Asmens duomenų apsaugos politika

C6.PLC.01

1.0 versija

Įsigaliojimo data: 2018-05-25

Teisiniai pranešimai

Santrauka

PAVADINIMAS	Asmens duomenų apsaugos politika
ID	C6.PLC.01
PROCESO PRIŽIŪRĖTOJAS	A.A. Iljin, Finansų direktorius, EuroChem Group
PROCESO ŠEIMININKAS	V.V. Sidnev, Generalinis patarėjas, EuroChem Group
AUTORIUS	E.V. Cholmanskich, Atitikties pareigūnė, EuroChem Group
VERSIJA	1.0
ĮSIGALIOJIMO DATA	2018-05-25
PATVIRTINIMO DATA	2018-05-24

Atnaujinimo istorija

Versija	Įsigaliojimo data	Paskirtis	Atnaujinimo informacija
1.0	2018-05-25		Netaikoma

Turinys

1. Sąvokos ir apibrėžimai

Išskyrus atvejus, kai nurodyta priešingai, šioje Asmens duomenų apsaugos politikoje („Politika“) vartojami žodžiai ir sąvokos turi tokią pačią reikšmę (arba atitinka tokią pačią koncepciją) kaip Elgesio kodekse ir Atitikties politikoje apibrėžti (arba išreikšti tam tikra koncepcija) žodžiai ir sąvokos.

Papildomai taikytinos šios apibrėžtys:

Sąvoka	Apibrėžtis
„Asmens duomenys“	bet kokia informacija apie duomenų subjektą; platus asmens identifikatorių spektras, įskaitant fizinio asmens vardą ir pavardę, (darbo) telefono numerį, (darbo) e. pašto adresą, identifikavimo numerį, buvimo vietos duomenis, interneto identifikatorių ir pan.
„Jautraus pobūdžio duomenys“	asmens duomenys, kuriais atskleidžiama rasinė ar etninė kilmė, politinės pažiūros, religiniai ar filosofiniai įsitikinimai arba narystė profesinėse sąjungose, taip pat tvarkomi genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.
„Duomenų valdytojas“ arba „Valdytojas“	fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones.
„Duomenų tvarkytojas“ arba „Tvarkytojas“	fizinis arba juridinis asmuo, kuris duomenų valdytojo vardu tvarko asmens duomenis.
„Duomenų subjektas“	bet kuris gyvas individas, kuris yra Grupės saugomų asmens duomenų subjektas.
„Duomenų tvarkymas“	bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.
„Asmens duomenų saugumo pažeidimas“	saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.
„Duomenų subjektas sutikimas“	bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais, kuriais jis sutinka, kad būtų tvarkomi asmens duomenys.
„ES duomenų apsaugos pareigūnas“	Grupės darbuotojas, atsakingas už Politikos įgyvendinimą ES valstybėse narėse, kuriose veikia Grupės įmonės.
„Visuotinių duomenų apsaugos pareigūnas“	Grupės darbuotojas, atsakingas už Politikos įgyvendinimą Grupėje.
„Vietinis duomenų apsaugos pareigūnas“	atsakingas Grupės darbuotojas

„Duomenų tvarkytojo sutartis“	sutartis, kurią sudaro Grupė ir bet kuri šalis, atsakinga už Politikos įgyvendinimą Grupėje.
„Saugojimo planas“	specialus planas, pagal kurį nustatomas konkretus dokumentų saugojimo laikotarpis.

2. Taikymas

2.1. Paskirtis

Šioje Politikoje apibrėžiami esminiai Grupėje taikomi asmens duomenų apsaugos ir asmens duomenų tvarkymo principai.

Kaip darbdavys, klientas ir tiekėjas, kiekviena Grupės įmonė renka ir naudoja asmens duomenis, susijusius su darbuotojais, verslo partneriais, klientais, galimais klientais ir pan. Nors šių asmens duomenų tvarkymas yra būtinas mūsų veiklai, Grupė supranta, kad kiekvieno asmens teisių ir privatumo apsauga yra bet kokių santykių pasitikėjimo pagrindas. Todėl Grupė pageidauja patobulinti asmens duomenų apsaugą ir tvarkymą.

Grupei labai svarbi atitiktis asmens duomenų apsaugos reikalavimams valstybėse, kurioje ji vysto savo verslą ir kuriose gyvena duomenų subjektai. Visos Grupės įmonės visame pasaulyje privalo atitikti vietos įstatymus, reglamentuojančius asmens duomenų valdymą ir tvarkymą.

Aukščiausias Grupės prioritetas yra užtikrinti visuotinai galiojančius, visame pasaulyje taikomus asmens duomenų tvarkymo standartus. Ši Duomenų apsaugos politika yra bendra sistema, kuri taikoma visoms Grupės įmonėms. Jei skiriasi vietos įstatymai ar veiklos pobūdis, šių Duomenų apsaugos principų įgyvendinimas negali reikšmingai skirtis Grupės narių atžvilgiu.

Ši Politika turi būti pristatyta visiems darbuotojams, kurie turi laikytis Politikos ir vykdyti joje nustatytus reikalavimus. Be to, Politika taip pat taikoma sutarties šalims, kurios bendradarbiauja su bet kuria Grupės įmone ir turi ar gali turėti prieigą prie asmens duomenų. Tokios sutarties šalys privalo perskaityti, suprasti Politiką ir laikytis jos sąlygų.

2.2. Taikymo sritis ir privalomi teisiniai reikalavimai

Valstybės, kuriose Grupė vysto savo verslą, gali būti suskirstyta į tris stambias grupes, priklausomai nuo vietovės: ES, Rusija ir kitos valstybės.

Išskyrus buveines Šveicarijoje ir Rusijoje, kai kurios Grupės įmonės įsikūrusios ES. ES duomenų apsaugos taisyklės (Reglamentas (ES) 2016/679 (Bendrasis duomenų apsaugos reglamentas arba BDAR) yra griežtos ir taikomos suderintai visoje ES. BDAR taikymo sritis yra platesnė nei ES, nes ji taip pat taikoma Grupės įmonėms, įsteigtoms už ES ribų, jei duomenų subjektas yra ES gyventojas.

Grupė nusprendė naudoti BDAR principus ir prievoles kaip Duomenų apsaugos politikos planą. Tačiau paskiros Grupės įmonės taip pat privalo laikytis vietos įstatymų. Duomenų apsaugos politika tik papildo Duomenų apsaugos taisykles. Atitinkami vietos įstatymai turi pirmenybę tuo atveju, jei jie prieštarauja šiai Duomenų apsaugos politikai arba juose yra griežtesnių reikalavimų nei šioje Duomenų apsaugos politikoje. Vietos įstatymų, taikytinų kai kurioms Grupės įmonėms, pavyzdžiai:

- 2006 m. Federalinis asmens duomenų įstatymas Nr. 152-FZ (galioja Rusijoje);
- 1992 m. birželio 19 d. Federalinis duomenų apsaugos įstatymas (FADP) (galioja Šveicarijoje);
- vietos teisės aktai dėl bendrovių valdysenos ir duomenų saugojimo laikotarpių.

