ROQUETTE
Offering the best of nature™

Privacy & Data Protection

KAIP MES KASDIEN SAUGOME PRIVATUMĄ IR ASMENS DUOMENIS

Privatumas ir duomenų apsauga

Deramo elgesio vadovas

ROQUETTE GROUP

Legal & Compliance

Didžiausi „Roquette“ iššūkiai atitikties srityje

Vadovaujant General Management, už atitikties apimtį ir jos kontrolę bendrovėje „Roquette“ atsako Group Legal & Compliance skyriaus padalinys Compliance Office.

Compliance Office padalinys yra „Roquette“ Elgesio kodekso autorius, atsako už jo turinį ir prižiūri, kaip jo laikomasi.

Taip pat jis atsako už šias tris pagrindines sritis:

- finansinė sauga,
- profesinė etika ir
- privatumas ir duomenų apsauga.

Tam parengta ir nuolat tobulinama Atitikties programa – jos tikslas yra užtikrinti, kad teisiniu ir finansiniu požiūriu mūsų veikla būtų nepriekaištinga.

Kokia yra atitikties paskirtis?

Atitikties paskirtis yra įtvirtinti **etiško elgesio vertybes** ir taikyti priemones laikantis **teisinių reikalavimų**, **standartų** ir **geros praktikos.**

Mūsų programa skirta įtvirtinti procedūras, užtikrinančias „Roquette“ taikomų taisyklių laikymąsi.

Mūsų 4 vertybės – **autentiškumas, meistriškumas, orientacija į ateitį ir gerovė** – yra tvirtas pamatas, kuriuo vadovaujamės **kasdienėje** veikloje.

Atminkite: šiandien tvari bendrovė yra etiška bendrovė.
Rytojaus bendrovė yra skaidri bendrovė.

Mastyk globaliai
Veik vietiniu mastu

Pratarmė

Privatumo ir duomenų apsaugos principai yra bendrovės Elgesio kodekso nuostatų dalis.

Visi mūsų darbuotojai bei trečiosios šalys, su kuriomis „Roquette“ turi santykių, turi teisę į privatumą. Todėl „Roquette“ privalo apsaugoti jų asmens duomenis.

Asmens duomenys yra informacija, pagal kurią galima tiesiogiai ar netiesiogiai nustatyti fizinio asmens tapatybę (vardas ir pavardė, gimimo data, socialinio draudimo numeris, nuotrauka, el. pašto adresas, kompiuterio identifikatoriai ir pan.).

Asmens duomenų apsauga yra pamatinė teisė, užtikrinanti asmens privatumą

Asmens duomenų apsauga garantuoja kiekvienam asmeniui teisę valdyti tokių duomenų rinkimą, tvarkymą, naudojimą ir atskleidimą.

Asmens duomenys turi būti naudojami sąžiningai konkrečiam, aiškiam ir teisėtam tikslui ir privalo būti saugomi tik tiek laiko, kiek to reikia konkrečiu jų tvarkymo tikslu.

Europoje asmens duomenų tvarkymą reglamentuoja 2018 m. gegužės 25 d. įsigaliojęs Bendrasis duomenų apsaugos reglamentas (BDAR).

Asmens privatumą ir duomenų apsaugą reglamentuojantys teisės aktai įvairiose šalyse skiriasi, o kadangi „Roquette“ veikia tarptautinėje rinkoje, Grupė yra patvirtinusi Grupės asmens duomenų apsaugos politiką. Šios politikos nuostatos galioja visiems Grupės darbuotojams visame pasaulyje.

Šiame Vadove paaiškinamas deramas elgesys, kuriuo privalome vadovautis savo kasdienėje veikloje, kad laikytumėmės asmens duomenų apsaugos principų ir mūsų politikos reikalavimų.

Jennifer GODIN, duomenų apsaugos pareigūnė

Déléguée à la protection des données

Turinys

Legal & Compliance 3
Duomenų apsaugos pareigūno pratarmė 4

Paskirtis 6
Aprašymas 7
Atsakomybė 8
Klausimų ir problemų išsakymas 9
Įstatymų ir reikalavimų laikymasis 10
Duomenų apsaugos principai 12
Pavojus privatumui 14
Pavojus atitikties pažeidimo atveju 16

Mūsų santykių su Duomenų subjektais principai > p. 19

- Privatumo kultūra 20
- Asmens duomenų tvarkymas 22
- Duomenų subjekto teisės 24
- Pranešimas apie privatumą 26
- Tik būtino duomenų kiekio rinkimas 28
- Duomenų saugumas 30
- Asmens duomenų klasifikacija 32
- Duomenų saugojimo laikotarpis 34

Mūsų santykių su Partneriais ir Subrangovais principai > p. 37

- Duomenų tvarkytojo ir valdytojo kvalifikacijos 38
- Sutarties straipsniai dėl duomenų apsaugos 40
- Sutartis dėl duomenų perdavimo 42

Mūsų santykių su Profesiniu tinklu ir Priežiūros institucijomis principai > p. 45

- Duomenų apsaugos pareigūnas 46
- Duomenų apsaugos tinklas ir suinteresuoti asmenys 48
- Priežiūros institucijos 50
- Valdymas 52
- Atskaitomybė 54
- Dokumentavimas 56
- Poveikio privatumui vertinimas 58
- Pritaikytoji ir standartizuotoji duomenų apsauga 60
- Pranešimas apie duomenų saugumo pažeidimą 62
- Kontrolė ir stebėsena 64

Susiję dokumentai 66
Literatūra 67
Šaltiniai 68

Paskirtis

Apie Privatumo ir duomenų apsaugos politiką

„Roquette Group“ yra patvirtinusi Privatumo ir asmens duomenų apsaugos politiką (toliau – Politika), kuri nustato privatumo ir asmens duomenų apsaugos principus pagal bendrovės įvaizdį, interesus ir galiojančius duomenų apsaugą reglamentuojančius teisės aktus.

Ši Politika nustato asmens duomenų apsaugos principus ir reikalavimus bei taisykles, kurių privatumo ir duomenų apsaugos srityje privalo laikytis visi „Roquette“ vardu veikiantys darbuotojai, visų lygių vadovai bei trečiosios šalys.

Asmens duomenų apsaugos politikos principai ir taisyklės išsamiai išdėstytos dokumentų platformoje trimis lygmenimis:

- Vadovybės įsipareigojimas: Elgesio kodeksas
- Vidaus taisyklės: Asmens duomenų apsaugos vadovas ir direktyvos Q-Docs platformoje.
- Duomenų apsaugos valdymo sistemos (DPMS) dokumentacija: Tvarkos aprašai, rekomendacijos, metodikos, mokymai ir pan.

Visa dokumentacija atitinka teisinius ir norminius duomenų apsaugos reikalavimus.

Apie Deramo elgesio, susijusio su privatumu ir duomenų apsauga, vadovą

Privatumas ir duomenų apsaugos vadovas (toliau – Vadovas) skirtas diegti ir laikytis mūsų Privatumo ir duomenų apsaugos Politikos.

Jame supaprastintu būdu supažindinama su taisyklėmis ir gera praktika, kurios atitinka Grupės direktyvas bei mums aktualių duomenų apsaugą reglamentuojančių teisės aktų reikalavimus.

Pagal Elgesio kodekso struktūrą Vadovą sudaro 3 temos, iš kurių „Privatumas ir duomenų apsauga“ yra viena iš atitikties temų.

Aprašymas

Kam skirtas Deramo elgesio, susijusio su privatumu ir duomenų apsauga, vadovas?

Politika ir Vadovas skirti visoms grupės įmonėms. Šie dokumentai skirti:

- visiems darbuotojams, direktoriams ir vadovams (toliau – Darbuotojai),
- kitiems asmenims, dirbantiems „Roquette“ vardu, įskaitant:
  - rangovus, įskaitant konsultantus, laisvųjų profesijų asmenis ir laikinus darbuotojus,
  - praktikantus,
  - asmenis, komandiruotus į „Roquette“ iš kitų įmonių,
  - nenuolatinius darbuotojus,
  - kitus atstovus,
  - bet kokius asmenis, kuriuos „Roquette“ įdarbino ar kuriems moka atlyginimą.

Kur galima rasti Deramo elgesio, susijusio su privatumu ir duomenų apsauga, vadovą?

Visi darbuotojai ir trečiosios šalys, veikiančios „Roquette“ vardu, privalo suprasti privatumo ir duomenų apsaugos principus, išdėstytus mūsų dokumentuose ir visų pirma šiame vadove, ir jų laikytis.

Vadovas yra skelbiamas ONE portale:

Visuotinės funkcijos > Duomenų apsauga > Deramo elgesio vadovas.

Šis Vadovas skelbiamas atskirai kartu su priemonių rinkiniu, kurį sudaro el. mokymo moduliai, skirti privatumo ir duomenų apsaugos principams (apibrėžtiems pagal tarptautines normas ir konkrečius BDAR reikalavimus).

Mokymo kursas yra įtrauktas į Supažindinimo su duomenų apsauga programą.

Atsakomybė

Kas atsako už veiklos principų įgyvendinimą?

Duomenų apsauga yra aktuali kiekvienam mūsų organizacijos nariui ir kiekvienas narys yra už ją atsakingas.

Visų mūsų pareiga yra laikytis veiklos principų, aprašytų DPMS dokumentacijoje, kurią parengė Compliance Office skyriaus ir duomenų apsaugos tinklo nariai. Šis Vadovas skirtas paremti principų laikymąsi ir didinti mūsų atitikties lygį.

Kaip žinoti, ar elgiamės teisingai?

Vadovo paskirtis yra padėti mums priimti teisingą sprendimą dažniausiose profesinės veiklos situacijose, kuriose gali kilti klausimų dėl privatumo. Tačiau šiame dokumente neįmanoma numatyti visų įmanomų aplinkybių, su kuriomis susiduriame savo darbe.

Jei abejojate, kaip elgtis konkrečiu atveju, turite vadovautis sveika nuovoka ir atsakyti sau į tokius klausimus:

- Ar mano elgesys nepažeis įstatymų?
- Ar konkretūs veiksmai teigiamai charakterizuos mane ar bendrovę?
- Ar papasakočiau apie tai savo draugui, šeimos nariui ar kolegai?
- Ar jausčiausi gerai, jei apie tai būtų paskelbta viešai?

Jei į bent vieną klausimą atsakėte neigiamai, neturėtumėte taip elgtis. Jei dėl ko nors abejojate, kreipkitės į Grupės duomenų apsaugos pareigūną arba kitą atsakingą asmenį (jie nurodyti skyriuje „Klausimų ir problemų išsakymas“).

Kas nutiks, jei nesilaikysime Privatumo ir duomenų apsaugos principų?

Principų nesilaikymas gali sukelti bendrovei neigiamų pasekmių. Tokios pasekmės gali būti labai rimtos tiek bendrovei, tiek ir atskiriems asmenims (drausminė nuobauda, bauda, laisvės atėmimas, sugadinta reputacija ir pan.).

Visi pranešimai apie realų ar įtariamą Principų pažeidimą vertinami rimtai. Mes juos išnagrinėjame greitai, sąžiningai ir laikydamiesi teisės aktų reikalavimų.

Atsižvelgiant į duomenų saugumo pažeidimo pobūdį, pagal vietos teisės aktų reikalavimus ir bendrovės vidaus taisykles gali būti taikomos drausminės nuobaudos.

Tyrimo metu visi darbuotojai privalo bendradarbiauti su tyrėjais. „Roquette“ saugo tyrime dalyvaujančių asmenų konfidencialumą.

Klausimų ir problemų išsakymas

Darbuotojai, asmenys, veikiantys „Roquette“ vardu, ir kitos suinteresuotosios šalys skatinamos išsakyti savo klausimus ir nuogąstavimus, kurie padėtų „Roquette“ išvengti žalos bendrovei arba ją sumažinti.

Apie kokio tipo problemas galima pranešti?

Darbuotojai gali išsakyti klausimus dėl galimo ar realaus Privatumo ir duomenų apsaugos principų, bendrovės tvarkos taisyklių ar galiojančių teisės aktų pažeidimo.

Į ką kreiptis?

Duomenų saugumo pažeidimo atveju kreipkitės į duomenų apsaugos pareigūną adresu dpo@Roquette.com ir praneškite apie incidentą naudodamiesi mūsų internetine forma „Privacy Alert“.

Jei norite pranešti apie galimą atitikties pažeidimą, galite susisiekti su įprastu kontaktiniu asmeniu arba pranešti apie problemą naudodami "Speakup©" įrenginį. Visi per šį įrenginį gauti pranešimai nagrinėjami konfidencialiai, laikantis atitinkamų įstatymų ir kitų teisės aktų.

SpeakUp®

„Roquette“ netoleruoja jokios formos atsakomųjų veiksmų ar kerštо darbuotojui arba kitam „Roquette“ vardu veikiančiam asmeniui, gera valia pranešusiam apie galimą ar faktinį Privatumo ir duomenų apsaugos principų ar galiojančių teisės aktų pažeidimą.

Todėl jei pranešimo autorius turi nurodyti savo tapatybę, bendrovė privalo tvarkyti jo tapatybę konfidencialiai, kad tokio asmens atžvilgiu būtų išvengta atsakomųjų veiksmų ar kerštо, diskriminacijos ar drausminių nuobaudų už pažeidimų atskleidimą.

Įstatymų ir reikalavimų laikymasis

Kiekvienas iš mūsų, dirbantis bet kurioje grupės įmonėje, turi laikytis galiojančių duomenų apsaugos teisės aktų reikalavimų.

Jei vietos teisės aktai numato griežtesnį reglamentavimą už mūsų Politiką ir Vadovą, būtina laikytis vietos teisės aktų.

Kitais atvejais (jei nėra vietos teisės aktų arba jie numato ne tokį griežtą reglamentavimą) privaloma laikytis mūsų vidaus gerosios praktikos visa teisės aktų leidžiama apimtimi.

Mūsų įsitikinimai

- Būtina nedelsiant įgyvendinti visus naujus vietos teisės aktų reikalavimus.
- Kiekvienas iš mūsų turi suvokti, kad bet koks įstatymų ar kitų reikalavimų nesilaikymas gali užtraukti civilinę ar baudžiamąją atsakomybę prasižengusiam asmeniui ir mūsų bendrovei.
- Fizinių asmenų apsauga tvarkant jų asmens duomenis yra pamatinė teisė.
- Fizinių asmenų apsaugos, susijusios su jų asmens duomenų tvarkymu, principai ir taisyklės turi atsižvelgti į fizinių asmenų pamatines teises ir laisves, ypač į jų teisę į asmens duomenų apsaugą, neatsižvelgiant į asmenų tautybę ar gyvenamąją vietą.
- Teisė į asmens duomenų apsaugą nėra absoliuti. Ji turi būti vertinama atsižvelgiant į jos svarbą visuomenei ir derinama su kitomis pamatinėmis teisėmis vadovaujantis proporcingumo principu.

Kurios šalys yra priėmusios duomenų apsaugos teisės aktus arba jose veikia duomenų apsaugos institucija?

Išsamiau apie tai žr. žemėlapyje: https://www.cnil.fr/en/data-protection-around-the-world.

Mūsų pareigos

- Visuomet privalome laikytis visų duomenų subjekto šalyje galiojančių duomenų apsaugos įstatymų ir teisės aktų bei bendrovės veiklos vietose taikomų taisyklių.

- Vykdydami savo profesines pareigas privalome pranešti apie bet kokį elgesį, kuris, mūsų nuomone, prieštarauja galiojantiems duomenų apsaugos teisės aktų reikalavimams (pvz., BDAR) mūsų duomenų apsaugos pareigūnui adresu dpo@Roquette.com ir konfidencialų "Roquette" perspėjimo įrenginį: "Speakup©".

- Privalome parengti asmens duomenų apsaugos priemones, kurios būtų tinkamos ir proporcingos bei kartu leistų lengviau laikytis galiojančių įstatymų ir teisės aktų. Ir atvirkščiai, mūsų veiksmai, kuriais siekiame laikytis Grupei privalomų įstatymų ir teisės aktų, turi neprieštarauti asmens duomenų apsaugos taisyklėms ir gerai praktikai (pavyzdys: Kovos su kyšininkavimu ir korupcija programoje privalome užtikrinti pranešimą apie galimą pažeidimą padariusio asmens apsaugą konfidencialumo ir jo asmens duomenų apsaugos priemonėmis).

