

UAB BALTIC RED PRIVATUMO POLITIKA

UAB Baltic RED (duomenų valdytojas ir (arba) tvarkytojas) (toliau - **Bendrovė**), įmonės kodas 300582361, adresas Islandijos pl. 32, Kaunas, Tel. +370 37 239 010, El. p. info@balticred.com, gerbia Jūsų privatumą ir įsipareigoja saugoti jį, laikydamasi šios privatumo politikos (toliau – **Privatumo politika**). Privatumo politikoje viešai pateikiama informacija apie tai, kokie fizinio asmens duomenys tvarkomi, tvarkymo tikslai, teisinis duomenų tvarkymo pagrindas, duomenų saugojimo laikotarpiai, ir kita informacija, kurią reikalauja pateikti galiojantys teisės aktai. Ši Privatumo politika taikoma tvarkant fizinių asmenų duomenis automatinio būdu, taip pat ir neautomatinio būdu tvarkant asmens duomenų susistemintas rinkmenas. Ši politika netaikoma internetiniame puslapyje www.balticred.lt pateikiamoms nuorodoms į kitų asmenų tinklalapius, todėl mes rekomenduojame atskirai pasidomėti minėtų tinklalapių privatumo politikomis ar taisyklėmis.

1. Sąvokos

- 1.1. **Asmens duomenys / Duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima tiesiogiai arba netiesiogiai nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens kodą, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.
- 1.2. **Darbuotojas** reiškia asmenį, kuris su Duomenų valdytoju yra sudaręs darbo sutartį, laikinojo darbo sutartį arba savanoriškos veiklos sutartį.
- 1.3. **Duomenų tvarkymas** – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas.
- 1.4. **Duomenų valdytojas** – UAB Baltic RED, kuri, tvarkydama fizinių asmenų duomenis, nustato tų duomenų naudojimo būdus ir priemones.
- 1.5. **Duomenų subjektas** – Fiziniai asmenys, kurių duomenis tvarko UAB Baltic RED.
- 1.6. **Duomenų tvarkytojas** – subjektai, kurie tvarko UAB Baltic RED valdomus asmens duomenis pagal UAB Baltic RED nurodymus.
- 1.7. **Duomenų teikimas** - Asmens duomenų atskleidimas perduodant ar kitu būdu padarant juos prieinamus (išskyrus paskelbimą visuomenės informavimo priemonėse).
- 1.8. Kitos Privatumo politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (ADTAĮ) ir / arba Bendrajame asmens duomenų apsaugos reglamente (BDAR).

2. Fizinio asmens duomenų apsauga

- 2.1. Su fizinio asmens duomenimis Bendrovė elgiasi atsakingai. Duomenų apsaugai naudojamos techninės ir organizacinės saugumo priemonės. Duomenys laikomi saugiai ir yra prieinami ribotam asmenų skaičiui. Asmens duomenys tvarkomi Europos Sąjungos / Europos ekonominės erdvės ribose.
- 2.2. Bendrovė be fizinio asmens išankstinio sutikimo asmens duomenų neperduoda jokiems nesusijusiems tretiesiems asmenims. Fizinio asmens duomenis be atskiro fizinio asmens sutikimo Bendrovė gali pateikti mokestinėms institucijoms, teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų, ar kitais teisės aktų numatytais atvejais.
- 2.3. Bendrovės tvarkomus fizinio asmens duomenis gali gauti atsakingi už sutarties sudarymą ar vykdymą Darbuotojai. Savo veiklai vykdyti Bendrovė taip pat naudoja trečiųjų asmenų teikiamomis paslaugomis, kurių tinkamam suteikimui gali būti būtina suteikti prieigą prie fizinio asmens duomenų. Šiuo atveju Bendrovė užtikrina, kad duomenų tvarkytojai laikosi konfidencialumo bei užtikrina tinkamą asmens duomenų apsaugą.

3. Asmens duomenų tvarkymo principai ir tikslai

- 3.1. Darbuotojai, atlikdami savo pareigas ir tvarkydami asmens duomenis, privalo:
 - a) asmens duomenis tvarkyti teisėtai, sąžiningai ir skaidriai;
 - b) rinkti nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkyti su tais tikslais nesuderinamu būdu;
 - c) renkant ir tvarkant asmens duomenis laikytis tikslingumo, proporcingumo ir duomenų kiekio mažinimo principų, nereikalauti pateikti tų duomenų, kurie nėra reikalingi, nekaupiami ir netvarkyti perteklinių duomenų;
 - d) užtikrinti asmens duomenų tikslumą ir, jei reikia dėl asmens duomenų tvarkymo, nuolat juos atnaujinti; netikslus ar neišsamius duomenis ištaisyti, papildyti, sunaikinti arba jų tvarkymą sustabdyti;
 - e) asmens duomenis saugoti tokia forma, kad Duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi;
 - f) asmens duomenis tvarkyti tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

