

Duomenų tvarkymo sutartis,

sudaryta tarp

- Duomenų valdytojo, toliau vadinamo Klientu,
ir

ALSO Lietuva UAB, Verslo g. 6, Kumpių k., Domeikavos sen., 54311 Kauno raj.

- Duomenų tvarkytojo, toliau vadinamo Paslaugų teikėju

1. Užsakymo arba Sutarties objektas ir galiojimo trukmė

1) Objektas

Užsakymo arba Sutarties dėl duomenų tvarkymo objektas yra toliau išvardytos Paslaugų teikėjo teikiamos paslaugos arba vykdomos užduotys: techninė pagalba, užsakymų tvarkymas, IT paslaugos, klientų aptarnavimas, debesijos paslaugos.

2) Galiojimo trukmė

Šio Užsakymo galiojimo trukmė (terminas) atitinka Paslaugų sutarties, susijusios su atitinkama produkty, paslaugų, pirkimo ir (arba) darbų sutartimi, terminą.

2. Išsamūs Užsakymo arba Sutarties duomenys

(1) Numatyto duomenų tvarkymo pobūdis ir paskirtis

Išsamus Paslaugų teikėjo teikiamų paslaugų pobūdžio ir paskirties aprašymas:

| Duomenų pobūdis | Tvarkymo tikslas | Duomenų subjektas |
|---|---|---|
| Asmens duomenys: vardas, pavardė, kontaktiniai duomenys, banko sąskaitos duomenys | Užsakymų tvarkymas, techninė pagalba, IT paslaugos, klientų aptarnavimas, debesijos paslaugos | Duomenų valdytojo darbuotojai, verslo partneris, klientas, tiekėjas, suinteresuotieji asmenys |

Sutartyje aptartas Duomenų tvarkymas turi būti vykdomas tik Europos Sąjungos (ES) valstybėje narėje, Europos ekonominės erdvės (EEE) valstybėje narėje arba šalyje, įtrauktoje į Europos Komisijos sprendimą dėl tinkamumo. Visiems be išimties duomenų perdavimo į valstybę, kuri nėra ES arba EEE valstybė narė, atvejams reikalingas išankstinis Kliento sutikimas, ir duomenys gali būti perduoti tik tuo atveju, jeigu įvykdytos BDAR 44 str. ir kitų straipsnių sąlygos. Tinkamas duomenų apsaugos lygis šalyje, kuri nėra ES narė, turėtų būti užtikrintas standartinėmis ES standartinėmis duomenų apsaugos sąlygomis. (BDAR 46 straipsnio 2 dalies c punktas)

2) Duomenų rūšys

Tvarkomų asmens duomenų objektą sudaro šių rūšių / kategorijų duomenys: pagrindiniai asmens duomenys; kontaktiniai duomenys; pagrindiniai sutarties duomenys (sutartiniai arba teisiniai santykiai, sutartiniai ar su produktu susiję interesai); kliento istorija; sąskaitų išrašymo ir mokėjimų pagal Sutartį duomenys; atskleista informacija (gauta iš trečiųjų šalių, pavyzdžiui, kredito reitingų agentūrų arba viešųjų katalogų); informacija apie sistemos konfigūraciją ir klientų aplinką.

(3) Duomenų subjektų kategorijos

Duomenų subjektų kategorijos yra šios: duomenų valdytojo darbuotojai, verslo partneriai, klientai, potencialūs klientai, prenumeratoriai, darbuotojai, tiekėjai, kontaktiniai asmenys.

3. Techninės ir organizacinės priemonės

1) Prieš pradėdamas tvarkyti duomenis, Paslaugų teikėjas turi dokumentuoti pritaikytas būtinausias technines ir organizacines priemones, kurios buvo apibrėžtos dar prieš pateikiant Užsakymą arba sudarant Sutartį (ypač jei jos susijusios su išsamiai apibūdintu Sutarties vykdymu), ir šias dokumentuotas priemones turi pateikti Klientui patikrinti. Gavus Kliento pritarimą, dokumentuotos techninės ir organizacinės priemonės tampa Sutarties pagrindu. Jeigu patikrinęs arba atlikęs auditą Klientas nustato, kad minėtas priemones reikia pakeisti, tokie pakeitimai turi būti įgyvendinti bendru susitarimu.

