SUSITARIMAS Nr. 1 /2025/41-321
DĖL 2024 M. SPALIO 29 D. PASLAUGŲ PIRKIMO SUTARTIES NR. 2024/41-240 PAKEITIMO

2025 m. gruodžio __ d.
Vilnius

Lietuvos bankas (toliau – Užsakovas), atstovaujamas Valdybos pirmininko Gedimino Šimkaus, veikiančio pagal Prekių, paslaugų ir darbų pirkimo bei kitų sutarčių rengimo, įforminimo, saugojimo ir sąskaitų tvarkymo Lietuvos banke taisyklių, patvirtintų Lietuvos banko valdybos pirmininko 2015 m. gruodžio 22 d. įsakymu Nr. V 2015/(1.7-260603)-02-245, 19.5 papunkčio nuostatas, ir **UAB „Baltic Amadeus“** (toliau – Teikėjas), atstovaujama Projektų direktoriaus Ruslan Grumbianin, veikiančio pagal Generalinio direktoriaus 2025 m. kovo 13 d. įsakymą Nr. 1.01-155, vadovaudamiesi 2024 m. spalio 29 d. TRS paslaugų pirkimo sutarties Nr. 2024/41-240 (toliau - Sutartis) Bendrųjų sąlygų 9.1.2. 9.3 ir 14.2 punktų ir Viešųjų pirkimų įstatymo 89 str. 1 ir 5 dalių nuostatomis, ir atsižvelgdami į Teikėjo 2025 m. lapkričio 27 d. prašymą, sudaro šį susitarimą dėl Sutarties pakeitimo (toliau – susitarimas) ir susitaria:

1. Pakeisti Sutarties Specialiųjų sąlygų 3 priedą ir jį išdėstyti taip:

„Specialiųjų sąlygų 3 priedas

Sutarties vykdymui skiriamų specialistų sąrašas

Eil. Nr.	**Paslaugas teikiančio specialisto kompetencija, specialisto vardas, pavardė**	**Specialistų kvalifikacijos reikalavimai** (Kiekvienas specialistas atskirai turi atitikti žemiau išvardintus reikalavimus)
1	2	3
1.	**Projekto vadovas**	1. turi tarptautiniu mastu pripažįstamą PMP arba Prince 2, arba CompTIA Project+ ar lygiavertę projektų vadovo kvalifikaciją; 2. per pastaruosius 5 metus (iki pasiūlymų pateikimo termino pabaigos) turi ne mažesnę kaip 3 metų patirtį vadovaujant informacinių sistemų kūrimo (modernizavimo) ir diegimo projektui (-ams) (sutarčiai (-tims)); 3. per pastaruosius 5 (penkis) metus iki pasiūlymų pateikimo termino pabaigos turi turėti projekto vadovo patirtį, vadovaujant informacinių sistemų kūrimui ir (ar) tobulinimui ir (ar) plėtrai ir (ar) priežiūrai, bent 1 (viename) užbaigtame projekte (sutartyje), kurio vertė ne mažesnė kaip 170 000,00 Eur be PVM, neįskaitant techninės įrangos ir licencijų kainos, t. y. atliko paslaugų teikimo valdymą, sutarties eigos kontrolę, sutarties vykdymo rizikos veiksnių valdymą, vadovavo ne mažiau kaip 5 specialistų, dalyvaujančių vykdant sutartį, komandai.
2.	**Informacinės sistemos architektas**	1. turi tarptautiniu mastu pripažįstamą TOGAF (The Open Group Architecture Framework) arba CITA (Certified Information Technology Architect) ar lygiavertę informacinių sistemų architekto kvalifikaciją; 2. per pastaruosius 3 (trejus) metus iki pasiūlymo pateikimo termino pabaigos yra dirbęs bent 1 (viename) užbaigtame projekte, kurio metu parengė visą informacinės sistemos sukūrimo arba modernizavimo (plėtros) architektūrinį sprendimą, kuris apėmė duomenų bazės objektų, duomenų srautų modeliavimą, sąsajų su ne mažiau nei 5 skirtingais duomenų šaltiniais (informacinėmis sistemomis) ir skirtingais integravimo metodais projektavimą.
3.	**Programuotojai:** 3.1. 3.2.	1. turi tarptautiniu mastu pripažįstamą MCSD: App builder ar lygiavertę informacinių sistemų programuotojo kvalifikaciją; 2.per pastaruosius 5 (penkis) metus iki pasiūlymų pateikimo termino pabaigos turi darbo patirtį programuojant VB.net, C# ar lygiavertėmis programavimo kalbomis bent vienoje įvykdytoje sutartyje (projekte).
4.	**Informacinių sistemų veiklos procesų analitikas**	1.turi tarptautiniu mastu pripažįstamą OMG Certified UML Professional, Advanced arba Certified Business Analysis Professional™ (CBAP®) ar lygiavertę informacinių sistemų analitiko kvalifikaciją; 2. per pastaruosius 3 (trejus) metus iki pasiūlymo pateikimo termino pabaigos vykdė informacinių sistemų veiklos procesų (angl. business process) analizės specialisto pareigas (dalyvavo kaip veiklos procesų analizės specialistas) bent 1 (vienoje) informacinės sistemos kūrimo, diegimo sutartyje (projekte), kurio vykdymo metu buvo projektuojami ir (ar) transformuojami veiklos procesai į informacines sistemos funkcionalumus, sprendimus.
5.	**Testavimo specialistas**	1. turi turėti tarptautiniu mastu pripažįstamą ISTQB (International Software Testing Qualifications Board) advanced lygio ar lygiavertę testuotojo kvalifikaciją; 2. per pastaruosius 5 metus iki pasiūlymo pateikimo termino pabaigos

		turi ne trumpesnę nei 3 (trejų) metų testuotojo darbo patirtį vykdant informacinių sistemų testavimą; 3. per pastaruosius 3 (trejus) metus iki pasiūlymo pateikimo termino pabaigos vykdė testavimo specialisto pareigas (dalyvavo kaip testavimo specialistas) bent 1 (vienoje) informacinės sistemos kūrimo (modernizavimo), diegimo sutartyje (projekte), kurio vykdymo metu parengti sistemos testavimo planai, testavimo scenarijai ir atlikti testavimai bei parengtos testavimo ataskaitos.
6.	**Ergonomikos (naudotojo sąsajos kokybės) specialistas**	1. turi tarptautiniu mastu pripažįstamą Certified Usability Analyst (CUA) arba BCPE (Board of Certification in Professional Ergonomics) ar lygiavertę informacinių sistemų naudotojo sąsajos specialisto kvalifikaciją; 2. per pastaruosius 5 metus iki pasiūlymo pateikimo termino pabaigos turi ne trumpesnę kaip 3 metų darbo patirtį teikiant informacinių sistemų naudotojo sąsajos patogumo (angl. usability) analizės paslaugas; 3. per pastaruosius 3 (trejus) metus iki pasiūlymo pateikimo termino pabaigos vykdė ergonomikos specialisto pareigas (dalyvavo kaip ergonomikos specialistas) bent 1 (vienoje) sutartyje (projekte), kurio metu atliko informacinės sistemos naudotojo sąsajos kokybės vertinimą.
7.	**IT/ Informacinių sistemų saugos specialistas**	1.turi tarptautiniu mastu pripažįstamą CISM (Certified Information Security Manager) arba CISSP (Certified Information Systems Security Professional) arba CompTia security+ ar lygiavertę IT/ Informacinių sistemų saugos specialisto kvalifikaciją; 2. per pastaruosius 3 (trejus) metus iki pasiūlymo pateikimo termino pabaigos vykdė IT saugos specialisto pareigas (dalyvavo kaip IT saugos specialistas) bent 1 (viename) informacinių sistemų kūrimo, diegimo sutartyje (projekte), kuriame buvo atsakingas už sistemos saugos reikalavimų nustatymą ir jų įgyvendinimo priežiūrą.

