



LOGISTIK IM FLUSS.

## Duomenų tvarkymo sutartis (pagal BDAR 28 str.)

tarp

**Naudotojo** (kaip apibrėžta Pagrindinėje sutartyje)

(toliau vadinamo „**Užsakovu**“)

ir

„**TB Digital Services GmbH**“, Oskar-Schlemmer-Str. 19 - 21, 80807 Miunchenas

(toliau vadinamo „**Vykdytoju**“)

(toliau Užsakovas ir Vykdytojas kartu vadinami „**Šalimis**“, o kiekvienas atskirai – „**Šalimi**“).

### Preambulė

- (A) Ši duomenų tvarkymo sutartis (toliau vadinama „**Sutartimi**“) taikoma visoms veikloms, kurias atlikdamas Vykdytojas susiduria su Užsakovo, trečiųjų šalių paslaugų teikėjų arba kitų subjektų, kuriems daromas poveikis, asmens duomenimis (kaip apibrėžta 1.5 punkte) ryšium su 2 punkte aprašyta veikla pagal Platformos bendrąsias naudojimo sąlygas ir pagal jas galimai sudarytas atskiras sutartis dėl kitų paslaugų (toliau vadinama „**Pagrindine sutartimi**“).
- (B) Pagal šią Sutartį Užsakovas veikia kaip duomenų valdytojas, o Vykdytojas – kaip duomenų tvarkytojas, tvarkydamas duomenis pagal Vokietijos duomenų apsaugos įstatymo 28 str. (kaip apibrėžta toliau).

Šalys susitaria:

### 1 Apibrėžtys ir aiškinimas

- 1.1** „**Europos teisė**“ yra Europos Sąjungos taikoma teisė, dabartinių Europos Sąjungos valstybių narių taikomi įstatymai ir kiekvienos vėliau Europos Sąjungos valstybe nare tapsiančios valstybės taikomi įstatymai.
- 1.2** „**Europos duomenų apsaugos teisė**“ yra Europos Sąjungos taikoma teisė, susijusi su asmens duomenų tvarkymu (ypač Bendrasis duomenų apsaugos reglamentas), dabartinių Europos Sąjungos valstybių narių taikomi įstatymai, susiję su asmens duomenų tvarkymu (ypač galiojančios redakcijos Vokietijos duomenų apsaugos įstatymas), ir kiekvienos vėliau Europos Sąjungos valstybe nare tapsiančios valstybės taikomi įstatymai, susiję su asmens duomenų tvarkymu.
- 1.3** „**BDAR**“ yra „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)“.



LOGISTIK IM FLUSS.

**1.4** „VDAI“ yra Vokietijos duomenų apsaugos įstatymas.

**1.5** „Asmens duomenys“ turi tokią pat prasmę, kaip apibrėžta VDAI / BDAR.

## **2 Duomenų tvarkymo dalykas / užsakovo pareigos**

**2.1** Ši Sutartis reglamentuoja Šalių įsipareigojimus, susijusius su Vykdytojo atliekamu Užsakovo asmens duomenų tvarkymu pagal 1 priede įvardytą Pagrindinę sutartį.

**2.2** Duomenų tvarkymo dalykas ir trukmė, duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšys, subjektų, kuriems daromas poveikis, kategorijos ir duomenų valdytojo teisės bei pareigos nustatytos šios Sutarties 1 priede ir Pagrindinėje sutartyje pateiktame teikiamų paslaugų apraše.

**2.3** Užsakovas išlieka atsakingas BDAR požiūriu ir užtikrina visų reikalavimų, susijusių su subjektų, kuriems daromas poveikis (vairuotojų ir kitų asmenų), asmens duomenų tvarkymu, vykdymą. Užsakovas laikosi įsipareigojimo teikti informaciją ir užtikrina, kad asmens duomenų tvarkymas būtų grindžiamas duomenų apsaugos teisiniu pagrindu (pavyzdžiui, sudarant bendrovės sutartis, apribojant užimtumą įdarbinimo tikslais).

## **3 Vykdytojo pareigos**

**3.1** Vykdytojas tvarko Užsakovo asmens duomenis tik 1 priede nurodytais tikslais ir pagal Pagrindinės sutarties nuostatas, taip pat pagal užsakyme ir 1 priede dokumentais įformintus Užsakovo nurodymus; pagal šią Sutartį Vykdytojas netvarko asmens duomenų jokiai kitu tikslu. Ši nuostata netaikoma tvarkymui, atliekamam ne pagal šią Sutartį ir skirtam savoms reikmėms pagal Pagrindinės sutarties 8.3.4 punktą. Asmens duomenų kopijos ir publikatai nedaromi be Užsakovo žinios. Šis reikalavimas netaikomas atsarginėms kopijoms, jeigu jos būtinos siekiant užtikrinti tinkamą duomenų tvarkymą, ir duomenims, jeigu jie reikalingi laikantis įstatymų reikalavimų dėl duomenų saugojimo.

**3.2** Baigęs teikti duomenų tvarkymo paslaugas, Vykdytojas turi Užsakovo pasirinkimu jam perduoti visus Užsakovo asmens duomenis ir (arba) juos sunaikinti pagal duomenų apsaugos reikalavimus, jeigu tai neprieštarauja nustatytiems įstatymų reikalavimams dėl duomenų saugojimo terminų ir jeigu Vykdytojas nevykdo duomenų tvarkymo ne pagal šią Sutartį savo reikmėms pagal Pagrindinės sutarties 8.3.4 punktą. Tas pats galioja bandomiesiems ir nekokybiškiems duomenims. Užsakovui paprašius, visiškas duomenų sunaikinimas arba perdavimas Užsakovui patvirtinamas raštu nurodant datą.

**3.3** Atsižvelgiant į paslaugų apimtį, Vykdytojas suteikia Užsakovui paramą vykdant duomenų subjekto teises (informacijos, taisymo, atsisakymo, sunaikinimo) pagal Užsakovo nurodymus.

**3.4** Vykdytojas patvirtina, kad jis – jeigu tai teisiškai privaloma – paskyrė įmonės duomenų apsaugos priežiūros pareigūną (žr. VDAI 38 str. BDAR 37 punktą).