3. Bendrosios nuostatos

3.1. Politikos tikslai

Pagrindiniai Politikos tikslai:

- apsaugoti duomenų subjektų teises ir laisves ir informuoti juos apie jas;
- tinkamai tvarkyti asmens duomenis;
- vengti bet kokių asmens duomenų saugumo pažeidimų ir bendrųjų saugos problemų;
- didinti bendrąjį supratimą apie asmens duomenų apsaugos režimą.

3.2. Politikos principai

Bet koks asmens duomenų tvarkymas turi būti vykdomas pagal duomenų apsaugos principus, nustatytus BADR. Grupės politikos ir procedūros skirtos atitikčiai šiems principams užtikrinti.

Konkrečiai, mes, kaip Grupė, įsipareigojame atitikti šiuos principus:

- sąžiningumo ir teisėtumo principą: įsipareigojame tvarkyti asmens duomenis tik tuo atveju, jei informavome apie tai duomenų subjektą ir tik jei yra teisinis pagrindas tvarkyti duomenis;

- tikslo apribojimo principą: tvarkysime asmens duomenis tik nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkysime duomenų su tais tikslais nesuderinamu būdu;

- duomenų kiekio mažinimo principą: tvarkysime asmens duomenis, kurie yra adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi;

- tikslumo principą: tvarkysime tik duomenis, kurie yra tikslūs ir prireikus atnaujinami. Imsimės visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, būtų nedelsiant ištrinami arba ištaisomi;

- saugojimo trukmės apribojimo principą: visus asmens duomenis laikysime tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi;

- konfidencialumo principą: duomenis tvarkysime tik tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo;

- atskaitomybės principą: būsime atsakingi už tai, kad bet kuriuo atveju sugebėtume įrodyti kompetentingoms institucijoms ar duomenų subjektams, kad laikomės aukščiau išvardytų duomenų apsaugos principų.

4. Duomenų apsaugos priemonės

Grupės įsipareigojimas įgyvendinti aukščiau išvardytus duomenų apsaugos principus įrodomas šiomis priemonėmis:

4.1. Teisėtas ir sąžiningas tvarkymas

Grupė užtikrina, kad duomenys renkami ir tvarkomi sąžiningai ir teisėtai. Imamės visų protingų veiksmų, siekdami užtikrinti, kad asmens duomenys būtų atnaujinti, tikslūs ir saugomi tik nustatytu laikotarpiu.

Grupė užtikrina, kad, priklausomai nuo kategorijos, kuriai priklauso duomenų subjektas, surinkti duomenys bus naudojami tik čia apibrėžtu sąžiningu ir teisėtu pagrindu.

4.1.1. Darbuotojų duomenys

Darbuotojų duomenys – visi bet kurios Grupės įmonės tvarkomi duomenys, susiję su darbuotojais ir (jei būtina) jų sutuoktiniais. Tačiau darbuotojų duomenų sąvoka yra platesnė nei tiesiog esamų darbuotojų asmens duomenys. Taip pat taikomos kitos duomenų kategorijos, susijusios su darbo santykiais, pavyzdžiui, į pensiją išėjusių darbuotojų ir kandidatų į laisvas darbo vietas duomenys.

Visus darbuotojų duomenis renka Grupės įmonė, kurioje dirba atitinkamas darbuotojas. Darbdavys laikomas duomenų valdytoju (tai reiškia, kad Grupė nustato duomenų tvarkymo tikslus ir priemones).

1. Tvarkymo veiksmų teisinis pagrindas

Darbo santykiuose didžioji duomenų tvarkymo veiklos dalis yra įteisinta dėl būtinybės vykdyti darbo sutartį: Grupės įmonės negalėtų tinkamai įvykdyti savo įsipareigojimų pagal darbo sutartis, jei negalėtų tvarkyti savo darbuotojų duomenų.

Kai kurie duomenų tvarkymo veiksmai įteisinami pagal teisinį įpareigojimą: visose šalyse, kuriose Grupės įmonės vykdo verslą, jos yra teisiškai įpareigotos tvarkyti tam tikrus darbuotojų asmens duomenis, pvz., socialinio draudimo, draudimo, atlyginimų mokėjimo ir kt. tikslais.

Kai kurie duomenų tvarkymo veiksmai taip pat gali būti leidžiami pagal kolektyvines sutartis. Kolektyvinės sutartys yra susitarimai dėl darbo užmokesčio ribų arba darbdavių ir darbuotojų atstovų susitarimai pagal atitinkamą darbo teisę. Jose turi būti numatyti konkretus duomenų tvarkymo tikslas ir jos turi būti parengtos pagal nacionalinių duomenų apsaugos teisės aktų parametrus.

Kiekviena Grupės įmonė beveik visais atvejais taip pat remiasi teisėtais interesais tvarkyti asmens duomenis, nes jie būtini siekiant tinkamai vykdyti jos verslą (pvz., nors Grupės įmonė nepasirašo darbo sutarties su kandidatais, Grupė turi teisėtą interesą įvertinti galimus kandidatus, ypač kai jie teikia darbo prašymus, susisiekdami su Grupės įmone).

Labai ribotais atvejais tvarkymo veiksmai turi būti įteisinti aiškiu darbuotoju sutikimu (pvz., interviu ar nuotraukos paviešinimo vidaus laikraštyje ar pan. atveju).

Kiekviena Grupės įmonė yra atsakinga už tvarkymo veiksmų teisinio pagrindo nustatymą.

