PATVIRTINTA
UAB ILTE valdybos
2026-10-15 sprendimu
(posėdžio protokolo Nr.77)

ASMENS DUOMENŲ TVARKYMO POLITIKA

Turinys:

1. Naudojamos sąvokos ir sutrumpinimai 2
2. Bendrosios nuostatos 3
3. Duomenų valdytojo įsipareigojimai tvarkant asmens duomenis 3
4. Atsakomybės kuriant ir plėtojant asmens duomenų apsaugos kultūrą.....5
5. Baigiamosios nuostatos 5

1. NAUDOJAMOS SĄVOKOS IR SUTRUMPINIMAI

1.1. Asmens duomenų tvarkymo politikoje vartojamos pagrindinės sąvokos ir sutrumpinimai:

ADTAĮ	Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas.
Asmens duomenų apsaugos kultūra	Požiūris, vertybės ir praktika, kuriomis siekiama užtikrinti atsakingą ir saugų asmens duomenų tvarkymą.
BDAR	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
Bendrovė arba ILTE	UAB ILTE.
Bendrovės grupės įmonės arba ILTE grupės įmonės	Bendrovės dukterinės bendrovės ir jų tiesiogiai valdomi juridiniai asmenys.
Bendrovės vadovas	Bendrovės generalinis direktorius ar jį pavaduojantis asmuo.
DAP komanda	Bendrovės duomenų apsaugos pareigūnas bei Rizikų valdymo ir atitikties tarnybos Atitikties departamento Atitikties valdymo ir prevencijos skyriaus atitikties teisininkas (-ai), atsakingas (-i) už BDAR sritį.
Darbuotojai	Visi Bendrovės kolegialių valdymo ir priežiūros organų, kitų kolegialių organų nariai, darbuotojai, taip pat asmenys, priimti atlikti praktiką.
DocLogix	Dokumentų ir procesų valdymo sistema „DocLogix“.
Duomenų valdytojas	Bendrovė ar jos valdoma įmonė, priklausomai nuo tikslų, kuriais ji tvarko asmens duomenis: UAB ILTE, juridinio asmens kodas 110084026, adresas korespondencijai Ukmergės g. 124, 08100 Vilnius, tel. (0 5) 210 7510, el. p. info@ilte.lt arba uzklausos@ilte.lt; UAB „Kofinansavimas“, juridinio asmens kodas 304295647, adresas korespondencijai Vilniaus g. 33, 01402 Vilnius, el. p. info@coinvest.lt; UAB „Valstybės investicijų valdymo agentūra“, juridinio asmens kodas 305612545, adresas korespondencijai Ukmergės g. 124, 08100 Vilnius, el. p. info@viva.lt; KŪB „Tvariųjų išteklių plėtros skatinimas“, juridinio asmens kodas 304874975, adresas korespondencijai Ukmergės g. 124, 08100 Vilnius, el. p. info@ilte.lt.
Politika	Ši Asmens duomenų tvarkymo politika.

1.2. Kitos Politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR ir kituose teisės aktuose, reglamentuojančiuose asmens duomenų tvarkymą ir apsaugą.

