					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P17					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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	5.1., 6.1.3., 8.1. un 10. punkts	Attiecīgie vispārīgie, tehniskie un nepārtrauktās pilnveides/datu aizsardzības kontroles pasākumi
ISO/IEC 27002:2022	5.34., 8.10., 8.11. un 8.12. kontroles pasākumi	Kontroles pasākumi PII apstrādei, glabāšanai, dzēšanai, anonimizācijai un datu subjektu tiesībām
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Pārvaldības, risku, piekļuves pārvaldības, žurnālfiksēšanas, reaģēšanas uz datu aizsardzības pārkāpumiem un privātuma programmas prasības
EU GDPR	5., 6., 12.–23., 25., 28., 30., 32.–34. pants; 78. apsvērums	Visas galvenās privātuma, pārskatatbildības, datu subjektu tiesību, DSR, pārkāpumu, datu aizsardzības pēc projektēšanas un pēc noklusējuma prasības
EU NIS2	21. panta 2. punkta e) un f) apakšpunkts	Uz risku balstīti drošības kontroles pasākumi būtiskajām un svarīgajām struktūrām
EU DORA	6. panta 2. punkta d) apakšpunkts, 11. panta 1. punkta c) apakšpunkts, 15. panta 1. punkts, 17. pants	Pārvaldības, trešo pušu riska un drošas apstrādes termiņu prasības
COBIT 2019	APO12, DSS01, DSS05, MEA	Risku pārvaldība, drošas operācijas, atbilstības uzraudzība

1. Mērķis

1.1 Šī politika nosaka obligātos organizatoriskos principus un tehniskās prasības personas datu aizsardzībai un datu aizsardzības pēc projektēšanas principu ieviešanai visās vidēs.

1.2 Tā formalizē organizācijas pienākumus saskaņā ar starptautiskajiem standartiem un normatīvajiem regulējumiem, nodrošinot, ka personas dati tiek vākti, apstrādāti, glabāti, kopīgoti un likvidēti likumīgi, droši un pārredzami.

1.3 Šī politika stiprina arī atbilstību piemērojamiem privātuma normatīvajiem aktiem un regulējumiem, tostarp ES Vispārīgajai datu aizsardzības regulai (GDPR), ES NIS2 direktīvai, ES Digitālās darbības noturības aktam (DORA), ISO/IEC 27001:2022 un COBIT 2019.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām organizācijas struktūrvienībām, personālu un sistēmām, kas ir iesaistītas personas datu apstrādē, tostarp:

2.1.1 darbiniekiem, līgumslēdzējiem, konsultantiem un trešo pušu pakalpojumu sniedzējiem.

2.1.2 datiem, kas iegūti no iekšējiem un ārējiem avotiem visās uzņēmējdarbības funkcijās.

2.1.3 fiziskajiem un digitālajiem nesējiem, tostarp mākoņpakalpojumiem, SaaS platformām, mobilajām ierīcēm un papīra formāta ierakstiem.

2.1.4 visām vidēm, tostarp produkcijas, izstrādes, testēšanas un rezerves kopiju sistēmām, kurās var atrasties personas dati.

2.2 Tā aptver visas apstrādes darbības, kuras regulē piemērojamie privātuma normatīvie akti un standarti, tostarp, bet ne tikai:

2.2.1 personas datu vākšanu, glabāšanu, izmantošanu, nosūtīšanu un likvidēšanu.

2.2.2 datu subjektu tiesību nodrošināšanu, tiesiskā pamata dokumentēšanu un piekrišanas pārvaldību.

2.2.3 datu pārsūtīšanu pāri robežām, paziņošanu par pārkāpumiem un personas datu kopīgošanu ar trešajām pusēm.

2.2.4 drošas projektēšanas un privātuma pēc noklusējuma principu piemērošanu sistēmās un procesos.

3. Mērķi

3.1 Nodrošināt likumīgu, pārredzamu un pārskatatbildīgu personas datu apstrādi atbilstoši ISO/IEC 27001:2022 un saistītajām tiesiskajām prasībām.

3.2 Iekļaut datu aizsardzības pēc projektēšanas un datu aizsardzības pēc noklusējuma principus visās informācijas sistēmās, pakalpojumos un uzņēmējdarbības procesos.

3.3 Piemērot tehniskos un organizatoriskos pasākumus (TOM), kas aizsargā personas datu konfidencialitāti, integritāti un pieejamību (CIA) visā to dzīves ciklā.

3.4 Noteikt pārvaldības lomas un pārskatatbildības struktūru datu aizsardzības jomā, tostarp datu aizsardzības speciālista, informācijas drošības funkcijas, juridiskās funkcijas un datu īpašnieku pienākumus.