2) Paslaugų teikėjas turi nustatyti saugos priemones, atitinkančias BDAR 28 straipsnio 3 dalies c punktą ir 32 straipsnį, atsižvelgiant į BDAR 5 straipsnio 1 ir 2 dalis. Priemonės, kurių reikia imtis, yra duomenų apsaugos priemonės ir priemonės, užtikrinančios tokį apsaugos lygį, kuris atitiktų su konfidencialumu, vientisumu, prieinamumu ir sistemų atsparumu susijusią riziką. Turi būti atsižvelgiama į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat dėl duomenų tvarkymo kylančius įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, kaip apibrėžta BDAR 32 straipsnio 1 dalyje. [Išsami informacija pateikiama 1 priede]

3) Techninės ir organizacinės priemonės priklauso nuo techninės pažangos ir tolesnio tobulinimo. Atsižvelgiant į tai, Paslaugų teikėjui leidžiama taikyti alternatyvias priemones, tačiau konkrečiomis priemonėmis užtikrinamas apsaugos lygis neturi sumažėti. Esminiai pakeitimai turi būti dokumentuoti.

4. Duomenų taisymas, apribojimas ir ištrynimasis

1) Paslaugų teikėjas negali savo nuožiūra taisyti, ištrinti arba apriboti Kliento vardu tvarkomų duomenų – jis tai gali padaryti tik gavęs dokumentais patvirtintus Kliento nurodymus.

Tais atvejais, kai Duomenų subjektas tiesiogiai susisiekiama su Paslaugų teikėju dėl duomenų taisymo, ištrynimo arba apribojimo, Paslaugų teikėjas privalo nedelsdamas perduoti Duomenų subjekto prašymą Klientui.

2) Tiek, kiek tai įtraukta į teikiamų paslaugų aprėptį, prašymus, susijusius su duomenų ištrynimo politika, „teisės būti pamirštam“ įgyvendinimu, duomenų taisymu, perkėlimu ir ištrynimu, Paslaugų teikėjas, vadovaudamasis dokumentais patvirtintais Kliento nurodymais, turi įvykdyti be nepagrįsto delsimo.

5. Kokybės užtikrinimas ir kitos Paslaugų teikėjo pareigos

Paslaugų teikėjas privalo laikytis ne tik šio Užsakymo arba Sutarties taisyklių, bet ir teisinių reikalavimų, išdėstytų BDAR 28–33 straipsniuose. Visų pirma Paslaugų teikėjas turi užtikrinti, kad būtų laikomasi šių reikalavimų: [pažymėkite atitinkamą langelį arba įrašykite:]

- a) Turi būti paskirtas duomenų apsaugos pareigūnas, kuris vykdo savo pareigas laikydamasis BDAR 38 ir 39 straipsnių reikalavimų.

Klientui turi būti pateikti duomenų apsaugos pareigūno kontaktiniai duomenys, kad jis galėtų susisiekti tiesiogiai. Taip pat Klientui turi būti nedelsiant pranešta apie bet kokį duomenų apsaugos pareigūno pakeitimą.

Paslaugų teikėjas paskyrė poną / ponią [nurodyti vardą, pavardę, organizacijos padalinį, telefoną, el. paštą]

.....
.....
.....
.....

eiti duomenų apsaugos pareigūno pareigas. Taip pat Klientui turi būti nedelsiant pranešta apie bet kokį duomenų apsaugos pareigūno pakeitimą.

Duomenų apsaugos pareigūno kontaktiniai duomenys turi būti lengvai prieinami Paslaugų teikėjo svetainėje.

- b) Paslaugų teikėjas neprivalo paskirti duomenų apsaugos pareigūno. Paslaugų teikėjas paskyrė poną / ponią [nurodyti vardą, pavardę, organizacijos padalinį, telefoną, el. paštą]

.....
.....
.....

Paslaugų teikėjo kontaktiniu asmeniu.

