					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P17S					Dokumendi pealkiri: **Andmekaitse ja privaatsuspoliitika**						
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	Punktid 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontrollimeetmed 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 5, 6, 12-23, 30, 32-34	
ELi NIS2 direktiiv	Artikkel 21(2)(e), 21(2)(f)	
ELi DORA määrus	Artiklid 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Eesmärk

1.1. Käesolev poliitika määratleb, kuidas organisatsioon kaitseb isikuandmeid kooskõlas õiguslike kohustuste, regulatiivsete raamistike ja rahvusvaheliste turbestandarditega.

1.2. See tagab, et isikuandmeid — olenemata sellest, kas need pärinevad klientidelt, töötajatelt või partneritelt — kogutakse, kasutatakse, säilitatakse ja kustutatakse seaduslikult, õiglaselt ja turvaliselt.

1.3. Käesolev poliitika toetab ka vastavust standardile ISO/IEC 27001:2022 ning auditivalmidust, rakendades järjepidevat riskipõhist lähenemist privaatsuse kaitsele.

1.4. Käesoleva poliitika kaudu tõendab organisatsioon vastutustundlikkust ning suurendab klientide usaldust, seades esikohale läbipaistvuse, andmete minimaalsuse ja tugeva privaatsusjuhtimise.

2. Kohaldamisala

2.1. Käesolev poliitika kohaldub järgmisele:

2.1.1. kõigile töötajatele, töövõtjatele ja teenuseosutajatele, kes pääsevad ligi isikuandmetele, töötlevad neid või haldavad neid;

2.1.2. kõikidele süsteemidele, rakendustele ja asukohtadele, kus isikuandmeid säilitatakse või edastatakse;

2.1.3. kõigile isikuandmetele sõltumata sellest, kas neid säilitatakse elektrooniliselt, paberkandjal, pilvesüsteemides või mobiilseadmetes.

2.2. Käesolev poliitika kohaldub andmetele, mis on seotud klientide, töötajate, tarnijate ja muude tuvastatavate füüsiliste isikutega.

2.3. Poliitika kehtib sõltumata sellest, kas andmeid töödeldakse organisatsioonisiseselt või kolmandatest osapooltest teenuseosutajate poolt.

3. Eesmärgid

3.1. Tagada, et isikuandmete töötlemine toimub kooskõlas andmekaitsealaste õigusaktide ja turbestandarditega, sealhulgas GDPRi, NIS2 ja ISO 27001 nõuetega.

3.2. Kaitsta isikuandmeid loata juurdepääsu, väärkasutuse, muutmise või kao eest selgete tehniliste ja korralduslike meetmete abil.

3.3. Austada füüsiliste isikute privaatsusõigusi, sealhulgas õigust oma andmetele juurde pääseda, neid parandada ja kustutada.

3.4. Kehtestada organisatsioonis selged andmekaitsega seotud rollid ja vastutused.

3.5. Rakendada andmete minimaalsuse põhimõtet, turvalist säilitamist ja õigeaegset kustutamist kõigis süsteemides ja protsessides.

3.6. Vähendada mittevastavuse, õiguslike sanktsioonide, mainekahju või klientide usalduse vähenemise riski.

4. Rollid ja vastutused

4.1. tegevjuht

4.1.1. kiidab käesoleva poliitika heaks ja tagab selle rakendamise;

4.1.2. tagab privaatsusriskide haldamiseks ja intsidentidele reageerimiseks vajalikud ressursid;

4.1.3. kannab üldvastutust privaatsust käsitlevate õigusaktide ja standardite järgimise eest.

4.2. andmekaitsekoordinaator (sisemine või sisseostetud)

4.2.1. peab isikuandmete töötlemistoimingute arvestust;

4.2.2. vastab füüsiliste isikute privaatsustaotlustele ja regulatiivsetele päringutele;

4.2.3. toetab riskihindamisi, koolitusi ja poliitika rakendamist;

4.2.4. dokumenteerib rikkumiste juhtumid ja teavitab vajaduse korral pädevaid asutusi.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Korrapärased läbivaatamised

9.1.1. andmekaitsekoordinaator peab käesoleva poliitika läbi vaatama vähemalt üks kord 12 kuu jooksul ning selle peab heaks kiitma tegevjuht;

9.1.2. läbivaatamisel tuleb hinnata poliitika asjakohasust, kooskõla regulatiivsete nõuetega ja tegevuslikku tõhusust.

9.2. Vahepealse läbivaatamise alused

9.2.1. poliitika ajakohastamine tuleb algatada ka järgmiste asjaolude korral:

9.2.1.1. uued või muudetud andmekaitsealased õigusaktid (nt GDPR, DORA);

9.2.1.2. turbeintsidendid või privaatsusrikkumised, mis hõlmavad isikuandmeid;

9.2.1.3. uute süsteemide, tööriistade või teenuste kasutuselevõtt, mis töötlevad isikuandmeid;

9.2.1.4. olulised auditileiud või regulaatori soovitused.

9.3. Muudatuste ohje ja teabevahetus

9.3.1. kõik poliitikamuudatused tuleb ametlikult dokumenteerida muudatuste logis;

9.3.2. muudetud versioonid tuleb edastada kõigile töötajatele ja asjakohastele töövõtjatele;

9.3.3. arhiveeritud versioone tuleb säilitada vastavuse auditijälje tagamiseks.

