

Asmens duomenų apsaugos politika

Versija	Versija 1
Istorija	Įsigaliojo nuo 2016 m. balandžio mėn.
Patvirtinimo procedūra komisijos sprendimu	Patvirtinta 2016 m. balandžio mėn. Verslo etikos
Tikslinė grupė	Visi įmonės „Danone“ darbuotojai
Dokumento turėtojas	Vyriausiasis atitikties užtikrinimo pareigūnas
Konfidencialumo lygis	Įmonės viduje
Puslapių skaičius	19
Kalbos	anglų (pagrindinė kalba), prancūzų (informacijos)

„Danone“ S.A. yra visų autorių teisių, susijusių su šiuo dokumentu, savininkas. Visos teisės saugomos.

TURINYS

Asmens duomenų apsaugos politika	1
TURINYS	3
IVADAS	5
1.1 Asmens duomenų privatumo politikos (toliau – politika) tikslas ir taikymas.....	5
1.2 Rizika, susijusi su privatumo teisės aktų pažeidimais	5
1.3 Atitikties funkcijos ir atsakomybė	6
ASMENS DUOMENŲ TVARKYMO NUOSTATOS	8
2.1 Specifiniai ir teisėti tikslai	8
2.2 Duomenų proporcingumas ir kokybė.....	8
2.3 Ribotas duomenų saugojimas	9
2.5 Duomenų subjekto sutikimas	10
2.6 Informacija apie Duomenų subjektą	10
2.7 Jautrių duomenų apsauga	11
2.8 Duomenų subjekto teisės	11
2.9 Atsižvelgimas į asmens duomenų tvarkymo svarbą	12
2.10 Duomenų tvarkytojų naudojimas	13
SUPRATIMO DIDINIMAS	14
3.1 Supratimo sąvokos apibrėžimas (pranešimas apie pažeidimą)	14
3.2 „Danone“ politika dėl pranešimų apie pažeidimus	14
3.3 Nagrinėjimas	14
1 PRIEDAS	15
ŠALIAI BŪDINGOS TAISYKLĖS	15
Asmens duomenų apibrėžimas	15
Jautrių duomenų apibrėžtis	15
Sutikimas	16
Perdavimas	17
2 PRIEDAS	18
ŽODYNĖLIS	18

ELEKTRONINIŲ RYŠIŲ IŠTEKLIŲ PRIEIGOS DIREKTYVA (TOLIAU – DIREKTYVA)	19
Valdžios institucijų tyrimai	19
Vidaus tyrimai.....	20
Verslo operacijos (toliau – darbuotojų laikinas nebuvimas ir išvykimas)	20

ĮVADAS

1.1 Asmens duomenų privatumo politikos (toliau – politika) tikslas ir taikymas

Ši politika taikoma visoms „Danone“ įmonėms visame pasaulyje, įskaitant visas kontroliuojamojo valdymo arba veiksmingai valdomose dukterinėse įmonėse ir filialuose (t. y. konsoliduotose dukterinėse įmonėse) ir visiems jų darbuotojams. Tam, kad būtų užtikrintas atitikties programos veiksmingumas ir nuoseklumas, ši politika pakeičia „Danone“ esamą asmens duomenų privatumo politiką. Papildomos politikos kryptys gali būti parengtos dėl vietinių ar verslui būdingų poreikių, bet tik tiek, kiek būtina, ir atsižvelgiant į patvirtintą Verslo etikos komisijos (VEK) sprendimą.

Trečiosios šalys, kurioms „Danone“ perduoda visą ar dalį asmens duomenų tvarkymo veiksmų (toliau – tvarkymas), taip pat turi atitikti šią politiką.

Šioje asmens duomenų privatumo politikoje išsamiai nustatomos taisyklės ir pareigos, kurių „Danone“ darbuotojai privalo laikytis tvarkydami asmens duomenis (toliau – asmens duomenys¹). Pirmiausia tai skirta asmeniui, atsakingam už „Danone“ darbuotojų ir vartotojų asmens duomenų tvarkymą: asmens duomenų privatumo ruošiniai gali būti tolesnės gairės darbuotojams.

Skaitmeniniame amžiuje, kuriame gyvename, asmens duomenys yra labai svarbūs verslui, o tinkamai tvarkomi, atveria naujas augimo galimybes. Tačiau atsakingas asmens duomenų valdymas yra gyvybiškai svarbus verslo tvarumui, o „Danone“ nesiima veiksmų, kurie galėtų pakenkti mūsų įmonėms ar bendruomenėms, kuriose veikiame. Mes visiškai pripažįstame pagrindinę asmenų teisę į privatumą ir jų teisę į asmens duomenų privatumą. Darbuotojų ir kitų asmenų privatumo teisių apsauga yra svarbiausias šio Asmens duomenų privatumo politikos, esančios pagrindiniu „Danone“ įsipareigojimo laikytis pasaulinių asmens duomenų privatumo standartų, tikslas.

Ši politika neapima reikalavimų, susijusių su duomenų konfidencialumu, vientisumu ir prieinamumu apskritai, taip pat atsitiktiniu asmeniniu Elektroninių ryšių išteklių (toliau – elektroninių ryšių ištekliai) naudojimu: juos ir toliau reglamentuoja Informacijos saugumo ir ryšių sistemos gairės, kitos verslo ar vietos politikos nuostatos bei taikomi įstatymai.

Vietiniai privatumo įstatymai gali skirtis; tais atvejais, kai teisiniai reikalavimai ir ši politika yra nesuderinami, visada privaloma taikyti aukštesnį standartą.

1.2 Rizika, susijusi su privatumo teisės aktu pažeidimais

¹ Nuorodos į terminus žodynėlyje.