Pastaba. Sutartyje numatytais atvejais keičiant darbuotoją (specialistą) ar pasitelkiant naują darbuotoją (specialistą), šių specialistų darbo patirtis skaičiuojama atitinkamai už 3/5 (kaip nurodyta TRS priežiūros ir plėtros paslaugų pirkimo 5.10 punkto kvalifikacijos reikalavimuose) metus nuo prašymo pakeisti darbuotoją (specialistą) ar pasitelkti naują darbuotoją (specialistą) pateikimo dienos.“

2. Papildyti Sutarties Specialiųjų sąlygų 8 punktą „Sutarties priedai“ nauju papunkčiu: „8.1.7. Susitarimas dėl asmens duomenų tvarkymo (7 priedas)“.

3. Papildyti Sutarties Specialiąsias sąlygas nauju 7 priedu (pridedama).

4. Šis susitarimas sudarytas skaitmenine forma lietuvių kalba. Šalys susitarimo skaitmeninę versiją pasirašo kvalifikuotais elektroniniais parašais. Susitarimo skaitmeninės versijos pasirašymas kvalifikuotu elektroniniu parašu prilyginamas susitarimo pasirašymui raštu.

5. Šis susitarimas įsigalioja nuo jo pasirašymo dienos ir yra laikomas neatskiriama Sutarties dalimi.

UŽSAKOVAS
Lietuvos bankas
Gedimino pr. 6, 01103 Vilnius
Tel.: +370 5 268 0029
Identifikavimo kodas 188607684
PVM mokėtojo kodas LT886076811
El. paštas info@lb.lt
Sąsk. LT41 1010 0000 0012 3456
Lietuvos banke

Valdybos pirmininkas
Gediminas Šimkus

TEIKĖJAS
UAB „Baltic Amadeus“
Lvivo g. 21A, 09313 Vilnius
Tel.: +370 527 80400
Juridinio asmens kodas 110320619
PVM mokėtojo kodas LT103206113
El. paštas info@ba.lt
A. s. LT57 7044 0600 0102 9018
AB SEB bankas

Projektų direktorius
Ruslan Grumbianin

Specialiųjų sąlygų 7 priedas

SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO

2025 m. _____ d.

Šalys, atsižvelgdamos į tai, kad:

(I) 2024 m. spalio 29 d. sudaryta Paslaugų pirkimo sutartis Nr. 2024/41-240 (toliau – Sutartis);
(II) Teikėjas, pagal Sutartį teikdamas TRS - Sandorių ataskaitų sistemos - (toliau – TRS arba Sistema) TRS priežiūros ir plėtros paslaugas (toliau – Paslaugos) Užsakovui, Užsakovo nustatytais tikslais ir priemonėmis tvarko asmens duomenis;
(III) tęsdamos sutartinius santykius Šalys siekia susitarti dėl nuostatų, kuriomis užtikrinamas Europos Parlamento ir Tarybos 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) (toliau – BDAR) reikalavimų įgyvendinimas;
sudaro šį Susitarimą dėl asmens duomenų tvarkymo (toliau – Susitarimas).

1. TAIKYMO SRITIS
1.1. Susitarimu Užsakovas (toliau gali būti vadinamas ir Duomenų valdytoju) ir Teikėjas (toliau gali būti vadinamas ir Duomenų tvarkytoju), susitaria dėl asmens duomenų tvarkymo sąlygų.
1.2. Bet kokios kitos Susitarime vartojamos sąvokos turi tokią reikšmę, kokią joms suteikia BDAR Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas ir kiti taikytini teisės aktai, reglamentuojantys asmens duomenų apsaugą, tvarkymo reikalavimus.
1.3. Šio Susitarimo nuostatos taikomos tiek, kiek Duomenų tvarkytojas tvarko asmens duomenis Duomenų valdytojo vardu, pavedimais ir Susitarime nustatytu tikslu.

2. ASMENS DUOMENŲ TVARKYMAS
2.1. Vykdant Sutartį Šalys vykdys šį asmens duomenų tvarkymą, kurio dalykas detalizuojamas žemiau:
2.1.1. asmens duomenų subjektų kategorijos – prekybą vykdantis asmenys (pirkėjo/pardavėjo/sprendimo priėmėjo); asmenys, atsakingi už investicinį sprendimą ir sandorio vykdymą;
2.1.2. asmens duomenų tvarkymo tikslas – Duomenų tvarkytojo Paslaugų teikimas Užsakovui pagal Sutartį, kas reikalinga Duomenų valdytojui užtikrinant tinkamą asmens duomenų tvarkymą TRS, vykdomą dėl finansų rinkos priežiūros, kai atliekamos LBĮ septintajame skirsnyje ir kituose finansų rinką reglamentuojančiuose teisės aktuose nustatytos Lietuvos banko funkcijos (vertybinių popierių rinkos priežiūros apimtyje, kiek susiję su prekyba finansinėmis priemonėmis), kaip tai numatytą taikytinuose teisės aktuose;
2.1.3. asmens duomenų kategorijos:
- Prekybą vykdančio asmens (pirkėjo/pardavėjo/sprendimo priėmėjo) duomenys, tokie kaip: vardas, pavardė, gimimo data, asmens identifikavimo kodas (kuriame gali būti asmens kodas, nacionalinio paso Nr. arba CONCAT kodas pagal Reglamento 2017/590 6 str. 1, 4 d. ir II priedą), nacionalinė pilietybė (dviraidis kodas) (Reglamento 600/2014 26 str. 3 d., Reglamento 2017/590 7 str., I priedo 2 lentelė), Sandorio detalės (pateikimo data ir laikas, operacija (pirkimas ar pardavimas), perkamo ar parduodamo vertybinio popieriaus kodas, kaina, kiekis, prekybos vieta, instrumento tipas, kiti Reglamento 600/2014 26 str. 3 d. ir Reglamento 2017/590 I priedo 2 lentelėje nurodyti duomenys);
- Papildomai, prekybą vykdančio asmens (pirkėjo/pardavėjo) sandorio duomenys: sandorio detalės (pateikimo data ir laikas, operacija (pirkimas ar pardavimas), perkamo ar parduodamo vertybinio popieriaus kodas, kaina, kiekis, prekybos vieta, instrumento tipas, kiti Reglamento 600/2014 26 str. 3 d. ir Reglamento 2017/590 I priedo 2 lentelėje nurodyti duomenys);
- Asmenų, atsakingų už investicinį sprendimą ir sandorio vykdymą, duomenys, tokie kaip: vardas, pavardė, gimimo data, asmens identifikavimo kodas (kuriame gali būti asmens kodas, nacionalinio paso Nr. arba CONCAT kodas pagal Reglamento 2017/590 6 str. 1, 4 d. ir II priedą), pareigos, kiti Reglamento 600/2014 26 str. 3 d., Reglamento 2017/590 7, 8 str., I priedo 2 lentelėje nurodyti duomenys.

