UAB „NEVDA“ SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO

versija 1.1

Turinys

1. Įvadas

UAB „Nevda“ pagrindinė veikla – informacinių sistemų kūrimas, diegimas ir priežiūra viešojo sektoriaus organizacijoms ir verslo bendrovėms.

Apžvalga

Šis susitarimas dėl asmens duomenų tvarkymo yra sudarytas tarp UAB „Nevda“ įmonės kodas 121931451, toliau (Paslaugų teikėjas) ir Kliento, kartu Susitarime vadinamos „Šalimis“ arba kiekviena atskirai „Šalimi“ ir atsižvelgdamos į tai, kad:

- Šalys sudarys paslaugų teikimo sutartį, kurios pagrindu Duomenų tvarkytojas teikia paslaugas Duomenų valdytojui (toliau – Sutartis);
- Sutarties pagrindu Duomenų tvarkytojas, Duomenų valdytojo vardu tvarko Duomenų valdytojo pateiktus atitinkamų duomenų subjektų asmens duomenis;
- Šalys siekia, jog Sutartis būtų vykdoma laikantis asmens duomenų apsaugos reikalavimų ir todėl sudarė šį Susitarimą (toliau – Susitarimas) dėl asmens duomenų tvarkymo prie Sutarties žemiau nurodytomis sąlygomis

Naudojamos sąvokos, sutrumpinimai

Sąvokų trumpiniai	Aprašymas
Asmens duomenys	asmens duomenys (neįskaitant specialių kategorijų asmens duomenų), kaip jie apibrėžti Reglamento 4 straipsnio 1 dalyje, kuriuos Duomenų valdytojas pateikia Duomenų tvarkytojui ar/ir sudaro prieigą prie jų, laikantis šiame Susitarime nurodytų sąlygų;
Asmens duomenų subjektas	fizinis asmuo, kurio Asmens duomenys tvarkomi laikantis Reglamento, kitų asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų, šiame Susitarime nurodytų sąlygų;
Duomenų tvarkymas	bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis atliekama operacija ar operacijų seka, įskaitant, bet neapsiribojant: rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;
Reglamentas arba BDAR	reiškia Europos Parlamento ir Tarybos reglamentą (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)“;

Incidentas	Duomenų valdytojo valdomoje informacinių technologijų infrastruktūroje įvykęs įvykis ar aplinkybių visuma, kuri įtakoja Duomenų tvarkytojo teikiamų paslaugų ar sistemų veiklos sutrikimus;
Asmens duomenų saugumo pažeidimas	įvykis ar aplinkybių visuma, kuri gali įtakoti asmens duomenų sunaikinimą, praradimą, pakeitimą, neteisėtą atskleidimą ar prieigos prie asmens duomenų neteisėtą gavimą;
Duomenų valdytojo atsakingas asmuo	Duomenų valdytojo paskirtas atsakingas asmuo (administratorius arba saugos įgaliotinis), kuris koordinuoja incidentų sprendimą ir kontroliuoja prieigos teisių suteikimą prie Duomenų valdytojo IS saugomų duomenų;

Kitos sąvokos Susitarime vartojamos ta reikšme, kaip ji apibrėžta Sutartyje ir Asmens duomenų apsaugos teisės aktuose.

2. Duomenų tvarkymo tikslas, pobūdis

Sutarties vykdymo tikslu Duomenų tvarkytojui perduodami Duomenų valdytojo tvarkomi asmens duomenys ir (ar) jų rinkiniai, su kuriais Duomenų tvarkytojui yra reikalinga automatizuotomis priemonėmis atlikti duomenų tvarkymo veiksmus.

3. Duomenų tvarkymo trukmė

Šis Susitarimas taikomas tol, kol Duomenų tvarkytojas tvarko asmens duomenis Duomenų valdytojo vardu pagal Sutartį ir šį Susitarimą.