4. Asmens duomenų šaltiniai

- 4.1. **Asmens duomenis Duomenų subjektas pateikia pats.** Duomenų subjektas kreipiasi į Bendrovę, naudoja Bendrovės teikiamomis paslaugomis, perka prekes ir (ar) paslaugas, palieka komentarus, užduoda klausimus, kreipiasi į Bendrovę prašant suteikti informaciją ir pan.
- 4.2. **Asmens duomenys gaunami iš kitų šaltinių.** Duomenys gaunami iš kitų įstaigų ar įmonių, viešai prieinamų registų ir pan.

5. Asmens duomenų tvarkymas

- 5.1. **Asmens duomenis Bendrovė tvarko šiais tikslais:**

5.1.1. Bendrovės veiklos užtikrinimo ir tęstinumo vykdymas. Šiuo tikslu tvarkomi šie duomenys:

- ✓ Sutarčių sudarymo bei vykdymo tikslu gali būti tvarkomi tiekėjų (fizinių asmenų) asmens duomenys: vardas (-ai), pavardė (-ės), asmens kodas arba gimimo data, gyvenamoji vieta (adresas), telefono numeris, elektroninio pašto adresas, darbovietė, pareigos, parašas, verslo liudijime esantys duomenys (veiklos rūšis, grupė, kodas, pavadinimas, veiklos vykdymo laikotarpiai, išdavimo data, suma), individualios veiklos pažymėjimo numeris, duomenys ar Duomenų subjektas yra PVM mokėtojas, banko atsiskaitomoji sąskaita ir bankas, paslaugos/prekės suma, valiuta bei kiti duomenys, kuriuos pateikia pats asmuo, kuriuos Bendrovė gauna pagal teisės aktus vykdydama Bendrovės veiklą ir (arba) kuriuos tvarkyti Bendrovę įpareigoja įstatymai ir (arba) kiti teisės aktai.
- ✓ Sutarčių sudarymo bei vykdymo tikslu tvarkomi tiekėjų atstovų duomenys: vardas (-ai), pavardė (-ės), telefono numeris, elektroninio pašto adresas, įmonės pavadinimas, adresas, pareigos, įgaliojimų duomenys (numeris, data, įgaliotinio asmens gimimo data, parašas).
- *Sutartys, PVM sąskaitos – faktūros ir kiti susiję dokumentai yra saugomi vadovaujantis Bendrųjų dokumentų saugojimo rodyklėje, patvirtintoje Lietuvos vyriausiojo archyvaro įsakymu, nurodytais terminais.*
- *Duomenų tvarkymo teisinis pagrindas – būtinybė įvykdyti sutartį, kurios šalis yra klientas kaip Duomenų subjektas, arba siekiant imtis veiksmų kliento prašymu prieš su juo sudarant sutartį (BDAR 6 str. 1 d. b punktas), kai tam tikrus asmens duomenis įpareigoja tvarkyti teisės aktai (BDAR 6 str. 1 d. c punktas).*

5.1.2. Įmonės skolininkų administravimas. Šiuo tikslu tvarkomi šie duomenys:

- ✓ Administruojant Bendrovės skolininkus, perduodant skolas išieškojimui gali būti tvarkomi klientų (skolininkų, fizinių asmenų) asmens duomenys: vardas (-ai), pavardė (-ės), telefono numeris, elektroninio pašto adresas, įsiskolinimo suma, informacija apie suteiktas paslaugas ir/ar parduotas prekes, kiti su įsiskolinimu susiję duomenys.
- *Sutartys, PVM sąskaitos – faktūros ir kiti susiję dokumentai yra saugomi vadovaujantis Bendrųjų dokumentų saugojimo rodyklėje, patvirtintoje Lietuvos vyriausiojo archyvaro įsakymu, nurodytais terminais.*
- *Duomenys, susiję su Bendrovės skolininkų administravimu, saugojami ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi.*
- *Duomenų tvarkymo teisinis pagrindas – būtinybė įvykdyti sutartį, kurios šalis yra klientas kaip Duomenų subjektas, arba siekiant imtis veiksmų kliento prašymu prieš su juo sudarant sutartį (BDAR 6 str. 1 d. b punktas), kai tam tikrus asmens duomenis įpareigoja tvarkyti teisės aktai (BDAR 6 str. 1 d. c punktas) bei būtinybė siekti teisėtų Bendrovės interesų gerinti savo veiklą ir verslo sėkmės rodiklius (BDAR 6 str. 1 d. f punktas).*