Ar jums aktualus Bendrasis duomenų apsaugos reglamentas (BDAR)?

BDAR aktualus jums kaip duomenų **tvarkytojui**(1) arba **valdytojui**(2):

- jei jūsų veiklos vieta yra ES, arba
- jei jūsų veiklos vieta yra už ES ribų, jei: jūsų „duomenų tvarkymo veikla yra susijusi su:
  - prekių arba paslaugų siūlymu duomenų subjektams ES; arba
  - elgesio, kai jie veikia Sąjungoje, stebėsena“.

Oficialus tekstas: BDAR 3 straipsnis apie teritorinę taikymo sritį.

(1) ir (2): Apibrėžtis žr. p. 38.

Duomenų apsaugos principai

Asmens duomenys turi būti:

- saugūs,
- tikslūs ir naujausi,
- tvarkomi sąžiningai ir teisėtai,
- tvarkomi tik konkrečiu tikslu,
- tinkami, aktualūs ir neperteklinai,
- laikomi ribotą ir nustatytą laikotarpį,
- tvarkomi nepažeidžiant duomenų subjekto teisių,
- perdavimo į kitas valstybes atveju apsaugoti tinkamomis teisinėmis priemonėmis.

Jūsų teisės

Pagal galiojančius įstatymus ir teisės aktus jūs turite teisę susipažinti su savo asmens duomenimis, juos ištaisyti, nesutikti su jų tvarkymu dėl teisėtų priežasčių, taip pat teisę juos ištrinti dėl teisėtų priežasčių, teisę į duomenų perkeliamumą bei teisę riboti jūsų asmens duomenų tvarkymą.

Norėdami pasinaudoti bet kuria iš šių teisių, užpildykite formą adresu Roquette.com/Data Protection.

Visais klausimais šia tema kreipkitės į **duomenų apsaugos pareigūną** (dpo@Roquette.com).

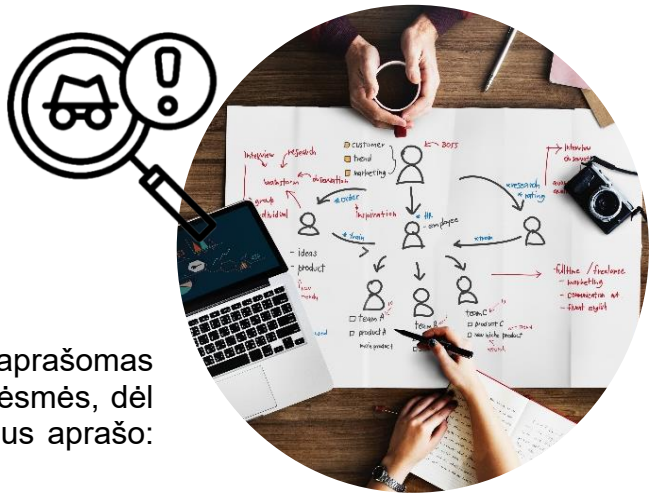
Mūsų pareigos

Mes privalome:

- laikytis vietos asmens duomenų apsaugos teisės aktų ir Grupės Politikos taisyklių;
- pranešti duomenų apsaugos pareigūnui apie naują duomenų tvarkymą ar pakeitimus;
- nerinkti, nenaudoti, neatskleisti ir nelaikyti asmeninio pobūdžio duomenų, išskyrus jei tokie duomenys reikalingi konkrečiu, teisėtu ir būtinu tikslu;
- užtikrinti, kad asmenys būtų informuojami apie tai, kad mes renkame jų duomenis;
- apsaugoti asmens duomenis juos renkant, tvarkant, naudojant, perduodant, laikant ir perkeliant;
- užtikrinti tvarkomų duomenų saugumą ir konfidencialumą;
- laikyti duomenis tik tiek laiko, kiek būtina jų tvarkymui, ir laikantis galiojančių teisės aktų;
- asmens duomenų pažeidimo atveju kreiptis duomenų apsaugos pareigūną.

Mokome savo darbuotojus ir tobuliname vidaus procesus.

Pavojus privatumui



Kas yra pavojus privatumui?

Pavojus yra hipotetinis scenarijus, kuriame aprašomas galimas nepageidaujamas įvykis ir visos grėsmės, dėl kurių jis gali įvykti. Konkrečiai toks scenarijus aprašo:

- kaip pavojaus šaltiniai (pvz., darbuotojas, kuris gavo kyšį iš konkurento)
- gali išnaudoti pažeidžiamas pagalbinio turto savybes (pvz., failų valdymo sistemą, kurioje galima manipuliuoti duomenimis)
- grėsmės akivaizdoje (pvz., neleistinas naudojimas išsiunčiant el. laiškus)
- ir leisti įvykti nepageidaujamam įvykiui (pvz., neteisėtai prieigai prie asmens duomenų),
- susijusiam su asmens duomenimis (pvz., kliento failu),
- tokiu būdu sukeliant poveikį duomenų subjektų privatumui (pvz., jie gauna nepageidaujamų pasiūlymų, jaučia, kad jų privatumas yra pažeistas, kyla asmeninių ar profesinių problemų).

Netikrumo poveikis privatumui

Pavojaus laipsnis nustatomas pagal pavojaus rimtumą. Visų pirma rimtumas vertinamas galimo poveikio mastu (**fizinis, turtinis, moralinis**) duomenų subjektams, atsižvelgiant į esamas, suplanuotas ar papildomas kontrolės priemones.

Pavyzdys

Didžiausias pavojus, kurį negerovės paviešinimas kelia vidaus informatoriui – atsakomieji veiksmai, diskriminacija arba drausminės nuobaudos už tokį veiksmą.

Mūsų įsitikinimai

Tvarkant duomenis būtina laikytis visų žmogaus teisių, neatsižvelgiant į pavojaus laipsnį.

Tačiau mes privalome lanksčiai koreguoti tai, kaip laikomės duomenų apsaugos reikalavimų pagal mūsų asmens duomenų tvarkymo veiksmų keliamo pavojaus asmens pamatinėms teisėms ir laisvėms laipsnį.

Taip elgtis mus papildomai skatina ir BDAR. Todėl dėl duomenų tvarkymo veiksmų, kurie kelia mažesnį pavojų asmens pamatinėms teisėms ir laisvėms, gali būti taikoma mažiau atitikties prievolių, o didelės rizikos tvarkymo veiksmų atveju kyla daugiau atitikties prievolių, pvz., atlikti poveikio duomenų apsaugai vertinimą (PDAV)(1)

Mūsų pareigos

Labai svarbu yra atlikti rizikos vertinimą. Pagal BDAR rizikos vertinimas yra esminis organizacijos atskaitomybės ir bet kokio duomenų tvarkymo komponentas.

Didelės rizikos duomenų tvarkymo atveju privalome atlikti rizikos vertinimą, kurio reikalaujama pagal PDAV bei daugybę kitų BDAR reikalavimų, įskaitant duomenų saugumo, saugos, pranešimų apie duomenų saugumo pažeidimą, pritaikytojo privatumo, teisėto intereso, tikslo apribojimų ir sąžiningo tvarkymo.

(1): žr. apibrėžtį p. 58.

Pavojus pažeidimo atveju

Juridiniams ir fiziniams asmenims, pažeidusiems duomenų apsaugos įstatymus ir teisės aktus (e.g. BDAR), gresia tokios sankcijos ir sąnaudos.

Baudžiamosios sankcijos:

- laisvės atėmimas,
- bauda juridiniams asmenims.

Civilinės sankcijos:

- žalos atlyginimas.

Administracinės sankcijos:

- oficialus įspėjimas,
- įspėjimas,
- draudimas,
- laikinas ar visiškas tvarkymo apribojimas,
- sertifikato atšaukimas arba nurodymas atšaukti sertifikatą,
- laikinas duomenų perdavimo nutraukimas,
- įsakymas nutraukti tvarkymą arba tvarkymo leidimo panaikinimas;
- pritaikytų sankcijų paviešinimas,
- sankcijos be atskiro oficialaus įspėjimo (pagal skubos kriterijų),
- atsižvelgiant į pažeidimą, administracinė bauda.

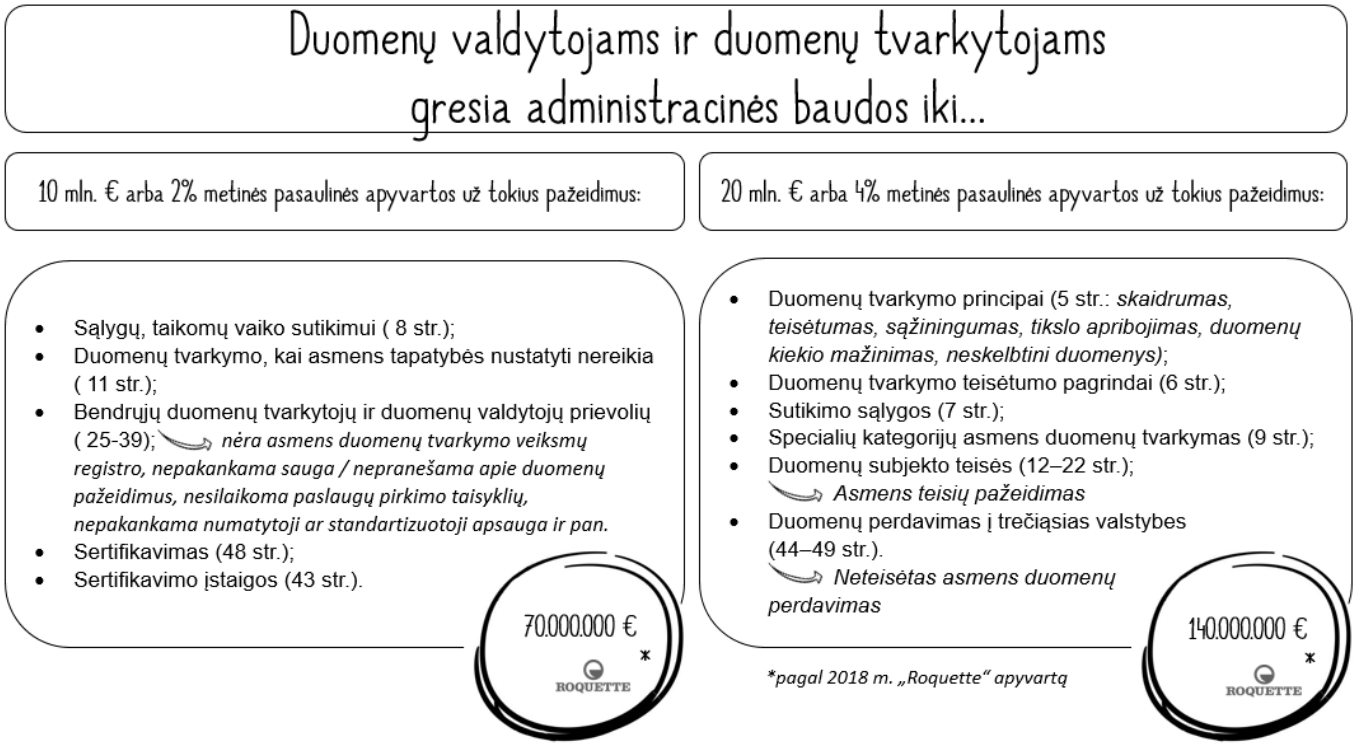
Ženklios sąnaudos:

- pajamų praradimas dėl pakenktos reputacijos.

Kokia didžiausia administracinė bauda numatyta BDAR?

Baudos nėra privalomos, jos svarstomos kiekvienu atskiru atveju. Baudos turi būti skiriamos išnagrinėjus konkretų atvejį ir turi būti „veiksmingos, proporcingos ir atgrasomos“.

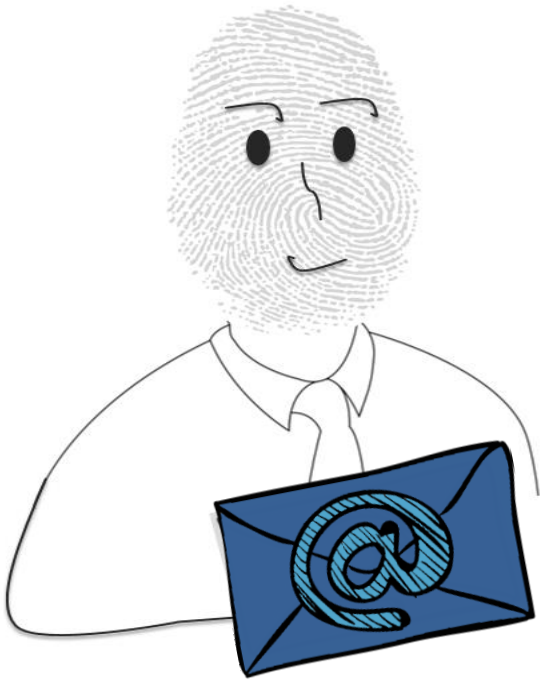
Baudų dydį lemia tai, kokį BDAR straipsnį organizacija pažeidė.



Kokios gali būti baudžiamosios sankcijos?

Toliau pateikiame keletą Prancūzijos įstatymų pavyzdžių.

- Asmens duomenų rinkimas apgaulingu, nesąžiningu ar neteisėtu būdu užtraukia 5 metų laisvės atėmimo bausmę ir 300.000 € baudą (Baudžiamojo kodekso 226-18 str.).
- Siekiant garantuoti realias vidaus informatoriaus teises ir apsaugą, Antikorupcijos įstatymas („Sapin II“ įstatymas) numato griežtas bausmes už trukdymą pranešti apie negeroves. Teisės aktai atkreipia ypatingą dėmesį į pranešimo konfidencialumo užtikrinimo svarbą. Taigi atskleidus konfidencialius pranešimo duomenis (vidaus informatoriaus ar pareiškėjo tapatybę, informaciją, susijusią su pranešimo turiniu), išskyrus jei jie atskleidžiami teisėsaugos institucijai, užtraukia 2 m. laisvės atėmimo bausmę ir 30.000 € baudą.



1 Mūsų SANTYKIŲ SU DUOMENŲ SUBJEKTAIS principai

Privatumo kultūra

Duomenų apsauga – tai įstatymų, reglamentų ir geriausios praktikos pavyzdžių rinkinys, susijęs su asmens duomenų rinkimu ir naudojimu.

Asmens duomenys reiškia bet kokią informaciją, susijusią su asmeniu, kurio tapatybė yra žinoma arba kurio tapatybę galima nustatyti.

Duomenų privatumas yra susijęs su asmens duomenų tvarkymu.

Kam tai aktualu?

Duomenų apsauga yra aktuali kiekvienam mūsų organizacijos nariui ir kiekvienas narys yra už ją atsakingas.

Kodėl tai svarbu?

Netinkamas duomenų tvarkymas gali turėti rimtų pasekmių organizacijoms, jų darbuotojams ir klientams.

Už privatumo pažeidimus gali būti skiriamos neriboto dydžio finansinės baudos, skelbiama nepalanki informacija žiniasklaidoje, nukentėti reputacija, prarastas klientų pasitikėjimas, prarastas verslas ir darbuotojai, teikiami skundai ir netgi ieškiniai, jei pažeidžiami asmens duomenų apsaugos reikalavimai, arba, kitais atvejais, gali būti taikomos drausminės nuobaudos. Mes visi suinteresuoti tinkamai tvarkyti duomenis.

Mūsų įsitikinimai

- Visi „Roquette“ darbuotojai turi žinoti savo vaidmenį ir atsakomybę asmens duomenų apsaugos srityje. Skatindami jų sąmoningumą siekiame puoselėti pagarbos privatumui ir duomenų apsaugos kultūrą „Roquette“ bendrovėje.

[DDPG001EN – 1 taisyklė]

- Būtina surengti darbuotojų mokymus apie asmens duomenų apsaugos Politikos įgyvendinimą.

[DDPG001EN – 2 taisyklė]

GALVOK APIE privatumą

Tai – mūsų atsakomybė!

Be klientų ir darbuotojų asmens duomenų negalime sėkmingai vykdyti savo veiklos.

Mumis pasitiki, kad prižiūrėsime šią esminę informaciją.

Kiekvienas darbuotojas privalo laikytis atitinkamų duomenų apsaugos įstatymų.