4. Duomenų tvarkytojo įsipareigojimai

- Duomenų tvarkytojas įsipareigoja tvarkyti tik šiame Susitarime nurodytus asmens duomenis bei Susitarime nustatytais tikslais, taip pat laikydamasis Asmens duomenų apsaugos teisės aktų, Reglamento bei Duomenų valdytojo dokumentais įformintų nurodymų.
- Duomenų tvarkytojas paskiria Duomenų apsaugos pareigūną, kuris užtikrina užduočių, nurodytų BDAR 39 straipsnyje, tinkamą vykdymą.
- Duomenų tvarkytojas Susitarimo galiojimo laikotarpiu įgyvendina tinkamas technines bei organizacines priemones, užtikrinančias, kad jo vykdomas asmens duomenų tvarkymas pagal šio Susitarimo nuostatas atitiktų taikomus duomenų apsaugos teisės aktų reikalavimus, konkrečiai – BDAR reikalavimus, ir garantuotų duomenų subjekto teisių apsaugą. Sutarties bei šio Susitarimo sudarymo metu Duomenų tvarkytojo naudojamų techninių ir organizacinių priemonių aprašas pateiktas Priede Nr. 1.
- Duomenų tvarkytojas, atsižvelgdamas į duomenų tvarkymo pobūdį ir galima apimtimi panaudodamas tinkamas technines bei organizacines priemones, padeda Duomenų valdytojui įvykdyti Duomenų valdytojo prievolę atsakyti į prašymus pasinaudoti duomenų subjekto teisėmis. Pagal šį Susitarimą, duomenų subjekto teisės apima teises prašyti

informacijos ir – duomenų subjekto pageidavimu – pataisyti, sunaikinti asmens duomenis arba sustabdyti asmens duomenų tvarkymo veiksmus.

- Duomenų tvarkytojas, atsižvelgdamas į duomenų tvarkymo pobūdį bei turimą informaciją, padeda Duomenų valdytojui įvykdyti konkrečias prievoles pagal taikomus duomenų apsaugos teisės aktus. Konkrečios prievolės apima duomenų tvarkymo saugumą (BDAR 32 straipsnis), pranešimą apie asmens duomenų saugumo pažeidimą (BDAR 33–34 straipsniai) ir poveikio duomenų apsaugai vertinimą bei išankstines konsultacijas (BDAR 35–36 straipsniai).
- Duomenų tvarkytojas įsipareigoja pateikti Duomenų valdytojui visą informaciją ir suteikti jam visą pagalbą siekiant įrodyti, kad yra vykdomi pagal šį Susitarimą prisiimti įsipareigojimai, taip pat sudaro sąlygas bei padeda Duomenų valdytojui arba kitam jo įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus vietoje.
- Duomenų valdytojas savo sąskaita gali atlikti išsamesnį auditą, kuris turi būti:
    - apribotas tik klausimais, konkrečiai susijusiais su Duomenų valdytoju ir iš anksto suderintais su Duomenų tvarkytoju;
    - atliktas įspėjus prieš protingą laikotarpį, kuris negali būti trumpesnis kaip 4 savaitės, išskyrus atvejus, kai tam iškyla atpažįstamų esminių kliūčių;
    - atliekamas tokiu būdu, kad netrukdytų kasdienei Duomenų tvarkytojo veiklai.

5. Pagalbiniai duomenų tvarkytojai

- Duomenų tvarkytojas turi teisę pasitelkti kitą duomenų tvarkytoją. Duomenų tvarkytojas privalo užtikrinti, jog jo pasitelktas asmuo laikytųsi Asmens duomenų apsaugos teisės aktų reikalavimų (įskaitant tinkamų organizacinių ir techninių priemonių įgyvendinimą) ir šiuo Susitarimu Duomenų tvarkytojui nustatytų pareigų ne mažesne apimtimi nei pats Duomenų tvarkytojas bei atsako Duomenų valdytojui už pasitelkto trečiojo asmens prievolių vykdymą.
- Duomenų tvarkytojas užtikrina ir, Duomenų valdytojo prašymu, dokumentais patvirtina, kad pagalbiniai duomenų tvarkytojai yra įsipareigoję pagal rašytines sutartis, pagal kurias – be šiame Susitarime nustatytų įsipareigojimų jie privalo vykdyti atitinkamas duomenų tvarkymo prievoles. Duomenų tvarkytojas yra visiškai atsakingas Duomenų valdytojui už pagalbinių duomenų tvarkytojų vykdomus įsipareigojimus.