- 3.5** Vykdytojas privalo nedelsdamas pranešti Užsakovui apie duomenų apsaugos priežiūros institucijų patikrinimų rezultatus, jeigu jie susiję su Užsakovo duomenų tvarkymu. Vykdytojas per pagrįstą laikotarpį pašalina nustatytus trūkumus ir apie tai praneša Užsakovui.
- 3.6** Vykdytojas ir Užsakovo patvirtinti subrangovai tvarko duomenis tik Vokietijos Federacinės Respublikos teritorijoje, Europos Sąjungos valstybėse narėse arba kitoje Europos ekonominės erdvės susitarimą pasirašiusioje valstybėje. Norint perkelti duomenų tvarkymą į kitą valstybę (toliau vadinamą „**trečiaja valstybe**“), prieš tai reikia gauti aiškų Užsakovo sutikimą, ir toks perkėlimas galimas tik tuo atveju, jeigu įvykdomi specialūs reikalavimai dėl duomenų perdavimo į trečiąsias valstybes (žr. BDAR 40 str.). Tam būtina pateikti duomenis 1 priede ir, prireikus, pridėti papildomus (Sutarties) dokumentus.
- 3.7** Vykdytojas privalo supažindinti darbus atliekančius darbuotojus su jiems svarbiomis duomenų apsaugos nuostatomis, juos įpareigoti užtikrinti duomenų konfidencialumą (žr. BDAR 28 str. 3b p.) bei imtis atitinkamų veiksmų, siekiant užtikrinti, kad šių darbuotojų asmens duomenys būtų tvarkomi tik pagal Užsakovo nurodymus.
- 3.8** Viso Sutarties galiojimo laikotarpiu Vykdytojas reguliariai stebi, kaip laikomasi šios Sutarties duomenų apsaugos reikalavimų ir dokumentais įformintų Užsakovo nurodymų. Patikrų rezultatai paprašius pateikiami Užsakovui, jeigu jie svarbūs Užsakovo duomenų tvarkymui. Stebėsenos priemonės aprašytos duomenų apsaugos koncepcijoje, kuri paprašius pateikiama Užsakovui.
- 3.9** Vykdytojas, atsižvelgdamas į duomenų tvarkymo pobūdį, padeda Užsakovui taikydamas tinkamas technines ir organizacines priemones, kiek tai įmanoma, kad būtų įvykdyta duomenų valdytojo prievolė atsakyti į prašymus pasinaudoti BDAR III skyriuje nustatytais duomenų subjekto teisėmis. Užsakovas turi padengti Vykdytojo patirtas išlaidas.
- 3.10** Vykdytojas, atsižvelgdamas į duomenų tvarkymo pobūdį ir turimą informaciją, padeda Užsakovui vykdyti BDAR 32–36 str. nurodytas prievoles.

#### **4 Techninės ir organizacinės duomenų apsaugos priemonės**

- 4.1** Vykdytojas įgyvendina tinkamas technines ir organizacines duomenų apsaugos priemones (žr. BDAR 32 str.) Vykdytojas ypač privalo įgyvendinti šios Sutarties 2 priede įtvirtintas technines ir organizacines priemones. Šias priemones Sutarties galiojimo metu Vykdytojas suderina su techninių ir organizacinių priemonių pažanga, nesumažindamas apsaugos lygio. Svarbūs pakeitimai derinami raštu.
- 4.2** Užsakovui paprašius, Vykdytojas pateikia įrodymus, kaip faktiškai įgyvendinamos techninės ir organizacinės priemonės.

- 4.3** Vykdytojas privalo pildyti atitinkamus dokumentus apie duomenų tvarkymą, pagal kuriuos Užsakovui gali įrodyti tinkamą duomenų tvarkymą. Įrodyti taip pat galima taikant patvirtintą sertifikavimo mechanizmą pagal BDAR 42 str. nuostatas.

## **5 Subrangovas**

- 5.1** Vykdytojui leidžiama pasitelkti 1 priede nurodytą subrangovą.
- 5.2** Taigi iš esmės leidžiama įtraukti daugiau subrangovų. Vykdytojas praneša Užsakovui apie kiekvieną numatomą pakeitimą, susijusį su subrangovų įtraukimu arba pakeitimu; Užsakovas gali prieštarauti numatomiems pakeitimams. Pagal šią tvarką subrangos santykiais nelaikomos tokios trečiųjų šalių paslaugos, kuriomis Vykdytojas pasinaudoja kaip pagalbinėmis paslaugomis, siekdamas palengvinti sutarties vykdymą. Tokioms paslaugoms priskiriamos, pvz., ryšių, valymo, auditoriaus arba duomenų laikmenų utilizavimo paslaugos. Vis dėlto Vykdytojas, užtikrindamas Užsakovo duomenų apsaugą ir saugumą, taip pat trečiosioms šalims patikėtų pagalbinių paslaugų atveju privalo sudaryti tinkamus ir įstatymams neprieštaraujančius susitarimus ir įgyvendinti kontrolės priemones.
- 5.3** Jeigu Vykdytojas pasinaudoja subrangovo paslaugomis, tai Vykdytojas turi užtikrinti, kad pagal (i) subrangovo ir Vykdytojo pasirašomą sutartį arba (ii) kitą teisinę priemonę pagal Europos duomenų apsaugos teisę būtų nustatomos tokios pačios duomenų apsaugos prievolės, kokios nustatomos Vykdytojui pagal šią Sutartį. Tokiu atveju Vykdytojas turi ypač užtikrinti, kad subrangovas suteiktų pakankamas garantijas, jog tinkamos techninės ir organizacinės priemonės bus įgyvendintos taip, kad asmens duomenys būtų tvarkomi pagal BDAR reikalavimus. Užsakovui pateikus prašymą raštu, Vykdytojas pateikia Užsakovui informaciją apie svarbų subrangos sutarties turinį ir duomenų apsaugos prievolių vykdymą, o prireikus leidžia susipažinti su svarbiais sutarties dokumentais. Komercines sąlygas Vykdytojas gali retušuoti. Užsakovas privalo laikytis konfidencialumo reikalavimų dėl gautos informacijos.