Tai – mūsų reputacija!

Reputaciją sunku įgyti, tačiau lengva prarasti.

Siekdami apsaugoti savo reputaciją, klientų ir darbuotojų duomenis privalome tvarkyti atsargiai.

JŪS esate geriausia apsauga nuo reputacijos sugadinimo.

Tai – pagarba!

Jei norime išlaikyti mums suteiktą pasitikėjimą, privalome gerbti savo klientų ir darbuotojų sprendimus dėl jų asmens duomenų naudojimo.

Tai – mūsų rankose!

Visi privalome užtikrinti, kad klientų ir darbuotojų asmens duomenys būtų laikomi saugiai ir konfidencialiai.

Bet kokiai informacijai, kurią reikia išsiųsti arba išnešti už bendrovės ribų, reikalingas papildomas dėmesys.

Mokome savo darbuotojus ir tobuliname vidaus procesus.

- Elgesio kodeksas – Privatumas ir duomenų apsauga - p. 42–43.
- Naujiems darbuotojams: Bendrojoje darbuotojų integracijos programoje yra keletas el. mokymo modulių apie duomenų apsaugą.
- Darbuotojams: Darbuotojams: mokymasis įkeliamas į mokymosi platformą.
- Duomenų apsaugos koordinatoriams: Bendruomenė: dokumentais dalijamasi mūsų bendruomenėje „Data Protection Network“.
- Visiems: Daugiau informacijos rasite vidaus portale > „Data Protection“.

Asmens duomenų tvarkymas

Asmens duomenų tvarkymas reiškia bet kokį automatinį ar neautomatinį veiksmą ar veiksmų seką, atliekamą asmens duomenų ar jų rinkinių atžvilgiu, pvz., jų rinkimą, registravimą, organizavimą, sisteminimą, laikymą, pritaikymą ar keitimą, gavimą, susipažinimą, naudojimą, atskleidimą perduodant, platinant ar kitokiu būdu atskleidžiant, taip pat suderinimą ar grupavimą, apribojimą, ištrynimą ar sunaikinimą.

Pagal duomenų apsaugos (ir BDAR) reikalavimus rinkti asmens duomenis galima tik turint teisinį pagrindą.

Vietos teisės aktai gali skirtingai apibrėžti teisinį pagrindą.

Kokiu teisiniu pagrindu galiu tvarkyti asmens duomenis?

Turite galėti aiškiai atsakyti į tokį klausimą:

„Kaip jūs gavote mano duomenis ir ar turite teisę juos turėti?“

Kitaip tariant, privalote turėti bent vieną iš šešių teisinių pagrindų tvarkyti duomenis. Pagal BDAR nuostatas jūs negalite tvarkyti jokių duomenų, jei nėra bent vieno iš šių teisinių pagrindų:

1. Sutikimas
2. Sutartis
3. Teisinė prievolė
4. Gyvybiniai interesai
5. Viešasis interesas
6. Teisėtas interesas

Teisėtumas, sąžiningumas ir skaidrumas

Mūsų pareigos

Laikydamiesi taisyklių privalome užtikrinti teisėtą asmens duomenų tvarkymą.

Taisyklės	Q-Docs	BDAR
• Duomenis rinkti teisėtai, sąžiningumai ir skaidriai	DDPG002EN 1 taisyklė	5 str. 1 d. a)
• Įrodyti, kad gautas duomenų subjekto sutikimas (jei reikia)	DDPG002EN 2 taisyklė	7 str.
• Laikytis nustatytų duomenų rinkimo tikslų	DDPG002EN 3 taisyklė	5 str. 1 d. b)
• Popierinėje ar skaitmeninėje formoje rinkti tik būtiną informaciją	DDPG002EN 4 taisyklė	5 str. 1 d. c)
• Duomenis laikyti ne ilgiau, nei tai būtina	DDPG002EN 5 taisyklė	5 str. 1 d. e)
• Perkeliant asmens duomenis į trečiąsias valstybes ar tarptautines organizacijas imtis reikiamų apsaugos priemonių	DDPG002EN 6 taisyklė	44–50 str.

Mokome savo darbuotojus ir tobuliname vidaus procesus.

Duomenų subjekto teisės

Duomenų subjektas yra fizinis asmuo, kurio tapatybę galima nustatyti tiesiogiai arba netiesiogiai pagal jo asmens duomenis, pvz., vardą ir pavardę, identifikacinį numerį, jo buvimo vietą, internetinį identifikavimo ženklą arba pagal vieną ar kelis jo fizinius, fiziologinius, genetinius, psichinius, ekonominius, kultūrinius ar socialinius požymius.

Kas yra duomenų subjektas?

Tai yra asmuo, su kuriuo susiję konkretūs asmens duomenys.

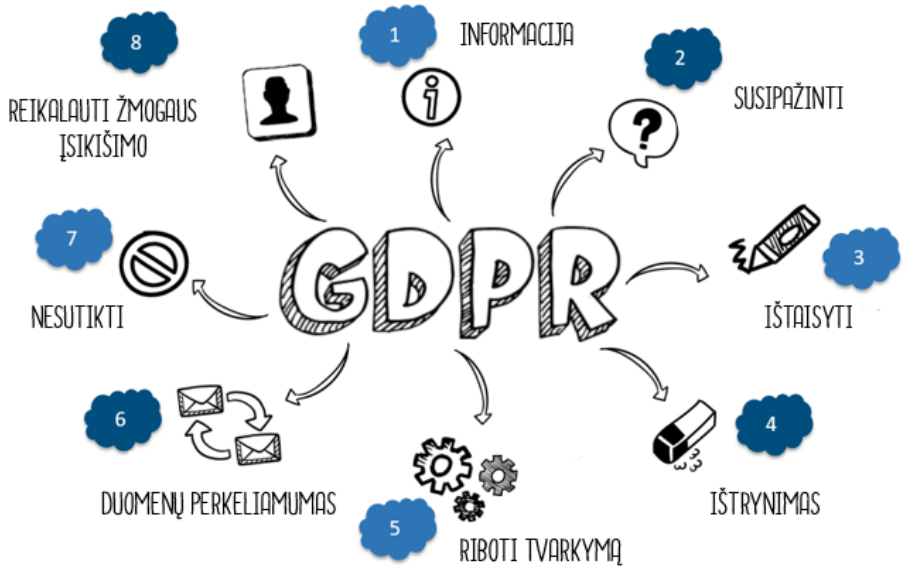
Kas yra duomenų subjekto prašymas?

Viena iš pagrindinių teisių, kurią privaloma užtikrinti pagal duomenų apsaugos teisės aktų reikalavimus, yra asmens teisė susipažinti su asmenine informacija, kuri yra su juo susijusi.

Asmuo turi teisę pateikti duomenų subjekto prašymą susipažinti su laikoma jo asmenine informacija bei gauti tokios informacijos kopiją. Daugeliu atvejų tokį prašymą privalote įvykdyti per 30* kalendorinių dienų nuo prašymo gavimo.

*: šis laikotarpis priklauso nuo galiojančių teisės aktų arba duomenų tvarkymo veiksmų pobūdžio.

Kokias kitas teises turi duomenų subjektas?



Mūsų pareigos

Laikydamiesi taisyklių privalome užtikrinti duomenų subjektų teises.

Taisyklės	Q-Docs	BDAR
• Įsitikinti, kad teisiniai pranešimai atitinka prievoles	DDPG006EN 1 taisyklė	12 str.
• Užtikrinti duomenų subjektui teisę susipažinti su duomenimis	DDPG006EN 2 taisyklė	15 str.
• Užtikrinti duomenų subjektui teisę ištaisyti duomenis	DDPG006EN 3 taisyklė	16 str.
• Užtikrinti duomenų subjektui teisę į duomenų perkeliamumą	DDPG006EN 4 taisyklė	20 str.
• Užtikrinti duomenų subjektui teisę ištrinti duomenis (būti pamirštam)	DDPG006EN 5 taisyklė	17 str.
• Užtikrinti duomenų subjektui teisę riboti jo duomenų tvarkymą	DDPG006EN 6 taisyklė	18 str.
• Pranešti apie asmens duomenų ištaisymą, ištrynimą arba tvarkymo ribojimą	DDPG006EN 7 taisyklė	19 str.
• Kontroliuoti automatizuotą atskirų sprendimų priėmimą, įskaitant profiliavimą	DDPG006EN 8 taisyklė	22 str.

Mokome savo darbuotojus ir tobuliname vidaus procesus.

Pranešimas apie privatumą

Teisė būti informuotam, jei naudojami asmens duomenys

Privalome informuoti visus savo darbuotojus bei kitus asmenis, su kuriais „Roquette“ palaiko santykius, jei bendrovė naudoja jų asmens duomenis.

Turime aiškiai nurodyti:

- kodėl „Roquette“ naudoja jų duomenis,
- kokius duomenis „Roquette“ naudoja,
- kiek laiko surinkti duomenys bus laikomi,
- asmens teisę būti informuotam,
- iš kur duomenys surinkti,
- ar „Roquette“ ketina perduoti surinktus duomenis, įskaitant asmens vardą ir pavardę, trečiosioms šalims, nurodant perdavimo priežastis,
- ar „Roquette“ ketina perduoti surinktus duomenis į kitą valstybę, nurodant šią valstybę ir kas bus daroma su duomenimis,
- ar „Roquette“ naudoja surinktus duomenis profiliavimui (tai yra automatizuotas duomenų tvarkymas, kai asmens duomenys naudojami analizuoti arba nuspėti asmens veiklos rezultatus darbe, jo ekonominę padėtį, sveikatos būklę ir pan.),
- kaip kreiptis į DAP,
- kad kilus klausimų, asmuo turi teisę kreiptis į priežiūros instituciją.

Tokia informacija vadinama **Informacija apie privatumą** arba **Pareiškimu dėl privatumo**.

Informaciją apie privatumą privalome suteikti bendrovei „Roquette“ renkant asmens duomenis. Jei „Roquette“ gavo asmens duomenis iš kito šaltinio, informaciją apie privatumą turi pateikti „Roquette“. Tai galima padaryti per pranešimą apie privatumą.

Tai yra **teisė būti informuotam**.

Taisyklės	Q-Docs	BDAR
• Įsitikinti, kad teisiniai pranešimai atitinka prievoles	DDPG006EN 1 taisyklė	12 str.

Pavyzdžiai

- Informacija apie privatumą „Roquette“ svetainėje: https://www.Roquette.com/data-protection.
- Informacija apie privatumą vykdant personalo procesus Workday@Roquette sistemoje pateikiama ONE platformoje: Darbuotojų kampelis>Workday@Roquette.

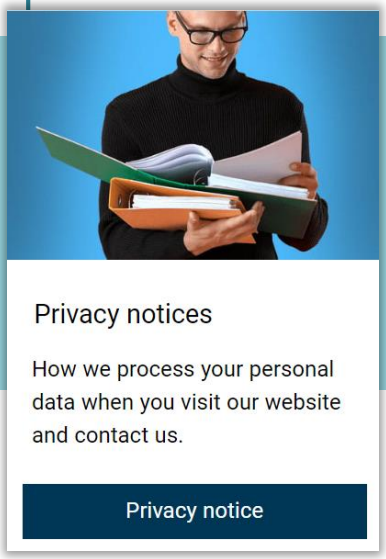
Kada „Roquette“ gali neinformuoti asmenų apie savo veiksmus?

Apskritai privalome informuoti asmenis apie privatumą, tačiau ne visuomet. Išimtys:

- asmeniui jau suteikta informacija apie privatumą ir nuo to laiko ji nepasikeitė,
- neįmanoma suteikti asmeniui informacijos arba tai pareikalautų neproporcingų pastangų, arba
- suteikus asmeniui informaciją taptų neįmanoma naudoti jo duomenis arba dėl to būtų labai pakenkta naudojimo priežasčiai.

Pastaba: jei būtina imtis laikinų priemonių užkirsti kelią įkalčių nuslėpimui arba sunaikinimui, tokia informacija gali būti suteikiama jau pritaikius tokias laikinas priemones.

Mokome savo darbuotojus ir tobuliname vidaus procesus.



Tik būtino duomenų kiekio rinkimas

Koks yra duomenų kiekio mažinimo principas?

BDAR 5 str. 1 d. c punkte sakoma:

> „1. Asmens duomenys turi būti:
>
> c) adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas)“

Pagrindinių funkcijų sukurtose popierinėse arba skaitmeninėse formose, skirtose rinkti asmens duomenis, turi būti tik informacijos, kuri būtina duomenų tvarkymui, laukai, kad būtų išvengta tvarkymo tikslu nepateisintų duomenų rinkimo.

Mūsų pareigos

Privalome užtikrinti, kad jūsų tvarkomi asmens duomenys yra:

- adekvatūs – pakankami tinkamai pasiekti nurodytą tikslą;
- tinkami – racionaliai susiję su tokiu tikslu; ir
- tik tokie, kurių reikia – negalime turėti daugiau duomenų, nei jų reikia konkrečiu tikslu.

Taisyklės	Q-Docs	BDAR
• Popierinėje ar skaitmeninėje formoje rinkti tik būtiną informaciją	DDPG002EN 4 taisyklė	5 str. 1 d. c)

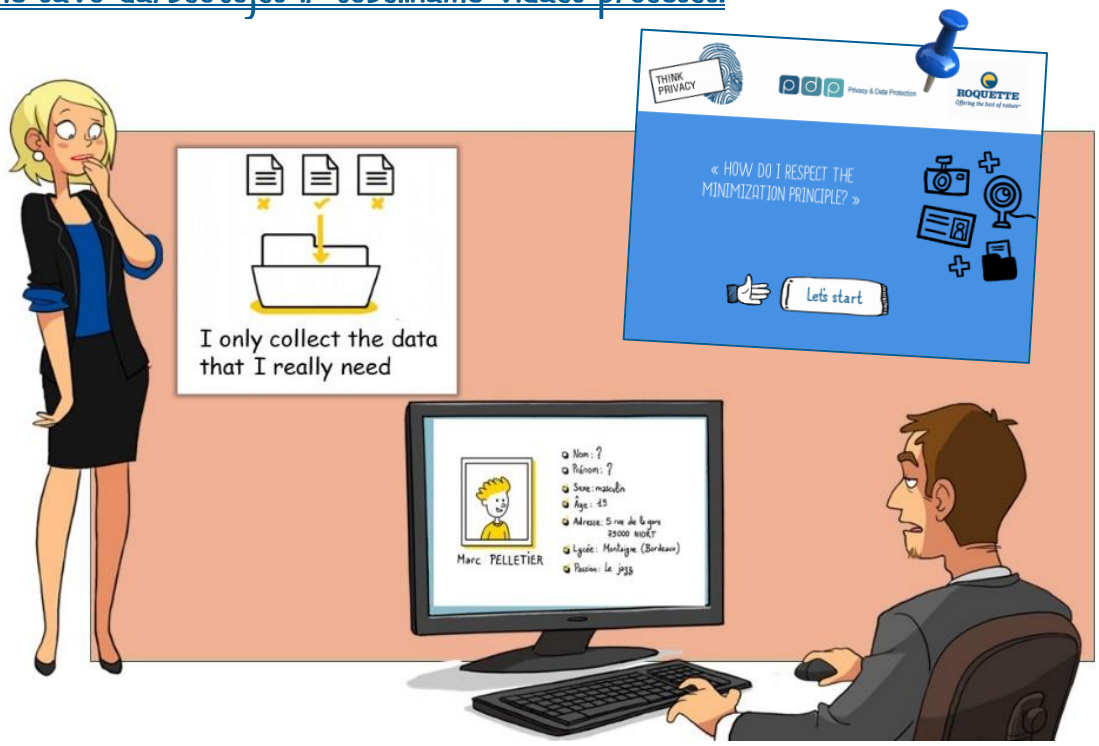
Kontrolinis sąrašas

- ☑ Renkame tik tuos asmens duomenis, kurie būtini konkrečiam tikslui.
- ☑ Turime pakankamai asmens duomenų tinkamai pasiekti konkrečius tikslus.
- ☑ Reguliariai tikriname turimus duomenis ir ištriname tuos, kurių mums nereikia.
- ☑ Turime apibrėžti minimalų asmens duomenų kiekį, kurio reikia konkrečiam tikslui. Turime laikyti tik tiek duomenų, ne daugiau.