2. Sąžiningas tvarkymas

Išsamus darbuotojų duomenų tvarkymo aprašas pateiktas išsamesnėse politikose. Šiame dokumente pateiktas tik glaustas tam tikrų tvarkymo veiksmų aspektų aprašas:

- kiekio mažinimas: Grupė užtikrina, kad tvarkomi darbuotojų duomenys apribojami iki mažiausio būtino kiekio;
- tikslumas: Grupė užtikrina, kad visi darbuotojų duomenys nuolat atnaujinami juridinio asmens lygmeniu ir kad kiekvienas darbuotojas bet kuriuo metu gali pareikalauti pataisyti netinkamus duomenis;

- saugojimo trukmės apribojimas: visi darbuotojų duomenys bus tvarkomi darbo sutarties galiojimo laikotarpiu. Pasibaigus darbo sutarčiai, didžioji dalis duomenų bus ištrinta laikantis duomenų saugojimo laikotarpio reikalavimo, nebent įstatymas numatytų kitaip, arba duomenų subjektas aiškiai sutiko saugoti jo duomenis byloje tolesnių konkrečių tvarkymo veiksmų tikslais;
- saugumas: visi asmens duomenys tvarkomi saugiai. Pvz., prieiga prie duomenų yra ribojama pagal poreikį žinoti, Grupės duomenys dažnai koduojami, kai jie perduodami trečiajai šaliai ir pan.;
- jautraus pobūdžio duomenų tvarkymas: jautraus pobūdžio duomenys, kuriais atskleidžiama rasinė ar etninė kilmė, politinės pažiūros, religiniai ar filosofiniai įsitikinimai arba narystė profesinėse sąjungose, taip pat sveikatos duomenys arba duomenys apie duomenų subjekto lytinį gyvenimą, tvarkomi taikant papildomas apsaugos priemones.
- Grupė kiek įmanoma mažina automatinį asmens duomenų tvarkymą. Jei asmens duomenys automatiškai tvarkomi vykdant darbo santykius ir vertinami konkretūs asmens duomenys (pvz., atliekant personalo atranką arba vertinant įgūdžių profilį), toks automatinis tvarkymas negali būti vienintelis pagrindas priimant sprendimus, kurie gali turėti neigiamų pasekmių arba sukelti reikšmingų problemų paveiktam darbuotojui.

Kiekviena Grupės įmonė yra atsakinga už sąžiningą darbuotojų duomenų tvarkymą.

4.1.2. Sutarties šalių duomenys

Sutarties šalių duomenys – klientų, subrangovų, tiekėjų, verslo partnerių, tinklalapio lankytojų ir pan. asmens duomenys. Nors tokie duomenys visada apsiribos profesiniais santykiais, t. y., beveik niekada nebus tvarkomi jautraus pobūdžio duomenys, visi e. pašto adresai ar telefono numeriai bus laikomi asmens duomenimis.

Jei Grupė gauna sutarties šalių duomenis tiesiogiai iš duomenų subjekto, ji bus laikoma tokių duomenų valdytoja. Priklausomai nuo Grupės verslo pobūdžio, sutarties šalių duomenys gali būti gaunami iš kitos šalies. Tokiu atveju Grupė bus laikoma tik duomenų tvarkytoja, o ne duomenų valdytoja, jei nesusitariama priešingai.

1. Tvarkymo veiksmų teisinis pagrindas

Sutartiniuose santykiuose didžioji duomenų tvarkymo veiklos dalis yra įteisinta dėl būtinybės vykdyti darbo sutartį: Grupė negalėtų tinkamai įvykdyti savo įsipareigojimų pagal sutartis, jei negalėtų tvarkyti atitinkamų duomenų.

Kai kurie duomenų tvarkymo veiksmai įteisinami pagal teisinį įpareigojimą: kai kuriose šalyse, kuriose Grupė vykdo verslą, ji yra teisiškai įpareigota tvarkyti tam tikrus tiekėjų asmens duomenis.

Beveik visais atvejais Grupė gali remtis teisėtu interesu tvarkyti asmens duomenis, kadangi jie būtini tinkamai verslo veiklai užtikrinti.

Labai ribotais atvejais tvarkymo veiksmai turi būti įteisinti aiškiu trečiosios šalies sutikimu (pvz., gauti Grupės naujienlaiškį ar pan.).

Jeigu sutarties šalių duomenis valdo Grupė (tai reiškia, kad Grupės įmonė nustato duomenų tvarkymo tikslus ir būdus), Grupė bus atsakinga už teisėtą duomenų tvarkymo pagrindą.

2. Sąžiningas tvarkymas

Išsamus sutarties šalių duomenų tvarkymo aprašas pateiktas išsamesnėse politikose. Bendrai kalbant, taikomi tie patys principai, kurie taikomi tvarkant darbuotojų duomenis, kaip aprašyta 4.1.1 p.

Pažymėtini šie papildomi principai:

- Jei tvarkomi sutarties šalių duomenys renkami Grupės tinklalapyje ir kitomis interneto priemonėmis: jei asmens duomenys renkami, tvarkomi ir naudojami tinklalapiuose, duomenų subjektai apie tai informuojami privatumo pareiškime ir, jei taikoma, slapukų naudojimo pranešimuose. Privatumo pareiškimas ir slapukų naudojimo pranešimas bus integruoti taip, kad duomenų subjektai galėtų juos lengvai identifikuoti, tiesiogiai pasiekti ir jie būtų nuolat matomi.

  Jei savo tinklalapiuose kuriame naudotojų profilius (sekimą), duomenų subjektai bus atitinkamai informuojami apie tai privatumo pareiškime. Asmens sekimas gali būti atliekamas tik tada, kai tai leidžiama pagal nacionalinę teisę arba duomenų subjekto sutikimu.

  Jei tinklalapiai ar programėlės gali naudoti asmens duomenis tik registruotų naudotojų zonoje, prieigos metu duomenų subjekto identifikavimas ir autentifikavimas bus pakankamai apsaugotas.

- Skaitmeninė rinkodara: Grupė dažniausiai įgyvendina skaitmeninės rinkodaros strategijas „verslas verslui“ kontekste, kai nėra teisinio reikalavimo gauti sutikimą dėl skaitmeninės rinkodaros privatiems asmenims, jei jiems suteikiama galimybė atsisakyti.

  Tačiau bendrai Grupė visada sieks gauti sutikimą prieš išsiųsdama reklaminę ar tiesioginės rinkodaros medžiagą sutarties šalies duomenų subjektui.

Jei Grupė yra sutarties šalių duomenų valdytoja, grupė bus atsakinga už duomenų tvarkymo teisinio pagrindo nustatymą.

4.1.3. Sutikimas

Jei Grupė remiasi sutikimu kaip teisiniu pagrindu tvarkyti duomenis, taikomos šios sąlygos:

Sutikimo pareiškimai pateikiami savanoriškai, raštu ir laikantis vietos įstatymų. Bet koks šios sąlygos neatitinkantis sutikimas laikomas negaliojančiu. Sutikimo pareiškimas gaunamas raštu ar elektroninėmis priemonėmis dokumentavimo tikslais. Prieš pateikdamas sutikimą, duomenų subjektas informuojamas apie duomenų tvarkymo mastą. Duomenų subjektas turi teisę bet kuriuo metu atšaukti savo sutikimą.

Jautraus pobūdžio duomenų atveju turi būti gautas aiškus duomenų subjektų rašytinis sutikimas, nebent egzistuoja aiškus alternatyvus teisėtas duomenų tvarkymo pagrindas.

