					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P17S					Dokumenta nosaukums: **Datu aizsardzības un privātuma 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**

Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienu šī dokumenta daļu nedrīkst kopēt, atkārtoti izmantot, izplatīt vai grozīt komerciāliem vai ieviešanas nolūkiem bez iepriekšējas skaidras rakstiskas atļaujas.
Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.
Par licencēšanu sazinieties: info@clarysec.com

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontroles pasākumi 5.34, 8.10–8.12	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
ES VDAR	5., 6., 12.–23., 30., 32.–34. pants	
ES NIS2	21. panta 2. punkta e) un f) apakšpunkts	
ES DORA	6., 15., 17. pants	
COBIT 2019	APO12, DSS05, MEA03	

1. Mērķis

1.1. Šī politika nosaka, kā organizācija aizsargā personas datus atbilstoši tiesiskajiem pienākumiem, regulatīvajiem ietvariem un starptautiskajiem drošības standartiem.

1.2. Tā nodrošina, ka personas dati — neatkarīgi no tā, vai tie attiecas uz klientiem, personālu vai partneriem — tiek vākti, izmantoti, glabāti un dzēsti likumīgi, godprātīgi un droši.

1.3. Šī politika nodrošina arī atbilstību ISO/IEC 27001:2022 prasībām un atbalsta gatavību auditam, ieviešot konsekventu, uz risku balstītu pieeju privātuma aizsardzībai.

1.4. Ar šo politiku organizācija apliecina pārskatatbildību un stiprina klientu uzticēšanos, par prioritāti izvirzot pārredzamību, datu minimizēšanu un stingru privātuma pārvaldību.

2. Piemērošanas joma

2.1. Šī politika attiecas uz:

2.1.1. visiem darbiniekiem, līgumslēdzējiem un pakalpojumu sniedzējiem, kuri piekļūst personas datiem, tos apstrādā vai pārvalda;

2.1.2. jebkuru sistēmu, lietotni vai vietu, kur personas dati tiek glabāti vai pārsūtīti;

2.1.3. visiem personas datiem neatkarīgi no tā, vai tie tiek glabāti elektroniski, papīra formā, mākoņvidē vai mobilajās ierīcēs.

2.2. Šī politika attiecas uz datiem, kas saistīti ar klientiem, personālu, piegādātājiem un citām identificējamām fiziskām personām.

2.3. Politika ir saistoša neatkarīgi no tā, vai dati tiek apstrādāti organizācijas iekšienē vai tos apstrādā trešo pušu pakalpojumu sniedzēji.

3. Mērķi

3.1. Nodrošināt, ka personas datu apstrāde notiek atbilstoši privātuma aizsardzības tiesību aktiem un drošības standartiem, tostarp VDAR, NIS2 un ISO 27001.

3.2. Aizsargāt personas datus pret nesankcionētu piekļuvi, nepareizu izmantošanu, izmainīšanu vai zaudēšanu, ieviešot skaidrus tehniskos un organizatoriskos kontroles pasākumus.

3.3. Ievērot fizisko personu tiesības uz privātumu, tostarp tiesības piekļūt saviem datiem, tos labot un dzēst.

3.4. Noteikt skaidras lomas un pienākumus datu aizsardzības jomā organizācijā.

3.5. Nodrošināt datu minimizēšanu, drošu glabāšanu un savlaicīgu dzēšanu visās sistēmās un procesos.

3.6. Samazināt neatbilstības, tiesisko sankciju, reputācijas kaitējuma un klientu uzticēšanās zuduma risku.

4. Lomas un pienākumi

4.1. Ģenerāldirektors (GM)

4.1.1. apstiprina šo politiku un nodrošina tās ieviešanu;

4.1.2. nodrošina nepieciešamos resursus privātuma risku pārvaldībai un reaģēšanai uz incidentiem;

4.1.3. uzņemas vispārējo pārskatatbildību par atbilstību privātuma aizsardzības tiesību aktiem un standartiem.

4.2. Privātuma koordinators (iekšējs vai ārpakalpojuma)

4.2.1. uztur personas datu apstrādes darbību reģistru;

4.2.2. atbild uz datu subjektu un regulatoru pieprasījumiem;

4.2.3. atbalsta risku novērtēšanu, apmācības un politikas ieviešanu;

4.2.4. dokumentē pārkāpumus un, ja nepieciešams, paziņo par tiem kompetentajām iestādēm.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Plānotā pārskatīšana

9.1.1. Šī politika jāpārskata vismaz reizi 12 mēnešos Privātuma koordinatoram, un tā jāapstiprina ģenerāldirektoram.

9.1.2. Pārskatīšanā jāizvērtē politikas atbilstība, atbilstība normatīvajām prasībām un darbības efektivitāte.

9.2. Starpposma pārskatīšanas ierosinātāji

9.2.1. Politikas atjaunināšana jāuzsāk arī, reaģējot uz:

9.2.1.1. jauniem vai grozītiem datu aizsardzības tiesību aktiem (piemēram, VDAR, DORA);

9.2.1.2. drošības incidentiem vai privātuma pārkāpumiem, kas saistīti ar personas datiem;

9.2.1.3. jaunu sistēmu, rīku vai pakalpojumu ieviešanu, kuros tiek apstrādāti personas dati;

9.2.1.4. būtiskiem audita konstatējumiem vai regulatora ieteikumiem.