Atskaitomybės principas reiškia, kad turite galėti įrodyti, kad taikote reikiamus procesus, skirtus užtikrinti, jog renkate ir laikote tik jums būtinus asmens duomenis.

Taip pat atminkite, kad pagal BDAR asmuo turi teisę ištaisyti duomenis – papildyti neišsamius mūsų turimus jo duomenis, kurie nėra tinkami mūsų tikslui. Taip pat asmuo turi teisę ištrinti duomenis (būti pamirštas) – pareikalauti ištrinti bet kokius duomenis, kurie nėra būtini mūsų tikslui.

Mokome savo darbuotojus ir tobuliname vidaus procesus.



Duomenų saugumas

Kibernetinė sauga yra įvairialypė veikla, skirta užtikrinti galimybę dalintis duomenimis ir juos naudoti tinkamo lygio ir garantuotos informacijos bei turto apsaugos aplinkoje:

- **Konfidencialumas**: užtikrina, kad informacija išlieka konfidenciali ir neatskleidžiama pašaliniams fiziniams ar juridiniams asmenims;
- **Vientisumas**: užtikrina informacijos bei tvarkymo būdų tikslumą ir išsamumą;
- **Prieiga**: užtikrina, kad įgalioti naudotojai visuomet turi prieigą prie jiems reikiamos informacijos, programų ir paslaugų;
- **Atsekamumas**: gebėjimas registruoti veiksmus, kad prireikus būtų galima įrodyti, kaip informacija buvo tvarkyta mūsų sistemose. Atsekamumas taip pat apima teisinius tikslus, pvz., nepripažinimo ir atskaitomybės.

Asmeninės informacijos formos:

- Popieriniai dokumentai (tekstai, žemėlapiai, nuotraukos ir pan.);
- Skaitmeninė informacija biure;
- Skaitmeninė informacija mobiliajame prietaise;
- Profesiniai gebėjimai ir įgūdžiai (kurie priklauso asmenims arba kuriais dalijamasi žodžiu);
- Fiziniai daiktai (mėginiai, kamienai, modeliai ir pan.).

[DSUG006EN] Direktyva dėl kibernetinės saugos valdymo

Pseudonimizavimas yra asmens duomenų tvarkymo būdas, kai asmens duomenų nebeįmanoma priskirti konkrečiam duomenų subjektui be papildomos informacijos, su sąlyga, kad tokia papildoma informacija laikoma atskirai ir jai taikomos techninės bei organizacinės priemonės, skirtos užtikrinti, kad asmens duomenys nebūtų susieti su fiziniu asmeniu, kurio tapatybė yra žinoma arba gali būti nustatyta.

Anonimizavimas yra procesas, kurio metu asmens duomenys negrįžtamai pakeičiami tokiu būdu, kad **duomenų valdytojas**(1) atskirai ar kartu su kita šalimi nebegali tiesiogiai ar netiesiogiai nustatyti duomenų subjekto tapatybės.

Šifravimas yra duomenų apdorojimo būdas, kai tekstas ar kito formato duomenys konvertuojami iš skaitomos formos į šifruotą formą, kurią kita šalis gali iššifruoti tik jei turi šifravimo kodą. Šifravimas yra vienas iš svarbiausių duomenų apsaugos būdų, ypač apsaugant visišką tinklais siunčiamų duomenų saugumą.

(1): žr. apibrėžtį p. 38.

Mūsų įsitikinimai

Siekdama užtikrinti saugumą ir užkirsti kelią tvarkyti duomenis pažeidžiant duomenų apsaugos teisės aktų reikalavimus, „Roquette“ ir bendrovės subrangovai privalo įvertinti su tvarkymu susijusius pavojus bei taikyti jų mažinimo priemones, pvz., **šifravimą** arba **pseudonimizavimą**.

Mūsų pareigos

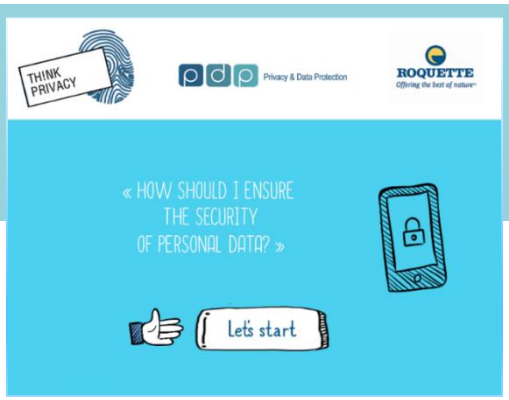
Tvarkydami visų rūšių asmens duomenis privalome taikyti jų apsaugos priemones, tačiau konkrečios priemonės priklauso nuo konkrečių aplinkybių. Privalome užtikrinti tvarkyti asmens duomenis naudojamų sistemų ir paslaugų konfidencialumą, integralumą ir prieigą prie jų.

Tai gali apimti informacijos apsaugos politikas, prieigos kontrolę, saugos stebėseną, atkūrimo planus ir pan.

Visi suinteresuoti asmenys privalo taikyti tinkamas apsaugos priemones visu asmens duomenų tvarkymo laikotarpiu.

Taisyklės	Q-Docs	BDAR
• Taikyti ir kontroliuoti saugos priemones, apibrėžtas saugos politikose ir direktyvose	DDPG007EN 1 taisyklė	32 str.
• Projektuose taikyti integruotas informacinės saugos ir duomenų apsaugos priemones.	DDPG007EN 2 taisyklė	32 str.
• Pritaikytoji ir standartizuotoji sauga, privatumo ir duomenų apsauga	DDPG007EN 3 taisyklė	25 str.
• Į sutartis su subrangovais įtraukti straipsnius dėl informacinės saugos ir duomenų apsaugos	DDPG007EN 4 taisyklė	32 str.

Mokome savo darbuotojus ir tobuliname vidaus procesus.



Asmeninė informacija Klasifikacija

Draudžiama tvarkyti neskelbtinus ir kai kurių kitų kategorijų asmens duomenis, išskyrus atskirus atvejus.

Vykdant tokį tvarkymą privaloma taikyti apsaugos priemones, skirtas:

duomenų žymėjimui, prieigai prie jų, perdavimui, gabenimui, kopijavimui ir spausdinimui, laikymui ir archyvavimui bei sunaikinimui.

Klasifikacija skirta nustatyti neskelbtinos informacijos išteklius, jos pobūdį ir laikymo formą bei, jei būtina, nurodyti apsaugos priemones, skirtas sumažinti riziką netyčinio atskleidimo atveju.

Konfidencialumo klasifikacija tiesiogiai susijusi su įvertintu netyčinio informacijos atskleidimo poveikiu.

[DSUG001EN] Informacijos apsaugos direktyva

Informacijos apsaugos klasifikacija	Asmens duomenų rūšys	Asmens duomenų kategorijos
1 lygis – RIBOTAM „ROQUETTE" NAUDOJIMUI Apibrėžtis: informacija, kurios nerekomenduojama atvirai ir plačiai paskleisti	Tradiciniai asmens duomenys	Šeiminė padėtis, tapatybė, tapatybės duomenys
		Asmeninis gyvenimas (įpročiai, santuokinė padėtis, išskyrus neskelbtinus duomenis)
		Profesinis gyvenimas (gyvenimo aprašymas, bendrasis ir profesinis išsilavinimas, pasiekimai)
		Ekonominė ir finansinė informacija (pajamos, finansinė padėtis, mokestinė padėtis)
		Ryšių duomenys (IP adresai, įvykių žurnalai)
		Buvimo vietos duomenys (kelionės, GPS duomenys, GSM duomenys)
2 lygis – „ROQUETTE" KONFIDENCIALI INFORMACIJA Apibrėžtis: informacija, kurią atskleidus galima ženkliai pakenkti Grupės interesams	Asmens duomenys, kurie laikomi neskelbtinais	Socialinio draudimo numeris
		Biometriniai duomenys
		Banko sąskaitos duomenys
3 lygis – „ROQUETTE" PASLAPTIS Apibrėžtis: informacija, kurią atskleidus galima stipriai pakenkti Grupės interesams	Neskelbtini asmens duomenys pagal Duomenų apsaugos įstatymą	Politinės pažiūros, religiniai ir filosofiniai įsitikinimai, narystė profesinėse sąjungose, lytinis gyvenimas, sveikatos, rasinės ar etninės kilmės duomenys
		Apkaltinamieji nuosprendžiai, nusikalstamos veikos, saugumo priemonės

Mūsų pareigos

Taisyklės	Q-Docs	BDAR
• Laikytis neskelbtinų duomenų tvarkymo teisinių reikalavimų	DDPG004EN 1 taisyklė	9 str.
• Draudžiama tvarkyti baudžiamųjų nuosprendžių ir nusikaltimų duomenis	DDPG004EN 2 taisyklė	10 str.
• Apriboti prieigą prie sveikatos duomenų – juos gali tvarkyti tik įgalioti asmenys	DDPG004EN 3 taisyklė	9 str.
• Draudžiama naudoti nacionalinį asmens kodą kaip unikalų identifikacinį numerį	DDPG004EN 4 taisyklė	87 str.
• Apriboti prieigą prie bankinių duomenų ir jų naudojimą	DDPG004EN 5 taisyklė	9 str.
• Apriboti prieigą prie neskelbtinų duomenų – juos gali tvarkyti tik įgalioti asmenys	DDPG004EN 6 taisyklė	9 str.
• Atlikti poveikio duomenų subjektų, kurių neskelbtini duomenys tvarkomi, privatumui vertinimą	DDPG004EN 7 taisyklė	35 str.
• Pastabų lauką naudoti tik bendro pobūdžio informacijai	DDPG004EN 8 taisyklė	Geriausia praktika

Praktiniai patarimai

Apsaugos priemonių, kurių būtina imtis kiekvienai klasifikuotos informacijos šaltinių kategorijai (popierinė, skaitmeninė, žinios, fizinė), pavyzdžiai.

Duomenų saugojimo laikotarpis

Dėl vis didėjančio poreikio skaitmeninti veiklą ir keitimąsi informacija Grupės viduje, su mūsų klientais ir verslo partneriais, taip pat dėl teisinių ir norminių reikalavimų „Roquette“ privalo laikytis tam tikrų duomenų saugojimo laikotarpio ir jos įrašų valdymo prievolių.

Dėl bendrovės veiklos specifikos „Roquette“ renka ir tvarko didelius neskelbtinų duomenų kiekius. Šie duomenys yra susiję su mūsų strategija, finansiniais rezultatais, komercine veikla ar įsipareigojimais, **taip pat tai yra mūsų klientų, verslo partnerių ir darbuotojų asmens duomenys**.

Informacija, kurią „Roquette“ perduoda ar gauna veiklos metu, turi būti saugoma mažiausią numatytą saugojimo laikotarpį, nors niekas nedraudžia jų laikyti ir ilgiau, **išskyrus atvejus, kai tokioje informacijoje yra asmens duomenų**.

Šio laikotarpio, kurio metu administracinės ir kompetentingos institucijos gali atlikti tikrinimus, trukmė gali skirtis ir priklauso nuo saugomos informacijos pobūdžio bei galiojančių teisinių reikalavimų.

Draudžiama saugoti informaciją neribotą ar nenustatytą laiką.

BDAR 5 str. 1 d. e)

saugojimo apribojimas

Asmens duomenys laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi.

Asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves.

Mūsų pareigos

- Kaip duomenų valdytoja, bendrovė „Roquette“ privalo kiekvienai renkamų ir tvarkomų asmens duomenų kategorijai nustatyti konkretų ir tinkamą saugojimo laikotarpį.
- Prieš pradėdamas tvarkyti asmens duomenis, projekto savininkas kartu su duomenų apsaugos koordinatoriumi privalo mūsų registre nustatyti duomenų saugojimo laikotarpį.
- Privalome saugoti duomenis tik tiek laiko, kiek būtina jų tvarkymui, taip pat laikytis galiojančių teisės aktų.

Taisyklės	Q-Docs	BDAR
• Duomenis laikyti ne ilgiau, nei tai būtina	DDPG002EN 5 taisyklė	5 str. 1 d. e)

Šiuo atžvilgiu Grupės funkcijos, GBU ir regionai privalo laikytis Grupės informacijos saugojimo trukmės taisyklių bei palaikyti susijusias procedūras darbinėje būsenoje.

Pavyzdys

Pasibaigus darbuotojo įdarbinimo procesui privalome ištrinti nesėkmingų kandidatų informaciją, nebent jie davė sutikimą saugoti ją mūsų duomenyne ribotą laikotarpį (2 m.).

Mokome savo darbuotojus ir tobuliname vidaus procesus.

2 Mūsų SANTYKIŲ SU PARTNERIAIS IR SUBRANGOVAIS principai

Duomenų tvarkytojo ir valdytojo kvalifikacijos

Duomenų valdytojas yra fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri viena ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones.

Bendras duomenų valdytojas yra du ar daugiau duomenų valdytojų, kurie kartu nustato duomenų tvarkymo tikslus ir priemones. Tačiau neatsižvelgiant į jų susitarimus, kiekvienam duomenų valdytojui pagal BDAR taikoma atsakomybė.

Duomenų tvarkytojas yra fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis.

Kaip Bendrasis duomenų apsaugos reglamentas apibrėžia duomenų tvarkytoją?

(BDAR 4 straipsnis – Apibrėžtys).

Teisine sąvokos prasme **duomenų tvarkytoju gali būti labai įvairūs paslaugų teikėjai**. Duomenų tvarkytojo veikla gali būti susijusi su labai konkrečia užduotimi (pašto pristatymo subrangovas) arba jo veikla gali būti bendresnio ir platesnio pobūdžio (visos paslaugos valdymas kitos organizacijos vardu, pvz., darbuotojų atlyginimo apskaičiavimo paslauga).

BDAR ypač aktualus tokių sričių įmonėms:

- IT paslaugų (prieglobos, priežiūros ir pan.), programinės įrangos integravimo, kibernetinės saugos ir IT konsultacijų (anksčiau jos vadintos IT inžinerinių paslaugų įmones) įmonėms, turinčioms prieigą prie duomenų;
- rinkodaros ir komunikacijos agentūroms, kurios tvarko asmens duomenis klientų vardu; ir
- apskritai bet kokiai organizacijai, teikiančiai paslaugą, apimančią asmens duomenų tvarkymą kitos organizacijos vardu;
- taip pat valdžios institucijoms ar asociacijoms.

BDAR nuostatos netaikomos programinės įrangos kūrėjams ir įrangos (laiko registravimo, biometrinės ar medicininės ir pan.) gamintojams, jei jie negauna prieigos prie asmens duomenų arba jų netvarko.

Duomenų tvarkytojo ir duomenų valdytojo kvalifikacijos pavyzdys

Įmonė A teikia rinkodaros laiškų pristatymo paslaugą naudodama įmonių B ir C klientų duomenų failus.

Įmonė A yra duomenų tvarkytoja įmonių B ir C atžvilgiu, jei ji tvarko būtinus klientų duomenis, kad galėtų siųsti laiškus įmonių B ir C vardu ir pagal jų nurodymus.

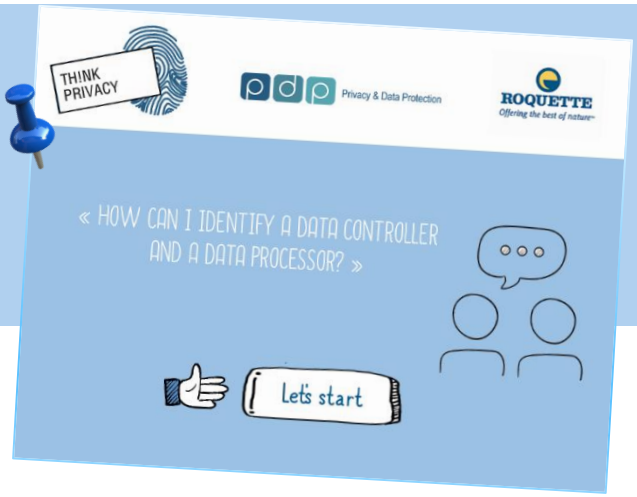
Įmonės B ir C yra jų klientų valdymo valdytojai, įskaitant rinkodaros laiškų pristatymą.