## **6 Teisė tikrinti**

- 6.1** Užsakovas turi teisę tikrinti, kaip laikomasi šios Sutarties įsipareigojimų (įskaitant pateiktus nurodymus), arba pavesti tai atlikti savo paskirtai tinkamai trečiajai šaliai.
- 6.2** Vykdytojas suteikia Užsakovui deramą pagalbą. Vykdytojas ypač suteikia prieigą prie duomenų tvarkymo įrangos ir suteikia reikiamą informaciją.
- 6.3** Tuo atveju, jeigu patikrinimo rezultatai parodo, kad Vykdytojas ir (arba) duomenų tvarkymas neatitinka šios Sutarties ir (arba) Europos duomenų apsaugos teisės nuostatų, Vykdytojas imasi visų šalinimo priemonių, kad būtų užtikrinamas šios Sutarties ir (arba) Europos duomenų apsaugos teisės nuostatų vykdymas.



LOGISTIK IM FLUSS.

- 6.4** Išlaidas, kurias Užsakovas patyrė atlikdamas patikras, padengia Užsakovas. Vykdytojas gali reikalauti iš Užsakovo padengti išlaidas, kurias Vykdytojas patyrė dėl Užsakovo patikrų, jeigu Užsakovas jas atlieka arba paveda atlikti dažniau nei kartą per kalendorinius metus.
- 6.5** Apie patikras reikia laiku pranešti Vykdytojui ir jos neturi nepamatuotai trukdyti Vykdytojui vykdyti veiklą.

## **7 Prievolės pranešti**

Vykdytojas nedelsdamas praneša Užsakovui, jeigu Užsakovo duotas nurodymas Vykdytojo nuomone prieštarauja Europos duomenų apsaugos teisės nuostatomis. Pagrįstai atmesto nurodymo vykdyti nereikia, kol Užsakovas jo nepakeis arba aiškiai nepatvirtins. Vykdytojas neprivalo tikrinti nurodymų materialinės teisės prasme.

Nustatęs duomenų tvarkymo klaidų ar neatitikimų arba kilus įtarimų dėl duomenų apsaugos pažeidimo (toliau kartu vadinama „**Incidentu**“), Vykdytojas nedelsdamas apie tai tinkamai praneša Užsakovui. Incidentą, įskaitant visas faktines aplinkybes, jo poveikį ir visas šalinimo priemones, Vykdytojas turi įforminti dokumentais ir, Užsakovui paprašius, šią dokumentais įformintą informaciją nedelsiant perduoti raštu arba elektroniniu būdu Užsakovui.

## **8 Atsakomybė ir atleidimas nuo atsakomybės**

- 8.1** Vykdytojas atsako už žalą, patirtą dėl Vykdytojo arba jo įgaliotų subjektų tyčinės veikos ir (arba) didelio neatsargumo. Už žalą, patirtą dėl Vykdytojo arba jo įgaliotų subjektų paprasto neatsargumo, Vykdytojas atsako tik tuo atveju, jeigu buvo nevykdoma pagrindinė prievolė. Pagrindinės prievolės yra svarbiausios sutarties prievolės, kurios sudaro būtinas prielaidas sutarčiai tinkamai vykdyti ir kurių įvykdymo tikėjosi ir galėjo tikėtis Užsakovas. Jeigu tokios pagrindinės prievolės nevykdomos dėl paprasto neatsargumo, tai Vykdytojo atsakomybė apsiriboja įprastai numatoma žala.
- 8.2** Užsakovas atleidžia Vykdytoją nuo atsakomybės už visus trečiųjų šalių (įskaitant subjektus, kuriems daromas poveikis ir (arba) duomenų apsaugos institucijas) reikalavimus, žalą ir išlaidas, atsiradusius dėl Užsakovo padaryto šios Sutarties ir (arba) Europos duomenų apsaugos teisės nuostatų pažeidimo; ši nuostata negalioja, jeigu Užsakovas nekaltas dėl padaryto pažeidimo arba Vykdytojas prisidėjo padarant pažeidimą.

## **9 Galiojimo laikas**

Šios Sutarties galiojimo laikas lygus Pagrindinės sutarties galiojimo laikui. Pagrindinei sutarčiai nustojus galioti dėl bet kokios priežasties, ši Sutartis savaime nustoja galioti. Ši nuostata negalioja sutarties nutraukimui dėl svarbios priežasties.

## 10 Kita

- 10.1** Už šioje Sutartyje nurodytas Vykdytojo paslaugas atsiskaitoma Pagrindinėje sutartyje nustatyta apmokėjimo tvarka.
- 10.2** Jeigu Vykdytojo disponuojamiems Užsakovo asmens duomenims kyla pavojus dėl trečiųjų šalių taikomų priemonių (pvz., arešto arba konfiskavimo), bankroto ar susitarimo su kreditoriais procedūros arba kitų panašių įvykių, tai Vykdytojas turi nedelsdamas apie tai pranešti Užsakovui.
- 10.3** Jeigu šios Sutarties atskiros nuostatos yra negaliojančios arba nustoja galioti, tai neturi įtakos kitų nuostatų galiojimui. Nuostatai nustojus galioti, Šalys sutaria dėl pakaitinės tvarkos, kuri dalykiniu ir ekonominiu požiūriu atitiktų Sutarties tikslą.
- 10.4** Tuo atveju, jeigu Didžioji Britanija pasitrauks iš Europos Sąjungos, Vykdytojas įsipareigoja jau dabar sudaryti visus susitarimus ir imtis visų veiksmų, kurie yra būtini siekiant tinkamai laikytis duomenų apsaugos teisės nuostatų, Didžiojoje Britanijoje vykdant duomenų tvarkymą pagal sutartis, jai pasitraukus iš Europos Sąjungos. Jeigu iki pasitraukimo datos Europos Komisija neturės teigiamo sprendimo dėl tinkamumo, šiandien galiojančiu požiūriu turi būti taikomos standartinės duomenų apsaugos nuostatos pagal 46 str. 2 d. c) punktą dėl asmens duomenų perdavimo duomenų tvarkytojui, kurio buveinė yra trečiojoje valstybėje, kuriose neužtikrinamas tinkamas apsaugos lygis.

Jeigu Vykdytojas nevykdo šių prievolių, tai nuo Didžiosios Britanijos pasitraukimo iš Europos Sąjungos datos Užsakovas turi teisę reikalauti iš Vykdytojo, kad duomenų tvarkymo paslaugas teiktų su Vykdytoju susijusi įmonė arba įmonės dalis, kurios nuolatinė buveinė yra Europos Sąjungos teritorijoje, nesukeliant Užsakovui didesnių sąnaudų ar papildomų išlaidų.