6. Duomenų perdavimas į trečiąsias šalis

- Įsipareigojimas tvarkyti asmens duomenis pagal Susitarimą gali būti vykdomas tik Europos Sąjungos (ES) valstybėje narėje arba Europos ekonominės erdvės (EEE) valstybėje narėje. Bet koks asmens duomenų perdavimas į šalį, kuri nėra ES ar EEE valstybė narė, gali būti vykdomas tik gavus Duomenų valdytojo išankstinį rašytinį sutikimą ir tik tuo atveju, jei yra įvykdytos specialios sąlygos, nurodytos taikomuose duomenų apsaugos teisės aktuose, BDAR V skyriuje.

7. Informacijos saugumas ir konfidencialumas

- Duomenų tvarkytojas užtikrina tinkamą asmens duomenų apsaugą pagal šį Susitarimą su tikslu apsaugoti asmens duomenis nuo sunaikinimo, pakeitimo, neteisėto platinimo arba neteisėtos prieigos. Asmens duomenys taip pat saugomi nuo kitokio pobūdžio neteisėto tvarkymo.

- Duomenų tvarkytojas parengia ir nuolat atnaujina savo techninių, organizacinių ir fizinių priemonių aprašymą, kad šis atitiktų taikomų duomenų apsaugos teisės aktų reikalavimus.
- Be Duomenų valdytojo išankstinio rašytinio sutikimo Duomenų tvarkytojas įsipareigoja neatskleisti pagal šį Susitarimą tvarkomų asmens duomenų ar kitaip neleisti su jais susipažinti jokiai trečiajai šaliai, išskyrus pagalbinius duomenų tvarkytojus, kurie pasitelkiami pagal šį Susitarimą.
- Duomenų tvarkytojas užtikrina, kad visi su asmens duomenų tvarkymu susiję asmenys konfidencialumo sutartimi visam laikui būtų įsipareigoję užtikrinti konfidencialumą arba, kad jiems būtų taikoma atitinkama įstatymais nustatyta konfidencialumo prievolė.
- Jei dėl kokių nors priežasčių bet kuri iš Šalių negali vykdyti šio Susitarimo sąlygų, ji privalo nedelsiant apie tai informuoti kitą Šalį.

8. Asmens duomenų saugumo pažeidimai

- Asmens duomenų saugumo pažeidimo atveju ar Duomenų tvarkytojui pagrįstai įtariant tokį pažeidimą, Duomenų tvarkytojas nedelsiant, tačiau bet kokiu atveju ne vėliau nei per 24 val. po to, kai sužinojo apie tai, raštu informuoja apie tai Duomenų valdytoją ir pateikia turimą informaciją bei duomenis, susijusius su tokiu pažeidimu.
- Duomenų valdytojui pareikalavus, Duomenų tvarkytojas atsižvelgdamas į technines galimybes nepagrįstai nedelsdamas pateikia Duomenų valdytojui papildomus reikalaujamus dokumentus, informaciją ir duomenis, reikalingus tam, kad Duomenų valdytojas galėtų nustatyti ir (ar) patikrinti Asmens duomenų saugumo pažeidimo faktą, ištirti jo aplinkybes ir imtis neatidėliotinų priemonių pažeidimui pašalinti ar neigiamoms jo pasekmėms sumažinti.

9. Duomenų tvarkytojo atsakomybė, ginčų sprendimo tvarka ir kontaktiniai asmenys

- Atsižvelgiant į Asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, įskaitant aplinkybę, jog Asmens duomenis Duomenų tvarkytojas yra priverstas tvarkyti kaip neatskiriamą Sutarties tinkamo įgyvendinimo sąlygą, Šalys laiko, jog Susitarimo pažeidimo/ netinkamo vykdymo, Reglamento pažeidimo atveju Duomenų tvarkytojas atlygins atsiradusią žalą.
- Šalys neprisiima atsakomybės už eksploatacinius nuostolius, pelno netekimą, prestižo praradimą ir bet kokius kitus netiesioginius nuostolius bei jų padarinių žalą.