Dažniausiai Grupė bendra tvarka gauna sutikimą tvarkyti asmens duomenis ir jautraus pobūdžio duomenis, naudodama standartinius sutikimo dokumentus.

4.2. Duomenų subjektų teisių apsauga

Kiekviena Grupės įmonė užtikrina, kad duomenų subjektas, kurio asmens duomenis tvarko Grupė, gali naudotis šiomis asmeninėmis teisėmis.

- **Teisė būti informuotam:**

  Politikoje išsamiai aprašyti bendrieji principai, pagal kuriuos Grupė tvarko asmens duomenis. Jie pateikiami duomenų subjektams tuo metu, kai renkami jų asmens duomenys (jei Grupė yra duomenų valdytojas) ir yra viešai prieinami tinklalapyje www.eurochemgroup.ru.

  Tačiau jei duomenų subjektas aiškiai reikalauja, atitinkama Grupės įmonė (t. y. asmens duomenų valdytojas arba tvarkytojas) duomenų subjektui pateikia informaciją apie jo asmens duomenis, kuri bus glausta, skaidri, suprantama ir lengvai prieinama. Grupė pasilieka teisę atmesti prašymą suteikti

informaciją, jei duomenų subjektas jau turi šią informaciją, arba jos pateikimui reikėtų neproporcingų pastangų.

Gavusi prašymą, Grupė privalo pateikti šią informaciją: 1) subjekto pavadinimą ir kontaktinius duomenis, 2) duomenų tvarkymo tikslus, 3) duomenų tvarkymo teisinį pagrindą; 4) atitinkamų asmens duomenų kategorijas; 5) asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas, 6) kai taikoma, apie duomenų valdytojo ketinimą asmens duomenis perduoti gavėjui trečiojoje valstybėje arba tarptautinei organizacijai, 7) asmens duomenų saugojimo laikotarpį, 8) duomenų subjektų teises dėl duomenų tvarkymo, 9) jei taikoma, teisę atšaukti sutikimą, 10) teisę pateikti skundą priežiūros institucijai.

- **Teisė susipažinti su duomenimis:**

  Siekdama užtikrinti, kad duomenų subjektai žinotų ir galėtų patikrinti tvarkymo veiklos teisėtumą, Grupė suteikia jiems teisę gauti patvirtinimą, kad duomenų subjekto duomenys yra tvarkomi; prieigą prie asmens duomenų; ir kitą reikalingą papildomą informaciją. Prieigos formatas turi būti suderintas tarpusavyje.

- **Teisė reikalauti ištaisyti duomenis:**

  Jei Grupės įmonė tvarko netikslius ar neišsamius asmens duomenis, duomenų subjektas gali duomenų subjektas turi teisę reikalauti, kad būtų ištaisyti ar papildyti neišsamūs asmens duomenys. Tačiau Grupė pasilieka sau teisę atmesti prašymą ištaisyti duomenis, jei tai leidžiama pagal galiojančius įstatymus.

- **Teisė reikalauti ištrinti duomenis ir teisė apriboti duomenų tvarkymą:**

  Duomenų subjektas turi teisę reikalauti, kad Grupė ištrintų su juo susijusius asmens duomenis, jei 1) asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi; 2) asmens duomenų subjektas atšaukia sutikimą, kuriuo Grupės įmonė grindžia duomenų tvarkymą, ir nėra jokio kito teisinio pagrindo tvarkyti duomenis; 3) asmens duomenų subjektas nesutinka su duomenų tvarkymu ir Grupės įmonė grindžia duomenų tvarkymą tik teisėtais interesais, ir nėra viršesnių teisėtų priežasčių tvarkyti duomenis; 4) Grupės įmonė tvarko asmens duomenis tiesioginės rinkodaros tikslais; 5) asmens duomenys Grupės įmonės tvarkomi neteisėtai.

  Vietoje reikalavimo ištrinti asmens duomenis, duomenų subjektas gali reikalauti, kad atitinkama Grupės įmonė apribotų asmens duomenų tvarkymą ir tik saugotų juos, kitaip nenaudodama. Toks apribojimas galimas, kai taikomas vienas iš šių atvejų: 1) asmens duomenų subjektas užginčija duomenų tikslumą tokiam laikotarpiui, per kurį Grupės įmonė gali patikrinti asmens duomenų tikslumą; 2) asmens duomenų tvarkymas yra neteisėtas ir duomenų subjektas nesutinka, kad duomenys būtų ištrinti, ir vietoj to prašo apriboti jų naudojimą; 3) Grupės įmonei nebereikia asmens duomenų tvarkymo tikslais, tačiau jų reikia duomenų subjektui siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus; 4) duomenų subjektas paprieštaravo Grupės įmonės vykdomam duomenų tvarkymui, kol bus patikrinta, ar teisėtos priežastys yra viršesnės už duomenų subjekto priežastis.

- **Teisė į duomenų perkeliamumą:**

  Laikantis griežtų sąlygų, duomenų subjektas gali pareikalauti Grupės įmonės pateikti su juo susijusius asmens duomenis susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu. Duomenų subjektas taip pat turi teisę persiųsti tuos duomenis kitai organizacijai. Duomenų subjektas turi teisę reikalauti, kad asmens duomenys būtų tiesiogiai persiųsti kitai organizacijai, kai tai techniškai įmanoma.

  Teisė į duomenų perkeliamumą taikoma tik: 1) asmens duomenims, kuriuos asmuo pateikė duomenų valdytojui; 2) kai duomenų tvarkymas yra grindžiamas duomenų subjekto sutikimu ar sutartiniais santykiais; ir 3) jei duomenys yra tvarkomi automatizuotomis priemonėmis.

- **Teisė nesutikti:**

  Duomenų subjektas turi teisę „dėl su jo konkrečiu atveju susijusių priežasčių“ nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi: 1) remiantis teisėtais interesais ir 2) tiesioginės rinkodaros tikslais, įskaitant profiliavimą.

  Šiuo atveju Grupės įmonė nebetvarko asmens duomenų, išskyrus atvejus, kai: 1) ji įrodo, kad duomenys tvarkomi dėl įtikinamų teisėtų priežasčių, kurios yra viršesnės už duomenų subjekto interesus, teises ir laisves; arba 2) siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus.

Visi aukščiau išvardytų teisių įgyvendinimo prašymai teikiami duomenų apsaugos pareigūnui. Jei galiojančiuose įstatymuose nenumatyta priešingai, kiekvienas prašymas turi būti pateiktas raštu.