Įmonė A taip pat yra duomenų valdytoja, nes valdo savo darbuotojus ir savo klientus, įskaitant įmones B ir C.

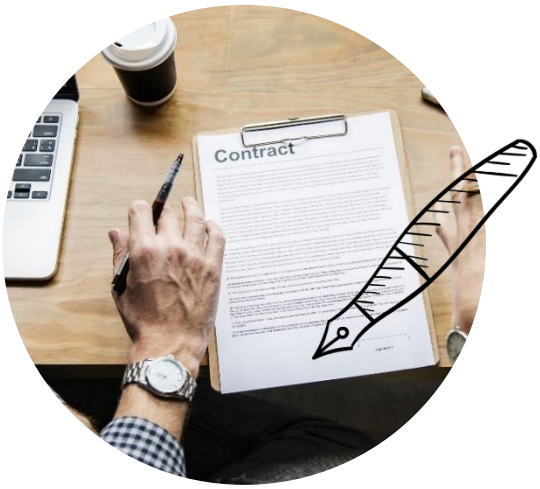
Oficialus tekstas

- BDAR 4 straipsnis: duomenų tvarkytojo ir duomenų valdytojo apibrėžtys
- BDAR 28 straipsnio 10 dalis: kada duomenų tvarkytojas laikomas duomenų valdytoju

Mokome savo darbuotojus ir tobuliname vidaus procesus.



Sutarties straipsniai dėl duomenų apsaugos



Kada būtina sutartis ir kodėl ji svarbi?

Visuomet, kai mes, kaip duomenų valdytojas, naudojamės duomenų tvarkytojo paslaugomis tvarkyti asmens duomenis mūsų vardu, tarp abiejų šalių būtina pasirašyti sutartį.
Turėti sutartį svarbu, kad abi šalys tiksliai suprastų mūsų pareigas ir atsakomybę.

Sutartys su duomenų apsaugai skirtais straipsniais ar susitarimu dėl duomenų apsaugos tarp „Roquette“, kaip duomenų valdytojo, ir duomenų tvarkytojų užtikrina, kad abi šalys supranta savo prievoles, pareigas ir atsakomybę. Sutartys taip pat leidžia mums laikytis BDAR reikalavimų bei padeda mums įrodyti asmenims bei priežiūros institucijoms, kad mes laikomės pagal atskaitomybės principą privalomų atitikties reikalavimų.

Kokias pareigas ir atsakomybę turime kaip duomenų valdytojas, kai naudojamės duomenų tvarkytojo paslaugomis?

Galime naudotis tik tokių duomenų tvarkytojų paslaugomis, kurie gali suteikti pakankamą įrodymą, kad jie įgyvendins tinkamas technines ir organizacines priemones, kurios užtikrins, jog duomenys bus tvarkomi laikantis BDAR reikalavimų bei apsaugant duomenų subjektų teises.

Kaip duomenų valdytojas, visų pirma mes atsakome už bendrą BDAR ir kitų galiojančių duomenų privatumo teisės aktų reikalavimų laikymąsi bei tokios atitikties įrodymą. Jei nepajėgiame to pasiekti, mums gali tekti padengti teismo priteistus nuostolius, mums gali būti skirtos baudos ar kitos sankcijos arba taisomosios priemonės.

Kas naujo yra BDAR?

Pagal BDAR rašytinė sutartis tarp duomenų valdytojo ir duomenų tvarkytojo tapo privaloma, o ne pasirenkama, kaip įrodymas, jog sutarties šalys laikosi galiojančių duomenų apsaugos teisės aktų numatytų duomenų apsaugos principų (taiko tinkamas apsaugos priemones).

Tokiose sutartyse turi būti numatytos konkrečios minimalios sąlygos. Šios sąlygos skirtos užtikrinti, kad duomenų tvarkytojo veiksmai atitinka visus BDAR reikalavimus, o ne tik tuos, kurie susiję su asmens duomenų apsauga.

Taisyklė	Q-Docs	BDAR
• Į sutartis su subrangovais įtraukti straipsnius dėl informacinės saugos ir duomenų apsaugos.	DDPG007EN 4 taisyklė	32 str.
• Subrangovų apsauga	DSUG016EN	

Ką būtina įtraukti į sutartis?

Sutartyse turi būti numatyta:

- ☑ duomenų tvarkymo atvejo dalykas ir trukmė;
- ☑ duomenų tvarkymo pobūdis ir tikslas;
- ☑ asmens duomenų rūšis ir duomenų subjektų kategorijos; ir
- ☑ duomenų valdytojo prievolės ir teisės.

Taip pat sutartyje turi būti numatytos konkrečios nuostatos ar sąlygos:

- ☑ duomenis tvarkyti tik laikantis dokumentuotų duomenų valdytojo nurodymų;
- ☑ išlaikyti konfidencialumą;
- ☑ taikyti tinkamas apsaugos priemones;
- ☑ dėl antrinių tvarkytojų paslaugų naudojimo;
- ☑ užtikrinti duomenų subjektų teises;
- ☑ padėti duomenų valdytojui;
- ☑ dėl sutarties pabaigos nuostatų; ir
- ☑ audito bei inspekcijų.

Mokome savo darbuotojus ir tobuliname vidaus procesus.

- Subrangovams skirtas duomenų apsaugos pagal BDAR reikalavimus vadovas.
- „Data Processing Agreement“ šabloną, kurį galima rasti mūsų „Privacy Management System“: OneTrust@Roquette > Vendor Risk Management modulis.

Sutartis dėl duomenų perdavimo

Duomenų perdavimas yra bet koks asmens duomenų perdavimas, kopijavimas ar tranzitas (pvz., per prieglobos serverius, priedų siuntimas el. paštu, nuotolinės prieigos įrankiai, ekrano bendrinimas ir pan.), skirtas perduoti duomenis tvarkyti į kitą valstybę, kurioje negalioja tokio paties lygio asmens duomenų apsaugos teisės aktų.

Šiuolaikinis pasaulis yra kaip niekada susijęs tarpusavyje. „Roquette“ veikia pasaulinėje rinkoje, todėl tarptautinis duomenų perdavimas yra svarbus mūsų kasdienės veiklos elementas. Pavyzdžiui, „Roquette“ saugo darbuotojų asmens duomenis naudodama debesijos paslaugas, kurios teikiamos iš užsienyje esančio serverio, bei dalijasi darbuotojų ir klientų asmens duomenimis tarp grupės įmonių, įsikūrusių įvairiose pasaulio šalyse.

Kokią įtaką BDAR ir kiti galiojantys duomenų apsaugos teisės aktai turi tokiam tarptautiniam duomenų perdavimui?

Mūsų pareigos

Bet koks tvarkomų ar tvarkyti skirtų asmens duomenų perdavimas į trečiąją valstybę ar tarptautinei organizacijai galimas tik jei:

- Vietos teisės aktai leidžia ir (arba) vietos priežiūros institucija nusprendė, kad trečioji valstybė, teritorija ar vienas ar keli konkretūs sektoriai trečiojoje valstybėje, arba konkreti tarptautinė organizacija užtikrina tinkamą apsaugos lygį arba suteikė leidimą; ir (arba)

- yra taikomos teisinės priemonės (pvz., įmonei privalomos taisyklės arba standartinės sutarčių sąlygos dėl asmens duomenų perdavimo duomenų tvarkytojams, įsikūrusiems trečiosiose valstybėse pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB ir pan.).

Taisyklė	Q-Docs	BDAR
• Perkeliant asmens duomenis į trečiąsias valstybes ar tarptautines organizacijas imtis reikiamų apsaugos priemonių	DDPG002EN 6 taisyklė	44–50 str.

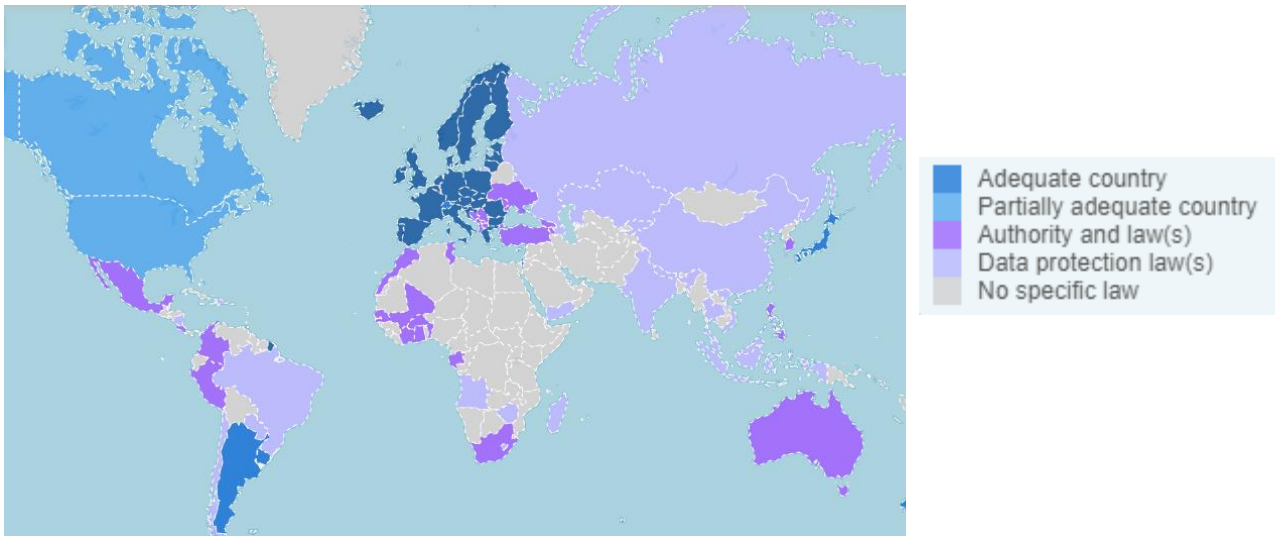
Bet kokiu atveju iš pradžių visuomet kreiptis į DAP.

Į kurias šalis galiu perduoti asmens duomenis ir kokiomis sąlygomis?

Išsamiau žr. žemėlapyje:

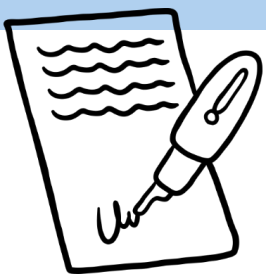
https://www.cnil.fr/en/data-protection-around-the-world.

Šiame žemėlapyje susipažinsite su duomenų apsaugos lygiu visose šalyse.



Sužinokite daugiau

- „Data Transfert Agreement“ skyriuje, įskaitant mūsų „Data Processing Agreement“ šablonas.
- DUK, skirti klausimams, kurie gali kilti įsiteisėjus ES Komisijos sprendimui dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams.



3 Mūsų SANTYKIŲ SU PROFESINIU TINKLU IR PRIEŽIŪROS INSTITUCIJOMIS principai

Duomenų apsaugos pareigūnas

Grupė yra paskyrusi duomenų apsaugos pareigūną.

Duomenų apsaugos pareigūnas (DAP) padeda mums stebėti vidinę atitiktį, informuoja ir pataria dėl mūsų duomenų apsaugos prievolių, teikia rekomendacijas dėl poveikio duomenų apsaugai vertinimo (PDAV) bei yra kontaktinis asmuo duomenų subjektams ir priežiūros institucijoms.

DAP turi būti nepriklausomas duomenų apsaugos srities specialistas ir turėti reikiamų išteklių. Jis yra pavaldus aukščiausiajai Grupės vadovybei.

DAP gali padėti mus įrodyti, kad laikomės visų reikalavimų; jis padeda skirti reikiamą dėmesį atskaitomybei.

DAP užduotys	Q-Docs	BDAR
• Mūsų DAP pareigos: kontroliuoti, kaip mes laikomės BDAR ir kitų duomenų apsaugos teisės aktų reikalavimų, mūsų duomenų apsaugos politikų, skatinti darbuotojų sąmoningumą šioje srityje, organizuoti mokymus ir auditą.	MDPG001EN Asmens duomenų apsaugos vadovas	BDAR 39 straipsnis Duomenų apsaugos pareigūno pareigos
• Mes atsižvelgiame į mūsų DAP rekomendacijas ir jo teikiamą informaciją apie mūsų duomenų apsaugos prievoles.		
• Atlikdami PDAV, turime kreiptis rekomendacijų į DAP, kuris taip pat stebi PDAV procesą.		
• Mūsų DAP yra kontaktinis asmuo priežiūros institucijoms.		
• Vykdydamas savo pareigas, DAP tinkamai įvertina pavojų, susijusį su duomenų tvarkymo veiksmais, ir atsižvelgia į tvarkymo pobūdį, apimtį, kontekstą ir tikslus.		

2018 m. gegužės 25 d., BDAR įsigaliojimo dieną, Grupės generalinis direktorius informavo CNIL, kad Grupėje pradėjo eiti pareigas DAP.

Kaip kreiptis į DAP

- Į mūsų duomenų apsaugos pareigūnę Jennifer Godin gali kreiptis visi darbuotojai, kiti asmenys ir priežiūros institucijos.
- DAP kontaktinė informacija yra paskelbta viešai bei perduota priežiūros institucijoms.

  ☑ https://www.Roquette.com/data-protection
  ☑ ONE > Visuotinė funkcija > Duomenų apsauga
  ☑ ONE > Mūsų bendruomenė > Duomenų apsaugos tinklas

Kreipkitės į DAP tokiais klausimais:

☑ Asmens duomenų tvarkymas

☑ Duomenų subjektų prašymai

☑ Asmens duomenų pažeidimas

☑ Reikia patarimo ar pagalbos

Kreiptis adresu: dpo@Roquette.com arba jennifer.godin@Roquette.com

Mokome savo darbuotojus ir tobuliname vidaus procesus.

Duomenų apsaugos tinklas

Atstovai skyriuose ir vietiniai DAP arba koordinatoriai sudaro tinklą, kuris leidžia Grupės duomenų apsaugos pareigūnui įgyvendinti asmens duomenų apsaugos taisykles kiekviename verslo padalinyje bei padėti skyriui laikytis galiojančių asmens duomenų apsaugos teisės aktų reikalavimų valstybėse, kurioje Grupė vykdo veiklą.

Vietinių DAP ir koordinatorių pareigos apima:

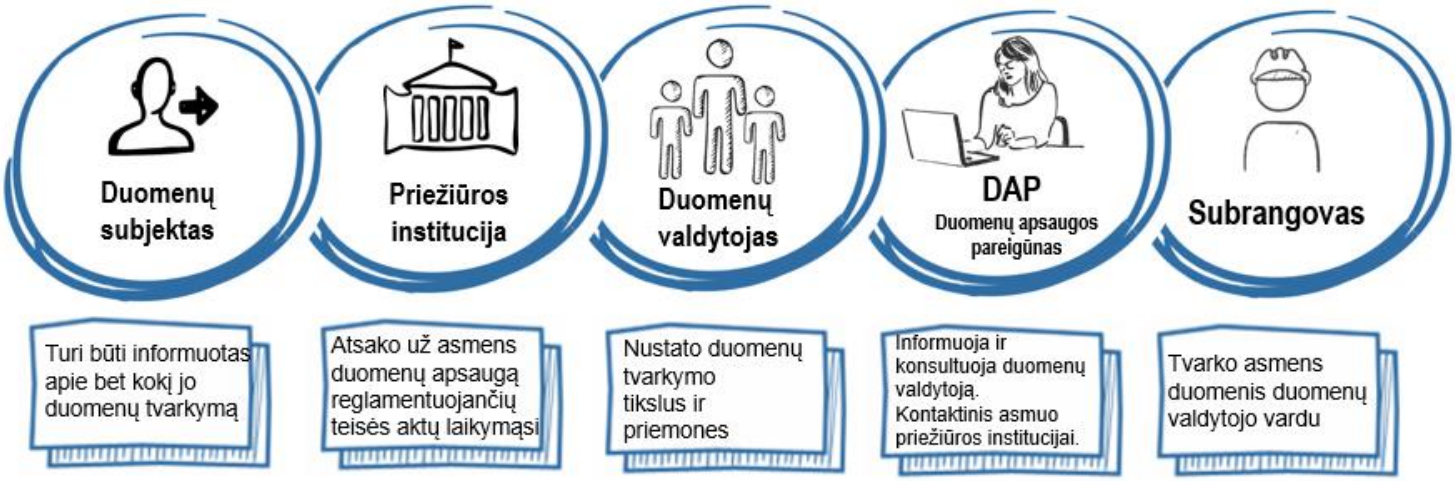
- Informuoti ir patarti dėl prievolių, susijusių su „Roquette“ asmens duomenų apsaugos politika, kurią nustato „Roquette Group“ DAP, bei galiojančių vietos asmens duomenų apsaugos teisės aktų;
- Stebėti, kaip laikomasi vietos ir kitų galiojančių asmens duomenų apsaugos teisės aktų, padedant „Roquette Group“ DAP, bei asmens duomenų apsaugos politikų;
- Paprašius vietoje konsultuoti dėl poveikio duomenų apsaugai vertinimo ir stebėti jo atlikimą;
- Bendradarbiauti su vietine priežiūros institucija;
- Būti kontaktiniu asmeniu „Roquette Group“ DAP klausimais, susijusiais su duomenų tvarkymu, taip pat, jei reikia, konsultuoti „Roquette Group“ DAP kitais klausimais;
- Atsiskaityti už savo veiklą „Roquette Group“ DAP bei prisidėti prie Grupės duomenų apsaugos valdymo sistemos tobulinimo.