5.1.3. Praktikos sutarčių vykdymas. Šiuo tikslu tvarkomi šie duomenys:

- ✓ Vardas (-ai), pavardė (-ės), asmens kodas, jeigu jo nėra – gimimo data, parašas, telefono numeris, elektroninio pašto adresas, adresas, mokymosi įstaiga, praktikos atlikimo laikas, veikla.
- *Praktikantų asmens duomenys, kurie yra atitinkamų dokumentų (sutartyse, įsakymuose, prašymuose ir kt.) tekstuose (elektroninėje erdvėje, popieriniame dokumente ar kitokio pavidalo laikmenoje), yra saugomi vadovaujantis Bendrųjų dokumentų saugojimo rodyklėje, patvirtintoje Lietuvos vyriausiojo archyvaro įsakymu, nurodytais terminais.*
- *Duomenų tvarkymo teisinis pagrindas – būtinybė įvykdyti sutartį, kurios šalis yra praktikantas kaip Duomenų subjektas, arba siekiant imtis veiksmų praktikanto prašymu prieš su juo sudarant sutartį (BDAR 6 str. 1 d. b punktas) ir kai tam tikrus asmens duomenis įpareigoja tvarkyti teisės aktai (BDAR 6 str. 1 d. c punktas).*

5.1.4. Naujų darbuotojų paieška į laisvas darbo vietas Bendrovėje. Šiuo tikslu tvarkomi šie kandidatų asmens duomenys:

- ✓ vardas, pavardė, gimimo data, adresas, tel. numeris, el. p. adresas, išsilavinimas, kiti duomenys, kurie nurodyti kandidatų Bendrovei pateikiamuose dokumentuose, įskaitant CV.
- *Kandidatų asmens duomenys yra saugomi iki atrankos į laisvą darbo vietą pabaigos. Jeigu kandidatas sutinka su ilgesniu asmens duomenų saugojimu, asmens duomenys saugomi sutikime dėl asmens duomenų tvarkymo nurodytą laikotarpį.*
- *Duomenų tvarkymo pagrindas yra sutikimas. Kandidatai į laisvas darbo vietas duoda susitikimą (konkliudentiniais veiksmais) tvarkyti jų duomenis tik iki atrankos pabaigos. Pasibaigus atrankai į laisvą darbo vietą nepasirinktų kandidatų duomenys ištrinami, išskyrus atvejus, jeigu kandidatai duoda atskirą sutikimą dėl duomenų tvarkymo pasibaigus atrankai (BDAR 6 str. 1 d. a punktas).*

5.1.5. Užklausų, komentarų ir nusiskundimų administravimas. Šiuo tikslu tvarkomi šie duomenys:

- ✓ Vardas (-ai), pavardė (-ės), elektroninio pašto adresas, telefono numeris, adresas, užklausos, komentaro ir nusiskundimo tema, užklausos, komentaro ir nusiskundimo tekstas.
- *Užklausų, komentarų ir nusiskundimų duomenys saugomi 1 (vieną) mėnesį nuo jų pateikimo, išskyrus jeigu asmens duomenis yra būtina tvarkyti ilgiau kitu teisiniu pagrindu (pvz. teisinių ginčų sprendimas). Tokiu atveju asmens duomenys yra saugojami ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi.*
- *Duomenų tvarkymo teisinis pagrindas – tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie Duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai Duomenų subjektas yra vaikas (BDAR 6 str. 1 d. f punktas) ir Duomenų subjekto sutikimas (BDAR 6 str. 1 d. a punktas).*

5.1.6. Bendrovės darbuotojų, kitų Duomenų subjektų ir turto saugumo užtikrinimo tikslu (vaizdo stebėjimas). Šiuo tikslu tvarkomi šie duomenys:

- ✓ Vaizdo atvaizdas. Vaizdo stebėjimo sistemos nenaudoja veido atpažinimo ir (ar) analizės technologijų, jomis užfiksuoti vaizdo duomenys nėra grupuojami ar profiliuojami pagal konkretų Duomenų subjektą (asmenį). Apie vykdomą vaizdo stebėjimą Duomenų subjektas informuojamas informaciniais ženklais su vaizdo kameros simboliu ir Bendrovės rekvizitais, kurie pateikiami prieš patenkant į stebimą teritoriją ir (ar) patalpą. Į vaizdo kamerų stebėjimo lauką nepatenka patalpos, kuriose Duomenų subjektas tikisi absoliučios asmens duomenų apsaugos.
- *Vaizdo stebėjimo įrašymo vaizdo kameromis funkcija yra aktyvi 24 valandas per parą, vaizdo stebėjimo kameros įsijungia nuo judesio daviklio ir jomis gauti asmens duomenys (vaizdo duomenys) saugomi iki 14 (keturiolikos) dienų nuo jų užfiksavimo momento, po to automatinio būdu sunaikinami, išskyrus atvejus, kai esama pagrindo manyti, kad yra užfiksuotas nusižengimas, darbo pareigų pažeidimas, daroma nusikalstama veika ar kiti neteisėti veiksmai (iki atitinkamo tyrimo ir (ar) bylos nagrinėjimo pabaigos).*
- *Duomenų tvarkymo teisinis pagrindas – tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie Duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai Duomenų subjektas yra vaikas (BDAR 6 str. 1 d. f punktą).*

5.1.7. Bendrovės organizuojamų iniciatyvų, apklausų, konkursų ir kitų visuomenės įtraukimo veiklų administravimas. Šiuo tikslu tvarkomi šie duomenys:

- ✓ Vardas (-ai), pavardė (-ės), telefono numeris, elektroninio pašto adresas, Duomenų subjekto pateikti pasiūlymai, komentarai, idėjos ar kita informacija, informacija apie pateiktus sutikimus ir patvirtinimus.
- *Asmens duomenys saugomi iniciatyvos vykdymo laikotarpiu ir 3 (trejus) metus po jos pabaigos, išskyrus atvejus, kai dėl pateikto pasiūlymo atsiranda kitas duomenų tvarkymo tikslas ar teisinis santykis. Jeigu duomenų saugojimas būtinas siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus, duomenys gali būti saugomi iki galutinio tokių reikalavimų išsprendimo.*
- *Duomenų tvarkymo teisinis pagrindas – tvarkyti duomenis būtina siekiant teisėtų Bendrovės interesų administruoti organizuojamas iniciatyvas, apklausas, konkursus ir kitas visuomenės įtraukimo veiklas, vertinti pateiktus pasiūlymus, užtikrinti galimybę naudoti pateiktus pasiūlymus bei pareikšti, vykdyti ar apginti teisinius reikalavimus (BDAR 6 straipsnio 1 dalies f punktą).*

5.1.8. Kitais tikslais, kuriais Bendrovė turi teisę tvarkyti Duomenų subjekto asmens duomenis, kai Duomenų subjektas išreiškė savo sutikimą, kai duomenis reikia tvarkyti dėl Bendrovės teisėto intereso arba kai tvarkyti duomenis Bendrovę įpareigoja atitinkami teisės aktai.

6. Socialinių tinklų naudojimas

- 6.1. Visą informaciją, kurią pateikiate socialinės žiniasklaidos priemonėmis (įskaitant pranešimus, laukelių „Like“ ir „Follow“ naudojimą, bei kitą komunikaciją), kontroliuoja atitinkamo socialinio tinklo valdytojas.
- 6.2. Šiuo metu mūsų Bendrovė turi paskyrą socialiniame tinkle „LinkedIn“, kurio privatumo politika yra pateikiama adresu <https://www.linkedin.com/legal/privacy-policy>
- 6.3. Rekomenduojame perskaityti trečiųjų šalių privatumo pranešimus ir tiesiogiai susisiekti su paslaugų teikėjais, jei Jums kyla bet kokių klausimų dėl to, kaip jie naudoja Jūsų asmens duomenis.