9.3. Izmaiņu kontrole un komunikācija

9.3.1. Visas politikas izmaiņas formāli jādokumentē izmaiņu žurnālā.

9.3.2. Pārskatītās versijas jāizplata visam personālam un attiecīgajiem līgumslēdzējiem.

9.3.3. Arhivētās versijas jāsaglabā, lai nodrošinātu atbilstības audita pēctecību.

10. Saistītās politikas un sasaiste

10.1. Šī politika darbojas kopā ar citām SME politikām, veidojot pilnīgu un ieviešamu privātuma pārvaldības ietvaru:

10.1.1. P13S – Datu klasificēšanas un marķēšanas politika: nodrošina, ka personas dati tiek atbilstoši klasificēti, lai privātuma aizsardzības pasākumus varētu piemērot atbilstoši riskam.

10.1.2. P14S – Datu glabāšanas un likvidēšanas politika: nosaka skaidrus noteikumus par to, cik ilgi personas dati jāglabā un kādas drošas metodes jāizmanto to likvidēšanai pēc termiņa beigām.

10.1.3. P16S – Datu maskēšanas un pseidonimizācijas politika: nosaka, kā personas identifikatori jāpārveido pirms datu izmantošanas neprodukcijas vidē vai to nodošanas ārpus organizācijas.

10.1.4. P30S – Incidentu reaģēšanas politika: aptver darbības, kas jāveic, reaģējot uz datu aizsardzības pārkāpumiem, tostarp regulatoru un skarto fizisko personu informēšanu noteiktajos termiņos.

10.1.5. P2S – Pārvaldības lomu un atbildības politika: precizē pārskatatbildības struktūru un lēmumu pieņemšanas lomas, kas attiecas uz privātuma ieviešanu un pārraudzību.

10.2. Šīs saistītās politikas jāpārskata un jāpiemēro kopā, lai nodrošinātu pilnīgu privātuma pārklājumu visās sistēmās, personāla darbībās un piegādātāju attiecībās.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 5. punkts – nosaka, ka augstākajai vadībai jāapliecina līderība un apņemšanās personas datu aizsardzībā.

11.1.2. 6.1.3. punkts – nosaka ar personas informācijas apstrādi saistīto risku apstrādi.

11.1.3. 8.1. punkts – nosaka darbības kontroles pasākumu ieviešanu datu aizsardzībai visā to dzīves ciklā.

11.2. ISO/IEC 27002

11.2.1. 5.34. kontrole – sniedz ieviešanas vadlīnijas privātuma aizsardzībai un drošai PII apstrādei.

11.2.2. 8.10. kontrole – attiecas uz personas datu drošu likvidēšanu, lai novērstu atlikušās informācijas izpaušanu.

11.2.3. 8.11. kontrole – atbalsta maskēšanas un pseidonimizācijas izmantošanu datu minimizēšanai.

11.2.4. 8.12. kontrole – novērš nesankcionētu datu noplūdi, izmantojot kontroles pasākumus datu piekļuvei un izmantošanai.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – nosaka lomas un pienākumus privātuma riska pārvaldībai.

11.3.2. PL-5 – nosaka privātuma plāna dokumentēšanu, aptverot datu izmantošanu un aizsardzību.

11.3.3. AC-6 – nosaka minimāli nepieciešamās tiesības un piekļuves kontroles pasākumus personas datiem.

11.3.4. IR-4 – nosaka incidentu apstrādes procesus pārkāpumiem, kas saistīti ar personas datiem.

11.4. ES VDAR

11.4.1. 5. pants – nosaka likumīgas, godprātīgas un pārredzamas datu apstrādes pamatprincipus.

11.4.2. 6. pants – nosaka derīgu tiesisko pamatu katrai personas datu apstrādes darbībai.

11.4.3. 12.–23. pants – nosaka datu subjektu tiesības, tostarp piekļuvi, labošanu, dzēšanu un iebildumu izteikšanu.

11.4.4. 30. pants – nosaka apstrādes darbību reģistra uzturēšanu.

11.4.5. 32. pants – nosaka atbilstošus tehniskos un organizatoriskos drošības pasākumus.

11.4.6. 33.–34. pants – nosaka paziņošanas pienākumus iestādēm un datu subjektiem datu aizsardzības pārkāpuma gadījumā.

11.5. ES NIS2

11.5.1. 21. panta 2. punkta e) apakšpunkts – nosaka pasākumus datu aizsardzības nodrošināšanai atbilstoši kiberdrošības politikām.

11.5.2. 21. panta 2. punkta f) apakšpunkts – nosaka mehānismus personas datu un konfidenciālas informācijas drošības pārvaldībai IKT sistēmās.

11.6. ES DORA

11.6.1. 6. pants – nosaka iekšējās pārvaldības ietvarus datu riska un aizsardzības pārvaldībai.

11.6.2. 15. pants – nosaka pienākumu finanšu iestādēm nodrošināt, ka trešo pušu pakalpojumu sniedzēji aizsargā personas datus un atbalsta regulatīvo atbilstību.

11.6.3. 17. pants – nosaka, ka IKT sistēmām, kurās tiek apstrādāti personas dati, jābūt drošām, noturīgām un uzraudzītām.

11.7. COBIT 2019

11.7.1. APO12 – Risku pārvaldība: nosaka privātuma un datu aizsardzības risku identificēšanu un apstrādi.

11.7.2. DSS05 – Drošības pakalpojumu pārvaldība: nosaka drošības pasākumus, lai novērstu nesankcionētu piekļuvi personas datiem.

11.7.3. MEA03 – Atbilstības uzraudzība: nosaka organizācijām pienākumu nodrošināt nepārtrauktu atbilstību privātuma un datu aizsardzības tiesību aktiem.