- 10.5** Ši duomenų tvarkymo sutartis parengta 18 kalbų, tačiau nustačius neatitikimų pirmenybė teikiama originalo versijai vokiečių kalba.
- 10.6** Šiai Sutarčiai galioja Vokietijos Federacinės Respublikos įstatymai, išskyrus Jungtinių Tautų konvenciją dėl tarptautinio prekių pirkimo-pardavimo sutarčių. Išskirtinė jurisdikcija suteikta Miuncheno teismui.
- 10.7** Toliau nurodyti priedai yra Sutarties sudedamoji dalis:
- 1 priedas. Duomenų tvarkymo aprašas
  - 2 priedas. Techninės ir organizacinės priemonės



LOGISTIK IM FLUSS.

## 1 PRIEDAS. Duomenų tvarkymo aprašas

### 1 Pagrindinė sutartis

Pagrindinė sutartis pagal Sutarties pagrindinės dalies 2.1 punktą yra „Platformos bendrosios naudojimo sąlygos“.

Pavadinimai / šalys: „**TB Digital Services GmbH**“, Oskar-Schlemmer-Str. 19 - 21, 80807 Miunchenas /  
**Naudotojas**

### 2 Sutarties dalykas ir trukmė

Užsakymo dalykas nustatytas Pagrindinės sutarties 1 punkte (*Dalykas*) ir 8 punkte (*Naudotojo duomenys ir duomenų apsauga*), o užsakymo trukmė nustatyta Pagrindinės sutarties 7 punkte (*Sutarties sudarymas, sutarties trukmė ir teisės nutraukti sutartį*).

### 3 Duomenų tvarkymo apimtis, pobūdis ir tikslas / duomenų tvarkymo priemonės

Asmens duomenų tvarkymo apimtis, pobūdis ir tikslas nustatyti Pagrindinės sutarties 8 punkte.

Išsamesnis užsakymo dalyko apimtys, pobūdžio ir tikslo aprašymas:

kad galėtų teikti siūlomas paslaugas (kaip apibrėžta Pagrindinėje sutartyje), Vykdytojas turi gauti Užsakovo asmens duomenis per susietąsias transporto priemones arba mobiliuosius įrenginius (ir prireikus trečiųjų šalių paslaugų teikėjo, su kuriuo naudotojas susitarė dėl trečiųjų šalių paslaugų, perduodamus asmens duomenis) paslaugoms teikti būtina apimtimi ir perduoti Vykdytojo platformai bei joje įrašyti. Platformoje įrašytus duomenis Vykdytojas tvarko paslaugoms teikti būtina apimtimi (pvz., pagal asmens duomenis analizuoti ir vertinti vairuotojų vairavimo ypatumus ir susietosios transporto priemonės arba mobiliojo įrenginio naudojimą ir pagal tai teikti specialiai Užsakovui pritaikytus pasiūlymus, pvz., vairuotojų mokymus, įrangą ir pasiūlymus efektyvumui didinti). Tikslią apimtį, pobūdį ir tikslą ypač lemia papildomai sudaromos atskiros sutartys.

### 4 Susijusių subjektų grupė (asmenų, kuriems daromas poveikis, kategorijos)

Duomenų tvarkymas daro poveikį šioms asmenų kategorijoms:

- **vairuotojai ir kiti darbuotojai** (Užsakovo bendrovės darbuotojai), pvz., darbuotojai, praktikantai, kandidatai, buvusieji darbuotojai;
- **vairuotojai**, kurie nėra darbuotojai;
- **kontaktiniai asmenys**, dirbantys pakrovimo / iškrovimo paslaugų įmonėse arba kitiems Užsakovo verslo partneriams; ir
- **koncerno darbuotojai** (kitos Užsakovo verslo grupės bendrovės darbuotojai).



LOGISTIK IM FLUSS.

## 5 Asmens duomenų rūšys

Duomenų tvarkymas apima tokias asmens duomenų rūšis:

- vairuotojo pavardė ir vairuotojo identifikacinis numeris;
- transporto priemonės identifikacinis numeris;
- duomenys apie buvimo vietą;
- duomenys apie vairavimo ir poilsio laiką;
- duomenys apie vairavimo ypatumus;
- duomenys apie susietosios transporto priemonės būseną;
- duomenys apie priekabos būseną;
- duomenys apie papildomos įrangos, agregatų ir kitų transporto priemonės konstrukcinių dalių būseną;
- duomenys apie galimai susietų IOT prietaisų būseną;
- duomenys apie mobiliųjų įrenginių būseną;
- krovinio duomenys;
- užsakymo duomenys; ir
- duomenys apie kontaktinius asmenis, dirbančius pakrovimo / iškrovimo paslaugų įmonėse arba kitiems Užsakovo verslo partneriams.

## 6 Dokumentais įforminti nurodymai

Jais Užsakovas nurodo Vykdytojui tvarkyti asmens duomenis kaip nurodyta Pagrindinės sutarties 8 punkte. Tvarkymas ypač apima tokius punktus:

- Asmens duomenys per susietąją transporto priemonę arba mobilųjį įrenginį perduodami Vykdytojo nuotolinei platformai ir joje įrašomi.
- Pagal šią Sutartį asmens duomenys tvarkomi tik tiek, kiek tai būtina Pagrindinei sutarčiai įvykdyti; tai neturi poveikio Pagrindinės sutarties 8.3.4 punktui.
- Vykdytojas perduoda asmens duomenis trečiųjų šalių paslaugų teikėjui (kaip apibrėžta Pagrindinėje sutartyje), jeigu toks duomenų perdavimas trečiųjų šalių paslaugų teikėjui yra būtinas, kad jis galėtų teikti Užsakovui savo trečiųjų šalių paslaugas (kaip apibrėžta Pagrindinėje sutartyje).
- Vykdytojas pagal asmens duomenis analizuoja ir vertina vairuotojų vairavimo ypatumus ir susietosios transporto priemonės naudojimą ir pagal tai teikia specialiai Užsakovui pritaikytus pasiūlymus, pvz., vairuotojų mokymus, įrangą ir pasiūlymus efektyvumui didinti.