7. Duomenų apsaugos pareigūnas

- 7.1. Vadovaujantis BDAR 37 str. 1 d. b p., duomenų valdytojas ir duomenų tvarkytojas turi pareigą paskirti duomenų apsaugos pareigūną, kai duomenų valdytojo ir duomenų tvarkytojo veikla atitinka visus šiuos kriterijus:
 - Pagrindinė veikla – asmens duomenų tvarkymas;
 - Reguliarus ir sistemingas Duomenų subjektų stebėjimas;
 - Duomenų subjektų stebėjimas vykdomas dideliu mastu.
- 7.2. Įvertinus Bendrovės veiklos specifiką, darytina išvada, kad Bendrovės pagrindinė veikla nėra asmens duomenų tvarkymas ir Bendrovės nevykdo subjektų stebėjimo plačiu mastu. Tai reiškia, kad pirmasis ir trečiasis kriterijus nėra tenkinami, todėl Duomenų apsaugos pareigūno skyrimas nėra būtinas.
- 7.3. Vadovaujantis 29 straipsnio duomenų apsaugos darbo grupės rekomendacijomis net kai nėra privaloma pagal BDAR paskirti duomenų apsaugos pareigūno, įmonėms kartais gali būti naudinga jį paskirti savanoriškai. 29 straipsnio duomenų apsaugos darbo grupė skatina šią savanorišką praktiką.
- 7.4. Atsižvelgdama į tai, Bendrovė skiria asmens duomenų apsaugos pareigūną. Pareigūnas gali būti paskirtas iš esamų Bendrovės darbuotojų, naujas darbuotojas arba asmuo, su kuriuo būtų sudaroma paslaugų teikimo sutartis.
- 7.5. Duomenų apsaugos pareigūnas padės laikytis reikalavimų įgyvendinant atskaitomybės priemones (pvz., atlikti poveikio duomenų apsaugai vertinimus ir atlikti arba padėti atlikti auditus). Duomenų apsaugos pareigūnas veikia kaip tarpininkas tarp įvairių suinteresuotųjų subjektų (pvz., priežiūros institucijų, Duomenų subjektų ir organizacijos verslo padalinių).
- 7.6. Duomenų apsaugos pareigūnas nėra asmeniškai atsakingas už netinkamą Duomenų tvarkymą. Duomenų valdytojas arba Duomenų tvarkytojas privalo užtikrinti ir sugebėti įrodyti, kad duomenys tvarkomi laikantis BDAR nuostatų, todėl ir už duomenų tvarkymo atitiktį reikalavimams atsakingas Duomenų valdytojas arba Duomenų tvarkytojas.
- 7.7. Duomenų apsaugos pareigūnas atlieka šias funkcijas:
 - Informuoja Bendrovę ir duomenis tvarkančius darbuotojus apie jų prievoles pagal BDAR ir kitus Europos Sąjungos arba valstybės narės duomenų apsaugos nuostatas ir konsultuoja juos šiais klausimais;
 - Stebi, kaip Bendrovė laikosi BDAR, kitų Europos Sąjungos arba nacionalinių duomenų apsaugos nuostatų ir vidinių įmonių dokumentų duomenų apsaugos srityje, įskaitant pareigų pavidimą, Duomenų tvarkymo operacijose dalyvaujančių darbuotojų informuotumo didinimą bei mokymą ir susijusius auditus;
 - Konsultuoja dėl poveikio duomenų apsaugai vertinimo ir stebi jo atlikimą pagal BDAR 35 straipsnį;

- Bendradarbiauja su priežiūros institucija, t. y. Valstybine duomenų apsaugos inspekcija;
- Atlieka kontaktinio asmens funkcijas priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais, įskaitant BDAR 36 straipsnyje nurodytas išankstines konsultacijas, ir prireikus konsultuoja visais kitais klausimais.

8. Asmens duomenų teikimas

- 8.1. Bendrovė įsipareigoja laikytis konfidencialumo pareigos Duomenų subjektų atžvilgiu. Asmens duomenys gali būti atskleisti trečiosioms šalims tik tada, jeigu to reikia sutarčiai Duomenų subjekto naudai sudaryti ir vykdyti, arba dėl kitų teisėtų priežasčių.
- 8.2. Bendrovė gali pateikti asmens duomenis savo duomenų tvarkytojams, kurie teikia Bendrovei paslaugas ir tvarko asmens duomenis Bendrovės vardu. Duomenų tvarkytojai turi teisę tvarkyti asmens duomenis tik pagal Bendrovės nurodymus ir tik ta apimtimi, kiek tai yra būtina siekiant tinkamai vykdyti sutartyje nustatytus įsipareigojimus. Bendrovė pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų BDAR reikalavimus ir būtų užtikrinta Duomenų subjekto teisių apsauga.
- 8.3. Bendrovė taip pat gali teikti asmens duomenis atsakydama į teismo arba valstybinių institucijų prašymus ta apimtimi, kiek tai būtina siekiant tinkamai vykdyti galiojančius teisės aktus ir valstybinių institucijų nurodymus.
- 8.4. Bendrovė garantuoja, kad asmens duomenys nebus nei pardavinėjami, nei nuomojami tretiesiems asmenims.

