2. PRIVALOMOS IR REKOMENDUOJAMOS POLITIKOS BEI TVARKOS

Jau minėta, kad atsakomybė dėl netinkamo asmens duomenų tvarkymo gali būti taikoma ne tik įmonėms, kurių tvarkomų asmens duomenų saugumas buvo pažeistas, bet ir toms, kurių tvarkomų asmens duomenų saugumas nebuvo pažeistas, tačiau kurios nesilaikė Reglamento reikalavimų dėl tokių duomenų tvarkymo. Kitaip tariant, vien aplinkybė, kad įmonė nesirūpina tinkamu asmens duomenų rinkimu, saugojimu bei tvarkymu, gali tapti pagrindu taikyti administracinę atsakomybę. Nors atsakymas į klausimą, kaip to išvengti, gana paprastas – reikia vadovautis Reglamento nuostatomis, realybėje tai įgyvendinti nėra lengva.

Kiekviena įmonė, įvertinusi, kokius duomenis, laikytinus asmens duomenimis, ji renka, saugo bei tvarko, turėtų pasitvirtinti aiškias taisykles (procedūras, politikas), kaip tokie duomenys turi būti renkami, kas juos tvarko, kaip jie saugomi ir pan. Tai padarius, įmonė galėtų teigti, kad ji ėmėsi reikiamų priemonių, skyrė dėmesio šiam klausimui, jog asmens duomenys būtų renkami ir saugomi tinkamai, – taip, kaip reikalauja teisės aktai. Tokios įmonėje parengtos vidinės procedūros bei tvarkos atspindėtų siekį tvarkyti šią sritį, o tai mažintų galimybę sulaukti sankcijų dėl netinkamai saugomų asmens duomenų. Žinoma, vien parengtų dokumentų nepakaktų. Būtina, kad įmonė, tvarkydama asmens duomenis, įgyvendintų juose realybėje.

Priminsime, kad ir Reglamento 24 str. nustatyta, kad, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad *užtikrintų ir galėtų įrodyti*, jog duomenys tvarkomi laikantis Reglamento. Ten pat įtvirtinta, kad **tokios nurodytosios priemonės apima duomenų valdytojo įgyvendinamą atitinkamą duomenų apsaugos politiką**. Taigi, Reglamentas lyg ir paaiškina, kad tokių įmonėje patvirtintų techninių organizacinių priemonių visuma laikytina asmens duomenų apsaugos politika, kuri gali tapti vienu iš įrodymu dėl tinkamo duomenų tvarkymo. Kad tokių priemonių visuma laikytina atitinkama įmonės asmens duomenų apsaugos politika, pakartojama ir Reglamento 39 str., aptariančiame duomenų apsaugos pareigūno pareigas. Nustatyta, kad viena iš jam keliamų užduočių – *stebėti, kaip laikomasi teisės aktų reikalavimų ir duomenų valdytojo arba duomenų tvarkytojo politikos asmens duomenų apsaugos srityje, įskaitant pareigų pavedimą, duomenų tvarkymo operacijose dalyvaujančių darbuotojų informuotumo didinimą bei mokymą ir susijusius auditus*. Štai kodėl įmonės vidaus dokumentus, kurie susiję su asmens duomenų tvarkymu, įvardijame kaip tam tikrą politiką asmens duomenų apsaugos srityje, nors faktiškai įmonės šiuos dokumentus gali vadinti tvarkomis, procedūromis ir pan. Svarbiausia, kad jų turinys būti tinkamas ir jose nustatyti reikalavimai būtų įgyvendinami.