Jei nesilaikoma privatumo įstatymo, gali būti taikoma civilinė ir baudžiamoji atsakomybė ir (arba) laisvės atėmimas. Be to, dėl privatumo įstatymų nesilaikymo gali būti labai pakenkta „Danone“ reputacijai. „Danone“ netoleruos šios politikos nesilaikymo (ar kitų atitikties taisyklių), todėl gali būti taikomos drausminės priemonės. Drausminės priemonės skirsis pagal nesilaikymo sunkumo laipsnį, bet gali apimti ir darbuotojo premijos atšaukimą, paaukštinimo atidėjimą, nušalinimą be užmokesčio, darbo sutarties nutraukimą ar pranešimą valdžios institucijoms.

1.3 Atitikties funkcijos ir atsakomybė

Visi „Danone“ darbuotojai yra atsakingi už tai, kad būtų laikomasi Verslo etikos kodekso (toliau – VEK) ir atitikties politikos, įskaitant asmens duomenų apsaugos politiką. Tai reiškia, kad dėl to įmonės vidaus politika neturėtų prieštarauti šioje politikoje nustatytais taisyklėms.

Generaliniai direktoriai (toliau – **GD**), atsižvelgiant į VEK; taip pat užsienio šalyse esančių įmonių generaliniai direktoriai atsižvelgiant į atitinkamą VEK:

- yra atsakingi už šioje politikoje numatytų procesų įgyvendinimą ir vykdymą bei jų laikymąsi.

COMEX nariai, susiję su WBU (*liet.* tarptautinės transliuotojų sąjungos), WBS (*liet.* hierarchinė struktūra), RBU (*liet.* regioninio verslo skyrius) ir RBS (*liet.* rizikos valdymo sistema), pagal savo atitinkamas atsakomybės sritis:

- prisiima atsakomybę, priskirtą GD už jų VEK.

Įmonių grupių atitikties pareigūnai² (toliau – **Grupių AP**):

- konsultuoja ir palaiko GD ir visas atitinkamos grupės funkcijas, susijusias su šios politikos taikymu, ir prireikus pasilieka išorinius patarėjus;
- stebi konfidencialumo įstatymų laikymąsi įmonių grupėje ir nuolat informuoja apie visus svarbius įvykius;
- nedelsdami informuoja bendrąją atitikties grupę, jei dėl bet kokių VEK grupėje pažeidimų privatumo institucija pradėjo tyrimą.

Tarptautinio verslo standartų atitikties grupė (toliau – **TVS atitiktis**):

- teikia nurodymus bendrais šios politikos taikymo klausimais;
- pataria ir atsako į klausimus, į kuriuos negali išsamiai atsakyti Grupės AP visų verslo įmonių padalinių atžvilgiu;

² Arba, jei buvo paskirti pagal atitikties pagrindų politikos nuostatas (6.1 skirsnis), atitikties pareigūnai nustatomi WBU, WBS, RBU, RBS ir CBU lygmenyse.

- gali, vadovaudamiesi vyriausiojo atitikties pareigūno (toliau – VAP) sprendimu, nuspręsti konsultuoti dėl atvejų ar pradėtų tyrimų, kurie turi didelės įtakos įmonės atitikties rizikai.

ASMENS DUOMENŲ TVARKYMO NUOSTATOS

„Danone“ asmens duomenų tvarkymas leidžiamas tik tada, kai jis vykdomas sąžiningai ir teisėtai, atitinka toliau išdėstytus principus ir yra tvarkomas naudojant atitinkamas technines ir tvarkymo priemones, kuriomis remiantis galima įrodyti, kad laikomasi visų taikomų įstatymų.

Siekiant tai užtikrinti, Grupių AP turi peržiūrėti kiekvieną naują veiklą, susijusią su asmens duomenimis (pvz., nauja apdorotų asmens duomenų kategorija, nauja apdorojimo platforma ar naujas apdorojimo tikslas).

2.1 Specifiniai ir teisėti tikslai

Mes tvarkome asmens duomenis tik konkrečiais ir aiškiais tikslais. Todėl asmens duomenų rinkimo laikotarpiu ar prieš tai nurodome apdorojimo tikslą, su kuriuo supažindiname ir asmens duomenų savininkus (toliau – duomenų subjektai), o surinkus, tvarkome asmens duomenis tik tokiu būdu, atitinkančiu šį tikslą.

Pavyzdžiui, jei vartotojo kontaktinė informacija buvo surinkta skundo nagrinėjimo tikslais, jo negalima pridėti prie mūsų naujienlaiškio platinimo sąrašo, nebent vartotojui būtų pranešta apie šį papildomą tikslą ir jam buvo pritarta.

Be to, mūsų tikslai privalo būti teisėti. Todėl, nustatydami juos, mes patikriname, ar pagal galiojančius įstatymus jie yra paremti įstatymais ir teisėti, patys klausdami, ar tai, ką ketiname daryti, yra sąžininga ir teisinga: dažniausiai tai darome, kai mūsų ir duomenų subjekto interesai nesiskiria. Akivaizdžiai neteisėtu tikslu laikomas toks tikslas, kuris reikštų nesąžiningą duomenų subjekto privatumo pažeidimą.

Pavyzdžiui, pagal daugelio šalių duomenų privatumo įstatymus uždaroji vaizdo stebėjimo sistema (toliau – UVSS) yra teisėta, kai siekiama užtikrinti darbuotojų saugumą, bet tampa neteisėta, jei ji naudojama nuolatiniam stebėjimui.

2.2 Duomenų proporcingumas ir kokybė

Mes renkame tik tuos asmens duomenis, kurių mums reikia savo tikslams, ir neprašome arba nenagrinėjame nesusijusios informacijos. Mes nesaugojame asmens duomenų, nes nemanome, kad jie ateityje galėtų būti naudingi.