## 7 Duomenų tvarkymo vieta

- Vokietija
- Jungtinė Karalystė; jeigu tvarkomi duomenys IT prieglobos ir (arba) IT pagalbos tikslais Europos Sąjungos teritorijoje, tai turi būti sudarytos atitinkamos duomenų tvarkymo sutartys.





LOGISTIK IM FLUSS.

- Jeigu Vykdytojas IT prieglobos ir (arba) IT pagalbos tikslais pasitelkia subrangovą ne iš Europos Sąjungos (žr. šio 1 priedo 8 punktą), tai asmens duomenų perdavimas vykdomas remiantis Vykdytojo ir subrangovo patvirtintomis standartinėmis sutartinėmis sąlygomis / standartinėmis duomenų apsaugos nuostatomis dėl asmens duomenų perdavimo trečiųjų šalių tvarkytojui pagal BDAR 46 str. 2 dalies c) punktą.

## **8 Subrangovas**

Vykdytojas pasitelkia šiuos subrangovus (kurie prireikus gali pasitelkti kitus subrangovus):



LOGISTIK IM FLUSS.

<b>Nr.</b>	Subrangovas (įmonė, adresas, kontaktinis asmuo)	Tvarkomų duomenų kategorijos	Tvarkymo veiksmai / duomenų tvarkymo pagal subrangos sutartį tikslas
<b>1</b>	Salesforce.com EMEA Limited  Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, JAV	Visi platformos asmens duomenys, susiję su pardavimo dalimi (t. y. ten, kur platformoje klientas gali registruotis ir atlikti užsakymus)	Platformos priegloba
<b>2</b>	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, JAV	Visi platformos asmens duomenys, susiję su pardavimo dalimi (t. y. ten, kur platformoje klientas gali registruotis ir atlikti užsakymus)	IT pagalba, susijusi su platforma
<b>3</b>	Amazon Webservices, Inc., Amazon Webservices, Inc. 410 Terry Avenue North Seattle WA 98109 JAV <a href="https://aws.amazon.com/de/compliance/contact/">https://aws.amazon.com/de/compliance/contact/</a>	Visi kiti naudotojų asmens duomenys, perduodami Vykdytojui per transporto priemonę	Platformos priegloba / IT pagalba, susijusi su platformos priegloba
<b>4</b>	Prireikus vėliau vietoj Nr. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 JAV <a href="https://aws.amazon.com/de/compliance/contact/">https://aws.amazon.com/de/compliance/contact/</a>	Visi kiti naudotojų asmens duomenys, perduodami Vykdytojui per transporto priemonę	Platformos priegloba
<b>5</b>	MAN Service und Support GmbH Dachauer Straße 667 80995 München Vokietija	Visi asmens duomenys, reikalingi apdorojant klientų užklausas pagal 1-ojo ir 2-ojo lygmens pagalbą	1-ojo lygmens pagalba



LOGISTIK IM FLUSS.

<b>6</b>	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 JAV	Visi asmens duomenys, reikalingi išrašant sąskaitą / vykdant užsakymą	Platformos priegloba (savininkas ES – priegloba „Amazon Web Services (EU)“ – žr. 4 punktą)
<b>7</b>	MAN Truck & Bus AG Dachauer Str. 667 80995 München Vokietija	Visi kiti naudotojų asmens duomenys, perduodami Vykdytojui per susietąją transporto priemonę ir (arba) mobilųjį įrenginį	Platformos priegloba
<b>8</b>	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Vokietija	Visi kiti naudotojų asmens duomenys, perduodami Vykdytojui per TBM1/2 transporto priemones	Platformos priegloba
<b>9</b>	Scania AB Vagnmakarvägen 1 15187 Södertälje Švedija	Visi kiti naudotojų asmens duomenys, perduodami Vykdytojui per transporto priemonę	Platformos priegloba
<b>10</b>	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Vokietija	Visi kiti naudotojų asmens duomenys, perduodami Vykdytojui per transporto priemonę	Platformos priegloba



LOGISTIK IM FLUSS.

## **2 PRIEDAS. Techninės ir organizacinės priemonės**

Vykdytojo įgyvendinamos techninės ir organizacinės priemonės užtikrinant riziką atitinkantį apsaugos lygį yra aprašytos RIO platformos duomenų apsaugos koncepcijoje ir visų pirma apima šiuos punktus:

### **1. Pseudonimų suteikimas**

Jeigu asmens duomenys naudojami tvarkymo tikslais, kurių galima pasiekti duomenims suteikiant pseudonimus, tai naudojami pseudonimų suteikimo metodai. Pirmiausia kiekvienam duomenų laukeliui iš anksto apibrėžiama, ar jam turi būti suteiktas pseudonimas, nes kitaip būtų įmanoma nustatyti asmenį. Pseudonimų suteikimo raktai saugomi „duomenų seife“, kuriam nustatomas griežčiausias įmanomas prieigos ribojimas.

### **2. Šifravimas**

Mobilieji įrenginiai šifruotai palaiko ryšį su galutiniu tašku naudodami individualų įrenginio sertifikatą. RIO platformoje duomenys perduodami šifruoti („Ubiquitous encryption“ arba „encryption everywhere“).

### **3. Konfidencialumo užtikrinimas**

Visi darbuotojai instruktuojami apie jiems galiojančią konfidencialumo prievolę ir raštu įsipareigoja užtikrinti duomenų slaptumą.

Naudojama IT infrastruktūra užtikrinama per „Amazon Web Services“ (toliau vadinama AWS) naudojant nuotolinį serverį („IaaS“ ir „PaaS“). Prieigos kontrolę užtikrina AWS duomenų centro operatorius: aukšto saugumo AWS kompiuterių centrai naudoja naujausių technologijų elektronines stebėsenos priemones ir daugiapakopės prieigos kontrolės sistemas. Kompiuterių centruose visą parą dirba aukštos kvalifikacijos saugos darbuotojai, o prieiga užtikrinama vadovaujantis mažiausių teisių principu ir tik sistemų administravimo tikslu.

Prieiga prie „TB Digital Services GmbH“ techninės įrangos komponentų (klientų), suteikiama taikant galiojančias, kiekvienu atskiru atveju tinkamas standartines priemones. Jos apima, pvz., prieigos ribojimą per skirstomuosius įrenginius (šakotuvus), vaizdo stebėjimo įrenginius, signalizacijos sistemą ir (arba) saugos tarnybą, elektroniniu arba mechaniniu būdu apsaugotas duris, nuo įsilaužimo apsaugotus pastatus, dokumentais įformintas prieigos teises (lankytojams, kitų įmonių darbuotojams) arba deklaruotas saugos zonas.