2.1. Įmonės asmens duomenų apsaugos politika

Kiekviena įmonė laisva nuspręsti, kiek ir kokių vidinių tvarkų, susijusių su asmens duomenų tvarkymu, ji pasirengs, kaip jas pavadins. Žinoma, tai priklauso ir nuo įmonės veiklos pobūdžio, nes įmonės, vykdančios skirtingą veiklą, tvarko skirtingus kiekius bei skirtingo pobūdžio asmens duomenis, tad jos turėtų pasirengti ir skirtingas tvarkas, tinkamas tik tai įmonei ir pritaikytas prie jos veiklos specifikos. Akivaizdu, kad įmonės, kurios pagrindinė veikla siejama su paslaugų teikimu juridiniams asmenims, asmens duomenų apsaugos politika gerokai skirsis nuo įmonės, kurios veikla orientuota į paslaugas fiziniams asmenims (pvz., sporto klubai, medicininių paslaugų centrai, vaikų ugdymo ir mokymo įstaigos bei pan.).

Nepaisant visko, manytina, kad kiekviena įmonė turėtų pasirengti vieną **visiems įmonėje renkamiems, saugomiems bei tvarkomiems asmens duomenims taikomą bendrą politiką** – *Asmens duomenų apsaugos politiką*. Joje turėtų būti aptarti esminiai bendri tokių duomenų tvarkymo klausimai. Ši politika būtų bendra ir apimtų visas asmens duomenų grupes, pvz., įmonės personalą, pirkėjus, skolininkus ir pan., o konkrečius tam tikros grupės asmens duomenų tvarkymo klausimus būtų galima aptarti *atskirose tvarkose, kurios būtų skirtos tik toms duomenų grupėms* (pvz., darbuotojų, pirkėjų, skolininkų ar pan.).

TVIRTINU:

_____

direktorius _____

Įsakymas 20 ___-___-___ Nr. _____

UAB „_____“
ASMENS DUOMENŲ APSAUGOS POLITIKA

Naudojamų sąvokų apibrėžimai

Įmonė – UAB „_____“, juridinio asmens kodas _____, registruotas buveinės adresas _____.

Darbuotojas – įmonėje darbo sutarties pagrindu dirbantis asmuo.

Vadovas – įmonės direktorius.

Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.

Politika – ši Asmens duomenų apsaugos politika.

Tikslas ir apimtis

Asmens duomenų apsaugos politika parengta ir taikoma siekiant apsaugoti įmonės darbuotojus, partnerius ir klientus nuo neteisėtų ir žalą sukeliančių tiesioginių ar netiesioginių, sąmoningų ar nesąmoningų asmenų veiksmų, tvarkant jiems prieinamus asmens duomenis, taip pat šiems tikslams naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.

Politika privalo būti taikoma įmonėje tvarkant bet kuriose sistemose ar bet kurioje laikmenoje esamus asmens duomenis, nepaisant to, ar jų tvarkymas yra susijęs su vidinėmis įmonės verslo operacijomis ar su išoriniais įmonės ryšiais su bet kokiomis trečiosiomis šalimis. Ji taip pat taikoma darbuotojams, jų darbinių pareigų atlikimo metu naudojantiems jiems suteiktą įrangą ir įrankius.

Bet kurie duomenys, kurie gali būti pripažinti asmens duomenimis, kurie tampa prieinami ir žinomi darbuotojams darbinių pareigų atlikimo metu, laikoma konfidencialia įmonei priklausančia informacija, kuri yra saugoma ir kuri negali būti atskleidžiama nei kitiems darbuotojams, nei kitiems asmenims. Išimtis – tokie duomenys gali būti atskleidžiami tik tiems darbuotojams, kurie pagal įmonės nustatytas tvarkas dėl jų atliekamų pareigų turi teisę susipažinti su tokiais duomenimis. Įmonė nurodo, kad tokie duomenys privalo būti saugomi nepaisant to, kokios formos jie pateko darbuotojui (atspausdinti ar bet kokiame duomenų saugojimo įrenginyje, kaip garso / vaizdo medžiaga ar kt.).