2. BENDROSIOS NUOSTATOS

2.1. Politika įtvirtina pagrindinius duomenų valdytojo įsipareigojimus tvarkant asmens duomenis, kuriant ir plėtojant asmens duomenų apsaugos kultūrą, kuri yra neatsiejama skaidrios, patikimos ir efektyvios Bendrovės, kaip nacionalinio plėtros banko, valdysenos dalis.
2.2. Politika grindžiama pagarba fizinių asmenų pagrindinėms teisėms ir laisvėms, siekiu užtikrinti teisėtą, sąžiningą ir skaidrų asmens duomenų tvarkymą bei stiprinti pasitikėjimą Bendrovės veikla, jos valdysena ir jai pavestų viešojo intereso funkcijų vykdymu.
2.3. Asmens duomenų apsauga yra viena iš Bendrovės atitikties valdymo sričių. Ši Politika yra specialusis vidaus dokumentas, parengtas vadovaujantis BDAR, ADTAĮ, kitais teisės aktais, reglamentuojančiais asmens duomenų saugumą ir tvarkymą.
2.4. Politikos nuostatos privalomos ir taikomos visiems darbuotojams. Bendrovės grupės įmonės vadovaujasi šia Politika, jei asmens duomenų tvarkymo ir apsaugos reikalavimų užtikrinimo procesai nėra reglamentuoti jų vidaus dokumentuose. Bendrovės grupės įmonių vidaus dokumentai, reglamentuojantys asmens duomenų tvarkymo ir apsaugos reikalavimų užtikrinimo procesus, gali papildomai detalizuoti šios Politikos nuostatas, tačiau turi joms neprieštarauti.
2.5. Politikos įgyvendinimo stebėseną, BDAR ir kitų teisės aktų, reglamentuojančių asmens duomenų apsaugą, reikalavimų laikymąsi Bendrovėje padeda užtikrinti Bendrovės DAP komanda. Jai suteikiami funkcijoms vykdyti reikalingi įgaliojimai, prieiga prie informacijos ir pakankami ištekliai, o jos veikla turi būti apsaugota nuo interesų konfliktų, netinkamos įtakos ir kitų aplinkybių, galinčių neigiamai paveikti nepriklausomą ir objektyvų funkcijų vykdymą.

3. DUOMENŲ VALDYTOJO ĮSIPAREIGOJIMAI TVARKANT ASMENS DUOMENIS

3.1. Duomenų valdytojas įsipareigoja:
3.1.1. kurti ir plėtoti asmens duomenų apsaugos kultūrą – kryptingai ir nuosekliai stiprinti darbuotojų sąmoningumą, žinias, atsakomybę ir kasdienius veiklos įpročius, susijusius su asmens duomenų saugiu ir teisėtu tvarkymu;
3.1.2. asmens duomenis tvarkyti vadovaujantis reikalavimais, nustatytais BDAR, ADTAĮ, kituose teisės aktuose ir vidaus dokumentuose, reglamentuojančiuose asmens duomenų tvarkymą ir apsaugą;
3.1.3. taikyti rizika grindžiamą požiūrį į asmens duomenų apsaugą – vadovaujantis Bendrovėje taikoma rizikos valdymo sistema ir vidaus kontrolės principais, nustatyti, vertinti ir valdyti su asmens duomenų tvarkymu susijusias rizikas fizinių asmenų teisėms ir laisvėms;
3.1.4. asmens duomenis tvarkyti vadovaujantis BDAR 5 straipsnyje įtvirtintais su asmens duomenų tvarkymu susijusiais principais:
3.1.4.1. **teisėtumo, sąžiningumo ir skaidrumo principu**. Asmens duomenys tvarkomi teisėtu, sąžiningu ir skaidriu būdu. Asmens duomenys gali būti tvarkomi tik jeigu yra bent viena iš BDAR įtvirtintų asmens duomenų teisėto tvarkymo sąlygų.
3.1.4.2. **tikslo apribojimo principu**. Asmens duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi, jei toks tvarkymo būdas su jais nėra suderinamas; tolesnis duomenų tvarkymas archyvavimo tikslais dėl viešojo intereso, mokslinių ar istorinių tyrimų arba statistiniais sumetimais nelaikomas nesuderinamu su pirminiais tikslais.
3.1.4.3. **duomenų kiekio mažinimo principu**. Asmens duomenys yra adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi. Tvarkomas mažiausias asmens duomenų kiekis, kuris būtinas ir pakankamas duomenų valdytojui nustatytiems asmens duomenų tvarkymo tikslams įgyvendinti. Jeigu tikslui pasiekti asmens duomenys nėra būtini, tokie duomenys negali būti tvarkomi.
3.1.4.4. **tikslumo principu**. Asmens duomenys yra tikslūs ir prireikus atnaujinami. Imamasi visų pagrįstų priemonių, kad būtų užtikrinta, jog asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi.
3.1.4.5. **saugojimo trukmės apribojimo principu**. Asmens duomenys yra laikomi tokios formos, kad asmens tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina siekiant tikslų, dėl kurių šie asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgiau, jeigu jie tvarkomi tik archyvavimo tikslais dėl viešojo intereso, mokslinių ar istorinių tyrimų arba statistiniais sumetimais, įgyvendinus tam tikras technines ir