Asmens duomenys, kuriuos mes laikome, turi būti tikslūs ir nuolat atnaujinami. Mes turime juos atnaujinti arba pašalinti netikslumus ar neišsamią informaciją nedelsiant, pastebėję bet kokį netikslumą ir (arba) informacijos trūkumą.

Pavyzdžiui, jei užduodame konkrečius klausimus apie kandidatų, į konkrečias darbo vietas, sveikatą, šie klausimai netampa mūsų įprastų klausimų dalis, nes dažniausiai mums jų nereikia.

Panašiai, jei apdorojimo paskirtis yra siųsti vartotojams naujienlaiškį su specialiais pasiūlymais, renkama tik vartotojų kontaktinė informacija be jokios nereikalingos informacijos, pvz., banko sąskaitos duomenų.

2.3 Ribotas duomenų saugojimas

Mes saugome asmens duomenis tokia forma, kuria remiantis galime nustatyti duomenų subjektą tik per duomenų tvarkymui reikalingą laikotarpį, atsižvelgiant į duomenų subjektui pateiktą informaciją. Mes nesaugosime asmeninių duomenų neribotą laiką, išskyrus atvejus, kai įstatymas to aiškiai reikalauja.

Gera praktika yra reguliariai peržiūrėti turimus asmens duomenis ir ištrinti tai, ko nereikia, visada atsižvelgiant į taisykles, taikomas tam tikroms asmens duomenų rūšims. Tačiau asmens duomenų nereikia saugoti neribotą laiką, „jeigu ką“ arba jei yra tik maža tikimybė, kad jie bus naudojami.

Pavyzdžiui, „Danone“ turėtų peržiūrėti darbuotojų asmens duomenis, kai jie naudojami ne įmonės viduje. Turime saugoti tiek duomenų, kad jų užtektų pateikti rekomendacijoms ar informacijai apie pensijų tvarką, tačiau turime pašalinti jų kontaktinius duomenis arba ankstesnius adresus.

2.4 Duomenų subjekto informacija

Renkant asmens duomenis arba bent pirmą kartą juos apdorojant, turime pateikti duomenų subjektui tinkamą ir pakankamą informaciją bent apie:

- tvarkymo tikslus;
- asmens duomenų tvarkytojų (toliau – duomenų tvarkytojas), asmens duomenų valdytojo (toliau – duomenų valdytojas) bei jų atstovų tapatybę ir kontaktinę informaciją;
- bet kokį asmens duomenų perdavimą už šalies, kurioje jie buvo pateikti, ribų nurodant, ar ir koku būdu suteikiamas toks pats apsaugos lygis;
- kiek laiko bus saugomi asmens duomenys;
- jo (jos) teises (žr. 2.8 dalį) ir jų panaudojimo būdus;
- privalomą ar savanorišką asmens duomenų atskleidimą.

Turime informuoti duomenų subjektą aiškiai ir paprastai, pateikiant aiškias, skaidrias, suprantamas ir lengvai prieinamas formas, pvz., skaitmeninį arba spausdintą privatumo apsaugos pareiškimą, privatumo politiką, pateiktą interneto svetainėje, el. laišką, kuriuo patvirtinama, kad

prašymas ar skundas gauti, naujienlaiškį arba vidaus taisykles, reglamentuojančias darbuotojų asmens duomenų tvarkymą.

„Danone“ darbuotojams pridedamoje Elektroninių ryšių išteklių prieigos direktyvoje pateikiamas priežasčių sąrašas, kodėl reikia naudotis elektroninių ryšių ištekliais „Danone“.

2.5 Duomenų subjekto sutikimas

Atsižvelgiant į vietinę taikomą teisę, visada turėtų būti gautas duomenų subjekto pateiktas vienareikšmis sutikimas dėl asmens duomenų tvarkymo.

Manome, kad duomenų subjektas pritarė asmens duomenų tvarkymui, kai jis savanoriškai pateikė asmens duomenis, gavo tinkamą informaciją ir, gavęs teisę prieštarauti duomenų tvarkymui, to neatsisakė.

Paprastai sutikimo nereikia, kai asmens duomenys yra tvarkomi įvykdant sutartis, kurios viena iš šalių yra duomenų subjektas, kad būtų laikomasi teisinio įsipareigojimo saugoti pagrindinius duomenų subjekto ar kito asmens interesus arba, teisėtas interesus, kurio siekiame mes ar trečioji šalis, kai neatsižvelgiama į duomenų subjekto interesus, teises ir laisves.

Visada turime aiškiai atskirti savo prašymą dėl sutikimo su kita informacija, pateikti ją taip, kad atitiktų duomenų subjekto amžių ir galimybes bei konkretaus atvejo aplinkybes. Be to, turime peržiūrėti, ar mūsų surinkti sutikimai galioja, nes santykiai su duomenų subjektu kinta.

Bet kuriuo atveju niekada neįsipareigojame užtikrinti, kad sutarties vykdymas būtų sąlygojamas asmens duomenų tvarkymo, kuris nėra būtinas jos vykdymui.

Prašome žiūrėti darbuotojams pridedamoje Elektroninių ryšių išteklių prieigos direktyvoje pateiktą priežasčių sąrašą, kodėl reikia naudotis elektroninių ryšių ištekliais be naudotojo (toliau – naudotojas) sutikimo.