Darbuotojų pareigos

Visi asmens duomenys ir kita informacija, pagal kurią galima nustatyti asmens tapatybę, renkama ir tvarkoma tik tada, kai tai reikalinga, ir tik tokia apimtimi, kokia reikalinga tam, kad darbuotojas galėtų atlikti darbines funkcijas jam suteiktų įgaliojimų ribose ir prisilaikant įstatyminių reikalavimų duomenų apsaugai, ypač 2016 m. balandžio 27 d. Reglamento (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).

Asmens duomenys, patenkantys darbuotojui darbinių pareigų atlikimo metu, yra laikomi ir traktuojami kaip konfidencialūs ir saugomi pagal šios politikos nuostatas; jie negali būti atskleidžiami be teisėto pagrindo. Darbuotojas, abejojantis, ar turi teisę kitam darbuotojui ar asmeniui atskleisti bet kokius asmens duomenis, privalo kreiptis į vadovą ar į vadovo paskirtą įgaliotą asmenį, kad gautų patvirtinimą dėl tolesnių veiksmų su asmens duomenimis.

Kiekvienas Darbuotojas privalo laikytis šios politikos, taip pat ir taikytinų įstatymų bei taisyklių, kuriomis nustatyti asmens duomenų rinkimo, saugojimo bei tvarkymo reikalavimai. Politikos nesilaikymas bus laikomas šiurkščiu darbo pareigų pažeidimu ir, įmonės pasirinkimu, gali užtraukti drausmines sankcijas arba darbuotojo atleidimą. Pažeidimą padariusiam darbuotojui taip pat gali kilti administracinė arba baudžiamoji atsakomybė.

Kompiuterinių sistemų naudojimas

Bet kokie kompiuteriniai įrenginiai bei elektroninės duomenų bazės darbuotojams yra pasiekiami atsižvelgiant į jų darbines pareigas, atsakomybę ir vadovaujantis „būtinumo žinoti“ principu. Taip pat įmonė pabrėžia, kad darbuotojo priėjimas prie bet kokios duomenų bazės nereiškia, kad darbuotojas yra įgaliotas peržiūrėti ir naudoti visą toje bazėje esančią informaciją.

Įmonėje gali būti taikomi naudotojų ID, kurie yra unikalūs ir identifikuoja konkretų darbuotoją. Kiekvienas darbuotojas yra atsakingas už visus veiksmus, susijusius su jo asmenine ID paskyra, todėl

pagrindinė pareiga yra užtikrinti, kad darbuotojo ID yra neprieinamas trečiosioms šalims, netgi kitiems darbuotojams, nebent įmonė būtų nustačiusi kitokią tvarką.

Kompiuterines sistemas ir duomenų bazes apsaugantys slaptažodžiai yra sudaromi atsakingai, kad nebūtų lengva juos atspėti, kad jie neapimtų asmens duomenų ir pagal poreikį būtų reguliariai keičiami. Kiekvienas darbuotojas yra asmeniškai atsakingas už savo slaptažodžio saugojimą ir atitiktį šios politikos nuostatoms ir bet kokioms kitoms įmonės taisyklėms.

Išskyrus konkrečias išimtis, jokiais atvejais ir jokiomis aplinkybėmis įmonei, jos klientams ar bendradarbiavimo partneriams priklausantys įrenginiai ir / ar sistemos negali būti naudojami su darbuotojo darbo pareigomis ar su įmonės verslo veikla nesusijusiems tikslams.

Saugumo priemonės

Visiems bet kokiu būdu surinktiems ir tvarkomiems bet kokios formos (popierinės, elektroninės, kt.) asmens duomenims ir su jais susijusiai informacijai taikomi šios politikos ir bet kokių įstatymų reikalavimai dėl duomenų bei informacijos rinkimo, tvarkymo, apsaugos ir tolesnio saugojimo – tokie dokumentai saugomi saugioje įmonės paskirtoje vietoje taikytinų įstatymų ir / arba įmonės nustatytą laikotarpį.