organizacines priemones, reikalingas duomenų subjekto teisėms ir laisvėms apsaugoti. Turi būti nustatomas kiekvieno tvarkomų asmens duomenų rinkinio ar kategorijos saugojimo terminas arba jo nustatymo kriterijai.

3.1.4.6. **vientisumo ir konfidencialumo principu**. Asmens duomenys yra tvarkomi tokiu būdu, kad taikant tam tikras technines ir organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba nuo neteisėto duomenų tvarkymo ir netyčinio praradimo, sunaikinimo ar sugadinimo. Duomenų valdytojo naudojamoms technologijoms turi būti taikomi asmens duomenų apsaugai palankūs nustatymai. Tvarkydamas asmens duomenis, duomenų valdytojas laikosi pritaikytosios duomenų apsaugos ir standartizuotos duomenų apsaugos reikalavimų, atsižvelgdama**s** į technines galimybes, jų įgyvendin**im**o sąnaudas, asmens duomenų tvarkymo pobūdį, taip pat į asmens duomenų tvarkymo keliamą riziką.

3.1.4.7. **atskaitomybės principu**. Duomenų valdytojas užtikrina ir geba įrodyti, kad laikomasi BDAR įtvirtintų principų. Tvarkydamas asmens duomenis, duomenų valdytojas įgyvendina asmens duomenų apsaugos teisinius reikalavimus, stebi, kaip jų laikomasi, ir kaupia duomenis atitikčiai BDAR reikalavimams įrodyti.

3.1.5. taikyti technines ir organizacines priemones, kurios užtikrintų tokio lygio saugumą, kuris atitiktų tvarkomų duomenų pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms ir juos tvarkant kylančias rizikas. Techninės ir organizacinės priemonės periodiškai peržiūrimos ir prireikus atnaujinamos, atsižvelgiant į technologinę pažangą, nustatytas grėsmes, rizikos vertinimo rezultatus, asmens duomenų tvarkymo pokyčius ir nustatytus asmens duomenų saugumo pažeidimus;

3.1.6. užtikrinti tinkamą ir veiksmingą BDAR III skyriuje nustatytų duomenų subjektų teisių įgyvendinimą ir skaidrios informacijos apie asmens duomenų tvarkymą pateikimą duomenų subjektams;

3.1.7. užtikrinti asmens duomenų saugumo pažeidimų valdymą pagal nustatytą procedūrą, informuoti Valstybinę duomenų apsaugos inspekciją ir duomenų subjektus apie asmens duomenų saugumo pažeidimus, kai to reikalauja teisės aktai;

3.1.8. sudaryti, tvarkyti, periodiškai peržiūrėti ir prireikus atnaujinti asmens duomenų tvarkymo veiklos įrašus;

3.1.9. planuojant, kuriant naujus produktus, paslaugas, finansavimo priemones, informacines sistemas, technologinius sprendimus ar reikšmingus veiklos procesų pakeitimus, asmens duomenų apsaugos reikalavimai ir su asmens duomenų tvarkymu susijusios rizikos įvertinamos kuo ankstesnėje stadijoje;

3.1.10. atlikti poveikio asmens duomenų apsaugai vertinimą, kai tikėtina, kad dėl duomenų tvarkymo, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms ir laisvėms gali kilti didelis pavojus;

3.1.11. tais atvejais, kai asmens duomenys tvarkomi teisėto intereso pagrindu, prieš pradedant tokį tvarkymą, įvertinti tokio tvarkymo būtinybę teisėtam interesui pasiekti, duomenų valdytojo teisėtų interesų bei duomenų subjektų teisių ir laisvių pusiausvyrą;