Prieigos kontrolė apima priemones, susijusias su įrenginių apsauga, tinklo apsauga ir programų apsauga.

Transporto priemonėse naudojamos įvairios įrenginių apsaugos priemonės: Mobilieji įrenginiai tvirtai sumontuoti transporto priemonėje ir turi saugiojo paleidimo funkciją, t. y. nėra galimybės įkelti ir paleisti svetimą operacinę sistemą. Mobilieji įrenginiai šifruotai palaiko ryšį su galutiniu tašku naudodami individualų įrenginio sertifikatą. RIO platformoje duomenys perduodami šifruoti („Ubiquitous encryption“ arba „encryption everywhere“).



LOGISTIK IM FLUSS.

everywhere“). Įrenginiuose reguliariai diegiami saugos naujinimai ir taip užtikrinamas naujausias saugos lygis („Patch-Management“).

Tinklo apsaugai taip pat naudojamos įvairios standartinės priemonės: Įdiegti tinkami (atitinkantys technikos lygį) reikalavimai slaptažodžiams (slaptažodžio ilgiui, sudėtingumui, galiojimo terminui ir kt.). Pakartotinai neteisingai įvedus naudotojo vardo ir slaptažodžio derinį (laikina) blokuojamas naudotojo identifikatorius. Įmonės tinklas apsaugotas nuo nesaugių atvirų tinklų naudojant užkardą. Įdiegtas procesas, užtikrinantis reguliarių saugos naujinimų siuntimą mobiliesiems įrenginiams (OTA procesas). Naudojamos tinkamos technologijos (pvz., įsilaužimo aptikimo sistemos), skirtos atakoms įmonės tinkle (intranete) aptikti ir išvengti. Reguliariai atkreipiamas darbuotojų dėmesys į gresiančius pavojus ir riziką.

Programų apsaugai naudojamos kai kurios standartinės priemonės:

Svarbios programos apsaugotos nuo nesankcionuotos prieigos naudojant tinkamus tapatybės nustatymo ir įgaliojimų suteikimo mechanizmus. Įdiegti tinkami (atitinkantys technikos lygį) reikalavimai slaptažodžiams (slaptažodžio ilgiui, sudėtingumui, galiojimo terminui ir kt.). Programoms, kurias ypač svarbu apsaugoti, naudojami itin saugūs tapatybės nustatymo mechanizmai (pvz., „Token“, PKU). Pakartotinai neteisingai įvedus naudotojo vardo ir slaptažodžio derinį (laikina) blokuojamas naudotojo identifikatorius. Tam tikro proceso metu naudojami duomenys saugomi šifruoti mobiliu būdu naudojamoje duomenų laikmenoje. Pavykę prisijungimai ir bandymai prisijungti prie programų protokoluojami. Sukurtos protokolų rinkmenos tinkamą laiką (mažiausiai 90 dienų) saugojamos ir (pasirinktinai) tikrinamos.

Naudotojų teisės (prisijungimui ir prieigai) užtikrinamos įvairiomis priemonėmis, kurios įprastai priskiriamos konkrečiam asmeniui. Už teisių suteikimą atsako už platformą atsakingas subjektas ir šis procesas yra reguliariai tikrinamas. Prieigos teisės suteikiamos tik vadovaujantis nustatytu ir dokumentais įformintu procesu. Prieigos teisių keitimas atliekamas vadovaujantis keturių akių principu ir registruojamas žurnalo rinkmenoje, kuriai suteikiama versija.

Prieigai kontroliuoti arba valdyti naudojamos įvairios priemonės: Prieigos teisės apibrėžiamos vadovaujantis vaidmenų / teisių koncepcija. Jas registruojant ir priskiriant atitinkamiems vaidmenims atsižvelgiant į poreikius, susijusius su atliekamomis užduotimis. Techniniams administratoriams sukurti specialūs vaidmenys / teisės (kurie, jei tai įmanoma, nesuteikia prieigos prie asmens duomenų). Techninei pagalbai sukurti specialūs vaidmenys / teisės (kurie neapima techninio administravimo teisių).

Jei tai įmanoma techniniu ir organizaciniu požiūriu, vaidmenys / teisės apibrėžia ir priskiria skirtingi asmenys nuo peržiūros apsaugotame (patvirtinimo) ir ribotos trukmės procese. Tiesioginė prieiga prie duomenų bazės, apėinant vaidmenų / teisių koncepciją, suteikiama tik įgaliotiems duomenų bazės administratoriams. Galioja atitinkama asmeninių laikmenų naudojimo tvarka arba asmeninių laikmenų naudojimas draudžiamas. Galioja privalomos procedūros, susijusios su prieiga prie duomenų atliekant išorinę ir nuotolinę techninę priežiūrą ir nuotolinius darbus. Dokumentus ir duomenų laikmenas naikina / utilizuoja (naudodamos, pvz., naikinimo



LOGISTIK IM FLUSS.

aparatus, naikinimo konteinerius) patikimos utilizavimo paslaugų įmonės besilaikydamos duomenų apsaugos reikalavimų.

Vaidmenų / teisių koncepcija suderinama su besikeičiančiomis darbo organizavimo struktūromis (pvz., naujais vaidmenimis), o priskirti vaidmenys / teisės reguliariai tikrinami (pvz., vadovų) ir prireikus keičiami ar panaikinami. Suteiktiems standartiniams profiliams taikoma reguliari centrinė kontrolė. Besikeičianti prieiga (rašymas, skaitymas) protokoluojama, o sukurtos protokolavimo rinkmenos saugomos tinkamą laiką (mažiausiai 90 dienų) ir (pasirinktinai) tikrinamos.

Perdavimui užtikrinti kaip bendrosios priemonės naudojamos įvairios standartinės priemonės:

Perdavimą atliekantys asmenys iš anksto supažindinami su taikytinomis užtikrinimo priemonėmis. Gavėjų grupė nustatoma iš anksto taip, kad būtų įmanoma atitinkama kontrolė (tapatybės nustatymas). Visas duomenų perdavimo procesas nustatytas ir įformintas dokumentais, o konkretaus duomenų perdavimo vykdymas protokoluojamas arba įforminamas dokumentais (pvz., gavimo patvirtinimu, kvitu). Perdavimą atliekantys asmenys prieš tai atlieka patikimumo, pilnumo ir teisingumo patikrą.