2.6 Informacija apie Duomenų subjektą

Įmonei „Danone“ patikėtų asmens duomenų konfidencialumas ir saugumas yra labai svarbūs. Todėl mes:

- visada laikome asmens duomenis konfidencialiais ir, jei turime atskleisti informaciją trečiosioms šalims, neatsižvelgiant į santykius, pasirašome sutartį, kurioje išdėstyti visi tokio atskleidimo veiksniai;
- įgyvendiname tinkamas technines ir tvarkymo priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, ar atsitiktinio praradimo, pakeitimo arba neteisėto atskleidimo ar prieigos;

- klausiamo, kas turi teisę naudotis mūsų elektroninių ryšių ištekliais (įskaitant informacinių technologijų komandos narius ir (arba) „Danone“ sistemos administratorius vykdant savo pareigas):
 - nenaudoti prieigos prie informacijos, išskyrus tą, kuriai buvo suteiktas leidimas,
 - riboti prieigą iki minimalaus turinio lygio ir kuo mažiau galimų veiksmų, apriboti dalyvaujančių asmenų skaičių tik tiems, kurių reikia norint pradėti ir vykdyti prieigą,
 - nerinkti, nenaudoti ar neatskleisti elektroninių ryšių išteklių turinio, išskyrus tuos atvejus, kai tai nurodo „Danone“,
 - nedelsiant kreipkitės į įmonės informacinių sistemų saugumo vadovą ir vyriausiąjį atitikties pareigūną, kai aptinkate bet kokią informaciją, kuri pagrįstai gali būti laikoma nusikalstama (pvz., vaikų pornografija, nusikalstamas sąmokslas ir kt.) arba kitaip pažeidžianti galiojančius įstatymus, reglamentus, taisykles ar politiką.

Prašome skaityti Elektroninių ryšių išteklių prieigos direktyvą, kad būtų laikomasi tvarkos, susijusios su „Danone“ elektroninių ryšių išteklių naudojimu.

2.7 Jautrių duomenų apsauga

Įprastai mes neapdorojame jautrių duomenų (toliau – jautrūs duomenys), nebent:

- duomenų subjektas aiškiai sutiko su tvarkymu arba;
- apdorojimas yra būtinas siekiant įvykdyti „Danone“ įsipareigojimus ir teises įdarbinimo, socialinės apsaugos ir socialinės apsaugos teisės srityje arba apsaugoti gyvybiškai svarbius duomenų subjekto interesus, arba jei tai susiję su duomenų, kuriuos aiškiai paskelbia duomenų subjektas, arba jei to reikia teisinio ieškinio sudarymui, vykdymui ar gynimui.

Kadangi jautrūs duomenys gali būti naudojami norint diskriminuoti, reikia daugiau dėmesio skirti tokių duomenų apsaugai.

2.8 Duomenų subjekto teisės

Mes visada siūlome duomenų subjektui veiksmingas priemones, norint:

- ginčyti asmens duomenų tvarkymą dėl teisėtų priežasčių (toliau – teisė ginčyti):
 - duomenų subjektas visada turi teisę ginčyti jo asmens duomenų tvarkymą tik rinkodaros tikslais: todėl mes visada turime nurodyti „atsisakyti“, pvz., „atsisakyti prenumeratos“, nuorodos naujienlaiškiuose, kuriuos siunčiame el. paštu.
- žinoti, kokius su asmeniu susijusius duomenis mes turime (toliau – teisė susipažinti);
- paprašyti juos ištaisyti (toliau – teisė į atnaujinimą), kai nustatoma, kad turimi asmens duomenys nėra tikslūs ar atnaujinami,);

- paprašyti ištrinti (toliau – teisė būti ištrintam), kai nustatoma, kad asmens duomenys yra nebesvarbūs pirminio apdorojimo tikslų atžvilgiu, arba jei asmuo atšaukia sutikimą arba pareiškia prieštaravimą dėl apdorojimo;
 - pavyzdžiui, vartotojas gali prieštarauti jo gimimo vietos nurodymui nagrinėjant skundą,
 - duomenų subjektui paprašius pasinaudoti teise būti pamirštam, labai svarbu prisiminti, kad tai nėra absoliuti teisė ir kad, atsižvelgiant į prašymo turinį, turime ištrinti visą arba tik dalį asmens duomenų, kuriuos mes turime. Todėl turėtume padėti duomenų subjektui nuspręsti, kurie duomenys yra išties nesvarbūs juos tvarkant, o ne ištrinti viską, išskyrus atvejus, kai jis aiškiai išreiškė norą ištrinti visus asmens duomenis. Šiuo tikslu visada turime pasiūlyti duomenų subjektams, o labiausiai vartotojams, pritaikytą ištrynimą, pvz., ištrinti el. pašto adresą, ištrinti pašto adresą, ištrinti informaciją apie šeimą,
 - kai kuriais atvejais išbraukimo prašymas yra neteisėtas. Jei, pavyzdžiui, darbuotojas prašo panaikinti savo socialinio draudimo numerį iš „Danone“ duomenų bazės, mes negalime patenkinti tokio prašymo, nes ši informacija yra būtina darbo sutarties įvykdymui. Tuo pačiu būdu, kai vartotojai registruojami vienoje iš mūsų interneto svetainių, kad galėtų dalyvauti reklaminėse akcijose ir prašyti pašalinti jų kontaktinius duomenis, vis dar patvirtinant, kad jie nori dalyvauti, tada priėmus šį išbraukimo prašymą, „Danone“ būtų pažeista reklaminė sutartis. Šiais dviem atvejais duomenys yra svarbūs ir būtini sutarties, kurią Duomenų subjektas pasirašė su „Danone“, vykdymui;
- kaip alternatyvą ištrynimui, apriboti asmens duomenų tvarkymą tokiam laikui, kiek reikia jų atnaujinimui, jei to reikia teisiniam ieškinio pateikimui, vykdymui ar gynimui, arba laikui, reikalingam patikrinti prieštaravimo dėl duomenų tvarkymo užklauso teisėtumą (toliau – teisė į tvarkymo apribojimą).

Jei mes turime imtis veiksmų, kad duomenų subjektas galėtų pasinaudoti savo teisėmis, mes nedelsdami teikiame informaciją ir pagalbą.