10. Seotud poliitikad ja seosed

10.1. Käesolevat poliitikat rakendatakse koos teiste VKE poliitikatega, et moodustada terviklik ja rakendatav privaatsusraamistik:

10.1.1. P13S – Andmete klassifitseerimise ja märgistamise poliitika: tagab, et isikuandmed klassifitseeritakse asjakohaselt, et privaatsuse kaitsemeetmeid saaks rakendada riskitaseme alusel.

10.1.2. P14S – Andmete säilitamise ja kõrvaldamise poliitika: sätestab selged reeglid selle kohta, kui kaua isikuandmeid tuleb säilitada ja milliseid turvalisi meetodeid tuleb nende säilitustähtaja lõppemisel kõrvaldamiseks kasutada.

10.1.3. P16S – Andmete maskeerimise ja pseudonüümimise poliitika: määratleb, kuidas isikut tuvastavad tunnused tuleb teisendada enne andmete kasutamist tootmisvälises keskkonnas või nende jagamist väliste osapooltega.

10.1.4. P30S – Intsidentidele reageerimise poliitika: käsitleb samme, mis on vajalikud andmekaitserikkumistele reageerimiseks, sealhulgas regulaatorite ja mõjutatud isikute teavitamist nõutud tähtaja jooksul.

10.1.5. P2S – Juhtimisrollide ja vastutuste poliitika: selgitab vastutusstruktuuri ja otsustusrolle, mida kohaldatakse privaatsuse rakendamisele ja järelevalvele.

10.2. Neid seotud poliitikaid tuleb läbi vaadata ja rakendada koos, et tagada terviklik privaatsuse katvus süsteemide, töötajate ja tarnijate lõikes.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 5.1 – nõuab, et tippjuhtkond näitaks üles juhtimist ja pühendumust isikuandmete kaitsele.

11.1.2. Punkt 6.1.3 – nõuab isikuandmete töötlemisega seotud riskide käsitlemist.

11.1.3. Punkt 8.1 – nõuab tegevuslike kontrollimeetmete rakendamist andmete kaitsmiseks kogu nende elutsükli jooksul.

11.2. ISO/IEC 27002

11.2.1. Kontrollimeede 5.34 – annab rakendussuunised privaatsuse kaitsmiseks ja isikut tuvastava teabe turvaliseks käitlemiseks.

11.2.2. Kontrollimeede 8.10 – käsitleb isikuandmete turvalist kõrvaldamist, et vältida jääkandmete avalikuks saamist.

11.2.3. Kontrollimeede 8.11 – toetab maskeerimise ja pseudonüümimise kasutamist andmete minimaalsuse saavutamiseks.

11.2.4. Kontrollimeede 8.12 – ennetab loata andmeleket andmetele juurdepääsu ja nende kasutamise kontrollimeetmetega.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – määrab rollid ja vastutused privaatsusriskide haldamiseks.

11.3.2. PL-5 – nõuab privaatsusplaani dokumenteerimist, mis hõlmab andmete kasutamist ja kaitset.

11.3.3. AC-6 – nõuab vähimate õiguste põhimõtte rakendamist ja juurdepääsukontrolli isikuandmete puhul.

11.3.4. IR-4 – nõuab intsidentide käsitlemise protsesse isikuandmeid hõlmavate rikkumiste korral.

11.4. ELi isikuandmete kaitse üldmäärus (GDPR)

11.4.1. Artikkel 5 – määratleb seadusliku, õiglase ja läbipaistva andmetöötluse põhiprintsiibid.

11.4.2. Artikkel 6 – nõuab iga isikuandmete töötlemistoimingu jaoks kehtivat õiguslikku alust.

11.4.3. Artiklid 12–23 – kirjeldavad andmesubjekti õigusi, sealhulgas õigust tutvuda andmetega, neid parandada, kustutada ja esitada vastuväiteid.

11.4.4. Artikkel 30 – nõuab töötlemistoimingute registrit.

11.4.5. Artikkel 32 – nõuab asjakohaseid tehnilisi ja korralduslikke turvameetmeid.

11.4.6. Artiklid 33–34 – sätestavad rikkumistest teavitamise kohustused pädevatele asutustele ja andmesubjektidele.

11.5. ELi NIS2 direktiiv

11.5.1. Artikkel 21(2)(e) – nõuab meetmeid, mis tagavad andmekaitse kooskõlas küberturvalisuse poliitikatega.

11.5.2. Artikkel 21(2)(f) – nõuab mehhanisme isikuandmete ja konfidentsiaalsete andmete turbe haldamiseks IKT-süsteemides.

11.6. ELi DORA määrus

11.6.1. Artikkel 6 – nõuab sisemisi juhtimisraamistikke, mis haldavad andmeriski ja andmekaitset.

11.6.2. Artikkel 15 – kohustab finantsüksusi tagama, et kolmandatest osapooltest teenuseosutajad kaitsevad isikuandmeid ja toetavad regulatiivset vastavust.

11.6.3. Artikkel 17 – nõuab, et ettevõtted tagaksid isikuandmeid töötlevate IKT-süsteemide turvalisuse, toimepidevuse ja seire.

11.7. COBIT 2019

11.7.1. APO12 – Riskide juhtimine: nõuab privaatsus- ja andmekaitseriskide tuvastamist ning käsitlemist.

11.7.2. DSS05 – Turvateenuste haldamine: nõuab kaitsemeetmeid, et vältida loata juurdepääsu isikuandmetele.

11.7.3. MEA03 – Vastavuse seire: nõuab, et organisatsioonid tagaksid pideva vastavuse privaatsus- ja andmekaitsealastele õigusaktidele.