Jei galiojančiuose įstatymuose nenumatyta priešingai, atsakymas į kiekvieną prašymą turi būti pateiktas per 30 dienų po duomenų subjekto rašytinio prašymo gavimo datos. Būtina įrodyti, kad prašymo teikėjas yra duomenų subjektas arba jo įgaliotasis teisinis atstovas.

Jei galiojančiuose įstatymuose nenumatyta priešingai, kiekvienas prašymas bus nemokamas, nebent prašymas būtų laikomas nereikalingu ar pertekliniu.

4.3. Asmens duomenų saugumas

Grupė įsipareigoja atitikti geriausią jai žinomą pramonės praktiką IT saugumo atžvilgiu.

Be to, Grupės įmonė įdiegė fizines, technines ir organizacines saugumo priemones, siekiant apsaugoti asmens duomenų saugumą. Įskaitant saugumo pažeidimų, dėl kurių sunaikinami, prarandami, neteisėtai pakeičiami ar tvarkomi arba prie jų be leidimo gaunama prieiga, prevenciją, taip pat siekiant išvengti kitų pavojų, kurie galimi dėl žmogaus veiklos arba fizinės ar gamtinės aplinkos poveikio.

Nors saugumo priemonės skiriasi ir priklauso nuo Grupės įmonės, šios priemonės bus laikomos minimaliomis saugumo priemonės priemonėmis:

Visiems asmens duomenims taikomas aukščiausias saugumo laipsnis ir jie saugomi:

- rakinamoje patalpoje su kontroliuojama prieiga; ir (arba)
- rakinamame stalčiuje arba spintoje; ir (arba)
- jei saugomi kompiuteryje – apsaugoti slaptažodžiu, laikantis bendrovės reikalavimų; ir (arba)
- saugomi (išimamose) kompiuterinėse laikmenose, kurios yra užkoduotos.

Rankiniu būdu valdomi įrašai negali būti palikti ten, kur juos gali pasiekti neįgalioti asmenys, ir jų negalima pašalinti iš verslo patalpų be specialaus leidimo. Kai rankiniu būdu valdomi įrašai nebereikalingi kasdienėms klientų paslaugoms palaikyti, jie turi būti pašalinti iš saugaus archyvavimo.

Asmens duomenys gali būti ištrinti ar pašalinti laikantis saugojimo tvarkaraščio.

Grupė turi užtikrinti, kad asmens duomenys nebūtų atskleisti neįgaliotoms sutarties šalims, įskaitant šeimos narius, draugus, vyriausybines įstaigas, nebent to reikalauja įstatymai. Visi prašymai pateikti duomenis dėl vienos iš šių priežasčių turi būti pagrįsti tinkamais dokumentais, ir visos tokios informacijos atskleidimas turi būti kaskart patvirtintas duomenų apsaugos pareigūno.

Visos Grupės įmonės užtikrina, kad visi darbuotojai laikosi šios Politikos ir Elgesio kodekso. Be to, visos Grupės įmonės garantuoja, kad visi darbuotojai, atsakingi už Politikos įgyvendinimą, būtų tinkamai apmokyti, informuoti ir palaikomi (žr. 4.6 straipsnį).

4.4. Asmens duomenų saugumo pažeidimai

Asmens duomenų saugumo pažeidimas yra pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga. Jis gali būti techninis ar fizinis incidentas. Atsižvelgiant į tai, kad tokie pažeidimai visada yra visiški netikėtumai, visos Grupės įmonės ėmėsi visų reikiamų apsaugos priemonių, siekdamos išvengti katastrofinių asmens duomenų saugumo pažeidimų pasekmių.

Visose Grupės įmonėse yra įdiegtos patikimos pažeidimų aptikimo, tyrimo ir ataskaitų teikimo procedūros. Jos aprašytos Grupės įmonės duomenų saugumo pažeidimo politikoje. Be to, visose Grupės įmonėse vedamas duomenų saugumo pažeidimo registras, kuriame saugoma informacija apie faktus, susijusius su visais asmens duomenų pažeidimais, pažeidimų padariniais ir pastangomis bei korekciniais veiksmais.

Nors skirtingų įmonių politikos gali skirtis, visose duomenų saugumo pažeidimo procedūroje turi būti aprašyti šie veiksmai:

- Visi darbuotojai nedelsdami turi informuoti savo vadovą apie pažeidimus, susijusius su šia Duomenų apsaugos politika ar kitais asmens duomenų apsaugos nuostatais (duomenų apsaugos incidentai). Vadovas vėliau informuoja vietos duomenų apsaugos pareigūną, ES duomenų apsaugos pareigūną ir visuotinių duomenų apsaugos pareigūną.

- Duomenų apsaugos pareigūnai nusprendžia, ar dėl duomenų apsaugos incidento iš tikrųjų kilo asmens duomenų saugumo pažeidimas. Pavyzdžiui, prarastos USB atmintinės, pavogti nešiojamieji kompiuteriai, kenkėjiškų programų infekcijos ar įsilaužimai į duomenų bazes, kuriose yra asmens duomenys, laikomi asmens duomenų saugumo pažeidimais. Saugumo priemonių grėsmė ar trūkumas, pvz., silpni slaptažodžiai ar pasenusios ugniasienės, nelaikomi asmens duomenų saugumo pažeidimu, jei nėra asmens duomenų nutekinimo.

- Jei duomenų apsaugos incidentas iš tiesų yra asmens duomenų saugumo pažeidimas, duomenų apsaugos pareigūnai ištirs pažeidimo apimtį. Jie ištirs asmens duomenų saugumo pažeidimų mastą, kiek duomenų subjektų gali būti paveikta, ar pažeidimas gali sukelti pavojų duomenų subjektų laisvėms ir teisėms, ar pažeisti asmens duomenys yra jautraus pobūdžio, ar pažeisti asmens duomenys buvo apsaugoti (užkoduoti ar kitaip apsaugoti), ar kitos šalys gali būti įtrauktos į duomenų saugumo pažeidimą ir kokių veiksmų reikia imtis norint sušvelninti (tolesnį) asmens duomenų praradimą.

- Remdamasis aukščiau pateiktu vertinimu, duomenų apsaugos pareigūnai spręs, ar atitinkama priežiūros institucija ir duomenų subjektas turi būti informuoti apie pažeidimą. Pranešimas priežiūros institucijai nėra būtinas, jei tikėtina, kad asmens duomenų saugumo pažeidimas nekelia pavojaus asmenų teisėms ir laisvėms.

- Jei reikalaujama pranešti apie asmens duomenų saugumo pažeidimą, Grupė praneš apie tai kompetentingai priežiūros institucijai, pateikdama visą reikiamą informaciją per 72 valandas nuo to laiko, kai ji sužino apie pažeidimą.