2.9 Atsižvelgimas į asmens duomenų tvarkymo svarbą

Kaip duomenų valdytojai tvarkydami asmens duomenis, tiesiogiai atsakome už tai, kad būtų laikomasi visų galiojančių įstatymų, taisyklių ir vidaus politikos, nesvarbu, ar mes tiesiogiai arba per trečiąją šalį tvarkome asmens duomenis.

Pavyzdžiui, VEK bus laikomas duomenų valdytoju, jei bus nustatoma rinkos tyrimo veikla su vartotojų asmeniniais duomenimis, valdomos vartotojų skambučių centro paslaugos (net jei tiekėjas tvarko prašymus jo vardu) arba pasirašoma darbo sutartis, kurioje nurodomi darbuotojo asmens duomenys.

Kai kitas duomenų valdytojas nurodo tvarkyti duomenis, privalome užtikrinti, kad laikomės duomenų valdytojo nurodymų.

VEK bus laikomas duomenų tvarkytoju, jei bus tvarkomi klientų asmens duomenys centrinėje klientų valdymo duomenų bazėje, atliekama rinkos analizė arba siunčiami rinkodaros pranešimai kitų VEK vardu.

Nepaisant mūsų vaidmens asmens duomenų tvarkymo procese, turime laikytis visų vietinių duomenų privatumo institucijų reikalavimų. Pavyzdžiui, kai kuriose šalyse apie kiekvieną asmens duomenų tvarkymo veiklą reikia informuoti kompetentingas duomenų privatumo institucijas ir užpildyti atitinkamą (internetinę ar popierinę) formą. Kitose šalyse darbo tarybos turi patvirtinti konkretų asmens duomenų tvarkymą ir negalima rinkti ar tvarkyti jautrių duomenų be išankstinio duomenų privatumo institucijos leidimo.

2.10 Duomenų tvarkytojų naudojimas

Kai mes perduodame visą ar dalį Duomenų apdorojimo proceso duomenų tvarkytojui, mes manome, kad esame atsakingi už visus veiksmus, kuriuos jie vykdo mūsų vardu. Šios atsakomybės negalima vengti. Todėl mes:

- laikomės „Danone“ verslo partnerių elgesio kodekso ir trečiųjų šalių tikrinimo procedūrų, pasirinkdami duomenų tvarkytojus;
- pasirašome su jais sutartį, kurioje išdėstomas tvarkymo objektas ir trukmė, pobūdis ir paskirtis, asmens duomenų ir duomenų subjektų tipas bei numatytos aiškios instrukcijos, įskaitant galimą duomenų perdavimą už šalies, kurioje duomenys buvo surinkti, ribų;
- paprašome įrodymų apie jų taikomas saugumo ir konfidencialumo priemones arba ketinimus tai įgyvendinti prieš jums pradedant asmens duomenų tvarkymą.

Jei perduodant asmens duomenų tvarkymą asmens duomenys perduodami už šalies, kurioje jie buvo surinkti, ribų, o valstybė gavėja nėra oficialiai pripažinta kaip užtikrinanti tinkamą duomenų apsaugos lygį, turime imtis atitinkamų apsaugos priemonių.

Jei trečioji šalis mums skiria duomenų tvarkytoją ir per šį tarpininką gauname asmens duomenis, turime patikrinti, ar buvo pateikta teisinga informacija ir kad iš duomenų subjektų buvo surinkti atitinkami sutikimai (ypač dėl informacijos atskleidimo mums).

SUPRATIMO DIDINIMAS

3.1 Supratimo sąvokos apibrėžimas (pranešimas apie pažeidimą)

Supratimo didinimas ar pranešimas apie pažeidimą yra tai, kai „Danone“ darbuotojas arba išorinė šalis informuoja „Danone“ apie įtariamą neteisėtą veiklą darbe. Pranešimo „Danone“ apie pažeidimo esmę sudaro elgesys, kurio „Danone“ reikalauja, kaip nurodyta mūsų elgesio kodekse, šioje politikoje ir kitose atitikties taisyklėse. Tam priskiriamas ir kitokio pobūdžio neteisėtas elgesys, finansinis sukčiavimas ir bet kokia kita veikla, kuri kelia ar galėtų kelti pavojų aplinkai ar visiems, dirbantiems mūsų įmonėje.

3.2 „Danone“ politika dėl pranešimų apie pažeidimus

Iš „Danone“ mes norime nedelsiant sužinoti apie bet kokį verslo etikos pažeidimą ar galimą pažeidimą, bet kokį neteisėtą elgesį, finansinį sukčiavimą ir bet kokią veiklą, kuri kelia ar galėtų kelti pavojų aplinkai ar visiems, dirbantiems mūsų įmonėje.

Visada skatiname „Danone“ darbuotojus tiesiogiai aptarti bet kokius reikalus su atitinkamu įmonės kontaktiniu centru (pvz., N + 1 ar N + 2, personalo vadybininku, finansų vadybininku arba atitikties komandos nariu).

Tačiau jei „Danone“ darbuotojas norėtų pranešti apie problemą per kitą kanalą konfidencialiai, turime ir specialią informacijos teikimo priemonę, vadinamą „Danone Ethics Line“, www.danoneethicsline.com. Jei reikia, šiuo įrankiu galima naudotis anonimiškai.

Kiekvienas, pranešęs apie tikrą problemą, negali būti apkaltintas.

3.3 Nagrinėjimas

Visos iškeltos problemos pirmiausia bus nagrinėjamos įmonės viduje, „Danone Ethics Line“ komitetui organizuojant tyrimą. Bendrovių atitikties valdyba informuojama apie tyrimo rezultatus (išskyrus visus susijusius dalyvius), kuri atsakys už sprendimą dėl tinkamų veiksmų, kurių turi būti imtasi, priėmimą.