3.5 Nodrošināt pilnīgu atbilstību GDPR 5., 6., 25., 30. un 32. pantam, kā arī NIS2 un DORA noteiktajām riska mazināšanas un noturības prasībām.

3.6 Nodrošināt datu subjektu tiesības, tostarp piekļuvi, labošanu, dzēšanu, apstrādes ierobežošanu, datu pārnesamību, tiesības iebilst un aizsardzību pret automatizētu lēmumu pieņemšanu.

3.7 Mazināt regulatīvos, reputācijas, tiesiskos un operacionālos riskus, kas izriet no neatļautas piekļuves, neatbilstošas izmantošanas vai personas datu zuduma.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Nodrošina stratēģisko pārraudzību un piešķir pietiekamus resursus privātuma programmas atbalstam.

4.1.2 Apstiprina šo politiku un nodrošina tās ieviešanu visā organizācijā.

4.2 Datu aizsardzības speciālists

4.2.1 Darbojas neatkarīgi, lai pārraudzītu atbilstību datu aizsardzības prasībām.

4.2.2 Uztur apstrādes darbību reģistru (RoPA) atbilstoši GDPR 30. pantam.

4.2.3 Vada sadarbību ar uzraudzības iestādēm, veic datu aizsardzības ietekmes novērtējumus (DPIA) un pārvalda paziņošanas procesus par pārkāpumiem.

4.2.4 Pārskata privātuma izņēmumus un uztur privātuma izņēmumu reģistru.

[... 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 iestājas kāds no šiem nosacījumiem:

9.1.1 būtiski tiesiski vai regulatīvi atjauninājumi (piemēram, GDPR grozījumi vai DORA termiņi);

9.1.2 jaunas sistēmas vai apstrādes darbības, kas ietver personas datus;

9.1.3 iekšējā audita konstatējumi, kas norāda uz politikas trūkumiem;

9.1.4 būtiski pārkāpumu incidenti vai uzraudzības iestādes sniegta atgriezeniskā saite.

9.2 Pārskatīšanas pienākumi

9.2.1 Datu aizsardzības speciālists uzsāk politikas pārskatīšanu, koordinējot to ar juridisko un atbilstības funkciju, risku funkciju, informācijas drošības un risku pārvaldības funkciju un izpildvadību.

9.2.2 Visi atjauninājumi jāreģistrē IDPS dokumentu kontroles reģistrā un jāizplata skartajām iesaistītajām pusēm.

9.3 Izmaiņu kontrole

9.3.1 Jebkuri šīs politikas grozījumi formāli jāapstiprina izpildvadībai.

9.3.2 Novecojušās versijas droši jāarhivē, un atjauninātajai versijai jāietver dokumentēta izmaiņu vēsture.

10. Saistītās politikas un sasaiste

10.1 P1 – Informācijas drošības politika. Nosaka visaptverošos drošības pārvaldības principus, kas ir šīs privātuma politikas pamatā. P1 atbalsta personas datu konfidencialitāti, integritāti un pieejamību visās sistēmās un pakalpojumos.

10.2 P6 – Risku pārvaldības politika. Nosaka organizācijas riska apstrādes metodoloģiju, kas ir būtiska privātuma risku izvērtēšanai, DPIA procesiem un atlikušā riska novērtējumiem, kuri nepieciešami saskaņā ar GDPR un ISO/IEC 27001 6.1.3. punktu.

10.3 P13 – Datu klasificēšanas un marķēšanas politika. Nosaka vadlīnijas personas datu un sensitīvu datu kategorizēšanai, kas ir pamats atbilstošu privātuma kontroles pasākumu piemērošanai, tostarp glabāšanas noteikumu ieviešanai, piekļuves ierobežošanai un drošai likvidēšanai.

10.4 P14 – Datu uzglabāšanas politika. Tieši atbalsta GDPR 5. panta 1. punkta e) apakšpunkta un 17. panta privātuma prasības, nodrošinot, ka personas dati tiek glabāti tikai tik ilgi, cik nepieciešams, un droši likvidēti atbilstoši tiesiskajām prasībām.

10.5 P16 – Datu maskēšanas un pseidonimizācijas politika. Nosaka kontroles pasākumus personas datu identificējamības samazināšanai, izmantojot tehniskos pasākumus, piemēram, tokenizāciju, dinamisko maskēšanu un pseidonimizāciju, tādējādi nodrošinot GDPR 32. panta un ISO/IEC 27002 5.34. kontroles prasību izpildi.