- Kai dėl asmens duomenų saugumo pažeidimo gali kilti „didelis pavojus“ fizinių asmenų teisėms ir laisvėms, Grupė apie tai tiesiogiai informuoja suinteresuotus asmenis. „Didelis pavojus“ reiškia, kad pranešimai fiziniams asmenims yra svarbesni nei pranešimai atitinkamai priežiūros institucijai. Jei atskiri pranešimai būtų neproporcingos pastangos, Grupė gali naudoti tam tikrą viešojo bendravimo būdą, jei jis bus vienodai veiksmingas informuojant fizinius asmenis.

- Siekdama išlaikyti aukštą matomumo ir skaidrumo lygį, kiekviena grupės įmonė dokumentuoja visus duomenų apsaugos incidentus (tiek praneštus, tiek ne), įskaitant faktus, susijusius su pažeidimu, jų poveikį ir veiksmus, kurių buvo imtasi ar planuojama imtis. Visi šie dokumentai turi sudaryti priežiūros institucijai galimybę patikrinti atitiktį pranešimų prievolėms. Visi duomenų saugumo pažeidimo faktai turi būti kaupiami specialiame dokumente „Duomenų saugumo pažeidimo registras“ (2 priedas).

4.5. Duomenų saugojimas ir šalinimas

Kaip jau aptarta Politikos 4.1 straipsnyje, asmens duomenys negali būti tvarkomi ilgiau nei reikalinga tvarkymo tikslui pasiekti.

Visos Grupės įmonės apibrėžė ir nustatė atskirą saugojimo planą pagal 3 priedą. Saugojimo laikotarpiai grindžiami vietos įstatymų reikalavimais, atsižvelgiant į skirtingus asmens duomenų kategorijų tipus. Paprastai vietos teisės aktuose asmens duomenys klasifikuojami į šias kategorijas:

1. Apskaita ir finansai
2. Sutartys
3. Bendrovės įrašai
4. Korespondencija ir vidiniai protokolai
5. E. laiškai ir kitos elektroninis susirašinėjimas
6. Teisinės bylos ir dokumentai
7. Atlyginimo dokumentai
8. Pensijų dokumentai
9. Personalo įrašai
10. Mokesčių įrašai

Bet kuriuo atveju visi asmens duomenys bus saugomi ne trumpiau, nei reikalinga, kad Grupė galėtų pateikti ieškinį ar apsiginti teisme pagal vietos įstatymus.

4.6. Personalo mokymai

Grupė užtikrina, kad visi darbuotojai, kuriems suteikta prieiga prie asmens duomenų, bus supažindinti su savo atsakomybėmis pagal šią Politiką įvadinių personalo mokymų metu. Be to, visose Grupės įmonėse bus rengiami nuolatiniai duomenų apsaugos mokymai ir darbuotojų procedūrinės konsultacijos.

Vietinis duomenų apsaugos pareigūnas atsakingas už tinkamą visų darbuotojų apmokymą. Tokių mokymų forma gali skirtis priklausomai nuo klausytojų auditorijos, apmokomų darbuotojų skaičiaus, mokymų tikslų ir kitų aplinkybių.

Mokymai turi vykti nuolat. Visos Grupės įmonės savarankiškai numato konkretų mokymų planą, tačiau jis turi atitikti visuotinių ar ES duomenų apsaugos pareigūno reikalavimus / pasiūlymus.

4.7. Tvarkymo veiklos įrašai

Kiekviena Grupės įmonė tvarko asmens duomenų tvarkymo veiklos, už kurią jis atsako, įrašus ir veda duomenų registrą (4 priedas).

Duomenų registru užtikrinama Grupės įmonių atitiktis pagrindiniams BDAR atskaitomybės reikalavimams:

- Visų duomenų tvarkymo veiksmų įrašų valdymas;
- Duomenų tvarkytojo susitarimų įrašų valdymas;
- Duomenų saugumo pažeidimų, įskaitant pranešimus apie pažeidimus priežiūros institucijoms ir duomenų subjektams, įrašų valdymas.

Nors įvairių Grupės įmonių duomenų registro turinys gali skirtis, jame turi būti bent šie duomenų tvarkymo veiksmų įrašai:

- Grupės ir, jei taikoma, bendro duomenų valdytojo, duomenų valdytojo atstovo vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;
- duomenų tvarkymo tikslai;
- duomenų subjektų kategorijų ir asmens duomenų kategorijų aprašymas;
- duomenų gavėjų, kuriems buvo arba bus atskleisti asmens duomenys, įskaitant duomenų gavėjus trečiosiose valstybėse ar tarptautines organizacijas, kategorijos;
- kai taikoma, asmens duomenų perdavimai į trečiąją valstybę arba tarptautinei organizacijai, įskaitant tos trečiosios valstybės arba tarptautinės organizacijos pavadinimą;
- kai įmanoma, numatomi įvairių kategorijų duomenų ištrynimo terminai;
- kai įmanoma, bendras Grupės nurodytų techninių ir organizacinių saugumo priemonių aprašymas.

Visos Grupės įmonės pačios atsakingos už registro valdymą.

4.8. Duomenų perdavimas

Siekiant kompensuoti galimą duomenų apsaugos trūkumą, asmens duomenų perdavimas kitoms sutarties šalims reikalauja papildomų saugumo priemonių. Grupė nustatė tris skirtingus duomenų perdavimo modelius organizacijos viduje, kuriems taikomos skirtingos saugumo priemonės:

- Duomenų perdavimas Grupės viduje: siekiant palengvinti duomenų perdavimą, bus įgyvendintos įmonėms privalomos taisyklės. Tai priežiūros institucijos patvirtintos taisyklės, kurios teisiškai privalomos visoms Grupės įmonėms. Be kita ko, įmonėms privalomos taisyklėse nurodomi duomenų perdavimo tikslai ir paveiktos duomenų kategorijos; atspindėti BDAR reikalavimai; patvirtinama, kad ES įsisteigę duomenų eksportuotojai prisiima atsakomybę visos grupės vardu; paaiškintos skundų nagrinėjimo procedūros; ir užtikrinti atitikties mechanizmai (pvz., auditai).

- Kai duomenys perduodami sutarties šalims EEE teritorijoje (ar vienai iš valstybių, kurios gali garantuoti tokią pat apsaugą), kurios atlieka duomenų tvarkytojo funkciją, tokiems duomenų perdavimams taikomi BDAR reikalavimai.

  Prieš perduodama bet kokius duomenis trečiajai šaliai, kiekviena Grupės įmonė atlieka patikrinimą pagal deramą patikrinimo procesą ir įvertina, ar ši sutarties šalis atitinka galiojančius teisės aktus.