- c) Kadangi Paslaugų teikėjas yra įsikūręs už ES ribų, vadovaudamasis BDAR 27 straipsnio 1 dalimi savo atstovu Europos Sąjungoje jis paskiria poną / ponią [nurodyti vardą, pavardę, organizacijos padalinį, telefoną, el. paštą]

.....
.....
.....

- d) Konfidencialumas užtikrinamas laikantis BDAR 28 straipsnio 3 dalies antro sakinio ir b punkto nuostatų bei 29 straipsnio ir 32 straipsnio 4 dalies nuostatų. Atlikti šioje Sutartyje apibrėžtus duomenų tvarkymo darbus Paslaugų teikėjas patiki tik tiems darbuotojams, kurie įsipareigoja laikytis konfidencialumo ir jau anksčiau buvo susipažinę su jų darbui svarbiomis duomenų apsaugos nuostatomis. Paslaugų teikėjas ir bet kuris kitas jam pavaldus asmuo, turintis prieigą prie asmens duomenų, neturėtų tvarkyti šių duomenų negavęs Kliento nurodymų, išskyrus atvejus, kai tokie įgaliojimai numatyti šioje Sutartyje arba kai to reikalaujama pagal įstatymus.

- e) Siekiant laikytis BDAR 28 straipsnio 3 dalies antro sakinio ir c punkto nuostatų bei 32 straipsnio nuostatų vykdant šį Užsakymą arba Sutartį, būtina įgyvendinti visas technines ir organizacines priemones [išsami informacija pateikiama 1 priede].

- f) Priežiūros institucijai paprašius, Klientas ir Paslaugų teikėjas turi su ja bendradarbiauti ir atlikti jos užduotis.

- g) Klientui turi būti nedelsiant pranešta apie bet kokius priežiūros institucijos atliekamus patikrinimus, kiek jie susiję su šiuo Užsakymu ar Sutartimi. Ši nuostata taip pat taikoma tuo atveju, jeigu atliekamas Paslaugų teikėjo patikrinimas arba jis yra kompetentingos institucijos vykdomo tyrimo dalis dėl bet kokių civilinės, baudžiamosios ar administracinės teisės aktų arba norminių dokumentų pažeidimų, susijusių su asmens duomenų tvarkymu vykdant šį Užsakymą arba Sutartį.
- h) Jeigu priežiūros institucija vykdo Kliento patikrinimą arba vykdomas tyrimas dėl administracinės teisės pažeidimo, smulkaus nusižengimo arba baudžiamojo nusikaltimo, arba duomenų subjektas ar trečioji šalis pateikė reikalavimą atlyginti žalą arba kitokią pretenziją, susijusią su Paslaugų teikėjo vykdomu Užsakymu arba Sutartimi, Paslaugų teikėjas turi visomis jėgomis palaikyti Klientą.
- i) Paslaugų teikėjas privalo periodiškai peržiūrėti vidinius procesus ir technines bei organizacines priemones siekdamas užtikrinti, kad duomenų tvarkymas, už kurį jis atsako, atitiktų galiojančių duomenų apsaugos teisės aktų reikalavimus ir užtikrintų reikiamą duomenų subjekto teisių apsaugą.
- j) Klientui suteikta teisė patikrinti technines ir organizacines priemones, kuri yra viena iš Kliento priežiūros teisių, apibrėžta šios Sutarties 7 dalyje.

6. Kitų duomenų tvarkytojų pasitelkimas (subranga)

1) Šioje Sutartyje kitų duomenų tvarkytojų pasitelkimas (subranga) suprantamas tik kaip su pagrindinės paslaugos teikimu tiesiogiai susijusios paslaugos. Ši sąvoka neapima tokių papildomų paslaugų kaip telekomunikacijų paslaugos, pašto ir transporto paslaugos, techninės priežiūros ir vartotojų palaikymo paslaugos, duomenų laikmenų šalinimo paslaugos, taip pat kitų priemonių, skirtų užtikrinti duomenų konfidencialumą, prieinamumą, vientisumą ir duomenų tvarkymo programinės įrangos bei aparatūros atsparumą. Tačiau Paslaugų teikėjas privalo sudaryti tinkamus ir teisiškai privalomus susitarimus bei imtis atitinkamų tikrinimo priemonių, kad užtikrintų Kliento duomenų apsaugą ir duomenų saugumą net ir teikiant užsakomąsias papildomas paslaugas.