9. Asmens duomenų saugojimo terminas

- 9.1. Bendrovės surinkti asmens duomenys yra saugomi spausdintiniuose dokumentuose ir (arba) Bendrovės informacinėse sistemose. Asmens duomenys tvarkomi ne ilgiau, negu reikia duomenų tvarkymo tikslams pasiekti arba ne ilgiau nei to reikalauja Duomenų subjektai ir (ar) numato teisės aktai.
- 9.2. Nors Duomenų subjektas gali nutraukti sutartį ir atsisakyti Bendrovės paslaugų, tačiau Bendrovė ir toliau privalo saugoti Duomenų subjekto duomenis dėl galbūt ateityje atsirasiančių reikalavimų ar teisinių pretenzijų tol, kol pasibaigs duomenų saugojimo terminai.

10. Duomenų subjekto teisės:

- 10.1. **Teisė gauti informaciją apie duomenų tvarkymą;**
- 10.2. **Teisė susipažinti su tvarkomais duomenimis;**
- 10.3. **Teisė reikalauti ištaisyti duomenis;**
- 10.4. **Teisė reikalauti ištrinti duomenis („Teisė būti pamirštam“).** Ši teisė netaikoma, jei asmens duomenys, kuriuos prašoma ištrinti, yra tvarkomi ir kitu teisiniu pagrindu, tokiu kaip tvarkymas būtinas sutarties vykdymui arba yra pareigos pagal taikomus teisės aktus vykdymas.
- 10.5. **Teisė apriboti duomenų tvarkymą;**
- 10.6. **Teisė nesutikti su duomenų tvarkymu;**
- 10.7. **Teisė į duomenų perkeliamumą.** Teisė į duomenų perkeliamumą negali daryti neigiamo poveikio kitų teisėms ir laisvėms. Duomenų subjektas teisės į duomenų

perkeliamumą neturi tų asmens duomenų atžvilgiu, kurie tvarkomi neautomatiniu būdu susistemintose rinkmenose, pavyzdžiui, popierinėse bylose;

10.8. Teisė reikalauti, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas;

10.9. Teisė pateikti skundą dėl asmens duomenų tvarkymo Valstybinei duomenų apsaugos inspekcijai;

Bendrovė privalo sudaryti sąlygas Duomenų subjektui įgyvendinti pirmiau nurodytas Duomenų subjekto teises, išskyrus įstatymų nustatytus atvejus, kai reikia užtikrinti valstybės saugumą ar gynybą, viešąją tvarką, nusikalstamų veiklų prevenciją, tyrimą, nustatymą ar baudžiamąjį persekiojimą, svarbius valstybės ekonominius ar finansinius interesus, tarnybinės ar profesinės etikos pažeidimų prevenciją, tyrimą ir nustatymą, Duomenų subjekto ar kitu asmenų teisių ir laisvių apsaugą.

11. Duomenų subjekto teisių įgyvendinimo tvarka

- 11.1. Kreiptis dėl Duomenų subjekto teisių įgyvendinimo Duomenų subjektas turi teisę žodžiu arba raštu, pateikiant prašymą (1 priedas) asmeniškai, paštu ar elektroninėmis priemonėmis šioje Privatumo politikoje nurodytais kontaktais. Prašymas įgyvendinti Duomenų subjekto teises turi būti įskaitomas, pasirašytas, jame turi būti nurodyti asmens, teikiančio prašymą, vardas, pavardė, adresas ir (ar) kiti kontaktiniai duomenys ryšiui palaikyti ar kuriais pageidaujama gauti atsakymą dėl Duomenų subjekto teisių įgyvendinimo.
- 11.2. Duomenų subjektas, kreipdamasis į Bendrovę dėl Duomenų subjekto teisių įgyvendinimo, turi patvirtinti savo tapatybę. To nepadarius, Duomenų valdytojas negalės priimti Duomenų subjekto prašymų ir Duomenų subjekto teisės nebus įgyvendinamos. Ši nuostata netaikoma, jeigu kreipiamasi dėl informavimo apie asmens duomenų tvarkymą pagal BDAR 13 ir 14 straipsnius.
- 11.3. Jeigu dėl Duomenų subjekto teisių įgyvendinimo asmuo nusprendžia kreiptis į Duomenų valdytoją asmeniškai, Duomenų subjektas turi pateikti Duomenų valdytojui savo asmens tapatybės dokumentą. Jeigu dėl Duomenų subjekto teisių įgyvendinimo asmuo nusprendžia kreiptis į Duomenų valdytoją raštu, pateikiant prašymą paštu, prie prašymo pridedama asmens tapatybę patvirtinančio dokumento kopija, patvirtinta notaro ar kita teisės aktų nustatyta tvarka. Asmens tapatybę patvirtinančio dokumento kopijos nepateikus, Duomenų subjekto prašoma atvykti į Bendrovę ir pateikti asmens tapatybės dokumentą. Jeigu asmuo nusprendžia pateikti prašymą elektroninėmis priemonėmis, prašymas turi būti pasirašytas kvalifikuotu elektroniniu parašu.
- 11.4. Jei Bendrovei kiltų abejonių dėl asmens teikiančio prašymą tapatybės, duomenų, Bendrovė turi teisę prašyti papildomos informacijos, reikalingos ja įsitikinti.
- 11.5. Bendrovės atsakymas Duomenų subjektui suteikiamas ne vėliau kaip per vieną mėnesį nuo Duomenų subjekto prašymo gavimo dienos, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes. Šis laikotarpis prireikus gali būti pratęstas dar dviem mėnesiams, atsižvelgiant į prašymų sudėtingumą ir skaičių.