  Po tokio įvertinimo kiekviena Grupės įmonė turi sudaryti sutartį su kiekviena iš tokių trečiųjų duomenų tvarkytojų (trečios šalies duomenų tvarkytojo sutartis). Visose sutartyse būtinai turi būti ši informacija:

- perduodant duomenis ne Grupės įmonėms už EEE ribų, jei joms taikomi BDAR reikalavimai (tai reiškia, kad Grupės įmonė įsisteigusi ES teritorijoje arba duomenų subjektas yra ES gyventojas):

  Sudarydamos aukščiau įvardytą duomenų tvarkytojo sutartį, Grupės įmonės turi patikrinti, ar sutarties šalis, kuriai bus siunčiami asmens duomenys taiko adekvačias papildomas apsaugos priemones. Jei tokios apsaugos priemonės netaikomos, Grupė neperduoda jokios informacijos šiai trečiajai šaliai.

4.9. Poveikio duomenų apsaugai vertinimas

Siekiant užtikrinti automatinį visų duomenų apsaugos reikalavimų atpažinimą ir taikymą kuriant naujas sistemas ar procesus ir (arba) atnaujinant ar išplečiant esamas sistemas arba procesus, visos Grupės įmonės privalo atlikti visų naujų ir (arba) atnaujintų sistemų ar procesų, už kuriuos jos atsakingos, poveikio duomenų apsaugai vertinimą (PDAV).

PDAV atliekamas bendradarbiaujant su visuotinių ir ES duomenų apsaugos pareigūnu. Jei taikoma, vertinant naujų technologijų poveikio duomenų apsaugai vertinimą su duomenų apsaugos pareigūnu bendradarbiauja Informacinių technologijų (IT) skyrius, vykdydamas savo IT sistemos ir taikomųjų programų projektavimo peržiūros funkcijas.

4.10. Duomenų apsaugos pareigūnai

4.10.1. Duomenų apsaugos pareigūnai

Kadangi Grupės veikla vykdoma skirtingose jurisdikcijose, įskaitant ES, paskirti keli duomenų apsaugos pareigūnai:

- visuotinių duomenų apsaugos pareigūnas (atsakingas už visą Grupę):

  visuotinių duomenų apsaugos pareigūną skiria ir atšaukia iš pareigų generalinis direktorius, pasikonsultavęs su generaliniu advokatu ir finansų direktoriumi.

  Grupės visuotinių duomenų apsaugos pareigūnas yra Pieter Callens. Jo informacija ryšiams: Aleksander.Puzanov@eurochem.ru.

  ES duomenų apsaugos pareigūnas (atsakingas už Grupės veiklą ES):

  ES duomenų apsaugos pareigūną skiria ir atšaukia iš pareigų generalinis direktorius, pasikonsultavęs visuotinių duomenų apsaugos pareigūnu.

  Grupės ES duomenų apsaugos pareigūnas yra Pieter Callens. Jo informacija ryšiams: Pieter.Callens@eurochem.be

  Vietinis duomenų apsaugos pareigūnas (atsakingas už Grupės įmonę, jei paskirtas):

  Kiekviena Grupės įmonė gali paskirti vietinį duomenų apsaugos pareigūną. Vietinį duomenų apsaugos pareigūną skiria ir atšaukia iš pareigų Grupės / Grupės įmonės generalinis direktorius. Jei vietinis duomenų apsaugos pareigūnas nepaskirtas, Grupės / Grupės įmonės generalinis direktorius atlieka vietinio duomenų apsaugos pareigūno funkcijas.

4.10.2. Duomenų apsaugos pareigūnų atsakomybės

Visuotinių duomenų apsaugos pareigūnas

Visuotinių duomenų apsaugos pareigūnas skiriamas atsižvelgiant į jo profesines savybes, o ypač į Duomenų apsaugos įstatymo ir praktikos išmanymą bei gebėjimą vykdyti šias visuotinių duomenų apsaugos pareigūno pareigas:

- konsultuoti Grupės vadovybę Politikos klausimais ir padėti suvaldyti reikšmingas duomenų apsaugos rizikas, pavojus ir problemas, jiems iškilus;
- sukurti kokybišką Grupės duomenų apsaugos sistemą ir užtikrinti jos veikimą;
- valdyti komunikacijos, švietimo ar mokymų strategijas bei iniciatyvas ir, prireikus, užtikrinti paramą verslo vienetams duomenų apsaugos srityje;
- prižiūrėti ES duomenų apsaugos pareigūno ir vietinio duomenų apsaugos pareigūno veiklą (jei jis paskirtas).

Bendradarbiaujant su ES duomenų apsaugos pareigūnu ir vietiniu duomenų apsaugos pareigūnu (jei jis paskirtas):

- užtikrinti, kad būtų įdiegtos tinkamos Grupės procedūros ir politikos, kad asmens duomenys būtų tikslūs ir atnaujinti, atsižvelgiant į surinktų duomenų apimtį, jų pokyčių dažnį ir kitus svarbius veiksnius;
- rengti nuolatinius duomenų apsaugos mokymus, teikti išaiškinimus susijusiais klausimais;
- informuoti ir konsultuoti Grupę ir jos darbuotojus, kurie tvarko duomenis, apie jų prievoles pagal šią Politiką;
- stebėti atitiktį Politikai ir vykdyti auditus;
- prireikus, konsultuoti dėl poveikio duomenų apsaugai vertinimo ir stebėti jo vykdymą;
- stebėti ir analizuoti taikytinos teisės pakeitimus;

- peržiūrėti visų Grupės tvarkomų asmens duomenų saugojimo datas ir nustatyti, kurie duomenys nebereikalingi, atsižvelgiant į jų saugojimo paskirtį;
- imtis tinkamų priemonių, jei sutarties šalis galimai perdavė netikslius ar pasenusios asmens duomenis, informuoti ją, kad informacija yra netiksli ir (arba) pasenusi, ir kad jos nebegalima naudoti priimant sprendimus dėl atitinkamų fizinių asmenų; ir, prireikus, pateikti pataisytus asmens duomenis, sutarties šaliai;
- apsvarstyti galimos žalos ar nuostolių, kurie gali būti padaryti fiziniams asmenims (pvz., darbuotojams ar sutarties šaliai) dėl saugumo pažeidimo, mastą, bet kokio saugumo pažeidimo poveikį Grupei ir bet kokią žalą reputacijai, įskaitant galimą klientų pasitikėjimo praradimą.