Mokome savo darbuotojus ir tobuliname vidaus procesus.

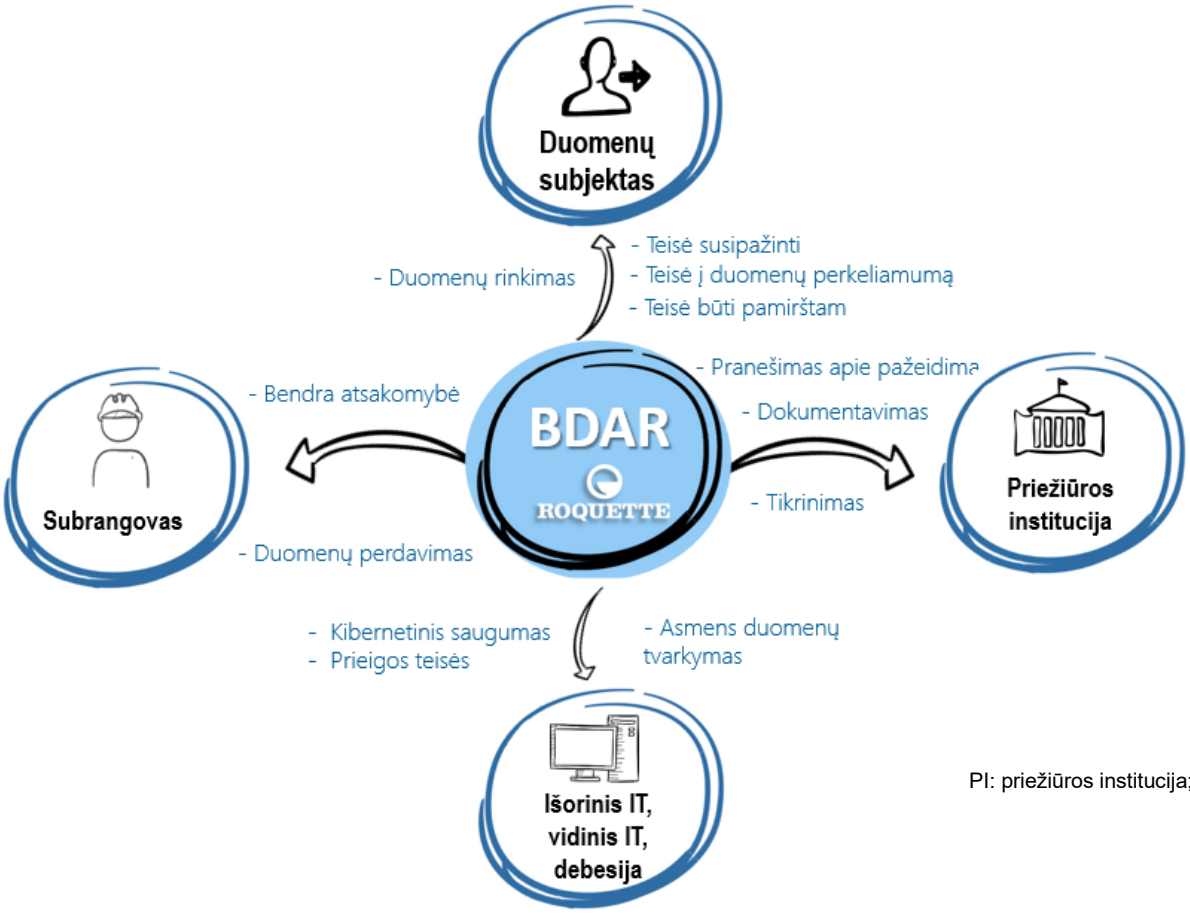
Kasmetiniame PDP seminare susitinka mūsų duomenų apsaugos ir privatumo srityje dirbantys asmenys.

ir suinteresuoti asmenys

Kas yra naujieji žaidėjai?



Koks yra santykis tarp šių suinteresuotų asmenų?



PI: priežiūros institucija; žr. p. 50

Priežiūros institucijos

Daugelyje šalių galioja duomenų apsaugos teisės aktai bei veikia nepriklausoma

duomenų apsaugos agentūra (DAA).

Tai yra nepriklausomos nacionalinės priežiūros institucijos, kurių pareigos yra užtikrinti asmens privatumą ir informacijos laisvę. Jos skatina ir užtikrina duomenų subjektų teisę susipažinti su organizacijų turima su jais susijusia informacija bei teisę į asmeninės informacijos apsaugą.

Koks yra priežiūros institucijos vaidmuo pagal BDAR?

Kiekviena valstybė narė užtikrina, kad viena arba kelios nepriklausomos valdžios institucijos yra atsakingos už šio reglamento taikymo stebėseną, kad būtų apsaugotos fizinių asmenų pamatinės teisės ir laisvės tvarkant duomenis bei sudarytos palankesnės sąlygos laisvam asmens duomenų judėjimui ES.

Pagal BDAR visos ES valstybės narės yra įsteigusios duomenų apsaugos tarnybą, kuri yra pagrindinė kontaktinė vieta visiems valstybės narės suinteresuotiems asmenims.

Siekiant, kad BDAR būtų nuosekliai taikomas visoje ES, visos priežiūros institucijos privalo bendradarbiauti tarpusavyje bei su Europos Komisija.

Kiekviena priežiūros institucija savo teritorijoje privalo skatinti visuomenės informavimą apie su duomenų tvarkymu susijusius pavojus, taisykles, apsaugos priemones ir teises bei jų supratimą.

Taip pat į jas galima kreiptis duomenų apsaugos teisės aktų pažeidimo atveju arba siekiant patarimo konkrečiais klausimais ir (arba) pagalbos organizacijų veikloje.

Priežiūros institucijos (PI) funkcijos trumpai:

- Užtikrinti taisyklių laikymąsi, taip pat ir skiriant baudas,
- Jei reikia, aiškinti taisyklių taikymą, pvz., teikiant rekomendacijas,
- Skatinti dialogo kultūrą su visais suinteresuotais asmenimis, įskaitant verslo įmones,
- Bendradarbiauti.

CNIL: Commission Nationale de l'Informatique et des Libertés (Prancūzijos duomenų apsaugos agentūra).

Vadovaujanti institucija

- Duomenų valdytojo ar duomenų tvarkytojo pagrindinės buveinės priežiūros institucija turėtų veikti kaip vadovaujanti institucija Ji turėtų bendradarbiauti su kitomis susijusiomis institucijomis.

- Nustatyti vadovaujančią instituciją svarbu tik tuomet, kai duomenų valdytojas arba duomenų tvarkytojas vykdo tarpvalstybinį asmens duomenų tvarkymą.

Kaip nustatyti vadovaujančią instituciją?

Nustatykite pagrindinio duomenų valdytojo būstinės vietą ES.
Šalies, kurioje įsikūrusi pagrindinio duomenų valdytojo būstinė, priežiūros institucija yra duomenų valdytojo vadovaujanti institucija.

CNIL *yra „Roquette“ vadovaujanti institucija*

Kaip BDAR sankcijų mechanizmas veikia praktikoje?

Valdymas

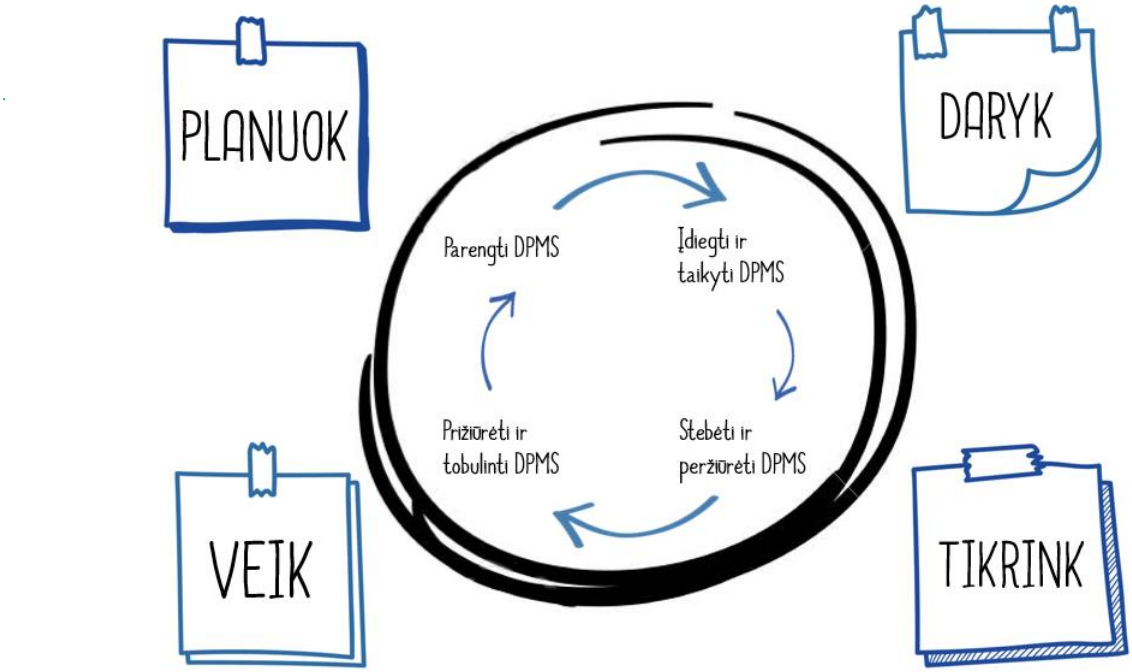
„**Duomenų apsaugos veiksmų organizavime** pagrindiniai veikėjai yra duomenų apsaugos pareigūnas, įmonės duomenų apsaugos koordinatoriai, generalinis direktorius kaip duomenų valdytojas, Grupės funkcijų vadovai, kurie yra atsakingi už asmens duomenų tvarkymo veiklą, ir subrangovai kaip duomenų tvarkytojai.“ [MDPG001EN]

Vadovaudamiesi proceso principu kuriame, diegiame, eksploatuojame, stebime, kontroliuojame, prižiūrime ir tobuliname „Roquette“ asmens duomenų apsaugos valdymo sistemą (**D**ata **P**rotection **M**anagement **S**ystem, **DPMS**).

Asmens duomenų apsaugos valdymo procesas ir metodas skatina jo naudotojus atkreipti dėmesį į šių klausimų svarbą:

1) suprasti „Roquette“ duomenų apsaugos reikalavimus ir būtinybę rengti duomenų apsaugos direktyvas ir procedūras;
2) diegti ir naudoti „Roquette“ duomenų apsaugos pavojų valdymo priemones atsižvelgiant į bendrą „Roquette“ verslo riziką;
3) stebėti ir kontroliuoti DPMS veiklos rezultatus ir efektyvumą; ir
4) nuolat tobulinti procesą atliekant objektyvių rodiklių vertinimą.

Mes taikome „Planuok, daryk, tikrink,veik“ (PDTV) modelį, kuris taikomas kuriant visus duomenų apsaugos valdymo sistemos (DPMS) procesus.



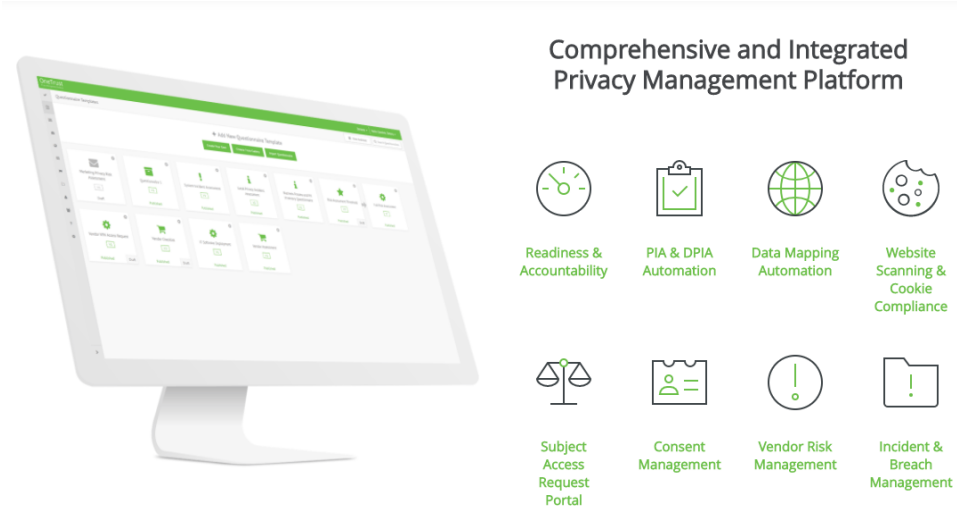
Mūsų požiūris

Svarbiausi mūsų BDAR atitikties programos akcentai:

- suprasti, kaip mūsų organizacija laikydamasi reikalavimų renka, saugo, naudoja ir perduoda duomenis;
- sukurti reikalavimų laikymosi kultūrą mūsų organizacijoje;
- atlikti poveikio privatumui vertinimą;
- pasiruošti duomenų saugumo pažeidimams;
- skirti išteklių Privatumo programai;
- taikyti duomenų apsaugos valdymo sistemą („Planuok, daryk, tikrink, veik“).

Siekdami šių tikslų ir vykdydami Programą, mes:

- parengėme Duomenų apsaugos politiką ir susijusias rekomendacijas bei dokumentaciją;
- įvykdėme BDAR atitikties projektą, skirtą patikrinti tvarkymą, valdyti duomenų saugumo pažeidimus, patikrinti sutartis ir jų sąlygas dėl duomenų apsaugos, duomenų perdavimo sutartis ir pan.;
- įdiegėme privatumo valdymo programinę įrangą, atitinkančią BDAR reikalavimus.



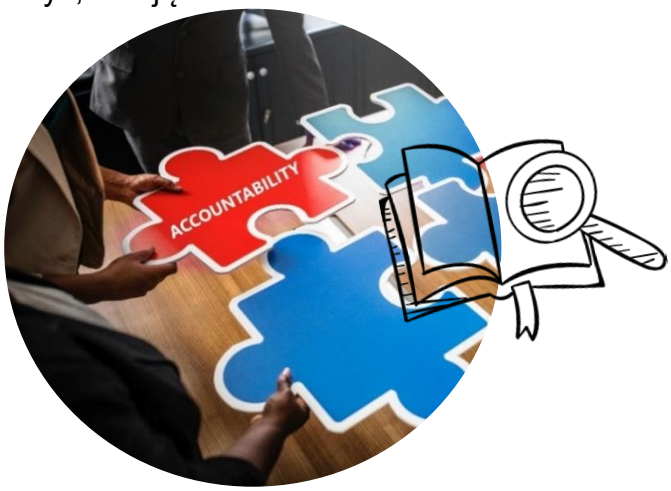
Pagrindinės šios valdymo platformos savybės:

- duomenų tvarkymo registras (duomenų atvaizdis);
- su tvarkymu susijusios rizikos valdymas (atliekant poveikio privatumui vertinimą ir pan.);
- prašymų ir teisių (susipažinti, ištaisyti, prieštarauti duomenų tvarkymui ir pan.) valdymas;
- incidentų ir duomenų saugumo pažeidimų valdymas;
- atitikties dokumentacijos valdymas.