3.1.12. automatinį sprendimų priėmimą, įskaitant profiliavimą, taikyti vadovaujantis BDAR 22 straipsnio sąlygomis;

3.1.13. planuojant, kuriant ar naudojant dirbtinio intelekto, mašininio mokymosi, pažangios duomenų analizės ar kitas naujas technologijas, užtikrinti, kad jų naudojimas atitiktų asmens duomenų apsaugos reikalavimus, o su tokiu naudojimu susijusios rizikos būtų įvertinamos ir valdomos teisės aktų bei vidaus dokumentų nustatyta tvarka;

3.1.14. asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkyti tik teisės aktų nustatytais atvejais ir sąlygomis, užtikrinant BDAR 10 straipsnyje nustatytus reikalavimus;

3.1.15. specialių kategorijų asmens duomenis tvarkyti tik tuomet, jeigu yra bent viena iš BDAR 9 straipsnio 2 dalyje įtvirtintų sąlygų ir tenkinama bent viena iš BDAR 6 straipsnio 1 dalyje numatytų sąlygų;

3.1.16. kai asmens duomenų tvarkymo tikslai ir priemonės nustatomi kartu su kitu subjektu, užtikrinti, kad su kitu bendru duomenų valdytoju būtų sudaromas susitarimas, kuriame aiškiai paskirstomos šalių atsakomybės, pareigos ir funkcijos, susijusios su asmens duomenų tvarkymu bei duomenų subjektų teisių užtikrinimu;

3.1.17. užtikrinti, kad duomenų tvarkytojai būtų parenkami, pasitelkiami ir prižiūrimi laikantis teisės aktų reikalavimų, o asmens duomenų tvarkymas jų vardu būtų grindžiamas BDAR 28 straipsnio reikalavimus atitinkančiais susitarimais;
3.1.18. asmens duomenis duomenų gavėjams teikti tik esant teisėtam pagrindui ir tik tokia apimtimi, kuri būtina nustatytam tikslui pasiekti arba teisės aktuose nustatytai pareigai įvykdyti;
3.1.19. asmens duomenis į trečiąsias valstybes ar tarptautinėms organizacijoms perduoti tik BDAR V skyriuje nustatytais atvejais ir laikantis jame nustatytų reikalavimų bei taikant tinkamas duomenų subjektų teisių ir laisvių apsaugos priemones;
3.1.20. užtikrinti, kad pasibaigus nustatytam asmens duomenų saugojimo terminui asmens duomenys būtų ištrinami, sunaikinami arba, kai taikoma ir teisės aktai leidžia, nuasmeninami, išskyrus atvejus, kai teisės aktai nustato kitokį jų saugojimą;
3.1.21. prieigą prie asmens duomenų suteikti tik tiems darbuotojams ir kitiems asmenims, kuriems ji būtina jų funkcijoms atlikti, atsižvelgiant į jų vykdomas funkcijas, suteiktas teises ir būtinybę žinoti, ir užtikrinti, kad asmenys, turintys teisę tvarkyti asmens duomenis, būtų įpareigoti laikytis konfidencialumo;
3.1.22. periodiškai vertinti asmens duomenų apsaugos sistemos veiksmingumą bei atsižvelgiant į teisės aktų reikalavimus, veiklos, technologinių sprendimų ar rizikų pokyčius, nuolat tobulinti asmens duomenų apsaugos priemones ir procesus;
3.1.23. užtikrinti, kad visi darbuotojai būtų supažindinti su jiems taikomais asmens duomenų apsaugos reikalavimais, reguliariai stiprintų žinias asmens duomenų apsaugos srityje ir pagal savo kompetenciją būtų atsakingi už šių reikalavimų laikymąsi.