ES duomenų apsaugos pareigūnas

ES duomenų apsaugos pareigūnas turi būti ES gyventojas ir yra skiriamas atsižvelgiant į jo profesines savybes, o ypač į Duomenų apsaugos įstatymo ir praktikos išmanymą bei gebėjimą vykdyti šias pareigas (be jau anksčiau išvardytų pareigų):

- bendradarbiauti su ES priežiūros institucijomis, visuotinių duomenų apsaugos pareigūnu ir vietiniu duomenų apsaugos pareigūnu (jei jis paskirtas);
- eiti priežiūros institucijų kontaktiniu asmens pareigas sprendžiant klausimus dėl duomenų tvarkymo ir duomenų saugumo pažeidimų;
- stebėti ir analizuoti ES teisės aktų pakeitimus bei pranešti apie juos visuotinių duomenų apsaugos pareigūnui.

Vietinis duomenų apsaugos pareigūnas

Kiekviena Grupės įmonė gali paskirti vietinį duomenų apsaugos pareigūną, kuris padeda visuotinių duomenų ir ES duomenų apsaugos pareigūnui vykdyti jų pareigas.

5. Politikos valdysena

5.1. Atsakomybė

Visos Grupės įmonės pačios atsako už atitiktį Politikai, jų teisinių įsipareigojimų vykdymą ir tinkamą asmens duomenų tvarkymą. Atitiktis Politikos reikalavimams yra privaloma visiems procese dalyvaujantiems darbuotojams.

Kilus įtarimui, kad teisiniai įsipareigojimai prieštarauja prievolėms pagal šią Duomenų apsaugos politiką, Grupės įmonė privalo informuoti visuotinių duomenų apsaugos pareigūną. Esant prieštaravimams tarp nacionalinių teisės aktų ir Politikos, Grupė stengsis rasti praktinį sprendimą, kuris atitiktų Duomenų apsaugos politikos paskirtį, bendradarbiaudama su atitinkama Grupės įmone.

Jei įmanoma, Grupės įmonė gali priimti taisykles, kurios papildo šią Politiką arba nukrypsta nuo jos. Tokias taisykles turi patvirtinti Grupės visuotinių duomenų apsaugos pareigūnas.

5.2. Valdymo priemonės

Visos Grupės įmonės garantuoja, kad joks darbuotojas nepatirs jokių neigiamų pasekmių laikydamiesi Politikos reikalavimų ar pranešę apie jau įvykusius arba galimus pažeidimus. O grupė netoleruos jokių darbuotojų veiksmų, pažeidžiančių Politiką.

Grupė numano ir tikisi, kad darbuotojai praneš apie visus Politikos pažeidimus ar galimus pažeidimus, naudodamiesi „Informavimo apie pažeidimus liniją“. Informacija apie šią liniją yra viešai prieinama ir skelbiama bendrovės tinklalapyje.

Grupė pasilieka sau teisę periodiškai tikrinti darbuotojų žinias apie asmens duomenų apsaugą, audituoti Politikos vykdymą ir veiksmingumą bei analizuoti jos rezultatyvumą.

5.3. Konfidencialumas

Kaip aprašyta 4.4 straipsnyje, asmens duomenims taikomos konfidencialumo prievolės.

Tačiau tam tikromis aplinkybėmis leidžiama dalintis asmens duomenimis be duomenų subjekto sutikimo. Atvejai, kai asmens duomenų atskleidimas yra būtinas:

• Nusikaltimo prevencija ir nustatymas.

• Nusikaltėlių sulaikymas ar persekiojimas.

• Mokesčio ar rinkliavos vertinimas ar surinkimas.

• Teismo sprendimu ar įstatymo taisyklėmis.

Jei kuri nors Grupės įmonė tvarko asmens duomenis vienu iš aukščiau išvardintų tikslu, ji gali taikyti konfidencialumo prievolės išimtį, bet tik jei tai būtina, siekiant išvengti neigiamo poveikio konkrečiu atveju.

Jei bet kuri Grupės įmonė gauna teismo ar bet kurios reguliavimo ar teisėsaugos institucijos prašymą pateikti duomenų subjekto informaciją, ji privalo nedelsdama pranešti visuotinių duomenų apsaugos pareigūnui, kuris suteikia išsamias gaires ir pagalbą.

5.4. Politikos peržiūra

Šią Politiką turi reguliariai, tačiau ne rečiau nei kartą per metus peržiūrėti Visuotinių duomenų pareigūnas, siekiant užtikrinti, kad ji būtų atnaujinama ir atitiktų visus galiojančius įstatymus ir taisykles.

Apie bet kokį pakeitimą nedelsiant pranešama Grupei, kuri įgyvendina pakeitimus.

Naujausia Duomenų apsaugos politikos versija pasiekiama Grupės tinklalapyje www. eurochemgroup.com.

5.5. Skundai ir klausimai

Bet kokios užklausos apie šią Politiką ir jos priedus siunčiamos visuotinių duomenų apsaugos pareigūnui ar atitinkamam vietiniam duomenų apsaugos pareigūnui.

Norėdami pateikti skundą dėl savo asmens duomenų tvarkymo, duomenų subjektai privalo raštu kreiptis į visuotinių duomenų apsaugos pareigūną. Skundas tiriamas tiek atsižvelgiant į konkrečios bylos aplinkybes. Visuotinių duomenų apsaugos pareigūnas per priimtiną laikotarpį informuoja duomenų subjektą apie ginčo tyrimo eigą ir rezultatą.

Jei ginčas negali būti išspręstas derybomis tarp duomenų subjekto ir visuotinių duomenų apsaugos pareigūno, duomenų subjektas savo nuožiūra gali kreiptis į atitinkamos jurisdikcijos duomenų apsaugos instituciją dėl tarpininkavimo, teisiškai įpareigojančio arbitražo, bylinėjimosi arba skundo.

Priedas Nr. 1. Nuorodos

r.	ID	Dokumento pavadinimas	Pastaba
Reglamentuojantis dokumentas			
1		„EuroChem Group“ AG atitikties politika	
2		„EuroChem Group“ AG elgesio kodeksas	
3		Federalinis duomenų apsaugos įstatymas (FADP)	

Priedas Nr. 2. Duomenų saugumo pažeidimo registras

Nr.	Grupės įmonė	Asmens duomenų kategorija	Apibūdinimas	Paveiktų duomenų subjektų skaičius	Duomenų subjektų kontaktinė informacija	Galimos pasekmės	Priemonės, kurių imtasi / bus imtasi

Priedas Nr. 3. Saugojimo planas

Nr.	Grupės įmonė	Asmens duomenų kategorija	Įrašo tipas	Saugojimo laikotarpis

Priedas Nr. 4. Duomenų registras

Nr.	Grupės įmonė*	Asmens duomenų kategorija ir aprašymas*	Tvarkymo tikslas*	Gavėjų kategorijos*	Perdavimas trečiajai šaliai	Ištrynimo laiko limitai	Saugumo priemonės

Žvaigždute * pažymėti stulpeliai yra privalomi.