2) Užsakymai subrangovams gali būti perduoti tik atsižvelgiant į Užsakyme apibrėžtą veiklą. Apie subrangovus Klientui pranešama šiam to paprašius. Paslaugų teikėjas turi labai kruopščiai pasirinkti subrangovus, atsižvelgdamas į jų tinkamumą ir ypač į sugebėjimą laikytis ES BDAR reikalavimų, bei privalo reguliariai juos tikrinti. Be to, Paslaugų teikėjas turi sudaryti su subrangovais sutartį dėl užsakymo vykdymo, kurios nuostatos turi atitikti šios sutarties nuostatas.

3) Asmens duomenys gali būti perduoti iš Kliento subrangovams, ir šie gali pradėti juos tvarkyti tik įvykdžius visus reikalavimus.

4) Jei subrangovas teikia sutartas paslaugas už ES ribų, Paslaugų teikėjas turi užtikrinti atitiktį ES duomenų apsaugos nuostatoms, taikydamas atitinkamas priemones. Tas pats taikytina, jeigu paslaugų teikėjai pasitelkiami 1 punkto antrame sakinyje apibūdintoms paslaugoms teikti.

5) Tam, kad subrangovas galėtų naudotis užsakomosiomis paslaugomis, jis turi gauti pagrindinio Kliento sutikimą (išreikštą bent jau tekstine forma). Visos sutarčių grandinėje taikomos sutartinės nuostatos turi būti taikomos ir kitam pasitelktam subrangovui.

7. Klientui suteikti priežiūros įgaliojimai

1) Klientas, pasitaręs su Paslaugų teikėju, turi teisę pavesti atlikti patikrinimus asmeniui, įsipareigojusiam saugoti profesinę paslaptį, arba kiekvienu atskiru atveju paskiriamam auditoriui. Klientas turi teisę įsitikinti, kad vykdydamas verslo veiklą Paslaugų teikėjas laikosi šios Sutarties

reikalavimų – šiuo tikslu Klientas gali atlikti atsitiktinius patikrinimus, apie kuriuos paprastai laiku pranešama iš anksto.

2) Paslaugų teikėjas turi užtikrinti, kad Klientas galėtų patikrinti, ar Paslaugų teikėjas laikosi savo įsipareigojimų, atitinkančių BDAR 28 straipsnio nuostatas. Klientui paprašius, Paslaugų teikėjas įsipareigoja pateikti jam visą reikiamą informaciją ir, visų pirma, parodyti, kaip taikomos techninės ir organizacinės priemonės.

3) Tokių priemonių, kurios gali būti susijusios ne tik su konkrečiu Užsakymu ar Sutartimi, įrodymai gali būti pateikti įrodant, kad laikomasi BDAR 40 straipsnyje minimų elgesio kodeksų; atliekant sertifikavimą pagal patvirtintą sertifikavimo procedūrą, kaip numatyta BDAR 42 straipsnyje; pateikiant galiojančius nepriklausomo subjekto (pavyzdžiui, duomenų apsaugos pareigūno, IT saugumo skyriaus, duomenų privatumo auditoriaus, kokybės auditoriaus) atlikto audito sertifikatus, ataskaitas arba ataskaitų išrašus; sertifikuojuojant, atlikus IT saugumo arba duomenų apsaugos auditą (pavyzdžiui, pagal „BSI-Grundschutz“ (IT pagrindinį apsaugos sertifikatą, parengtą Vokietijos federalinės informacinių technologijų saugumo (BSI) tarnybos) arba ISO/IEC 27001).

4) Už suteiktą leidimą Klientui atlikti patikrinimus, Paslaugų teikėjas gali reikalauti atlygio.