Darbuotojams neleidžiama laikyti bet kokios su asmens duomenimis susijusios informacijos savo įrenginiuose, išskyrus atvejus, kai jos laikinai reikia specifinei su darbu susijusiai veiklai. Visa reikalinga konfidenciali ir asmens tapatybę leidžianti nustatyti informacija turi būti saugoma tik įmonės specialiai nurodytoje nuotolinėje saugykloje ir įmonės intranete. Reikėtų vengti bet kokio tokių bylų parsisiuntimo į vietinius įrenginius ir tokius veiksmus atlikti tik esant būtinybei, susijusiai su informacijos tvarkymu darbiniais tikslais.

Laikydamiesi taikytinų įstatymų ir taisyklių, tinkamai įgalioti įmonės atstovai gali filtruoti ir stebėti darbuotojų interneto prieigą ir internete vykdomas operacijas.

Į įmonėje naudojamą įrangą gali būti instaliuojamos ir naudojamos tik įmonės leidžiamos sistemos ir licencijuota programinė įranga. Prieš parsisiunčiant ir instaliuojant bet kokią programinę įrangą į darbuotojų turimus ir naudojamos įrenginius, dėl šioje politikoje nurodytų priežasčių reikalingas atitinkamo įmonės specialisto leidimas.

Tais atvejais, kai darbuotojai, prisijungdami prie darbinių įmonės išteklių (pvz., ryšių su klientais valdymo sistemos, elektroninio pašto, internetinės / nuotolinės duomenų bazės), naudoja namų įrenginius, darbuotojai privalo laikytis šios politikos reikalavimų taip pat, kaip ir naudodami įmonės suteiktą įrangą. Atitinkamai draudžiama saugoti bet kokius su asmens duomenimis susijusius duomenis ir informaciją įrenginyje – bet koks duomenų tvarkymas leidžiamas tik per įmonės naudojamas nuotolines arba internetines saugyklas.

Visais atvejais griežtai draudžiama naudotis viešais prieigos įrenginiais (pvz., interneto kavinėse, bibliotekose, kt.), nebent tai ypač svarbus ir skubus darbas, ir darbuotojas gauna aiškų rašytinį sutikimą dėl tokių veiksmų.

Tuo atveju, jeigu darbuotojui suteikiama prieiga prie įmonės kliento ar bendradarbiavimo partnerio bylų saugojimo sistemos, darbuotojas privalo naudoti kliento arba partnerio suteiktus prieigos įrankius bei laikytis jam nurodytų informacijos / duomenų tvarkymo saugumo taisyklių reikalavimų (įskaitant šifravimo sistemų, slaptažodžių, duomenų naudojimo apribojimų, nurodytų buvimo vietų naudojimą ir kt.).

Kai įmonės nuožiūra saugomi asmens duomenys ir su jais susijusi informacija tampa nebereikalinga įmonės veikloje, tokie duomenys ir informacija ištrinama, visos jos kopijos sunaikinamos, o su atitinkamos informacijos ir duomenų tvarkymu susiję darbuotojai atitinkamai informuojami apie

jų pareigą ištrinti bei sunaikinti duomenis, kurių jiems nebereikia darbinėms funkcijoms vykdyti. Toks reikalavimas grąžinti įmonei, ištrinti ir sunaikinti kopijas automatiškai taikomas tuo atveju, kai nutraukiami atitinkamo darbuotojo darbo santykiai.

Pranešimas apie saugumo incidentus

Apie visus asmens duomenų tvarkymo saugumo incidentus ar grėsusius incidentus turi būti nedelsiant pranešta vadovui, be to, turi būti nedelsiant imamasi priemonių, kad būtų išvengta galimos žalos, panaikinta atsiradusi žala ir atkurta buvusi saugumo būsena.

Prireikus, vadovas imasi pareigos užtikrinti, kad apie asmens duomenų ir su jais susijusios informacijos saugumo pažeidimus būtų pranešta valdžios institucijoms ir susijusiems asmenims, kaip numatyta taikytinuose įstatymuose ir taisyklėse ir / arba Europos Sąjungos įstatymuose.