2.1.4. asmens duomenų tvarkymo pagrindas – BDAR 6 str. 1 d. e) p.;
2.1.5. atliekami asmens duomenų tvarkymo veiksmai – informacijos ir duomenų peržiūra TRS sistemoje, kiek tai Teikėjui neišvengiamai būtina paslaugų pagal Sutartį teikimui Užsakovui, Užsakovas pasilieka teisę išskirtiniais atvejais iš anksto nurodyti ir kitas konkrečias Teikėjo atliktinas asmens duomenų tvarkymo operacijas, neišvengiamai būtinas konkrečios Paslaugos Užsakovui suteikimui;
2.1.6. saugojimo terminai – įprastais atvejais Teikėjas asmens duomenų nesaugo, tačiau jeigu pagal Susitarimo 2.1.5. fiksuotą tvarką Užsakovas nurodė išskirtiniu atveju atlikti ir papildomas asmens duomenų tvarkymo operacijas, kurios sąlygoja asmens duomenų saugojimą, tokiam konkrečiam Paslaugų užsakymui / nurodymui pasibaigus ir / ar jį įgyvendinus (pvz.: atlikus konkrečią užduotį pašalinti sutrikimą), Duomenų tvarkytojas visus konkretaus užsakymo metu / dėl užsakymo / nurodymo tapusius žinomus ar gautus asmens duomenis (įskaitant, jeigu jie nurodyti užsakyme / nurodyme ar kita forma tampa žinomi), nedelsiant neatkuriamai ištrina arba (jeigu to pareikalauja Duomenų valdytojas) – nedelsiant juos grąžina Užsakovui arba patvirtina, jog jokiu formatu asmens duomenys Užsakovo žinioje neliko (kopijomis ar kt.);
2.1.7. kiti duomenų tvarkytojai – Duomenų valdytojas įgalioja Duomenų tvarkytoją pasitelkti kitus duomenų tvarkytojus, kaip nurodyta šioje Sutartyje, su sąlyga, kad Duomenų tvarkytojas tvarkys kitų duomenų tvarkytojų sąrašą ir informuos Duomenų valdytoją apie visus planuojamus pakeitimus, susijusius su kitų duomenų tvarkytojų pasitelkimu ar pakeitimu. Duomenų valdytojas pasilieka galimybę nesutikti su tokiais pakeitimais.
2.2. Teikėjas užtikrina, kad šio Susitarimo pagrindu pateikti / gauti / kita forma jam ar jo pasitelktiems kitiems duomenų tvarkytojams tapę žinomais asmens duomenis būtų tvarkomi tik šiame Susitarime numatytu asmens

duomenų tvarkymo tikslu, atliekant tik būtinas asmens duomenų tvarkymo operacijas bei tvarkant tik tokia apimtimi, kuri yra būtina šių Užsakovo asmens duomenų tvarkymo tikslų įgyvendinimui. Teikėjui, jo pasitelktiems kitiems duomenų tvarkytojams draudžiama tvarkyti Užsakovo Sutarties, Susitarimo pagrindu patikėtus asmens duomenis bet kokiais savo ar trečiųjų šalių asmens duomenų tvarkymo tikslais, pavedimais, nurodymais.
2.3. Teikėjas užtikrina, kad tiek iš jo, tiek iš pasitektų kitų duomenų tvarkytojų pusės duomenų subjektų asmens duomenys bus tvarkomi laikantis visų BDAR, kitų aktualių nacionalinių ar tarptautinių duomenų apsaugos įstatymų ar teisės aktų, taikomų šio Susitarimo galiojimo metu, priklausomai nuo konkretaus atvejo, Duomenų valdytojui ir / arba Duomenų tvarkytojui ir / ar pasitelktiems kitiems duomenų tvarkytojams (toliau – asmens duomenų apsaugos teisės aktai).

3. BENDROSIOS PAREIGOS
3.1. Duomenų tvarkytojo atliekamas asmens duomenų tvarkymas reglamentuojamas Susitarimu ir asmens duomenų apsaugos teisės aktais, kurie yra taikytini Duomenų tvarkytojui Duomenų valdytojo atžvilgiu ir kuriais nustatoma asmens duomenų tvarkymo dalykas ir trukmė, asmens duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšis ir asmens duomenų subjektų kategorijos, taikytinos techninės ir organizacinės priemonės bei Duomenų valdytojo prievolės ir teisės.
3.2. Duomenų tvarkytojas, tvarkydamas asmens duomenis pagal šį Susitarimą, laikosi visų asmens duomenų apsaugos teisės aktų bei LR Valstybinės duomenų apsaugos inspekcijos ar kitų kompetentingų institucijų rekomendacijų, nurodymų. Duomenų tvarkytojas sutiks su visais šio Susitarimo pakeitimais, kurie yra būtini dėl asmens duomenų apsaugos teisės aktų.
3.3. Duomenų tvarkytojas savo sąskaita padeda Duomenų valdytojui gavus jo konkretų nurodymą vykdyti Užsakovo pareigas, numatytas asmens duomenų apsaugos teisės aktuose, įskaitant, bet neapsiribojant, Duomenų valdytojo pareiga atsakyti į asmenų prašymus pasinaudoti teise susipažinti su apie juos turima informacija bei prašyti asmens duomenis ištaisyti, ištrinti ar apriboti su asmeniu susijusių duomenų tvarkymą. Šiame punkte nurodyta Duomenų tvarkytojo turima teikti pagalba Duomenų valdytojo atžvilgiu vyksta pagal konkretų Duomenų valdytojo pavedimą ir negali būti interpretuojama, kaip sudaranti Teikėjui platesnės apimties / kitas techniškai galimų atlikti veiksmų LB informacinėse sistemose, kitoje suteiktoje ir / ar Paslaugų teikimui reikalingoje infrastruktūroje teises, nei nurodoma šiame Susitarime ir / ar Sutartyje.
3.4. Duomenų tvarkytojas neatlieka jokių veiksmų, dėl kurių Duomenų valdytojas pažeistų asmens duomenų apsaugos teisės aktus.
3.5. Duomenų tvarkytojas nedelsdamas informuoja Duomenų valdytoją, jei nėra nurodymų dėl asmens duomenų tvarkymo konkrečioje situacijoje, arba jei pagrįstai mano, jog konkretūs Duomenų valdytojo nurodymai pažeidžia šį Susitarimą ir / arba asmens duomenų apsaugos teisės aktus.
3.6. Be Duomenų valdytojo išankstinio rašytinio sutikimo, Duomenų tvarkytojas įsipareigoja neatskleisti tvarkomų asmens duomenų jokioms trečioms šalims.
3.7. Jei asmenys, kompetentingos institucijos ar bet kokios kitos trečiosios šalys Duomenų tvarkytojo prašo informacijos apie tvarkomus asmens duomenis kaip nurodyta šiame Susitarime, Duomenų tvarkytojas informuoja Duomenų valdytoją apie tokį prašymą. Duomenų tvarkytojas jokiu būdu negali veikti Duomenų valdytojo vardu arba kaip jo atstovas, ir be išankstinių Duomenų valdytojo nurodymų negali perduoti ar bet kuriuo kitu būdu atskleisti asmens duomenų ar kitos informacijos, susijusios su asmens duomenų tvarkymu, trečiosioms šalims. Jei Duomenų tvarkytojas pagal asmens duomenų apsaugos teisės aktus privalo atskleisti asmens duomenis, kuriuos Duomenų tvarkytojas tvarko Duomenų valdytojo vardu, Duomenų tvarkytojas privalo nedelsdamas iš anksto informuoti Duomenų valdytoją su prašymu atskleisti asmens duomenis bei jų neatskleisti be išankstinio Užsakovo sutikimo.

4. KITI DUOMENŲ TVARKYTOJAI
4.1. Duomenų tvarkytojas, gavęs Duomenų valdytojo reikalavimą, turi pateikti dokumentais pagrįstus įrodymus dėl pasitelkto kito duomenų tvarkytojo atitikties jam keliamiems reikalavimams šio Susitarimo ir taikytinų asmens duomenų apsaugos teisės aktų įgyvendinimo apimtyje.
4.2. Duomenų valdytojas gali reikalauti, kad Duomenų tvarkytojas atliktų kito duomenų tvarkytojo auditą, arba pateiktų patvirtinimą, kad toks auditas jau įvyko, arba, jei įmanoma, padėtų Duomenų valdytojui gauti audito ataskaitą iš trečiųjų šalių, siekiant užtikrinti, kad būtų laikomasi asmens duomenų apsaugos teisės aktų. Pateikęs rašytinį prašymą, Duomenų valdytojas turi teisę gauti Duomenų tvarkytojo sutarčių su kitais duomenų tvarkytojais dėl asmens duomenų tvarkymo kopijas.