8. Bendravimas Paslaugų teikėjui pažeidus reikalavimus

1) Paslaugų teikėjas turi padėti Klientui laikytis BDAR 32–36 straipsniuose apibūdintų įsipareigojimų, susijusių su asmens duomenų saugumu, pranešimais apie duomenų saugumo pažeidimus, poveikio duomenų apsaugai vertinimu ir išankstinėmis konsultacijomis. Šie reikalavimai apima:

- a) būtinybę užtikrinti tinkamą apsaugos lygį pasitelkus technines ir organizacines priemones bei atsižvelgiant į duomenų tvarkymo aplinkybes ir tikslus, taip pat atsižvelgiant į teisės akto pažeidimo, kuris gali atsirasti dėl nepakankamo saugumo, tikimybę ir tikėtiną pažeidimo sunkumą, bei užtikrinti, kad būtų galima nedelsiant nustatyti atitinkamus pažeidimo atvejus;
- b) pareigą nedelsiant pranešti Klientui apie asmens duomenų saugumo pažeidimą;
- c) pareigą padėti Klientui įvykdyti Kliento prievolę teikti informaciją atitinkamam duomenų subjektui ir nedelsiant pateikti Klientui visą susijusią informaciją;
- d) padėti Klientui atlikti poveikio duomenų apsaugai vertinimą;
- e) padėti klientui dėl išankstinių konsultacijų su priežiūros institucija.

2) Už pagalbos paslaugas, kurios nėra įtrauktos į paslaugų aprašymą ir nėra susijusios su Paslaugų teikėjo klaidomis, Paslaugų teikėjas gali reikalauti atlygio.

9. Kliento teisė duoti nurodymus

1) Klientas turi nedelsdamas patvirtinti savo žodinius nurodymus (bent jau tekstine forma).

2) Paslaugų teikėjas privalo nedelsdamas pranešti Klientui, jeigu mano, kad Kliento nurodymas pažeidžia duomenų apsaugos reikalavimus. Po to Paslaugų teikėjas turi teisę nebevykdyti atitinkamų nurodymų, kol Klientas juos patvirtins arba pakeis.

10. Asmens duomenų ištrynimasis ir grąžinimas

1) Be Kliento žinios duomenys niekada neturi būti dubliuojami, arba kuriamos jų kopijos, išskyrus atsargines kopijas, kurių reikia siekiant užtikrinti tinkamą duomenų tvarkymą arba įvykdyti norminių dokumentų reikalavimus dėl duomenų išsaugojimo.

2) Pabaigus sutartyje numatytus darbus arba anksčiau, jeigu to paprašo Klientas, bet ne vėliau negu iki Paslaugų sutarties nutraukimo, Paslaugų teikėjas, laikydamasis duomenų apsaugos reikalavimų, turi perduoti Klientui arba (gavęs šio išankstinį sutikimą) sunaikinti visus turimus su minėta sutartimi susijusius dokumentus, duomenų tvarkymo ir naudojimo rezultatus bei duomenų rinkinius. Tie patys reikalavimai taikomi bet kokiai susijusiai bandomajai, atlikusiai, perteklinei arba pašalintai medžiagai. Paprašius, turi būti pateikti sunaikinimą ar ištrynimą patvirtinantys įrašai.

3) Dokumentus, skirtus įrodyti tinkamą duomenų tvarkymą pagal Užsakymo ar Sutarties nuostatas, Paslaugų teikėjas turi saugoti ir pasibaigus Sutarties galiojimui, laikydamasis atitinkamų dokumentų saugojimo terminų. Pasibaigus sutarties galiojimo terminui, dokumentai gali būti perduoti Klientui, taip atleidžiant Paslaugų teikėją nuo šios sutartinės prievolės.

Klientas: _____

Paslaugų teikėjas: _____

(vieta / data)

(vieta / data)

(parašas / antspaudas)

(parašas / antspaudas)

(pasirašiusiojo vardas, pavardė / pareigos)