10.6 P30 – Incidentu reaģēšanas politika. Nosaka obligātos reaģēšanas protokolus datu aizsardzības pārkāpumiem, kas ir integrēti ar GDPR 33. un 34. pantā noteiktajiem apstrādes un paziņošanas termiņiem.

10.7 P33 – Audita un atbilstības uzraudzības politika. Nosaka regulāru izvērtēšanu privātuma programmas efektivitātei, politikas ieviešanai un korektīvo darbību uzraudzībai organizācijas struktūrvienībās un trešo pušu apstrādātāju vidē.

11. Atsauces standarti un regulējumi

11.1 ISO/IEC 27001

11.1.1 5.1. punkts – Vadība un apņemšanās: nosaka izpildvadības atbildību par personas datu aizsardzību un privātuma principu ieviešanu.

11.1.2 6.1.3. punkts – Informācijas drošības risku apstrāde: atbalsta privātuma risku identificēšanu, izvērtēšanu un apstrādi, izmantojot DPIA un izņēmumus.

11.1.3 8.1. punkts – Darbības plānošana un kontrole: pieprasa tehniskos un procesu kontroles pasākumus, lai nodrošinātu drošu personas datu apstrādi.

11.1.4 10.1. punkts – Nepārtraukta pilnveide: nosaka periodisku privātuma programmas izvērtēšanu un pielāgošanu.

11.2 ISO/IEC 27002:2022 5.34., 8.10., 8.11. un 8.12. kontroles pasākumi: sniedz vadlīnijas PII apstrādei, glabāšanai, dzēšanai, anonimizācijai un datu subjektu tiesību pārredzamības nodrošināšanai.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: nosaka pārvaldības, lomu, pārskatatbildības un privātuma apmācības pienākumus.

11.3.2 PL-2, PL-8: pieprasa privātuma kontroles pasākumu integrēšanu sistēmu dzīves ciklā un uzņēmuma arhitektūrā.

11.3.3 AC-2, AC-6: nosaka minimāli nepieciešamās tiesības un kontu pārvaldību personas datu aizsardzībai.

11.3.4 AU-2, AU-6, AU-9: nosaka žurnālfiksēšanas, izsekojamības un audita integritātes prasības attiecībā uz piekļuvi personas datiem.

11.3.5 IR-4, IR-5, IR-6: nosaka strukturētus atklāšanas, analīzes un ziņošanas procesus datu aizsardzības pārkāpumiem.

11.3.6 PM-1, PM-21, PM-23: nosaka visaptverošu privātuma programmu, kas ir saskaņota ar stratēģiskajiem riska un datu pārvaldības mērķiem.

11.4 EU GDPR (2016/679)

11.4.1 5., 6., 12.–23., 25., 28., 30., 32.–34. pants: regulē likumīgu apstrādi, nolūka ierobežojumu, datu subjektu tiesības, pārskatatbildību, datu aizsardzību pēc projektēšanas un pēc noklusējuma, trešo pušu pienākumus un pārkāpumu pārvaldību.

11.4.2 78. apsvērums: nostiprina datu aizsardzības pēc projektēšanas principus.

11.5 EU NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta e) un f) apakšpunkts: pieprasa uz risku balstītu drošības kontroles pasākumu ieviešanu un personas datu aizsardzību būtisko un svarīgo struktūru tvērumā.

11.6 EU DORA (2022/2554)

11.6.1 6. panta 2. punkta d) apakšpunkts: nosaka iekšējās pārvaldības prasības IKT riskam, kas saistīts ar datu apstrādi.

11.6.2 11. panta 1. punkta c) apakšpunkts: nosaka trešo pušu riska pārraudzību pakalpojumiem, kas saistīti ar datiem.

11.6.3 15. panta 1. punkts un 17. pants: pieprasa pakalpojumu sniedzējiem drošu datu apstrādi un savlaicīgu informācijas sniegšanu uzraudzības iestādēm pēc ar IKT saistītiem incidentiem.

11.7 COBIT 2019

11.7.1 APO12 – Risku pārvaldība: integrē privātuma risku plašākā uzņēmuma risku pārraudzībā.

11.7.2 DSS01 – Pārvaldītas operācijas un DSS05 – Drošības pakalpojumi: nodrošina drošas operācijas, tostarp piekļuves kontroli, glabāšanu un sistēmu integritāti.

11.7.3 MEA03 – Atbilstības uzraudzība: pieprasa nepārtrauktu atbilstības statusa pārskatīšanu attiecībā pret normatīvajām un politikās noteiktajām privātuma prasībām.