5. PERDAVIMAS Į TREČIĄSIAS VALSTYBES
5.1. Duomenų tvarkytojas, be išankstinio konkretaus rašytinio Duomenų valdytojo leidimo, negali perduoti asmens duomenų už Europos Ekonominės Erdvės (toliau – EEE) ribų, trečiosioms šalims ar tarptautinėms organizacijoms. Jei Duomenų valdytojas patvirtina (duodant išankstinį leidimą raštu) tokį asmens duomenų perdavimą, duomenų perdavimo šalys sudaro privalomą susitarimą pagal galiojantį Europos Komisijos sprendimą dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems duomenų tvarkytojams, arba užtikrina, kad būtų bent viena BDAR nustatyta sąlyga, leidžianti perduoti asmens duomenis už EEE ribų, atitinkamai šaliai.
5.2. Duomenų valdytojas savo nuožiūra gali atšaukti leidimą perduoti asmens duomenis į trečiąsias valstybes, nurodytą 5.1. punkte. Tokiu atveju Duomenų tvarkytojas nedelsiant nutraukia asmens duomenų perdavimą į trečiąsias valstybės bei pateikia raštišką nutraukimo patvirtinimą.

6. INFORMACIJOS SAUGUMAS
6.1. Duomenų tvarkytojas tvarko asmens duomenis Duomenų valdytojo vardu, pagal šį Susitarimą, Sutartį ir galimus kitus Duomenų valdytojo (raštu) pateiktus nurodymus.

6.2. Duomenų tvarkytojas užtikrina, kad darbuotojai, kurie tvarko asmens duomenis Šalių vardu (įskaitant, pasitelktų kitų tvarkytojų darbuotojai, jeigu tai Užsakovas leido), laikytųsi griežtų konfidencialumo įsipareigojimų, susijusių su pagal Sutartį bei šio Susitarimo pagrindu tvarkomais asmens duomenimis bei pasirašytų pasižadėjimus saugoti asmens duomenų paslaptį. Duomenų tvarkytojas užtikrina, kad konfidencialumo, asmens duomenų paslapties saugojimo pareiga tokiems darbuotojams būtų taikoma ir po Sutarties nutraukimo bei darbo ar kitų teisinių santykių su Duomenų tvarkytoju pabaigos. Duomenų tvarkytojas užtikrina, kad tokie darbuotojai taip pat būtų tinkamai apmokyti asmens duomenų tvarkymo reikalavimų, duomenų saugumo reikalavimų ir atsakomybių, rengiant jų reguliarius mokymus, informavimo renginius ar instruktažus (ne rečiau kaip kartą per metus), t. y. kad dirbantys su asmens duomenimis asmenys (darbuotojai) užtikrintų Paslaugų teikimo sutartyje, šiame Susitarime ir asmens duomenų apsaugos teisės aktuose išdėstytus duomenų apsaugos reikalavimus. Duomenų tvarkytojas Duomenų valdytojui turi teikti reguliarius ne rečiau kaip kartą per metus patvirtinimus ir/ar įrodymus apie pasirašytus Paslaugų teikėjo darbuotojų ir/ar kitų pasitelktų tvarkytojų darbuotojų pasižadėjimus saugoti asmens duomenų paslaptį, jų tinkamą, reguliarų apmokymą, instruktavimą.
6.3. Šalys įsipareigoja nedelsdamos informuoti viena kitą, jeigu mano, kad kokie nors kitos Šalies veiksmai ir/ar neveikimas ir/ar nurodymai pažeidžia asmens duomenų apsaugos teisės aktus.
6.4. Duomenų tvarkytojas, siekdamas vykdyti duomenų tvarkymą, siekdamas padėti Duomenų valdytojui vykdyti teisines prievoles, įskaitant prievolę įgyvendinti duomenų saugumo priemones ir atlikti poveikio duomenų apsaugai vertinimą, užtikrina, kad ėmėsi ir visą Paslaugų teikimo laiką imasi tinkamų techninių ir organizacinių priemonių tvarkomiems asmens duomenims apsaugoti bei laikosi visų asmens duomenų apsaugos teisės aktų reikalavimų, Duomenų valdytojo nurodytų nurodymų, reikalavimų, taikytinų duomenų saugumo politikų. Priemonės turi užtikrinti tinkamą saugumo lygį, atsižvelgiant į:
6.4.1. esamas technines galimybes;
6.4.2. priemonių sąnaudas;
6.4.3. ypatingą riziką, susijusią su asmens duomenų tvarkymu;
6.4.4. specialių kategorijų asmens duomenų tvarkymą.
6.4.5.Paslaugų teikimo specifiką, reglamentuojamą Sutartyje ir Susitarime, kai dalis priemonių faktiškai nėra pritaikytinos konkretaus tvarkymo kontekste.
6.5. Duomenų tvarkytojas turi užtikrinti pakankamą asmens duomenų saugumo lygį, taikant tinkamas technines ir organizacines priemones, kurios yra ne žemesnes nei taikytinos vidutiniam rizikos lygmeniui, kaip tai numato taikytini teisės aktai (LR Valstybinės duomenų apsaugos inspekcijos patvirtintos Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams ir kt.).
6.6. Duomenų tvarkytojas saugo asmens duomenis nuo sunaikinimo, pakeitimo, neteisėto atskleidimo ar neteisėtos prieigos. Asmens duomenys taip pat saugotini nuo visų kitų neteisėtų asmens duomenų tvarkymo būdų. Priklausomai nuo jų tinkamumo, taikytina: asmens duomenų šifravimas; galimybė užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą; galimybė laiku atkurti prieinamumą ir prieigą prie asmens duomenų, įvykus fiziniam ar techniniam incidentui; techninių ir organizacinių priemonių, užtikrinančių duomenų tvarkymo saugumą, reguliaraus testavimo, tikrinimo ir įvertinimo procesas. Atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat asmens duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, Duomenų tvarkytojas (žemiau teikiamuose Susitarimo 6.6. papunkčiuose gali būti vadinamas ir organizacija) įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant *inter alia* (jei reikia):
6.6.1. Asmens duomenų saugumo politika ir procedūros: asmens duomenų ir jų tvarkymo saugumas organizacijoje (asmens duomenų saugumo politika) turi būti dokumentuotas kaip informacijos saugumo politikos dalis, kurioje numatyta asmens duomenų konfidencialumo, vientisumo ir prieinamumo kontrolės priemonės; asmens duomenų saugumo politika turi atitikti teisinius, įstatyminius, reguliavimo ir sutartinius reikalavimus bei būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus; asmens duomenų saugumo politika turi būti perduota susipažinti atitinkamam personalui ir suinteresuotosioms šalims; asmens duomenų saugumo politikos gavėjai turi būti patvirtinę, jog jie ją supranta ir sutinka jos laikytis (jei taikoma); asmens duomenų saugumo politika turi nustatyti bent: prieigos valdymą, turto valdymą, informacijos perdavimą, asmens duomenų saugumo pažeidimų valdymą, atsarginių kopijų darymo tvarką, personalo pareigas (funkcijas) ir atsakomybes, organizacines, žmonių, fizines ir technologines informacijos saugumo priemones, įdiegtas asmens duomenų saugumui užtikrinti, taip pat duomenų tvarkytojų ar trečiųjų šalių, susijusių su asmens duomenų tvarkymu, sąrašą; atsižvelgiant į asmens duomenų saugumo politiką, turi būti sukurtos ir prižiūrimos su asmens duomenų tvarkymu susijusios veiklos procedūros, kuriose turėtų būtų nurodyti atsakingi asmenys, saugaus asmens duomenų tvarkymo taisyklės ir reagavimas į asmens duomenų saugumo pažeidimus;
6.6.2. Vaidmenys ir atsakomybės: su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal asmens duomenų saugumo politiką; Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu); turi būti paskirti atsakingi asmenys, saugos specialistas (saugos įgaliotinis) ir duomenų apsaugos pareigūnas (jei taikoma), už konkrečias asmens duomenų saugumo užduotis organizacijoje;
6.6.3. Prieigos valdymas ir teisės: bendrieji prieigos valdymo reikalavimai (prieigos teisių suteikimo / keitimo / panaikinimo tvarka) turi būti dokumentuoti kaip asmens duomenų saugumo politikos dalys; kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) ir / arba „būtina naudoti“ (angl. need to use) principais; prieigos valdymo politika turi būti išsami ir dokumentuota, organizacija šiame dokumente turi nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis; prieigos valdymo kontrolę užtikrinančių funkcijų atskyrimas (pvz., prieigos užklausų, prieigos leidimų, pačios prieigos administravimas) turi būti aiškiai