Duomenų tvarkytojo naudojamų techninių ir organizacinių saugos priemonių kontrolinis sąrašas

Priemonės pavadinimas	Priemonės naudojimo aprašymas
Rizikos valdymas (reguliarus tikrinimas, vertinimas ir veiksmingumo vertinimas)	• vykdoma reguliari materialių ir nematerialių nuostolių, kurių gali atsirasti vykdant duomenų tvarkymo veiklą ir pagrindinėse duomenų tvarkymo sistemose, analizė;

	• vieną kartą metuose vykdomas rizikos vertinimas (ISO 27005 standartas) informacijos saugai, bei atitikties vertinimas.
Prieigos kontrolė	• nustatyta fizinio saugumo koncepcija, kuri apibrėžia saugumo zonas (viešąsias erdves, biurą, duomenų centrą); • prieiga kontroliuojama prieigos leidimais; • prieiga prie duomenų centro yra apsaugota išplėstinėmis apsaugos priemonėmis; • prieiga prie asmens duomenų yra suteikiama užtikrinant saugų registracijos procesą ir saugią slaptažodžio politiką (stiprūs slaptažodžiai, reguliarus slaptažodžių keitimas)‘ • nustatyta prieigos leidimų patvirtinimo ir atšaukimo procedūra, ir slaptažodžiai yra saugiai perduodami; • prieigos leidimai yra reguliariai tikrinami ir atnaujinami; • išorės prieigos prie asmens duomenų galima tik naudojant šifravimo metodus (SSL ir/arba VPN).
Informacinio tinklo kontrolė	• naudojama ugniasienė, siekiant saugiai izoliuoti informacines sistemas nuo išorinės prieigos iš viešųjų tinklų; • antivirusinės programinės įrangos naudojimas yra reguliariai tikrinamas; • reguliariai importuojami atitinkami saugumo atnaujinimai.
Perdavimo kontrolė	• nuotolinė prieiga (per viešuosius tinklus) visuomet yra šifruojama; • yra nustatytos fizinio dokumentų sunaikinimo specifikacijos ir procesai.
Saugojimo kontrolė	• yra nustatytos asmens duomenų saugojimo taisyklės; • prieiga prie asmens duomenų, pagrįsta priskirtomis asmeninėmis vartotojų paskyromis; • yra duomenų perdavimo žurnalo failai/protokolai.
Nurodymų kontrolė	• yra nustatytos pareigos (pvz., duomenų savininkas, sistemos prižiūrėtojas) duomenų tvarkymo ir susijusių sistemų užduotims; • yra aiškiai reguliuojamos atsakomybės už duomenų tvarkymą sritys (duomenų valdytojas <-> duomenų tvarkytojas, pagalbinis duomenų tvarkytojas ir t.t.);

	• darbuotojai yra mokomi duomenų apsaugos klausimais, ir yra numatytos informuotumo didinimo priemonės; • Duomenų tvarkytojo darbuotojų reikalaujama laikytis atskiro konfidencialumo susitarimo; • Pagalbiniai duomenų tvarkytojai, kuriems suteikiama prieiga prie duomenų valdytojo duomenų, laikosi visų techninių ir organizacinių priemonių, įtrauktų į šį kontrolinį sąrašą.
Prieinamumo užtikrinimo kontrolė	• yra numatytos fizinės saugos priemonės, skirtos apsaugoti galimybę naudotis asmens duomenimis (priešgaisrinės apsaugos priemonės, oro kondicionavimas, UPS apsauga); • yra reguliariai daromos atsarginės duomenų kopijos; • atsarginės duomenų kopijos yra saugomos išorės saugykloje ar saugioje alternatyvioje aplinkoje; • yra nuolat automatiškai stebimas sistemų veikimas; • pranešama apie IT incidentus ir priemones, taikytas sistemų veikimo problemoms išspręsti; • yra numatytos priemonės, skirtos nustatyti potencialius duomenų apsaugos incidentus.
Atskyrimo kontrolė	• yra atskirtos produkcijos ir testavimo sistemos; • Duomenų tvarkytojo darbuotojams yra duoti nurodymai, kad asmens duomenys gali būti tvarkomi tik numatytais tikslais.