1 PRIEDAS

ŠALIAI BŪDINGOS TAISYKLĖS

Suprantame, kad asmens duomenų privatumo požiūriu negalima taikyti „tinka visiems“ principo. Jei bet koks vietinis įstatymas prieštarauja šios politikos taikymui, jis laikomas pakeistu tik tiek, kiek reikalaujama, kad jis būtų vykdytinas tik toje vietos jurisdikcijoje. Dėl papildomos informacijos kreipkitės į Grupių AP.

Žemiau pateikiame keletą nacionalinių nuostatų, kurios turi įtakos asmens duomenų tvarkymui: gali būti taip, kad jos galioja tik nurodytoje šalyje.

Asmens duomenų apibrėžimas

Bendrasis asmens duomenų apibrėžimas pateikiamas 2 priede. **Europos Sąjungoje** asmens duomenys yra bet kokia informacija apie identifikuotą arba identifikuojamą fizinį asmenį, įskaitant, pvz., vardą, pavardę, asmens kodą, vietos nustatymo duomenis, internetinį adresą arba vieną ar kelis bruožus, būdingus duomenų subjekto fizinei, fiziologinei, genetinei, psichinei, ekonominei, kultūrinei ar socialinei tapatybei.

Asmens duomenys **Argentinoje** yra bet kokia informacija, susijusi su patikrintais ar nustatomais asmenimis, ar juridiniais asmenimis.

Jautrių duomenų apibrėžtis

Bendras jautrių duomenų apibrėžimas pateikiamas 2 priede. **Europos Sąjungoje** jautrūs duomenys yra asmeniniai duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius, moralinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose arba genetinius duomenis, biometrinius duomenis, arba duomenis apie sveikatą, lytinį gyvenimą ir privilegijas.

Kinijoje jautrieji duomenys apibrėžiami kaip asmeninė informacija, kurios nutekėjimas ar keitimas gali neigiamai paveikti duomenų subjektą. Pavyzdžiai gali būti asmens kodas, mobiliojo telefono numeris, rasė, politinės pažiūros, religiniai įsitikinimai, genetika ar pirštų atspaudai.

Indijoje jautrieji duomenys taip pat apibrėžiami kaip „asmeninė informacija“, kurią sudaro informacija, susijusi su bet kuria iš šių sričių: slaptažodžiais, finansine informacija, pvz., banko sąskaita arba kredito arba debeto kortele, ar kita informacija apie mokėjimo priemonę; bet kuri kita informacija, susijusi su minėtomis priemonėmis, teikiama juridiniam asmeniui teikiančiam paslaugą.

Japonijoje registruota buveinė gali būti laikoma jautriais duomenimis.

JAV duomenys apie kreditingumą, asmeninė informacija, renkama internetu iš vaikų iki 13 metų, ir informacija, kuri gali būti naudojama asmens tapatybės vagystei ar sukčiavimui, gali būti laikoma jautriais duomenimis.

Sutikimas

Kai kuriose šalyse gali prireikti aiškaus sutikimo. Konkrečiai:

- **Taivane ir Singapūre** privaloma gauti aiškų sutikimą duomenų subjekto asmens duomenų rinkimui, tvarkymui, naudojimui ir saugojimui: „Aš sutinku su savo asmens duomenų rinkimu, tvarkymu, naudojimu ir saugojimu aukščiau aprašytais tikslais“.
- **Italijoje, Australijoje, Honkonge, Naujojoje Zelandijoje** yra privaloma gauti aiškų sutikimą duomenų subjekto asmens duomenų rinkimui, tvarkymui, naudojimui ir saugojimui tiesioginės rinkodaros tikslais: „Aš sutinku, kad mano asmens duomenys būtų renkami, tvarkomi, naudojami ir saugomi tiesioginės rinkodaros tikslais, kaip aprašyta anksčiau“.
- **Italijoje ir Japonijoje** privaloma gauti aiškų sutikimą duomenų subjekto asmens duomenims tvarkyti profiliavimo tikslais: „Aš sutinku, kad mano asmens duomenys būtų tvarkomi profiliavimo tikslais“.
- **Kinijoje, Malaizijoje, Tailande, Honkonge, Japonijoje** privaloma gauti aiškų sutikimą perduoti Duomenų subjekto asmens duomenis filialams, paslaugų teikėjams ir verslo partneriams: „Aš sutinku perduoti savo asmens duomenis filialams, paslaugų teikėjams ir verslo partneriams [įrašyti renkančiojo VEK pavadinimą] už [įrašyti šalies, kurioje renkama informacija, pavadinimą] ribų“.
- **Kanados** įstatymai dėl šiukšlinimo internete reglamentuoja elektroninių pranešimų platinimą. Tam tikromis aplinkybėmis iš duomenų subjekto privaloma gauti aiškų sutikimą, kad jie galėtų siųsti elektroninius pranešimus, taip pat elektroninius pranešimus rinkodaros tikslais: „Kanados įstatymai dėl šiukšlinimo internete reglamentuoja elektroninių pranešimų platinimą. Atsižvelgiant į tai [įterpti duomenų rinkimo VEK pavadinimą] ir [įterpti bet kurio kito subjekto, siunčiančio el. laiškus vartotojams, pavadinimą], gali siųsti jums el. laiškus, susijusius su jūsų pirkimais, taip pat rinkodaros tikslais (įskaitant kvietimus į privačius pardavimus ar renginius, naujienlaiškius ir leidinius, pranešimus ir naujienas ar informaciją, kuri gali jus sudominti). Jūs galite atsisakyti šio sutikimo gauti tokius elektroninius pranešimus bet kuriuo metu, atsisakę prenumeratos el. paštu, kaip aprašyta el. laiške, arba susisiekę su mumis aukščiau minėtu el. pašto adresu arba pašto adresais,“ „Aš sutinku gauti elektroninius pranešimus iš [įterpti juridinio asmens, gaunančio duomenis, pavadinimą] ir [įterpti bet kurio kito subjekto, išsiuntusio el. laiškus vartotojams, pavadinimą].“ „Aš sutinku gauti

elektroninius pranešimus rinkodaros tikslais nuo [įrašyti juridinio asmens, gaunančio duomenis pavadinimą] ir [įterpti bet kurio kito subjekto, siunčiančio rinkodaros el. laiškus klientams] pavadinimą.“