apibrėžtas ir dokumentuotas; tam tikros pareigybės (funkcijos), turinčios dideles prieigos teises (privilegijuotosios prieigos teisės), turi būti aiškiai apibrėžtos ir priskirtos tik ribotam darbuotojų skaičiui;
6.6.4. Išteklių ir turto valdymas: organizacija turi turėti išteklių, naudojamų asmens duomenims tvarkyti, registrą. Išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą, virtualias mašinas), vietą (fizinę ar elektroninę), išorės paslaugų tiekėjus (jeigu pasitelkiami). Išteklių registro tvarkymas turi būti priskirtas konkrečiam asmeniui; išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas; visos pareigybės, turinčios prieigą prie išteklių, turi būti apibrėžtos ir patvirtintos dokumentais; turi būti nustatytos, dokumentuotos ir įgyvendintos išteklių (pvz. debesijos paslaugų, asmeninių įrenginių, duomenų tvarkytojų paslaugų) naudojimo taisyklės bei tvarkymo procedūros;
6.6.5. Kiti duomenų tvarkytojai: prieš pradedant vykdyti asmens duomenų tvarkymą, turi būti apibrėžtos, dokumentuotos ir suderintos formalios gairės ir procedūros, taikomos kitiems duomenų tvarkytojams (pvz., subrangovams) dėl asmens duomenų tvarkymo, šios gairės ir procedūros turi nustatyti tokį patį (ne žemesnį) asmens duomenų saugumo lygį, koks yra numatytas organizacijos saugumo politikoje, Susitarime, Sutartyje; kitas duomenų tvarkytojas privalo nedelsdamas pranešti Sutartyje ir Susitarime nustatyta tvarka apie nustatytus asmens duomenų saugumo pažeidimus; kitas duomenų tvarkytojas turi pateikti dokumentais pagrįstus įrodymus dėl atitikties jam keliamiems asmens duomenų saugumo reikalavimams ir įsipareigojimams; organizacijai reikalinga reguliariai tikrinti kito duomenų tvarkytojo atitiktį nustatytų reikalavimų ir įsipareigojimų lygiui;
6.6.6. Asmens duomenų saugumo pažeidimai ir saugumo incidentai: turi būti nustatytas reagavimo į saugumo incidentus planas, vaidmenys ir atsakomybės, kontaktinis asmuo, užtikrinantys greitą ir veiksmingą incidentų, susijusių su asmens duomenų saugumu, valdymą. Visa organizacija turi būti supažindinta su reagavimo į saugumo incidentus planu; asmens duomenų saugumo pažeidimai turi būti fiksuojami (dokumentuojami), apie juos turi būti nedelsiant pranešama Užsakovui, turi būti nustatyta pranešimo apie asmens duomenų saugumo pažeidimus tvarka; žinios, įgytos iš asmens duomenų saugumo pažeidimų, turėtų būti naudojamos asmens duomenų saugumo kontrolės priemonėms stiprinti ir gerinti; saugumo incidentų likvidavimo planas turi būti patvirtintas dokumentais, tarp kurių būtų galimų saugumo incidento poveikio mažinimo priemonių sąrašas ir aiškus atskirų funkcijų paskirstymas;
6.6.7. Veiklos tęstinumas: organizacija turi nustatyti pagrindines procedūras, kurių reikia laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas; veiklos tęstinumo planas turi būti išsamiai dokumentuotas (laikantis bendros saugumo politikos). Jame turi būti pateiktas aiškus veiksmų planas ir funkcijų paskirstymas; veiklos tęstinumo plane turi būti apibrėžtas garantuotas paslaugų lygio susitarimas (angl. Service-level agreement (SLA)), kuriuo nustatomas teikiamų paslaugų mąstas;
6.6.8. Asmens duomenų perdavimas: organizacijoje turi būti numatytos ir taikomos asmens duomenų perdavimo procedūros ir priemonės; asmens duomenų perdavimo politika turi būti dokumentuota asmens duomenų saugumo politikoje, asmens duomenų perdavimo politiką turi sudaryti taisyklės reglamentuojančios informacijos perdavimą elektroniniu, fiziniu ir verbaliniu perdavimo būdu;
6.6.9. Darbo santykiai: darbo sutartyje arba kitame dokumente turi būti aiškiai numatyti vaidmenys ir atsakomybės, bei įsipareigojimai susiję su organizacijoje taikoma asmens duomenų saugumo politika; turi būti aiškiai numatytos atsakomybės bei įsipareigojimai pasibaigus darbo santykiams (pvz., konfidencialumo; asmens duomenų grąžinimo / sunaikinimo);
6.6.10. Personalo ugdymas: organizacijoje personalas turi suprasti savo atsakomybes, pagrindines asmens duomenų saugumo procedūras ir pagrindines kontrolės priemones, užtikrinant asmens duomenų saugumą; organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu, darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus (siūlomas mokymų periodiškumas – kartą per metus); organizacija turi užtikrinti, kad personalas suprastų asmens duomenų saugumo politikos pažeidimo pasekmes, organizacijos drausminį procesą, tam, kad nepažeistų asmens duomenų saugumo politikos, su asmens duomenų saugumu susijusios konkretaus dalyko politikos ir procedūrų; organizacijos nuolatinėse personalo mokymų programose turi būti įtraukta speciali programa, skirta mokyti naujus darbuotojus duomenų apsaugos bei kibernetinio saugumo tema;
6.6.11. Personalo konfidencialumas: vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus; darbuotojai, prieš pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti su asmens duomenų saugumo politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo įsipareigojimus;
6.6.12. Nuotolinis darbas: organizacija turi užtikrinti, kad nuotolinio darbo vietoje būtų laikomasi ir įgyvendinama organizacijos asmens duomenų saugumo politika; nuotolinio darbo politika turi būti dokumentuota kaip asmens duomenų saugumo politikos dalis;
6.6.13. Reagavimas į informacijos saugumo incidentus: personalas turi būti informuotas apie atsakomybę nedelsiant pranešti apie informacijos saugumo incidentus; personalas turi žinoti pranešimo apie informacijos saugumo incidentų procedūrą ir kontaktinį asmenį, kuriam reikia pranešti apie įvykusį incidentą; pranešimo apie įvykius mechanizmas turėtų būti kuo paprastesnis (visų pasiekiamas, prieinamas ir žinomas);
6.6.14. Fizinė sauga: turi būti užtikrinama, kad organizacijoje prie tvarkomų asmens duomenų būtų galima fiziškai prieiti tik Užsakovo nustatytu ir leistinu būdu; fizinės saugos politika turi būti dokumentuota kaip asmens duomenų saugumo politikos dalis; turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos; taip pat turi būti užtikrinta, kad nebūtų paliktų laisvai prieinamų tinklo įrenginių, nenaudojamų tinklo kabelių; būtina naudoti aiškią visų darbuotojų ir lankytojų identifikavimo sistemą, naudojant tinkamas priemones, pvz., visiems norintiems patekti į organizacijos patalpas tapatybę patvirtinančius darbo leidimus; atitinkamos saugios zonos turėtų būti apibrėžtos ir apsaugotos tinkamomis patekimo kontrolės priemonėmis; popierinis ar elektroninis registravimo rinkmenų žurnalas turi būti saugiai laikomas, prižiūrimas ir stebimas; įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose; prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam

prieinamumui; laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos; tarnybinių stočių patalpoje turėtų būti: įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis; išorės subjektų (kitų duomenų tvarkytojų) personalui, teikiančiam paslaugas, turi būti suteikta ribota prieiga prie saugių zonų;
6.6.15. Švaraus „stalo“, „ekrano“ politika: organizacijoje turi būti įgyvendinama švaraus „stalo“, „ekrano“ politika; galiniai įrenginiai turi būti apsaugoti (pvz., slaptažodžiais, PIN kodais, biometriniais duomenimis ar kitomis apsaugos priemonėmis); nepalikti laisvai prieinamų, matomų asmens duomenų darbo vietoje; dokumentus ir galinius įrenginius išdėstyti tvarkingai, naudoti kitas priemones (pvz., naudoti stalus su pertvara, nelaikyti ekranų atsuktų į klientus / langus, naudoti monitorių privatumo filtrus), kad sumažinti riziką, jog naudojamą informaciją (tvarkomus asmens duomenis) pamatys leidimo neturintys asmenys; informacinėse sistemose turi būti sukonfigūruota užrakinimo po tam tikro laiko arba atjungimo funkcija (pvz., po 15 min. neaktyvumo automatiškai užsirakinantis kompiuterio ekranas); po darbo valandų nepalikti darbo vietoje laisvai prieinamų svarbių dokumentų ar laikmenų su asmens duomenimis (pvz., padėti į rakinamą stalčių);
6.6.16. Duomenų naikinimas, šalinimas: prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti; prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus; jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti; prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. Multiple passes of Software-based Overwriting); jei saugiems duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas;
6.6.17. Prieigų kontrolė ir autentifikavimas: turi būti įdiegta, įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams; prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras; turi būti vengiama naudoti bendras naudotojų paskyras; vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas; turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika); minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis; slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lyg; prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio; naudotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. Hash form); turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės; taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius, taip pat turi būti užtikrinta, kad slaptažodžiai nesikartotų; registruoti žurnaliniuose įrašuose prisijungimus ir nesėkmingus bandymus. Po nustatyto nesėkmingų bandymų prisijungti, blokuoti prisijungimą / paskyrą; privilegijuotiems naudotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas kelių veiksnių autentifikavimas, visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė, virtualus privatus tinklas (angl. VPN) ir kiti atitinkami saugumo mechanizmai, autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.;
6.6.18. Naudotojo galiniai įrenginiai (kompiuterinės darbo vietos): naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų; turi būti įdiegta antivirusinė programinė įranga, antivirusinės programinės įrangos duomenų bazės turi būti atnaujinamos ne rečiau, kaip kartą per parą, rekomenduojama atnaujinti duomenų bazes dažniau, priklausomai nuo grėsmių lygio ir sistemos saugumo reikalavimų, kad būtų užtikrinta efektyvi apsauga nuo naujausių virusų ir kenkėjiškų programų; naudotojams negalima turėti privilegijuotų teisių diegti, šalinti, administruoti neautorizuotos programinės įrangos; kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant; IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta (Rekomenduojamas neaktyvios sesijos laikas – ne ilgiau kaip 15 min); antivirusinės programinės įrangos ir informacija apie virusus bei kenkimo programinę įrangą duomenų bazėse turi būti atnaujinama ne rečiau kaip kartą per parą; turi būti uždrausta perduoti asmens duomenis iš kompiuterinių darbo vietų į išorinius saugojimo įrenginius (pvz., USB raktai, DVD, išorinius standžiuosius diskus ir kt.). Išjungti / blokuoti fizinius prievadus (USB raktų naudojimą);
6.6.19. Mobilieji, nešiojamieji įrenginiai: mobiliųjų, nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą, įskaitant asmeninius įtaisus, jei organizacija leidžia juos naudoti (angl. BYOD – Bring You Own Device); mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti; mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti; mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos; organizacija turi turėti galimybę nuotoliniu būdu ištrinti asmens duomenis mobiliuosiuose, nešiojamuose įrenginiuose, kurių saugumas buvo sukompromituotas (pvz., pažeistos saugumo nuostatos, prarastas patikimumas); mobiliuosiuose, nešiojamuosiuose įrenginiuose turi būti atskirti privatūs ir organizacijos veiklos duomenys, naudojant saugias programinės įrangos talpyklas (konteinerius) arba skirtingas paskyras; nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės;
6.6.20. Tarnybinių stočių, duomenų bazių apsauga: duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos privilegijomis; duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus; saugomoms byloms ar įrašams apsaugoti turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą;

duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis;
6.6.21. Techninių žurnalų įrašai ir stebėsena: techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti; techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai) (rekomenduojamas saugojimo terminas – ne trumpiau kaip 6 mėnesiai); techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį; visi sistemų administratorių veiksmai (taip pat ir jų atliekamas naudotojų teisių papildymas, panaikinimas, keitimas) turi būti registruojami; turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio; prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną; stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus; stebėti išeinantį ir įeinantį tinklo, sistemos bei programų duomenų srautą, resursų (pvz., CPU, standžiųjų diskų, atminties, pralaidumo) naudojimą ir jų našumą; organizacija turi nusistatyti įprastą resursų naudojimą / našumą ir pagal jį stebėti, ar nėra neatitikimų;
6.6.22. Tinklo ir komunikacijos sauga: kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL); belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems naudotojams ir procesams, belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių, belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais; reikėtų vengti nuotolinės prieigos prie IT sistemų, tais atvejais, kai ši prieiga yra išties reikalinga, ji yra galima tik organizacijos paskirtam darbuotojui (pvz., sistemų administratoriui, saugumo specialistui) kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius; bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas; jei organizacijoje yra aptarnaujami klientai, turi būti atskirtas viešas tinklas skirtas klientas, nuo organizacijos vidinio tinklo iš kuriuo yra pasiekiamos IT sistemos;
6.6.23. Atsarginės kopijos: atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis; atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų; atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą; pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai (rekomenduojamas atsarginių kopijų darymo dažnumas: kasdien – pridedamoji kopija; kas savaitę – pilna kopija); atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje; atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos;
6.6.24. Keitimų valdymas: organizacija turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto); turi būti įdiegta išsami ir dokumentais pagrįsta IT keitimų valdymo politika, keitimų valdymo politika turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir naudotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika turi būti reguliariai atnaujinama;
6.6.25. Programinės įrangos sauga: informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. Frameworks), standartus (pvz., Agile, OWASP ir kt.); specifiniai saugos reikalavimai, susiję su organizacijos veiklos ypatumais, turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose; turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos; po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją turi būti laikomasi pagrindinių saugos reikalavimų; prieš pradedant naudoti programinę įrangą, turi būti atliktas programinės įrangos ir infrastruktūros pažeidžiamumo ir atsparumo testavimas, programinė įranga turi atitikti reikiamą saugumo lygį; turi būti atliekami periodiški infrastruktūros atsparumo grėsmėms testavimai; programinės įrangos atnaujinimai turi būti testuojami ir vertinami prieš juos diegiant į darbo aplinką; programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis; testuojant sistemas, reikia naudoti testinius duomenis, o tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros, saugumo reikalavimai.

7. PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

7.1. Duomenų tvarkytojas, sužinojęs apie bet kokią neleistiną prieigą prie asmens duomenų ar kitą saugumo incidentą (toliau – asmens duomenų saugumo pažeidimas), turi imtis visų reikalingų veiksmų ir nepagrįstai nedelsdamas, jei tik įmanoma, pranešti apie tai Duomenų valdytojui, bet jokiu būdu ne vėliau kaip per 24 valandas, po to, kai sužinojo apie pažeidimą. Pranešime turi būti bent:
7.1.1. aprašytas asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų asmenų kategorijas ir apytikslį skaičių, taip pat atitinkamų Asmens duomenų įrašų kategorijas ir apytikslį skaičių;
7.1.2. nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;
7.1.3. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės asmens duomenų subjektams;
7.1.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.
7.2. Duomenų tvarkytojas privalo užtikrinti, kad prieiga prie asmens duomenų būtų suteikta tik tiems darbuotojams, kuriuos nurodė Užsakovui, nes jiems yra būtina atlikti Paslaugų teikimui darbus dėl tiesioginių darbo funkcijų atlikimo pagal Sutartį. Duomenų tvarkytojas užtikrina, kad tokie darbuotojai laikosi konfidencialumo įsipareigojimų tokiu pat mastu, kaip ir Duomenų tvarkytojas pagal šį Susitarimą.