Atskaitomybė

Atskaitomybė yra vienas iš duomenų apsaugos principų. Pagal jį esame atsakingi už BDAR reikalavimų laikymąsi ir privalome galėti įrodyti, kad jų laikomės.

Kodėl atskaitomybė svarbi?



Būdami atsakingi už tai, ką darome su asmens duomenimis, ir galėdami parodyti priemones, kurių ėmėmės siekdami užtikrinti asmenų teises, ne tik galime geriau laikytis reikalavimų, bet ir įgyjame konkurencinį pranašumą. Atskaitomybė suteikia palankią galimybę parodyti ir įrodyti, kad gerbiame žmonių privatumą. Tai padeda mums kurti ir stiprinti žmonių pasitikėjimą mumis.

Be to, kam nors atsitikus ir parodžius, kad mes aktyviai vertinome pavojus bei pritaikėme reikiamas apsaugos priemones, galime sušvelninti mums gresiančias galimas neigiamas pasekmes. Kita vertus, jei negalime parodyti, kad nuoširdžiai stengiamės tinkamai apsaugoti asmens duomenis, mums gali grėsti baudos ir žala reputacijai.

Kaip konkrečiai reikia laikytis atskaitomybės principo?

Asmens duomenų tvarkymas apima prievolę atsakingai tvarkyti duomenis ir imtis konkrečių priemonių juos apsaugoti. Laikytis atskaitomybės principo reiškia:

- tinkamai dokumentuoti ir komunikuoti visas su privatumu susijusias direktyvas, procedūras ir praktiką (mūsų Politika);
- paskirti organizacijoje už Politikos vykdymą atsakingą asmenį (kuris, jei reikia, gali perduoti šią pareigą kitiems organizacijos nariams);
- perduodant duomenis tretiems asmenims užtikrinti, kad gavėjas bus įpareigotas sutartimi ar kitais būdais, pvz., privalomomis vidaus taisyklėmis, užtikrinti tokį patį privatumo ir duomenų apsaugos lygį (galiojančiuose teisės aktuose gali būti numatyta papildomų reikalavimų tarptautinio duomenų perdavimo srityje);
- tinkamai išmokyti duomenų valdytojo darbuotojus, kurie turi prieigą prie asmens duomenų;
- sukurti veiksmingą skundų pateikimo ir sprendimo vidaus tvarką, skirtą naudoti duomenų subjektams;

- informuoti duomenų subjektus apie privatumo pažeidimus, dėl kurių jie gali patirti didelę žalą (nebent tai daryti būtų draudžiama, pvz., bendradarbiaujant su teisėsauga), bei priemones, kurių imtasi siekiant pašalinti pažeidimų padarinius;

- pranešti visiems reikiamiems suinteresuotiems asmenims apie privatumo pažeidimus, kaip to reikalaujama kai kuriose jurisdikcijose (pvz., už duomenų apsaugą atsakingoms institucijoms) ir atsižvelgiant į rizikos lygį;

- leisti nukentėjusiam duomenų subjektui pasinaudoti tinkamomis ir veiksmingomis sankcijomis ir (arba) kompensacinėmis priemonėmis, pvz., privatumo pažeidimo atveju, ištaisyti, ištrinti ar atkurti duomenis; ir

- apgalvoti tvarką, kaip kompensuoti situacijose, kuriose būtų sunku ar neįmanoma atkurti pradinę fizinio asmens privatumo būseną, tarsi nieko nebūtų nutikę.

Kontrolinis sąrašas

- ☑ Mes prisiimame atsakomybę laikytis BDAR reikalavimų aukščiausios grandies vadovų ir visos organizacijos lygiu.
- ☑ Mes saugome savo veiksmų, skirtų laikytis BDAR reikalavimų, įrodymus.

Mes turime ir taikome tinkamas technines ir organizacines priemones, pavyzdžiui:

- ☑ tvirtiname ir taikome duomenų apsaugos taisykles;
- ☑ laikomės pritaikytosios ir standartizuotosios duomenų apsaugos principų – taikome tinkamas duomenų apsaugos priemones viso duomenų tvarkymo proceso metu;
- ☑ pasirašome sutartis su organizacijomis, kurios tvarko asmens duomenis mūsų vardu;
- ☑ dokumentuojame savo tvarkymo veiksmus;
- ☑ taikome tinkamas apsaugos priemones;
- ☑ registruojame asmens duomenų pažeidimus ir, jei reikia, pranešame apie juos;
- ☑ atliekame poveikio duomenų apsaugai vertinimą, jei naudojant asmens duomenis gali kilti didelis pavojus asmens interesams;
- ☑ paskiriame duomenų apsaugos pareigūną; ir
- ☑ laikomės atitinkamų elgesio kodeksų nuostatų bei dalyvaujame sertifikavimo programose (jei įmanoma).

- ☑ Mes tinkamais intervalais peržiūrime ir atnaujiname atskaitomybės priemones.

Dokumentavimas

Kas yra dokumentavimas?

Mes privalome registruoti visus savo duomenų tvarkymo veiksmus, įskaitant tvarkymo tikslus, duomenų perdavimą ir saugojimo laikotarpius. Tai vadiname **dokumentavimu**.

Dokumentuoti savo duomenų tvarkymo veiksmus svarbu ne tik dėl to, kad privalome tai daryti pagal įstatymus, bet ir dėl to, kad tokiu būdu galime, jei reikia, įrodyti, kad laikomės gerų valdymo principų, BDAR bei kitų galiojančių duomenų apsaugos teisės aktų reikalavimų.

Kontrolinis sąrašas

Duomenų tvarkymo veiksmų dokumentavimas: reikalavimai

- ☑ Būdami tvarkomų duomenų valdytoju, mes dokumentuojame visą reikiamą informaciją pagal BDAR 30 straipsnio 1 dalies nuostatas.
- ☑ Duomenų tvarkymo veiksmus dokumentuojame raštu.
- ☑ Mes dokumentuojame visus atskirus tvarkymo veiksmus, kartu parodydami loginį ryšį tarp skirtingų informacijos fragmentų.
- ☑ Mes reguliariai peržiūrime mūsų tvarkomus asmens duomenis ir atitinkamai atnaujiname savo dokumentaciją.

Duomenų tvarkymo veiksmų dokumentavimas: geriausia praktika

- ☑ Mes dokumentuojame savo tvarkymo veiksmus elektronine forma, kad galėtume lengvai papildyti, pašalinti ar pakeisti informaciją.

Rengdamiesi dokumentuoti tvarkymo veiksmus, mes:

- ☑ atliekame informacijos auditą, kad sužinotume, kokius asmens duomenis mūsų organizacija turi;
- ☑ naudodami skaitmeninius, saugos ir privatumo įrankius atliekame apklausas bei bendraujame su darbuotojais visoje organizacijoje, kad susidarytume kuo išsamesnį mūsų asmens duomenų tvarkymo vaizdą; ir
- ☑ peržiūrime savo politikas, direktyvas, tvarkas, sutartis ir susitarimus, kad racionaliai spręstume duomenų saugojimo laikotarpio, saugumo ir perdavimo klausimus.

Registruodami duomenų tvarkymo veiksmus, mes dokumentuojame arba susiejame juos su tokiais dokumentais:

- ☑ informacija, kurios reikia pranešimams apie privatumą;
- ☑ sutikimas dėl duomenų tvarkymo (jei reikia);
- ☑ duomenų valdytojo ir duomenų tvarkytojo sutartimis;
- ☑ asmens duomenų vieta;
- ☑ poveikio duomenų apsaugai vertinimo ataskaitos; taip pat
- ☑ įrašus apie asmens duomenų pažeidimus;
- ☑ įrašus apie duomenų subjektų prašymus.

Kur yra mūsų dokumentacija apie duomenų apsaugą?

ONE
Globali funkcija
Duomenų apsauga

Privacy & Data Protection

„Duomenų apsauga yra aktuali kiekvienam mūsų organizacijos nariui ir kiekvienas narys yra už ją atsakingas“

Turinys

- Teisės aktai
- Informacija ir sąmoningumas
- Geriausia praktika ir politikos

ONE
Bendruomenė
Duomenų apsaugos tinklas

Data Protection Network

„Asmens duomenų apsauga priklauso nuo mūsų visų“

Turinys

- Asmens duomenų apsaugos politika
- Duomenų apsaugos valdymo sistema
- Šalies teisės aktai
- Žmogiškieji ištekliai
- Visuotinis skaitmeninimas
- Legal & Compliance
- Internal Audit & Control
- GBU ir Komercija
- Inovacijos, R&D
- Visuotinė sauga
- Draudimas ir rizikos valdymas

OneTrust
Privatumo valdymo programa

OneTrust
Privacy Management Software
@ ROQUETTE

„Mūsų privatumo valdymo programa, skirta privatumo apsaugai ir trečiųjų šalių rizikos valdymui“

Moduliai

Data Mapping Automation

PIA & DPIA Automation

Subject Access Request Portal

Incident & Breach Management

KULTŪRA

ATITIKTIS

ATSKAITOMYBĖ

Poveikio privatumui vertinimas

Poveikio privatumui vertinimo (PPV) procesas skirtas aprašyti duomenų tvarkymą, įvertinti jo būtinybę ir proporcingumą bei padėti valdyti pavojų, kuris gali kilti fizinių asmenų teisėms ir laisvėms dėl jų asmens duomenų tvarkymo įvertinant ir nustatant apsaugos priemones.

Santrumpa PPV naudojama įvardyti ir **poveikio privatumui vertinimą**, ir **poveikio duomenų apsaugai vertinimą** (**PDAV**).

Kaip yra atliekamas PPV?

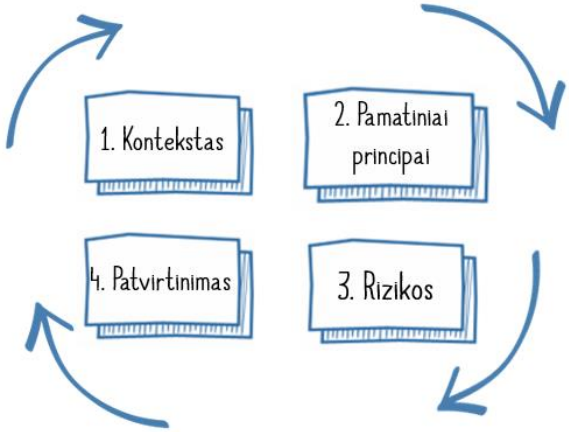
Atitikties principas, įgyvendinamas atliekant PPV, pagrįstas dviem ramsčiais:

1) **pamatinėmis teisėmis ir principais**, kurie yra besąlyginiai, įtvirtinti įstatymų ir kurių privaloma laikytis neatsižvelgiant į pavojaus pobūdį, sunkumą ir tikimybę;
2) **pavojaus duomenų subjekto privatumui valdymu**, kuris apibrėžia tinkamas technines ir organizacines duomenų apsaugos priemones.

Atitikties metodas naudojant PPV

Trumpai tariant, norint atlikti PVV, būtina:

1) apibrėžti ir aprašyti konkrečių asmens duomenų tvarkymo kontekstą;
2) atlikti saugiklių, skirtų užtikrinti pamatinių principų – tvarkymo proporcingumo ir būtinybės bei duomenų subjektų teisių apsaugos – reikalavimų laikymąsi, analizę;
3) įvertinti pavojų privatumui, susijusį su duomenų saugumu, ir užtikrinti, kad į juos būtų tinkamai atsižvelgta;
4) formaliai dokumentuoti PPV validumą atsižvelgiant į ankstesnius faktus arba nuspręsti peržiūrėti ankstesnius žingsnius.



Bendri PPV atlikimo principai

Tai yra nuolatinio tobulinimo procesas, todėl kartais gali prireikti kelių bandymų, kad pavyktų parengti priimtiną privatumo apsaugos sistemą. Taip pat būtina nuolat stebėti pokyčius (konteksto, valdymo priemonių, pavojų ir pan.), pavyzdžiui, kasmet, ir atnaujinti sistemą įvykus reikšmingiems pokyčiams.

Toks principas turi būti įdiegtas kai tik sukuriamas naujas asmens duomenų tvarkymo būdas. Taikydami tokį principą nuo pat pradžių galime nustatyti būtinas ir pakankamas kontrolės priemones bei tokiu būdu optimizuoti sąnaudas. Kita vertus, jei šį principą taikysime jau sukūrę sistemą ir įdiegę kontrolės priemones, gali kilti klausimų dėl mūsų pasirinktų priemonių.

Mūsų pareigos

- Jei tikėtina, kad konkretus duomenų tvarkymo būdas, ypač paremtas naujomis technologijomis, ir atsižvelgiant į tvarkymo pobūdį, kontekstą ir tikslus, gali sukelti didelį pavojų fizinių asmenų teisėms ir laisvėms, kaip duomenų valdytojas, „Roquette“ prieš pradėdama tvarkyti duomenis, atlieka planuojamų tvarkymo veiksmų poveikio asmens duomenų apsaugai vertinimą.
- Projekto savininkas tariasi su duomenų apsaugos pareigūnu, paskirtu dalyvauti atliekant poveikio duomenų apsaugai vertinimą.

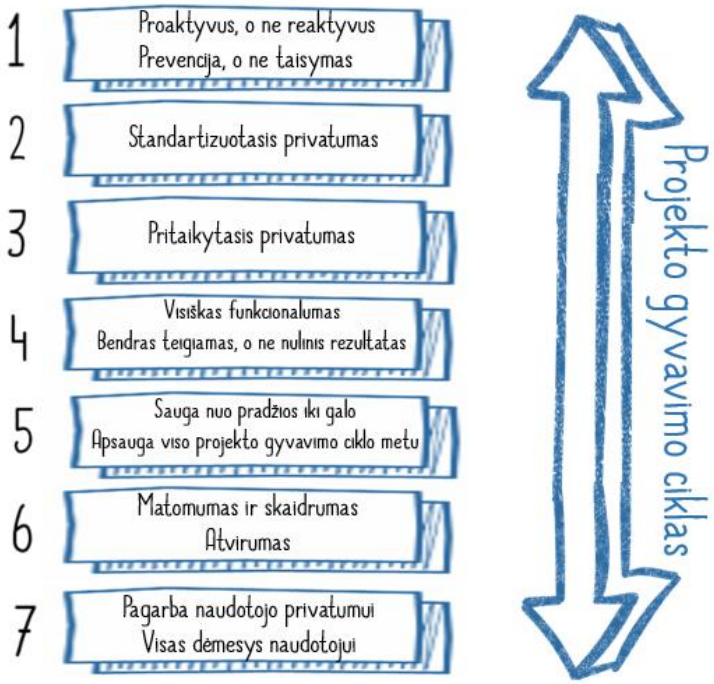
Taisyklės	Q-Docs	BDAR
• Esant dideliam pavojui atlikti PPV	DDPG003EN 1 taisyklė	35 str.
• PPV turinys	DDPG003EN 2 taisyklė	
• DAP veiksmai atliekant PPV	DDPG003EN 3 taisyklė	
• PPV peržiūra	DDPG003EN 4 taisyklė	

Mokome savo darbuotojus ir tobuliname vidaus procesus.

- Mokymasis saugumo „Security & Privacy Review“ į „Projects & Contracts“.
- „Privacy Impact“ šablonas automatiškai paleidžiamas mūsų privatumo valdymo programinėje įrangoje "OneTrust@Roquette", kai to reikia.
- **Sužinoti daugiau** : CNIL PPV atlikimo metodika, 2018 m. vasario redakcija - https://www.cnil.fr/en/home.

Pritaikytoji ir standartizuotoji duomenų apsauga

Pritaikytoji duomenų apsauga reiškia, kad privatumo apsaugos priemonės integruojamos kuriant sistemą, verslo procesą ar rengiant specifikacijas.



Kas yra pritaikytoji duomenų apsauga?

Duomenų apsaugos teisės aktuose nurodyti pagrindiniai duomenų subjektų privatumo apsaugos principai.

Pritaikytoji ir standartizuotoji duomenų apsauga leidžia užtikrinti, kad mūsų naudojamos informacinės sistemos atitinka šiuos duomenų apsaugos principus ir užtikrina duomenų subjektų teises.