Perdavimas

Europos Sąjungoje Asmens duomenų perduodamo metu šaliai, kurioje nėra užtikrinamas tinkamas saugos lygis, Duomenų valdytojai privalo pateikti tinkamas apsaugos priemonės, pvz., privalomas verslo taisyklės, Komisijos priimtas standartines duomenų apsaugos nuostatas, priežiūros institucijos priimtas standartines duomenų apsaugos nuostatas, kurias patvirtino Komisija, taip pat sutartines sąlygas tarp duomenų valdytojo ar tvarkytojo, duomenų valdytojo ar gavėjo trečiojoje šalyje.

2 PRIEDAS

ŽODYNĖLIS

Tekstinė nuoroda	Aprašymas
Duomenų valdytojas	Kas, atskirai ar kartu su kitais, nustato asmens duomenų tvarkymo tikslus ir priemones.
Duomenų tvarkytojas	Asmens duomenis tvarkantis Duomenų valdytojo vardu.
Duomenų subjektas	Fizinis asmuo (esantis vartotojas, darbuotojas, kliento ar tiekėjo darbuotojas ir bet kuri kita trečioji šalis), kuriam priklauso Asmens duomenys.
Elektroninių ryšių ištekliai	Elektroniniai prietaisai, programinė įranga ir elektroninės komunikacijos priemonės, įskaitant asmeninius kompiuterius ir darbo vietas, nešiojamuosius kompiuterius, telefonus ir išmaniuosius telefonus, spausdintuvus, modemus, fakso aparatus, elektroninį paštą, interneto pokalbių programas ir balso pašto sistemas, priklausančias, nuomojamas ar kitaip valdomas „Danone“.
Asmeniniai duomenys	Informacija, leidžianti atskirai ar kartu su kita informacija identifikuoti fizinį asmenį.
Apdorojimas	Bet kokia operacija ar operacijų rinkinys, atliekamas naudojant Asmens duomenis automatiškai arba ne, kaip antai rinkimas, įrašymas, saugojimas, tvarkymas, kaupimas, pritaikymas ar pakeitimas, atnaujinimas, paieška, konsultavimas, naudojimas, atskleidimas perduodant, platinant arba kitaip darant prieinamą, palyginimas ar sujungimas, blokavimas, ištrynimasis ar sunaikinimas.
Jautrūs duomenys	Asmens duomenys, kurie netinkamai naudojami, fiziniam asmeniui gali padaryti labai didelės žalos ar nepatogumų (pvz., politines pažiūras, religiniai įsitikinimai, narystė profesinėse sąjungose, duomenys apie sveikatą ar seksualinį gyvenimą). Daugiau informacijos rasite 1 priede.
Vartotojai	Darbuotojai, direktoriai, konsultantai ir tiekėjai, kuriems „Danone“ teikia elektroninių ryšių išteklius, kad padėtų jiems atlikti savo pareigas ar pristatymus.

ELEKTRONINIŲ RYŠIŲ IŠTEKLIŲ PRIEIGOS DIREKTYVA (TOLIAU – DIREKTYVA)

„Danone“ elektroninių ryšių išteklių turinys ir viskas, kas patenka per mūsų tinklą, yra „Danone“ atsakomybė. Mes galime priėti prie to bet kuriuo metu per vidinius ar išorės nurodytus subjektus pagal atitinkamus nacionalinius įstatymus ir „Danone“ politiką su ar be naudotojų sutikimo, ar išankstinio įspėjimo. Prieigos reikia dėl toliau nurodytų priežasčių:

- nustatyti, kaip laikomasi atitikties politikos ir kitų „Danone“ politikos nuostatų;
- rinkti informaciją, reaguojant į teismo nutarimą, arba atsakant į valdžios institucijų ar agentūrų užklausas arba ieškinio rašymui, vykdymui ar ginantis;
- atlikti vidaus tyrimą dėl tariamo netinkamo elgesio, pavyzdžiui, priekabiavimo, diskriminacijos, verslo paslapčių vagystės, informacijos saugos pažeidimo, ar konfidencialumo;
- užtikrinti mūsų elektroninių ryšių išteklių sistemos veikimą ir saugumą arba atlikti jo techninę priežiūrą;
- užtikrinti įprastas verslo operacijas ir veiklos tęstinumą bei visus kitus verslo tikslus, kuriems reikalinga prieiga prie mūsų elektroninių ryšių išteklių.

Prieš naudojantis elektroninių ryšių ištekliais, kai tik įmanoma, naudotojas turi pateikti sutikimą, jei įmanoma: norint nustatyti, ar tam yra priežasčių to nepadaryti, visada klausama Grupės AP patarimo ir laikomasi direktyvos. Jei nepaprastosios padėties atveju šios direktyvos negalima laikytis, veiksmai ribojami iki įsigilavimo į turinį, ir kiek įmanoma mažiau veiksmų, reikalingų kritinei situacijai išspręsti, o vėliau reikia nedelsiant kreiptis dėl atitinkamą leidimo gavimo.