Prieš atliekant konkretų duomenų perdavimą patikrinamas gavėjo adresas (pvz., el. pašto adresas). Duomenų tikrinimas internetu atliekamas šifruota forma (pvz., šifruojant duomenis). Jeigu įmanoma techniniu požiūriu, perduotų duomenų vientisumas užtikrinamas naudojant parašo procedūrą (skaitmeninį parašą). Elektroniniai gavimo patvirtinimai kaupiami tinkama forma archyvuose. Nepageidautinas duomenų perdavimas internetu blokuojamas taikant tinkamas technologijas (pvz., įgaliojimą serverį, užkardą).

Atskyrimo reikalavimui užtikrinti naudojamos šios standartinės priemonės:

Galioja privalomos procedūros, susijusios su atskyrimo reikalavimo užtikrinimo tam tikru tikslu tvarkant duomenis. Tam tikru tikslu renkami duomenys įrašomi atskirai nuo kitais tikslais renkamų duomenų. Naudojamos IT sistemos leidžia atskirai įrašyti duomenis (taikant galimybę aptarnauti keletą klientų arba prieigos koncepcijas). Atliekamas duomenų atskyrimas bandomosiose ir įprastai eksploatuojamose sistemose. Pseudonimais koduojamus duomenis susiejantis raktas, leidžiantis iš naujo identifikuoti duomenis, įrašomas arba saugojamas atskirai. Tvarkydamas duomenis arba perduodamas funkcijas, vykdytojas atskirai tvarko skirtingų užsakovų duomenis. Atitinkamai formuojant turimas vaidmenų / teisių koncepcijas galima logiškai atskirti tvarkomus duomenis.

#### **4. Vientisumo užtikrinimas**

Įvesties protokolavimui užtikrinti naudojamos įvairios standartinės priemonės:

Protokoluojami prieigos teisių pakeitimai ir visi administratoriaus veiksmai. Protokoluojama įrašymo prieiga (įvestys, pakeitimai, pašalinimai) ir duomenų laukelių pakeitimai (pvz., naujai įvesto arba pakeisto duomenų rinkinio turinio). Protokoluojami perdavimai (pvz., atsisiuntimas) ir prisijungimai.

Siekiant įvesčių atsekamumo naudojami registravimo dokumentai įforminami dokumentais ir kaupiami archyvuose. Protokoluojama nurodant datą ir laiką, naudotoją, veiksmo rūšį, taikomąją programą ir duomenų rinkinio eilės numerį. Protokolavimo nuostatos įforminamos dokumentais.

Suteikiama tik skaitymo prieiga prie protokolo duomenų. Prieigą prie protokolo duomenų turinčių įgaliotų asmenų grupė yra labai apribota (pvz., administratorius, duomenų apsaugos priežiūros pareigūnas, revizorius). Protokolų rinkmenos nustatytą laiką (pvz., 1 metus) saugojamos ir po to sunaikinamos laikantis duomenų apsaugos reikalavimų. Protokolų rinkmenos reguliariai automatiškai analizuojamos. Jeigu įmanoma, protokolo rinkmenų analizė parengiama suteikiant pseudonimus.

## 5. Parengties užtikrinimas

Struktūra apsaugota nuo duomenų praradimo taikant vidinius dubliavimo mechanizmus pačioje AWS platformoje. Objekto apsaugai užtikrinti naudojamos šios AWS standartinės priemonės:

Įgyvendinamos priešgaisrinės saugos priemonės (pvz., ugniai atsparios durys, dūmų signalizavimo įtaisai, ugniai atsparios sienos, draudimas rūkyti). Kompiuterių sistemos apsaugotos nuo potvynių (pvz., kompiuterių patalpa antrajame aukšte, vandens jutikliai). Įgyvendinamos priemonės apsaugai nuo vibracijos (pvz., kompiuterių patalpa neįrengiama šalia transporto kelių, geležinkelio bėgių, mašinų patalpų). Kompiuterių sistemos apsaugotos nuo elektromagnetinių laukų (pvz., plieninės plokštės išorinėse sienose). Įgyvendinamos priemonės apsaugai nuo vandalizmo ir vagysčių (žr. apie prieigos kontrolę). Kompiuterių sistemos įrengtos patalpose su klimato sąlygų kontrole (temperatūra ir oro drėgnumas reguliuojami oro kondicionavimo sistema). Kompiuterių sistemos apsaugotos nuo įtampos šuolių naudojant apsaugą nuo viršįtampių. Įgyvendinamos priemonės patikimam ir nepertraukiamam srovės tiekimui užtikrinti (pvz., NMŠ įrenginiai, avarinio srovės tiekimo agregatai).

Duomenų rinkiniai reguliariai išsaugomi atsarginių kopijų pavidalu AWS platformos viduje. Atsarginių kopijų koncepcija įforminama dokumentais ir reguliariai peržiūrima bei atnaujinama. Atsarginių kopijų laikmenos apsaugotos nuo nesankcionuotos prieigos. Naudojamos atsarginių kopijų darymo programos atitinka naujausius kokybės standartus ir šiuo požiūriu reguliariai atnaujinamos. Įrengtas rezervinis kompiuterių centras (nutolęs nuo duomenų tvarkymo vietos), kuris stichinių nelaimių atveju gali tęsti duomenų tvarkymą. Įvairios parengties kontrolės priemonės įformintos dokumentais AWS avarinių situacijų valdymo plane.

Prieš patvirtinant duomenų tvarkymo užsakymą, Vykdytojas kruopščiai ir pagal nustatytus kriterijus (techninės ir organizacinės priemonės) patikrinamas. Tam Vykdytojo prašoma pateikti išsamią informaciją apie įgyvendintas technines ir organizacines duomenų apsaugos priemones (pateikiami atsakymai į klausimyno klausimus arba pristatoma duomenų apsaugos koncepcija), kuri patikrinama. Atsižvelgiant į tvarkomų duomenų kiekį ir konfidencialumą, ši patikra gali būti atliekama vietoje pas Vykdytoją. Vykdytojų atranką atsižvelgiama į turimus tinkamus sertifikatus (pvz., ISO 27001). Vykdytojo tinkamumo nustatymas tinkamu ir suprantamu būdu įforminamas dokumentais.