4. ATSAKOMYBĖS KURIANT IR PLĖTOJANT ASMENS DUOMENŲ APSAUGOS KULTŪRĄ

4.1. Asmens duomenų apsaugos kultūros veiksmingumas priklauso nuo visų darbuotojų sąmoningumo, žinių, atsakomybės ir kasdienių veiklos įpročių. Prie jos kūrimo ir plėtojimo prisideda šie subjektai:
4.1.1. Bendrovės valdyba – tvirtina Politiką; prižiūri jos įgyvendinimą Bendrovėje; vertina informacijos apie asmens duomenų apsaugos sistemos veikimą pakankamumą.
4.1.2. Bendrovės vadovas ar jo įgaliotas asmuo – pagal kompetenciją tvirtina Politikos nuostatas įgyvendinančius vidaus dokumentus; skiria duomenų apsaugos pareigūną; užtikrina tinkamų techninių ir organizacinių priemonių įgyvendinimą bei pakankamų žmogiškųjų, organizacinių ir finansinių išteklių skyrimą Politikai įgyvendinti; užtikrina, kad asmens duomenų apsaugos kultūros kūrimo ir plėtojimo priemonių sistema būtų įgyvendinama, prižiūrima ir analizuojama, siekiant užtikrinti atsakingą ir saugų asmens duomenų tvarkymą Bendrovėje.
4.1.3. DAP komanda – koordinuoja, inicijuoja ir įgyvendina asmens duomenų apsaugos kultūros kūrimo ir stiprinimo priemones Bendrovėje; teikia metodinę pagalbą ir konsultuoja darbuotojus asmens duomenų apsaugos klausimais; prižiūri, kaip Bendrovėje įgyvendinamos asmens duomenų apsaugos kultūros kūrimo priemonės ir vertina jų veiksmingumą.
4.1.4. Bendrovės struktūrinių padalinių vadovai – vadovaujamame padalinyje užtikrina Politikos, teisės aktų ir kitų vidaus dokumentų, nustatančių asmens duomenų tvarkymą ir saugumą, reikalavimų ir procedūrų įgyvendinimą ir laikymąsi; organizuoja ir užtikrina teisės aktų ir kitų vidaus dokumentų, nustatančių asmens duomenų tvarkymą jų priskirtose veiklos srityse, parengimą, atnaujinimą ir laikymosi kontrolę; užtikrina, kad svarstant klausimus, susijusius su asmens duomenų tvarkymu ir apsauga, būtų laiku kreipiamasi konsultacijos į DAP komandą; savo elgesiu ir sprendimais formuoja tinkamą asmens duomenų apsaugos kultūrą padalinyje.
4.1.5. darbuotojai – dalyvauja asmens duomenų apsaugos kultūros kūrimo ir plėtojimo procese ir yra asmeniškai atsakingi už tinkamą asmens duomenų tvarkymą ir apsaugą pagal kompetenciją, nustatytų techninių ir organizacinių priemonių laikymąsi, reikalavimų žinojimą, dalyvavimą sąmoningumo, susijusio su asmens duomenų saugiu ir teisėtu tvarkymu, didinimo veikloje.

5. BAIGIAMOSIOS NUOSTATOS

5.1. Politiką ir jos pakeitimus tvirtina Bendrovės valdyba.

5.2. Politikos peržiūrą, atnaujinimą inicijuoja ir koordinuoja Atitikties departamento Atitikties valdymo ir prevencijos skyrius.
5.3. Politikos nuostatos peržiūrimos ir pagal poreikį keičiamos ne rečiau kaip kas du metus arba įvykus reikšmingiems pokyčiams.
5.4. Pasikeitus teisės aktams, Politika taikoma tiek, kiek neprieštarauja aktualiems teisės aktams.
5.5. Darbuotojai su Politika supažindinami DocLogix priemonėmis, o Bendrovės grupės įmonių darbuotojai – laikantis šiose įmonėse nustatytos darbuotojų supažindinimo su darbuotojams reikalinga informacija tvarkos. Susipažinimas su Politika yra prilyginamas kiekvieno darbuotojo įsipareigojimui laikytis Politikoje nustatytų reikalavimų.