7.3. Šalys visapusiškai bendradarbiauja atliekant asmens duomenų saugumo pažeidimų tyrimą ir imasi visų reikalingų priemonių, kad dar labiau apribotų asmens duomenų, susijusių su asmens duomenų saugumo pažeidimu, atskleidimą be leidimo ar tvarkymą.
7.5. Duomenų tvarkytojas, gavęs Užsakovo prašymą, savo lėšomis nedelsiant padeda Užsakovui pranešti apie asmens duomenų saugumo pažeidimus susijusiems asmens duomenų subjektams ir atitinkamoms institucijoms, jeigu Užsakovas nenurodo kitaip.
7.6. Konfidencialumo įsipareigojimai (įskaitant, nurodyti Pasižadėjime saugoti asmens duomenų paslaptį ir kituose taikytinuose dokumentuose, įskaitant šį Susitarimą) lieka galioti ir po Sutarties pasibaigimo arba jos nutraukimo.

8. TVARKYMO STEBĖJIMAS, TEISĖ ATLIKTI AUDITĄ
8.1. Užsakovas, Sutarties, Susitarimo galiojimo laikotarpį stebi, kaip Duomenų tvarkytojas laikosi asmens duomenų tvarkymo reikalavimų. Užsakovas, jo už Sutarties vykdymą atsakingu paskirtas tarnautojas, gali prašyti Užsakovo ataskaitų, informacijos, teikti Duomenų tvarkytojui rašytinius nurodymus dėl su Sutartimi susijusių veiksmų, kitų susijusių atitikties veiksnių tobulinimo. Pastebėjus neatitikimo asmens duomenų apsaugos teisės aktams, Sutarties, Susitarimo reikalavimams, požymių, Užsakovas, jo už Sutarties vykdymą atsakingu paskirtas tarnautojas, inicijuoja asmens duomenų tvarkymo veiklos, kurią atlieka Duomenų tvarkytojas pagal sudarytą Sutartį ir Susitarimą, auditą ar Duomenų tvarkytojo patikrinimą.
8.2. Patikrinimų ar auditų metu Duomenų valdytojas stebi ir tikrina, ar Duomenų tvarkytojas vykdo įsipareigojimus, prisiimtus sudaryta asmens duomenų tvarkymo sutartimi, įskaitant:
8.2.1. ar asmens duomenis tvarkantys Duomenų tvarkytojo darbuotojai yra pasirašę *Pasižadėjimą saugoti asmens duomenų paslaptį* ar jiems taikoma atitinkama Lietuvos Respublikos teisės aktuose nustatyta konfidencialumo pareiga;
8.2.2. ar asmens duomenis tvarkantys Duomenų tvarkytojo darbuotojai yra mokomi asmens duomenų apsaugos klausimais;
8.2.3. ar Duomenų tvarkytojas tinkamai valdo prieigos teisės vykstant personalo kaitai;
8.2.4. ar Duomenų tvarkytojas, tvarkydamas asmens duomenis Užsakovo vardu, įgyvendina tinkamas ir sutartas organizacines ir technines asmens duomenų saugumo priemones;
8.2.5. ar Duomenų tvarkytojas atlieka rizikos, susijusios su Lietuvos banko vardo atliekamo asmens duomenų tvarkymu, vertinimus, siekiant užtikrinti tinkamą asmens duomenų saugumą;
8.2.6. ar naudojasi tik tais kitais duomenų tvarkytojais, kurių pasitelkimui Užsakovas šio Susitarimo nustatyta tvarka yra iš anksto pritaręs;
8.2.7. ar kitiems duomenų tvarkytojams, tvarkantiems asmens duomenis Užsakovo vardu, Duomenų tvarkytojas yra nustatęs tuos pačius įsipareigojimus, kaip ir tie, kurie numatyti Užsakovo ir Duomenų tvarkytojo sudarytoje Sutartyje, Susitarime, taikytinuose asmens duomenų apsaugos teisės aktuose;
8.2.8. ar Duomenų tvarkytojas tinkamai prižiūri pasitelktus kitus duomenų tvarkytojus;
8.2.9. ar Duomenų tvarkytojas vykdo įsipareigojimus savalaikiai ir tinkamai pranešti apie visus asmens duomenų saugumo pažeidimus Užsakovui;
8.2.10. ar Duomenų tvarkytojas tinkamai informuoja Užsakovą apie gautus duomenų subjektų kreipimusis dėl savo asmens duomenų tvarkymo ir jų teisių įgyvendinimo;
8.2.11. ar Duomenų tvarkytojas laikosi Užsakovo nurodymų dėl asmens duomenų perdavimo;
8.2.12. ar Duomenų tvarkytojas vykdo kitus nurodymus, įsipareigojimus, nurodytus Sutartyje, Susitarime, taip pat duotus po Susitarimo su Užsakovu sudarymo;
8.2.13. kita.
8.3. Užsakovas gali nuspręsti atlikti Duomenų tvarkytojo auditą, patikrinimą pats arba pavesti jį atlikti nepriklausomam auditoriui / patikrinimo paslaugų teikėjui. Audito / patikrinimo metu gali būti tikrinamos Duomenų tvarkytojų patalpos ir (ar) Duomenų tvarkymo vieta.
8.4. Duomenų valdytojas pats turi teisę imtis priemonių, reikalingų patikrinti (audituoti), ar Duomenų tvarkytojas gali vykdyti savo įsipareigojimus pagal šį Susitarimą, ir ar Duomenų tvarkytojas iš tiesų ėmėsi priemonių, užtikrinančių tokį atitikimą. Duomenų tvarkytojas įsipareigoja Duomenų valdytojui pateikti visą reikalingą informaciją, įrodančią, kad laikomasi šiame Susitarime nustatytų įsipareigojimų, bei leidžia atlikti auditą, įskaitant patikrinimus vietoje, vykdomus Duomenų valdytojo ir/arba Duomenų valdytojo paskirto auditoriaus.
8.5. Duomenų tvarkytojo šiame Susitarime nustatytos tvarkos laikantis pasitelktų kitų duomenų tvarkytojų asmens duomenų tvarkymo auditai, patikrinimai, įskaitant patikrinimus vietoje, atliekami tomis pačiomis sąlygomis ir apimtimi bei tvarka, kaip ir Duomenų tvarkytojo.
8.6. Duomenų tvarkytojas, gavęs Duomenų valdytojo reikalavimą, turi pateikti dokumentais pagrįstus įrodymus dėl savo ir / ar pasitelkto kito duomenų tvarkytojo atitikties keliamiems reikalavimams ir įsipareigojimų vykdymui šio Susitarimo, Sutarties ir taikytinų asmens duomenų apsaugos teisės aktų įgyvendinimo apimtyje.

9. ATSAKOMYBĖ
9.1. Šalys atsako už savo pareigų pagal Susitarimą nevykdymą. Jei kiti pasitelkti duomenų tvarkytojai nevykdo / netinkamai vykdo duomenų apsaugos prievoles ar kitas Susitarimo nuostatas, pirminis Duomenų tvarkytojas (Paslaugų teikėjas) išlieka visiškai atsakingas Duomenų valdytojui už kitų duomenų tvarkytojų prievolių vykdymą ir už visas su tuo susijusias pasekmes.
9.2. Duomenų tvarkytojas įsipareigoja atsakyti už neteisėtą asmens duomenų tvarkymą ir atlyginti Duomenų valdytojui dėl Duomenų tvarkytojo vykdyto neteisėto asmens duomenų tvarkymo patirtus nuostolius, sumokėtas baudas ar kompensacijas. Be žalos atlyginimo už pažeidimą, jei jis atsirado dėl šio Susitarimo ir (arba) kitų sutarčių nesilaikymo, Duomenų valdytojas turi teisę gauti žalos atlyginimą iš Duomenų tvarkytojo už visas Duomenų valdytojo patirtas išlaidas, mokesčius, jei tvarkymas atliktas neteisėtai / neatliktas Duomenų tvarkytojo, nulėmė žalos atsiradimą.