LOGISTIK IM FLUSS.

Siekiant pagrįsti su užsakymu susijusius santykius, tarp Užsakovo ir Vykdytojo sudaroma duomenų tvarkymo sutartis. Joje išsamiai ir raštiškai nustatoma abiejų Šalių kompetencija ir atsakomybė bei pareigos. Jeigu paskirto paslaugų teikėjo buveinė yra ne ES ar EEE teritorijoje, taikomos ES standartinės sutarties nuostatos. Sutartyje nustatyta, kad Vykdytojas gali tvarkyti duomenis tik vadovaudamasis Užsakovo nurodymais. Vykdytojas privalo nedelsdamas pranešti Užsakovui, jeigu Užsakovo duotas nurodymas Vykdytojo nuomone prieštarauja duomenų apsaugos teisės nuostatoms. Siekiant užtikrinti subjektų, kuriems daromas poveikis, teises, duomenų tvarkymo sutartyje numatoma, kad Vykdytojas turi tinkamai padėti Užsakovui, jeigu to reikia, pvz., suteikiant informaciją šiems subjektams.

Vykdamas duomenų tvarkymo sutartį Užsakovas kontroliuoja Vykdytojo darbo rezultatų formą ir turinį. Reguliariai tikrinama, kaip laikomasi Vykdytojo įgyvendintų techninių ir organizacinių priemonių. Tam visų pirma naudojamos pateiktai atestatai ar tinkamais sertifikatais arba įrodymais apie atliktą IT saugumo ar duomenų apsaugos auditą. Jeigu pasitelkiamas subrangovas, sutartyje numatoma, kad jis atitinkamai kontroliuojamas.

## **6. Sistemų apkrovimo užtikrinimas**

AWS nuotolinių serverių infrastruktūra sukurta kaip viena lanksčiausių ir saugiausių nuotolinės kompiuterijos aplinkų. Ji suprojektuota siekiant užtikrinti optimalią parengtį ir visišką klientų atskyrimą. Ji užtikrina ypatingai lanksčiai keičiamą, labai saugiai eksploatuojamą platformą, sudarančią galimybes klientams greitai ir saugiai pateikti programas ir turinį visame pasaulyje. AWS paslaugos nepriklauso nuo turinio, nes jos visiems klientams suteikia aukštą saugumo lygį, nepriklausomai nuo turinio pobūdžio ar geografinio regiono, kuriame saugojami duomenys.

Aukšto saugumo AWS kompiuterių centrai naudoja naujausių technologijų elektronines stebėsenos priemones ir daugiapakopę prieigos kontrolės sistemas. Kompiuterių centruose visą parą dirba aukštos kvalifikacijos saugos darbuotojai, o prieiga užtikrinama vadovaujantis mažiausių teisių principu ir tik sistemų administravimo tikslu.

## **7. Asmens duomenų pateikties atkūrimo procesas įvykus stichinei nelaimei ar techniniam incidentui**

AWS kompiuterių centrai įrengiami grupėmis įvairiuose pasaulio regionuose. Visi kompiuterių centrai veikia tinkle ir aptarnauja klientus; nė vienas kompiuterių centras nėra išjungtas. Įvykus gedimui automatiniai procesai perkelia klientų duomenų judėjimą iš paveiktų sričių. Pagrindinės programos vykdomos pagal N+1 konfigūraciją, kad nustojus veikti vienam kompiuterių centrui būtų užtikrinamas pakankamas pajėgumas, kad duomenų srautas būtų paskirstytas likusioms vietoms.

AWS suteikia lankstumo vykdyti procesus ir saugoti duomenis keliuose geografiniuose regionuose bei keliuose parengties zonose („Availability Zones“). Kiekviena parengties zona sukurta kaip nepriklausoma zona gedimo atveju. Tai reiškia, kad parengties zonos viename tipiniame miesto regione yra fiziškai paskirstytos ir yra, pvz., mažesnės potvynių rizikos rajonuose (atsižvelgiant į regioną galioja skirtingos potvynių rizikos zonų kategorijos). Siekiant minimizuoti gedimų atsiradimą atskirose vietose, be vietoje užtikrinamo autonominio





LOGISTIK IM FLUSS.

nepertraukiamo srovės tiekimo ir avarinių srovės tiekimo generatorių, visos parengties zonos maitinamos iš skirtingų elektros tinklų, kuriuos valdo nepriklausomi elektros tinklo operatoriai. Visos parengties zonos turi rezervines jungtis su keletu „Tier-1“ lygio tinklų operatoriumi.

Siekdama paspartinti įmonėms kritinių incidentų šalinimą, „Amazon“ incidentų valdymo komanda taiko šioje srityje įprastas diagnostikos procedūras. Įmonės darbuotojai užtikrina nepertraukiamą darbą visą parą, septynias dienas per savaitę ir 365 dienas per metus, kad aptiktų triktis ir valdytų jų poveikį bei šalinimą.

## **8. Reguliarios techninių ir organizacinių priemonių patikros ir vertinimo procesas**

Įmonėje turimos direktyvos ir nurodymai arba įdiegti standartai, susiję su informacijos saugumu, taip pat taikomi diegiant ir eksploatuojant RIO platformą. Įmonėje užtikrinamos funkcijos, susijusios su duomenų apsauga ir informacijos saugumu (duomenų apsaugos priežiūros pareigūnas ir informacijos saugumo pareigūnas). Darbuotojai įsipareigoja užtikrinti duomenų slaptumą ir informuojami apie duomenų apsaugą ir IT saugumo priemones, naudojant informacinius leidinius, lankstinukus, intraneto nurodymus ir kt.

Šie vidaus procesai tikrinami atliekant patikrinimą dėl informacijos saugumo ir duomenų apsaugos, ar laikomasi duomenų saugos techninių ir organizacinių priemonių.

Tvarkymo operacijos ir duomenų saugos priemonės įforminamos dokumentais tvarkymo operacijų registre. Reguliariai atliekamos patikros (vidaus ir išorės), susijusios su priemonių veiksmingumu.