Valdžios institucijų tyrimai

Pagal galiojančius įstatymus „Danone“ gali būti įpareigota leisti susipažinti su elektroninių ryšių ištekliais ir atskleisti susijusį turinį be naudotojo sutikimo ar išankstinės informacijos valdžios institucijoms, kurios teisiškai turi teisę tai daryti. Atitinkamai „Danone“ gali atskleisti elektroninių ryšių išteklių turinį, kad įvykdytų teismo nurodymą, teismo šaukimą, orderį ar įstaigą, turinčią atitinkamą jurisdikciją, ir bet kokiomis kitomis aplinkybėmis, kai tokio atskleidimo reikalauja įstatymai.

Susidūrus su tokiomis situacijomis, „Danone“ darbuotojai turi informuoti atitinkamą Grupės AP, atsakingą už:

- kartu su teisėtu grupės vadovu arba pastarajam nesant, su teisininku, įvertinti prašymo pagrįstumą ir visų taikomų privatumo ir duomenų apsaugos įstatymų laikymosi, bei bet kokių specialių taisyklių, kurios gali apriboti prieigą, atskleidimą ar perdavimą;
- patvirtinti arba atsisakyti suteikti prieigą, kartu informuojant Regiono IS direktorių, vyriausiąjį atitikties pareigūną, įmonės informacinių sistemų saugumo vadovą ir Grupės IS vykdančiąjį direktorių.

Patvirtinus, prieiga bus suteikiama VEK lygmeniu, laikantis „Danone“ gairių dėl vyriausybės institucijų patikrinimų be išankstinio įspėjimo, vidinės tyrimo politikos, vidinių tyrimų gairių ir patikrinimų vietoje politikos.

Kai prieigos reikia prie elektroninių ryšių išteklių turinio, prie kurio negali tiesiogiai prieiti VEK darbuotojas, Grupės AP vyriausiasis atitikties pareigūnas pateiks prašymą raštu vyriausiajam atitikties pareigūnui. Patvirtinus prieigą perduodama vyriausiajam saugumo ir konkurencijos pareigūnui, regiono IS direktoriui, įmonės informacinių sistemų saugumo valdytojui ir IS valdybos direktoriui, techniniam vertinimui ir vykdymui per laikotarpį, suderintą su atitinkama institucija.

Jei nei Grupės AP, nei paskirtam grupės direktoriui nesuteikta teisė tai padaryti, tada įtraukiamas hierarchinė struktūros (*angl.* WBS) atitikimas.

Vidaus tyrimai

Kiekviena prieiga prie elektroninių ryšių išteklių, reikalingų vykdančiam vidaus tyrimą, vykdoma laikantis atitikties pagrindų politikos, vidaus tyrimo politikos, vidaus tyrimų gairių ir patikrinimų vietoje politikos.

Verslo operacijos (toliau – darbuotojų laikinas nebuvimas ir išvykimas)

Paprastai VEK skatinamos naudoti būdus ar procedūras, kurios kuo labiau mažintų darbuotojo prieigų skaičių prie elektroninių ryšių išteklių poreikį, pvz., pranešimai apie neatvykimą, darbo grupės paskyras, automatinį persiuntimą su filtrais, adresų sąrašus. Vis dėlto VEK taip pat turėtų būti įdiegtos procedūros, skirtos tvarkyti laikiniams neatvykimams ar išvykimams. Šios procedūros apima:

- sąlygas, reglamentuojančias VEK prieigą prie elektroninių ryšių išteklių ir jų turinio, pakartotinio naudojimo ar išvykus;
- asmeninių elektroninių ryšių įrašų tvarkymo nurodymus, pvz., ar turėtų būti ištrinta, ar perkelta į kitas asmenines el. pašto paskyras, ar kitas asmenines laikmenas;

- nurodymus, ar turi būti įdiegtas pranešimas apie neatvykimą, nurodant atjungimo datą ir papildomą kontaktinę informaciją VEK;
- data, kada paskyra bus uždaryta ir nebus prieinama išvykusiam darbuotojui.

Darbuotojai turi būti informuojami apie šias procedūras įdarbinant ir prireikus turėtų sutikti su pirmiau minėtomis sąlygomis.

Jei neatvykusio ar išvykusio darbuotojo prieiga prie elektroninio ryšio išteklių turi būti išlaikyta „Danone“ operacijų tikslu, ir nebuvo gautas tinkamas leidimas prieš neatvykimą ar išvykimą, tik Grupės AP gali jį suteikti. Prašymą prieigai raštu turi pateikti darbuotojo tiesioginis vadovas, taip pat visa svarbi informacija, pvz., prašymo pagrindimas, siūloma prieigos apimtis (yra primygtinai rekomenduojama pagal raktinius žodžius susieta prieiga arba apibrėžta siuntėjų ar gavėjų prieiga), prašyme turi būti įtrauktas asmenų, dalyvaujančių prieigose ir informacijos gavime bei jų saugojimo laikotarpis.

Grupės AP kartu su teisėtu grupės vadovu arba pastarajam nesant, teisininku, įvertina prašymo pagrįstumą ir laikosi visų taikomų privatumo ir duomenų apsaugos įstatymų bei konkrečių taisyklių, kurios gali riboti prieigą ir patvirtinti ar atmesti.

Prieiga leidžiama tik dėl atitinkamų verslo priežasčių, o kai reikės, kad atitiktų laiko ir kritinius operatyvinius poreikius.

Jei leidžiama, prieiga perduodama įmonės techniniam informacinių sistemų saugumo valdytojo ir IS valdybos direktoriaus vertinimui. Vyriausiasis atitikties pareigūnas ir vyriausiasis saugumo ir konkurencijos pareigūnas informuojami tuo pačiu metu. Po techninio įvertinimo, įmonės informacinių sistemų saugumo valdytojas per 48 valandas informuoja prašytoją, kam bus suteikta teisė prie prieigos ir kada.

Jei nei Grupės AP, nei paskirtas grupės direktorius nesuteikė teisės tai padaryti, tada įtraukiamas hierarchinė struktūros (*angl.* WBS) atitikimas.