10. KITOS NUOSTATOS

10.1. Jei Duomenų valdytojas pagrįstai reikalauja, Duomenų tvarkytojas turi įdiegti papildomas technines ir organizacines saugumo priemones ar įgyvendinti savo atliekamo tvarkymo pokyčius be papildomų išlaidų. Duomenų tvarkytojui pranešama apie bet kokius Duomenų valdytojo nurodymus, susijusius su saugumu ir asmens duomenų tvarkymu, patikslinimus per pagrįstą laiką, kad Duomenų tvarkytojas galėtų atlikti reikiamus procedūrų pakeitimus.

10.2. Duomenų tvarkytojas negali perduoti šio Susitarimo vykdymo be Duomenų valdytojo patvirtinimo.

10.3. Susitarimas įsigalioja jo pasirašymo dieną ir galioja iki visiškų sutartinių įsipareigojimų įvykdymo. Duomenų valdytojas turi teisę vienašališkai nutraukti Susitarimą, jeigu Duomenų tvarkytojas nevykdytų arba netinkamai vykdytų pateiktus pavedimus dėl asmens duomenų tvarkymo, pažeistų kitus šio Susitarimo ar taikytinų asmens duomenų apsaugos teisės aktų nuostatas. Apie vienašališką Susitarimo nutraukimą Duomenų valdytojas raštu įspėja Duomenų tvarkytoją prieš 1 (vieną) mėnesį.

10.4. Teikėjas, ne vėliau nei prieš 1 darbo dieną iki Susitarimo / Sutarties pabaigos dienos garantuoja Susitarime numatytų reikalavimų faktinį įgyvendinimą ir pateikia už Sutarties vykdymą paskirtam iš Užsakovo pusės atsakingam Lietuvos banko tarnautojui užpildytą bei Duomenų tvarkytojo atsakingo asmens pasirašytą (tuo patvirtinant) Duomenų tvarkytojo klausimyną nutraukiant asmens duomenų tvarkymo santykius (Susitarimo 1 priedas).

10.5. Jei Susitarime / Sutartyje aiškiai nenurodytas kitas terminas, ar Užsakovas konkrečiu atveju nenurodys kitaip, savo įsipareigojimus kiekviena iš Šalių privalo įvykdyti nepagrįstai nedelsdama, t. y. per trumpiausią protingą terminą.

10.6. Šis Susitarimas gali būti pakeistas ir (arba) papildytas tik raštišku Šalių susitarimu.

10.7. Susitarimo turinį sudaranti ir/ar su ja susijusi informacija, taip pat šio Susitarimo vykdymo metu Šalių viena kitai tiek sąmoningai, tiek atsitiktinai atskleista bet kokia kita informacija yra konfidenciali. Ši informacija tiek Paslaugų teikimo sutarties galiojimo laikotarpiu, tiek Paslaugų teikimo sutarčiai pasibaigus, tretiesiems asmenims gali būti atskleista tik tiek, kiek toks informacijos atskleidimas yra būtinas Sutarties tinkamam vykdymui, ir tik iš anksto gavus atitinkamą kitos Šalies raštišką sutikimą.

UŽSAKOVAS / DUOMENŲ VALDYTOJAS	**TEIKĖJAS / DUOMENŲ TVARKYTOJAS**
Lietuvos banko Valdybos pirmininkas Gediminas Šimkus	UAB „Baltic Amadeus“ Projektų direktorius Ruslan Grumbianin

DUOMENŲ TVARKYTOJO KLAUSIMYNAS
NUTRAUKIANT ASMENS DUOMENŲ TVARKYMO SANTYKIUS

I. DUOMENŲ TVARKYTOJO DUOMENYS

Pavadinimas:	
Adresas:	
Susitarimo dėl asmens duomenų tvarkymo data	

II. PATVIRTINIMAI

1.	Ar patvirtinate, kad visi Lietuvos banko patikėti asmens duomenys, esantys pas Duomenų tvarkytoją (jeigu buvo gautas leidimas – pas kitus duomenų tvarkytojus), buvo eksportuoti ir išsiųsti Lietuvos bankui sutartu būdu / formatu?	☐ Taip ☐ Ne ☐ Netaikoma, ne Lietuvos bankas reikalavo ištrynimo
2.	Ar patvirtinate, kad visi Lietuvos banko patikėti asmens duomenys, esantys pas Duomenų tvarkytoją (jeigu buvo gautas leidimas – pas kitus duomenų tvarkytojus), buvo neatkuriamai ištrinti iš visų tvarkymo saugojimo vietų?	☐ Taip ☐ Ne ☐ Netaikoma, nes Lietuvos bankas reikalavo grąžinimo
3.	Ar patvirtinate, kad Lietuvos banko pateikti duomenys nebus Duomenų tvarkytojo (jeigu buvo gautas leidimas – pas kitus duomenų tvarkytojus) saugomi ilgiau nei Susitarime dėl asmens duomenų tvarkymo sutartą laikotarpį?	☐ Taip ☐ Ne
4.	Ar patvirtinate, kad jokia Duomenų tvarkytojo (jeigu buvo gautas leidimas – kitų duomenų tvarkytojų) saugomų Lietuvos banko asmens duomenų dalis nebus naudojama jokiais kitais nei Susitarime dėl asmens duomenų tvarkymo Lietuvos banko nurodytais tikslais?	☐ Taip ☐ Ne

III. PRIEDAI

Kartu su šiuo klausimynu pateikite asmens duomenų sunaikinimo įrodymus (jeigu taikoma):

1. _____
2. _____
3. _____
4. _____
5. _____

IV. PAPILDOMI KOMENTARAI

_____
_____
_____

Patvirtinu, kad esu įgaliotas duomenų tvarkytojo vardu pateikti patvirtinimus, o pateikta informacija yra tiksli ir teisinga:

data	pareigos	parašas	vardas, pavardė“

Susitarimo dėl asmens duomenų tvarkymo
2 priedas

KITI DUOMENŲ TVARKYTOJAI

Duomenų valdytojas (Užsakovas) patvirtina, kad Duomenų tvarkytojas (Teikėjas) savo vykdomam Paslaugų teikimui pagal Sutartį turi teisę pasitelkti žemiau nurodytus kitus duomenų tvarkytojus (subtvarkytojus):

Eil. Nr.	Pavadinimas	Juridinio asmens kodas	Reg. buveinės adresas	Duomenų tvarkymo aprašymas
1.	MB Focus IT	305210799	Baltų pr. 59-54, LT-48232 Kaunas	Duomenų tvarkymas atliekamas tik tiek ir tokia apimtimi, kiek tai reikalinga Paslaugų teikimui informacinių sistemų veiklos procesų analitiko kompetencijos apimtyje
2.	MB Konrema	305432287	Rugių g. 9E-12, LT-08430 Vilnius	Duomenų tvarkymas atliekamas tik tiek ir tokia apimtimi, kiek tai reikalinga Paslaugų teikimui IT/ Informacinių sistemų saugos specialisto kompetencijos apimtyje..

Duomenų tvarkytojas užtikrina, kad tiek iš jo, tiek iš pasitektų kitų duomenų tvarkytojų pusės duomenų subjektų asmens duomenys bus tvarkomi laikantis visų asmens duomenų apsaugos teisės aktų, taikomų Susitarimo galiojimo metu, priklausomai nuo konkretaus atvejo, Duomenų valdytojui ir / arba Duomenų tvarkytojui ir / ar pasitelktiems kitiems duomenų tvarkytojams..

UŽSAKOVAS
Lietuvos bankas
Valdybos pirmininkas
Gediminas Šimkus

TEIKĖJAS
UAB „Baltic Amadeus“
Projektų direktorius
Ruslan Grumbianin