12. Duomenų subjekto atsakomybė

12.1. Duomenų subjektas turi:

- 12.1.1. informuoti Bendrovę apie pateiktos informacijos ir duomenų pasikeitimus.
Bendrovei svarbu turėti teisingą ir galiojančią Duomenų subjekto informaciją;

12.1.2. pateikti reikalingą informaciją, kad esant Duomenų subjekto prašymui Bendrovė galėtų identifikuoti Duomenų subjektą ir įsitikinti, kad bendrauja arba bendradarbiauja tikrai su konkrečiu duomenų subjektu (pateikti asmens tapatybę patvirtinantį dokumentą arba teisės aktų nustatyta tvarka ar elektroninių ryšių priemonėmis, kurios leistų tinkamai identifikuoti duomenų subjektą). Tai reikalinga duomenų subjekto ir kitų asmenų duomenų apsaugai, kad atskleista informacija apie duomenų subjektą būtų pateikta tik Duomenų subjektui, nepažeidžiant kitų asmenų teisių.

13. Organizacinės ir techninės asmens duomenų apsaugos priemonės

13.1. Bendrovė deda maksimalias pastangas, kad Bendrovės organizacinės ir techninės duomenų saugumo priemonės atitiktų BDAR reikalavimus. Siekiant apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo taikomos tokios infrastruktūrinės, administracinės ir telekomunikacinės (elektroninės) priemonės.

14. Baigiamosios nuostatos

14.1. Perduodamas Bendrovei asmens duomenis, Duomenų subjektas sutinka su šia Privatumo politika, supranta jos nuostatas ir sutinka jos laikytis.

14.2. Plėtojant ir tobulinant Bendrovės veiklą, Bendrovė turi teisę bet kuriuo metu vienašališkai pakeisti šią Privatumo politiką. Bendrovė turi teisę vienašališkai, iš dalies ar visiškai pakeisti Privatumo politiką apie tai pranešdama internetinėje svetainėje <https://www.balticred.com/>

14.3. Privatumo politikos papildymai ar pakeitimai įsigalioja nuo jų paskelbimo dienos, t. y., nuo tos dienos, kai jie yra patalpinami internetinėje svetainėje <https://www.balticred.com/>

15. Kontaktinė informacija

15.1. Jei turite klausimų apie fizinio asmens duomenų tvarkymą, pageidavimų ar pastabų, susisieki su mumis: UAB Baltic RED, įmonės kodas 300582361, adresas Islandijos pl. 32, Kaunas, Tel. +370 37 239 010, El. p. info@balticred.com. Duomenų apsaugos pareigūno kontaktiniai duomenys – duomenuapsauga@balticred.com.

Ši versija atnaujinta 2026 m. liepos 7 d.

PRAŠYMO ĮGYVENDINTI DUOMENŲ SUBJEKTO TEISĘ (-ES) FORMA

Duomenų subjekto (fizinio asmens) vardas, pavardė

(Kontaktinė informacija: gyvenamoji vieta, telefono numeris, elektroninio pašto adresas (nurodoma duomenų subjektui pageidaujant)
arba atstovas ir atstovavimo pagrindas, jeigu prašymą pateikia duomenų subjekto atstovas)

UAB Baltic RED vadovui

PRAŠYMAS DĖL DUOMENŲ SUBJEKTO TEISIŲ (-ĖS) ĮGYVENDINIMO 20 m. d.