Mūsų įsitikinimai

Atlikdama daugelį veiklos ir administracinių užduočių, „Roquette“ naudoja informacines sistemas ir duomenynus. Didelė dalis šių informacinių sistemų naudojama tvarkyti asmens duomenis, todėl labai svarbu, kad jos visiškai atitiktų reglamento reikalavimus.

Verslas, kuris atsakingai vertina duomenų apsaugą, sugeba kurti pasitikėjimą.

Todėl stiprios duomenų apsaugos priemonės gali suteikti konkurencinį pranašumą.

Priimant sprendimą taikyti pritaikytosios duomenų apsaugos principus organizacijos pirkimų ir programinės įrangos kūrimo procesuose yra labai svarbus Grupės vadovybės įsipareigojimas.

Taip pat vadovybė privalo skirti tam pakankamai išteklių.

Integruojant duomenų apsaugos priemones viso kūrimo metu galima sumažinti sąnaudas ir dirbti efektyviau, nes vėliau nereikia atlikti pakeitimų jau sukurtoje programinėje įrangoje.

Mūsų pareigos

BDAR pirmą kartą teisiškai įpareigoja taikyti pritaikytąją duomenų apsaugą. Tai reiškia, kad duomenų ir privatumo apsaugos priemonės turi būti numatomos dar projektuojant informacijos ir komunikacijos sistemas bei technologijas.

Kaip duomenų valdytojas, kurdama programinę įrangą bei užsakydama sistemas, sprendimus ir paslaugas „Roquette“ privalo laikytis pritaikytosios duomenų apsaugos reikalavimų.

Taip pat šie reikalavimai turi būti numatyti sudarant sutartis su tiekėjais bei naudojantis konsultantų paslaugomis (žr. mūsų bendravimo su subrangovais principus).

Taisyklė	Q-Docs	BDAR
• Pritaikytoji ir standartizuotoji sauga, privatumo ir duomenų apsauga	DDPG0072EN 3 taisyklė	25 str.

Kontrolinis sąrašas

- ☑ Patikrinti poveikio duomenų apsaugai vertinimo (PDAV) procedūrą
- ☑ Vengti, riboti ir mažinti poreikį rinkti ir tvarkyti neskelbtinus asmens duomenis
- ☑ Riboti ir mažinti nebūtiną funkcionalumą ir asmens duomenų naudojimą naudotojo sąsajoje
- ☑ Jei įmanoma, anonimizuoti ir pseudonimizuoti asmens duomenis
- ☑ Privatumą sauganti konfigūracija standartiškai turi būti įjungta
- ☑ Perėjimo iš vienos svetainės į kitą atsekimo funkcija standartiškai turi būti išjungta
- ☑ Programinės įrangos meniu numatyti galimybę duomenų subjektui atšaukti sutikimą. Atminkite, kad duomenų subjektui atšaukus sutikimą, jo asmens duomenų tvarkymas turi būti nutrauktas
- ☑ Parametrai turi būti pateikti meniu, kuriame duomenų subjektas galėtų sąmoningai pasirinkti mažiau privatumą saugančius parametrus
- ☑ Prietaiso atsekimo funkcija standartiškai turi būti išjungta

Mokome savo darbuotojus ir tobuliname vidaus procesus.

- Rekomendacija pateikta mūsų bendruomenės Duomenų apsaugos tinkle.
- Metodika: Projektų ir sutarčių saugumo ir atitikties nuostatų peržiūra
- Mokymasis HR platformoje.

Pranešimas apie duomenų saugumo pažeidimą

Kas yra asmens duomenų saugumo pažeidimas?

Asmens duomenų saugumo pažeidimas yra saugumo pažeidimas, dėl kurio netyčia ar neteisėtai asmens duomenys sunaikinami, prarandami, pakeičiami, neteisėtai atskleidžiami arba suteikiama prieiga prie jų, taip pat jie perduodami, saugomi ar kitaip tvarkomi.

Taigi tai yra ne tik asmens duomenų ***praradimas****.*

Pavyzdžiai

- Prarandamas klientų duomenynas
- Atskleidžiama darbuotojų veiklos rezultatų vertinimo informacija

Mūsų pareigos

Privalome taikyti taisykles, kad bet koks asmens duomenų pažeidimas būtų tvarkomas taip, jog jo poveikis duomenų subjektui būtų kuo mažesnis, o pats pažeidimas nesikartotų.

Taisyklės	Q-Docs	BDAR
• Pranešti apie asmens duomenų pažeidimą duomenų apsaugos pareigūnui	DDPG008EN 1 taisyklė	33 str.
• Pranešti apie asmens duomenų pažeidimą priežiūros institucijai	DDPG008EN 2 taisyklė	
• Pranešti apie asmens duomenų pažeidimą duomenų subjektui	DDPG008EN 3 taisyklė	34 str.

Į ką kreiptis duomenų saugumo pažeidimo atveju?

Kreipkitės į duomenų apsaugos pareigūną adresu dpo@Roquette.com bei „Roquette“ pasitikėjimo linija adresu alert@Roquette.com.

Per kiek laiko turime pranešti apie pažeidimą?

Įvykus pažeidimui, apie kurį privalome pranešti priežiūros institucijai, tai turime padaryti nepagrįstai nedelsdami, bet ne vėliau kaip per 72 val. nuo tada, kai sužinojome apie pažeidimą.

Apie kokius pažeidimus privalome informuoti atitinkamą priežiūros instituciją?

Pranešti apie pažeidimą atitinkamai priežiūros institucijai privalome tuomet, kai dėl pažeidimo kyla pavojus asmenų teisėms ir laisvėms. Jei pažeidimas yra nesprendžiamas, jis gali turėti didelių neigiamų pasekmių asmenims. Pavyzdžiui:

- asmuo gali būti diskriminuojamas;
- gali būti pažeista jo reputacija;
- jis gali patirti finansinių nuostolių; arba
- jis gali prarasti konfidencialumą arba jis gali patirti kitą didelę ekonominę ar socialinę žalą.

Kiekvieną pažeidimą turime vertinti atskirai bei galėti pagrįsti mūsų sprendimą pranešti apie jį priežiūros institucijai.

Kada privalome pranešti asmenims?

Jei tikėtina, kad dėl pažeidimo kils **didelis pavojus** asmens teisėms ir laisvėms, privalome nepagrįstai nedelsdami pranešti apie pažeidimą asmeniui, kurio asmens duomenų saugumas buvo pažeistas.

Pranešti asmeniui apie pažeidimą nereikalaujama, jei:

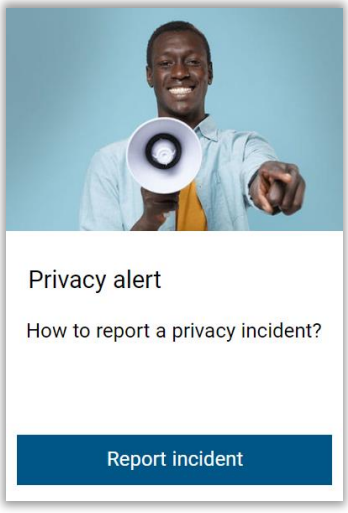
- įgyvendinome tinkamas technines ir organizacines priemones, kurias pritaikėme asmens duomenims, kurių saugumas buvo pažeistas;
- vėliau ėmėmės priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms; arba
- tai pareikalautų neproporcingai daug pastangų.

Tokiu atveju vietoj to apie tai viešai paskelbiama arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

Su kuo turėtume susisiekti duomenų saugumo pažeidimo atveju?

Kreipkitės **į Duomenų Apsaugos Pareigūną** adresu dpo@Roquette.com ir (arba) praneškite apie incidentą naudodamiesi mūsų interneto forma "Privacy Alert".

Jei norite pranešti apie galimą atitikties pažeidimą, galite susisiekti su įprastu kontaktiniu asmeniu arba pranešti apie problemą naudodamiesi konfidencialiu "Roquette" įspėjimo įrenginiu: "Speakup©".



Stebėsena ir peržiūra

Mūsų įsitikinimai

„Roquette“ yra įsipareigojusi:

- ☑ užtikrinti teisinę ir technologinę duomenų apsaugos reikalavimo vykdymo **stebėseną**,
- ☑ **peržiūrėti** ir **tobulinti** mūsų duomenų apsaugos valdymo sistemą (DPMS)

atsižvelgiant į reglamentavimo bei technologines naujienas ir vidinius paslaugų apribojimus. [DDPG009EN]

Mūsų pareigos

Taisyklės	Q-Docs	BDAR
• Užtikrinti teisinę ir technologinę duomenų apsaugos reikalavimo vykdymo stebėseną ir peržiūrą	DDPG009EN 1 taisyklė	Geriausia praktika
• Reguliariai stebėti DPMS ir duomenų apsaugos direktyvų taikymą	DDPG009EN 2 taisyklė	
• Reguliariai peržiūrėti asmens duomenų apsaugos politiką ir DPMS dokumentaciją	DDPG009EN 3 taisyklė	

Mokome savo darbuotojus ir tobuliname vidaus procesus.

Kurkite ir tobulinkite mūsų Privatumo programą

Teisės aktų paieškos programa

Mes naudojame platformą, kurioje pateikiame privatumo sprendimus, skirtus padėti mums stebėti reglamentavimo naujienas, mažinti pavojų ir pasiekti bendrą atitiktį:

- ☑ Reglamentavimo naujienos
- ☑ Lyginamosios tarpvalstybinės diagramos
- ☑ Rekomendacijos
- ☑ BDAR portalas
- ☑ Formos ir kontroliniai sąrašai
- ☑ Analitiko konsultacijos paslauga
- ☑ Teisės aktų paieška

Duomenų apsaugos valdymo sistemos auditas ir peržiūra

Atliekame vidaus auditus, siekdami nustatyti, ar DPMS elementai:

- ☑ atitinka šio Vadovo, Politikos ir taikomų teisės aktų reikalavimus;
- ☑ veiksmingai taikomi ir palaikomi; ir
- ☑ naudojami tinkamai.

Mūsų vadovybė atlieka DPMS peržiūrą, siekdama užtikrinti, kad būtų išlaikoma tinkama jos aprėptis ir nustatomos DPMS proceso tobulinimo galimybės.

Tam naudojame tokius elementus:

- ☑ DPMS tikslus, valdymo priemones, procesus ir procedūras;
- ☑ Ankstesnių atitikties auditų ir patikrų rezultatus;
- ☑ Suinteresuotų šalių atsiliepimus;
- ☑ Metodus, produktus ir procedūras, kurios galėtų būti taikomos ir naudojamos organizacijoje siekiant gerinti DPMS veiklos rezultatus ir veiksmingumą;
- ☑ Prevencinių ir taisomųjų veiksmų būseną;
- ☑ Silpnąsias vietas ar grėsmes, kurios netinkamai pašalintos ankstesnių rizikos vertinimų metu;
- ☑ Efektyvumo matavimo rezultatus;
- ☑ Veiksmus po ankstesnių vadovybės peržiūrų;
- ☑ Bet kokius pakeitimus, kurie gali turėti įtakos DPMS; ir
- ☑ Rekomendacijas dėl tobulinimo.

Susiję dokumentai

- [Elgesio kodeksas] „Roquette Group“ Elgesio kodeksas
- [GDPG001EN] Duomenų apsaugos sąvokų žodynėlis
- [MDPG001EN] Asmens duomenų apsaugos vadovas
- [DDPG001EN] Direktyva dėl pagarbos privatumui ir asmens duomenų apsaugai kultūros
- [DDPG002EN] Direktyva dėl asmens duomenų tvarkymo teisėtumo
- [DDPG003EN] Direktyva dėl poveikio privatumui vertinimo
- [DDPG004EN] Direktyva dėl neskelbtinų duomenų tvarkymo
- [DDPG005EN] Direktyva dėl tvarkymo veiksmų registravimo
- [DDPG006EN] Direktyva dėl asmens laisvių paisymo
- [DDPG007EN] Direktyva dėl asmens duomenų apsaugos
- [DDPG008EN] Direktyva dėl pranešimo apie asmens duomenų saugumo pažeidimą
- [DDPG009EN] Direktyva dėl asmens duomenų apsaugos valdymo sistemos peržiūros
- [DSUG001EN] Direktyva dėl informacinės saugos
- [DSUG006EN] Direktyva dėl kibernetinės saugos valdymo
- [DSUG016EN] Direktyva dėl rangovų saugos

Literatūra

[ES chartija] Europos Sąjungos pagrindinių teisių chartija, 2010/C 83/02.

[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).

[Duomenų apsaugos įstatymas] 1978 m. sausio 6 d. Prancūzijos įstatymas dėl duomenų apsaugos, Nr. 78-17 su pakeitimais

[WP29 gairės] Asmens duomenų valdytojo ar tvarkytojo pagrindinės priežiūros institucijos nustatymo gairės | WP 244 rev. 01 (2017 m. balandžio 5 d).

[WP29 gairės] Poveikio duomenų apsaugai vertinimo (PDAV) ir nustatymo, ar duomenų tvarkymas „gali sukelti didelį pavojų“ pagal Reglamentą Nr. 2016/679 gairės | WP 248 rev. 01 (2017 m. spalio 13 d.).

[WP29 gairės] Administracinių baudų taikymo ir nustatymo pagal Reglamentą Nr. 2016/679 gairės | WP 253 (2017 m. spalio 21 d.).

[WP29 gairės] Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą Nr. 2016/679 gairės | WP 251 rev. 01 (2018 m. vasario 13 d.).

[WP29 gairės] Duomenų apsaugos pareigūnų (DAP) gairės | WP 243 rev. 01 (2017 m. balandžio 5 d.).

[WP29 gairės] Skaidrumo pagal Reglamentą Nr. 2016/679 gairės | WP 260 rev 01 (2018 m. balandžio 11 d.).

[WP29 gairės] Sutikimo pagal Reglamentą Nr. 2016/679 gairės | WP 259 rev. 01 (2018 m. balandžio 18 d.).

[EDAV nuomonė] Nuomonė 23/2018 dėl Komisijos pasiūlymų dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių (70 straipsnio 1 dalies b punktas) (2018 m. rugsėjo 26 d.).

[EDAV nuomonė] Nuomonė 28/2018 dėl Europos Komisijos įgyvendinimo sprendimo dėl tinkamos asmens duomenų apsaugos Japonijoje projekto (2018 m. gruodžio 5 d.).

[EDAV nuomonė] Nuomonė 14/2019 dėl standartinių sutarčių sąlygų projekto, pateikto DK SA (BDAR 28 straipsnio 8 dalis) (2019 m. liepos 12 d.).

[EDAV gairė] Gairė 01/2019 dėl Europos duomenų apsaugos priežiūros pareigūno duomenų tvarkymo veiksmų, kuriems taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo projekto (Reglamento (ES) Nr. 2018/1725 39 straipsnio 4 dalis) (2019 m. liepos 10 d.).

[EDAV ir EDAPP bendras atsakymas] EDAV ir EDAPP bendras atsakymas LIBE komitetui dėl JAV Aiškinamojo teisėto duomenų naudojimo užsienyje įstatymo poveikio asmens duomenų apsaugos ES teisiniam reglamentavimui (priedas) (2019 m. liepos 10 d.).

[EDAV nuomonė] Nuomonė 13/2019 dėl Prancūzijos kompetentingos priežiūros institucijos duomenų tvarkymo veiksmų, kuriems netaikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo projekto (BDAR 35 straipsnio 5 dalis) (2019 m. liepos 10 d.)

Šaltiniai

- Commission Nationale de l'Informatique et des Libertés (Prancūzijos duomenų apsaugos agentūra)
    - https://www.cnil.fr/en/home
    - 2019 m. rugsėjis
    - Licencija Nr. CC-BY-ND 3.0 FR
- Informacijos komisaro biuras
    - https://ico.org.uk/
    - 2019 m. rugsėjis
    - Licencijuota pagal Atvirą valdžios licenciją
- Europos Sąjunga
    - https://eur-lex.europa.eu
    - 1998–2019
- https://www.iso.org/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

Šio vadovo anglų k. versija yra oficialus dokumentas.
Jo vertimuose gali pasitaikyti netikslumų.
Pirmas leidimas: 2019 m. rugsėjis
Leidėjas: ROQUETTE FRERES
Išdėstymas ir grafika: Compliance Office
Nuotraukos: galima naudoti nemokamai

ROQUETTE

Offering the best of nature™