat poliitikat rakendada koos järgmiste VKE poliitikatega:

10.1.1. P13S – andmete klassifitseerimise ja märgistamise poliitika: määratleb klassifikatsioonitasemed (nt „Konfidentsiaalne – isikuandmed“), mille alusel otsustatakse, millal tuleb rakendada maskeerimist või pseudonüümimist. Käesolev poliitika rakendab andmete teisendamise reegleid vastavalt andmete tundlikkuse tasemele.

10.1.2. P14S – andmete säilitamise ja kõrvaldamise poliitika: tagab, et teisendatud andmestikke, sealhulgas maskeeritud või pseudonüümitud andmeid sisaldavaid varukoopiaid, säilitatakse ja kõrvaldatakse kohaldatavate reeglite kohaselt, sealhulgas vastendusvõtmete kustutamine, kui neid enam ei vajata.

10.1.3. P17S – andmekaitse ja privaatsuse poliitika: kooskõlastab andmete teisendamise praktikad laiemate andmekaitsekohustustega, sealhulgas GDPR-i nõuetega andmete minimeerimise ja pseudonüümimise kasutamise kohta isikuandmete töötlemise kaitsemeetmena.

10.1.4. P30S – intsidentidele reageerimise poliitika: hõlmab teatamise ja eskaleerimise protseduure loata andmete avalikustamise korral, sealhulgas maskeeritud või pseudonüümitud andmete mittenõuetekohase kasutamise või pöördteisendamise korral.

10.1.5. P2S – juhtimisrollide ja vastutuste poliitika: määrab poliitika rakendamise, riski aktsepteerimise ja erandite heakskiitmise üldvastutuse peamiselt tegevjuhile.

10.2. Need poliitikad moodustavad integreeritud andmekaitseraamistiku, mis tagab, et maskeerimise ja pseudonüümimise meetmed toetavad ISO 27001 sertifitseerimist ja regulatsioonidevahelist vastavust.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 6.1.3: nõuab infoturberiskide käsitlemist, mis hõlmab andmete teisendamise meetodite abil kokkupuute vähendamist.

11.1.2. Punkt 8.1: nõuab turbe-eesmärkide täitmiseks vajalike kontrollimeetmete rakendamist, sealhulgas pseudonüümimist ja maskeerimist.

11.2. ISO/IEC 27002

11.2.1. Kontrollimeede 8.11: annab suuniseid tundlike andmete maskeerimiseks test- ja arendussüsteemides.

11.2.2. Kontrollimeede 8.12: kirjeldab meetmeid andmelekkete vältimiseks kontrollitud andmete teisendamise ja juurdepääsupraktikate kaudu.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: tagab teabe konfidentsiaalsuse andmete hägustamise kaudu.

11.3.2. SC-28: kaitseb teavet nii puhkeolekus kui kasutamisel.

11.3.3. PT-2/PT-3: edendab privaatsust suurendavate tehnoloogiate, sealhulgas pseudonüümimise, kasutamist isikut tuvastava teabe töötlemisel.

11.4. EL isikuandmete kaitse üldmäärus (GDPR)

11.4.1. Artikkel 4(5): määratleb õiguslikult pseudonüümimise ning nõuab kontrolli vastendusvõtmete ja identifikaatorite üle.

11.4.2. Artikkel 5(1)(c): toetab andmete minimeerimise põhimõtet maskeerimise kaudu.

11.4.3. Artikkel 32: käsitab pseudonüümimist tehnilise kontrollimeetmena, mis vähendab andmekaitseriske.

11.5. EL NIS2 direktiiv

11.5.1. Artikkel 21(2)(c): nõuab proportsionaalseid tehnilisi meetmeid andmeturbe riski minimeerimiseks, sealhulgas pseudonüümimist riskikontrolli osana.

11.6. EL DORA määrus

11.6.1. Artikkel 10(1): nõuab IKT-ga seotud riskide kontrollimeetmeid, mis hõlmavad andmete teisendamise kaitsemeetmeid toimepidevuse ja konfidentsiaalsuse tagamiseks allhanke ja süsteemiarenduse ajal.

11.7. COBIT 2019

11.7.1. DSS05.01: nõuab teabevarade kaitset, sealhulgas andmete teisendamist, kui see on asjakohane.

11.7.2. DSS06.06: nõuab sobivate hägustamise ja pseudonüümimise meetodite kasutamist, et piirata andmete kokkupuudet madalama usaldustasemega keskkondades.