(pasirašiusiojo vardas, pavardė / pareigos)

priedas. Techninės ir organizacinės priemonės

1. Konfidencialumas (ES BDAR 32 straipsnio 1 dalies b punktas)

- Fizinė prieigos kontrolė
Užtikrinti, kad leidimo neturintys asmenys negalėtų prieiti prie duomenų tvarkymo įrenginių, tam naudojant, pavyzdžiui, magnetines arba lustines korteles, raktus, elektroninius durų atidarymo įrenginius, objekto saugos tarnybų ir (arba) jėgimo apsaugos darbuotojų paslaugas, signalizacijos sistemas, vaizdo arba CCTV stebėjimo sistemas.
- Elektroninė prieigos kontrolė
Užtikrinti, kad leidimo neturintys asmenys negalėtų naudotis duomenų tvarkymo ir duomenų saugojimo sistemomis, tam naudojant, pavyzdžiui, (saugius) slaptažodžius, automatinius blokavimo arba užrakto mechanizmus, autentifikavimą pagal du veiksnius, duomenų laikmenų ir saugyklų šifravimą.
- Vidinė prieigos kontrolė (vartotojo prieigos teisė prie duomenų ir teisė keisti duomenis)
Užtikrinti, kad leidimo neturintys asmenys negalėtų skaityti, kopijuoti, keisti arba ištrinti sistemoje saugomų duomenų, tam naudojant, pavyzdžiui, teisių suteikimo koncepciją, poreikiais grindžiamas prieigos teises, prieigos prie sistemos atvejų registravimą.
- Atskyrimo kontrolė
Skirtingais tikslais surinkti duomenys, pavyzdžiui, teikiant pagalbą keliems Klientams, turi būti tvarkomi atskirai, pasitelkiant „smėlio dėžės“ saugumo užtikrinimo mechanizmą.
- Pseudonimų suteikimas (numatytas BDAR 32 straipsnio 1 dalies a punkte ir 25 straipsnio 1 dalyje)
Asmens duomenys turi būti tvarkomi tokiais metodais arba būdu, kad be papildomos informacijos jie negalėtų būti susieti su konkrečiu Duomenų subjektu. Be to, tokia papildoma informacija turi būti saugoma atskirai, ir jos saugumas turi būti užtikrinamas atitinkamomis techninėmis ir organizacinėmis priemonėmis.

2. Vientisumas (ES BDAR 32 straipsnio 1 dalies b punktas)

- Duomenų perdavimo kontrolė
Užtikrinti, kad leidimo neturintys asmenys negalėtų skaityti, kopijuoti, keisti arba ištrinti elektroniniu būdu perduodamų arba perkeliamų duomenų, tam naudojant, pavyzdžiui, šifravimą, virtualius privačiuosius tinklus (VPN), elektroninį parašą.
- Duomenų įvedimo kontrolė
Turi būti tikrinama, ar ir kokie asmens duomenys įvedami į duomenų tvarkymo sistemą, taip pat keičiami arba ištrinami, tam pasitelkiant, pavyzdžiui, registravimą, dokumentų tvarkymą.

3. Prieinamumas ir atsparumas (ES BDAR 32 straipsnio 1 dalies B punktas)

- Prieinamumo kontrolė
Būtina užtikrinti apsaugą nuo atsitiktinio ar tyčinio duomenų sunaikinimo arba praradimo, tam pasitelkiant, pavyzdžiui, atsarginio kopijavimo strategiją (internetu arba neprisijungus, įmonėje arba ne įmonėje), nepertraukiamo maitinimo šaltinį, apsaugą nuo virusų, užkardą, pranešimo procedūras ir avarinius planus.
- Spartusis atkūrimas (numatytas BDAR 32 straipsnio 1 dalies c punkte)

4. Reguliarios peržiūros, atitikties tikrinimas ir vertinimas (pagal BDAR 32 straipsnio 1 dalies d punktą ir 25 straipsnio 1 dalį)

- Duomenų apsaugos valdymas
- Reagavimo į incidentus valdymas

- Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga (BDAR 25 straipsnio 2 dalis)
- Užsakymo arba Sutarties vykdymo kontrolė
Jokie tretieji asmenys negali tvarkyti duomenų, kaip numatyta BDAR 28 straipsnyje, negavę atitinkamų Kliento nurodymų, kurie, be kita ko, gali apimti aiškius ir nedviprasmiškus sutartinius susitarimus, formalizuotą Užsakymo valdymą, griežtą Paslaugų teikėjų atrankos kontrolę, pareigą atlikti išankstinį vertinimą ir vėlesnius priežiūros patikrinimus.