(prašymo sudarymo vieta)

Prašau įgyvendinti šią (šias) duomenų subjekto teisę (-es)*:

*Tinkamą langelį pažymėkite kryželiu

- ☐ **Teisė gauti informaciją apie duomenų tvarkymą.**
- ☐ **Teisė susipažinti su tvarkomais duomenimis.**
- ☐ **Teisė reikalauti ištaisyti duomenis.**
- ☐ **Teisė reikalauti ištrinti duomenis („Teisė būti pamirštam“).** Ši teisė netaikoma, jei asmens duomenys, kuriuos prašoma ištrinti, yra tvarkomi ir kitu teisiniu pagrindu, tokiu kaip tvarkymas būtinas sutarties vykdymui arba yra pareigos pagal taikomus teisės aktus vykdymas.
- ☐ **Teisė apriboti duomenų tvarkymą.**
- ☐ **Teisė nesutikti su duomenų tvarkymu.**
- ☐ **Teisė į duomenų perkeliamumą.** Teisė į duomenų perkeliamumą negali daryti neigiamo poveikio kitų teisėms ir laisvėms. Duomenų subjektas teisės į duomenų perkeliamumą neturi tų asmens duomenų atžvilgiu, kurie tvarkomi neautomatiniu būdu susistemintose rinkmenose, pavyzdžiui, popierinėse bylose.
- ☐ **Teisė reikalauti, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas.**

Kita informacija**:

** Nurodykite, ko konkrečiai prašote ir pateikite kiek įmanoma daugiau informacijos, kuri leistų tinkamai įgyvendinti Jūsų teisę (-es) (pavyzdžiui, jeigu norite gauti asmens duomenų kopiją, nurodykite, kokių konkrečiai duomenų (pavyzdžiui, 2018 m. x mėn. x d. elektroninio pašto laiško kopiją, 2018 m. x mėn. x d. vaizdo įrašą (x val. x min. – x val. x min.) kopiją pageidaujate gauti; jeigu norite ištaisyti duomenis, nurodykite, kokie konkrečiai Jūsų asmens duomenys yra netikslūs; jeigu nesutinkate, kad būtų tvarkomi Jūsų asmens duomenys, tuomet nurodykite argumentus, kuriais grindžiate savo nesutikimą, nurodykite dėl kokio konkrečiai duomenų tvarkymo nesutinkate; jeigu kreipiatės dėl teisės į duomenų perkeliamumą įgyvendinimo, prašome nurodyti, kokių duomenų atžvilgiu šią teisę pageidaujate įgyvendinti, ar pageidaujate juos perkelti į savo įrenginį ar kitam duomenų valdytojui, jeigu pastarajam, tuomet nurodykite kokiam):

PRIDEDAMA*:**

*** Jeigu prašymas yra siunčiamas paštu, prie prašymo pridedama asmens tapatybę patvirtinančio dokumento kopija, patvirtinta notaro ar kita teisės aktų nustatyta tvarka. Jeigu kreipiamasi dėl netikslių duomenų ištaisymo, pateikiamos tikslius duomenis patvirtinančių dokumentų kopijos; jeigu jos siunčiamos paštu, tuomet turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka. Jeigu duomenų subjekto asmens duomenys, tokie kaip vardas, pavardė, yra pasikeitę, kartu pateikiamos dokumentų, patvirtinančių šių duomenų pasikeitimą, kopijos; jeigu jos siunčiamos paštu, tuomet turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka.

(parašas)

(Vardas Pavardė)

UAB BALTIC RED PRIVACY POLICY

UAB Baltic RED (Data Controller and/or processor) (hereinafter the **Company**), company registration number 300582361, address Islandijos pl. 32, Kaunas, tel. +370 37 239 010, e-mail info@balticred.com, respects your privacy and is committed to safeguarding it in accordance with this Privacy Policy (hereinafter the **Privacy Policy**). The Privacy Policy publicly provides information about the processing of personal data, including the types of personal data processed, processing purposes, legal basis for data processing, data storage periods, and other information required by applicable laws. This Privacy Policy applies to the processing of personal data, both automated and non-automated, involving the systematic collection of personal data. This policy does not apply to the links provided on the website www.balticred.lt to other websites, so we recommend separately reviewing the privacy policies or rules of those websites.

1. Definitions

- 1.1. **Personal data / Data** means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as name and surname, personal code, location data, and internet identifiers, or based on one or more physical, physiological, genetic, mental, economic, cultural, or social identity traits of that individual.
- 1.2. **Employee** means a person who has entered into an employment contract, a fixed-term employment contract, or a volunteer activity agreement with the Data Controller.
- 1.3. **Data processing** means any operation or sequence of operations, such as collecting, recording, sorting, organizing, storing, adapting or modifying, extracting, accessing, using, disclosing, transmitting, distributing, or otherwise changing, by automated or non-automated means of personal data or personal data sets and access to them, as well as matching or interconnection with other data, their restriction, erasure or destruction.
- 1.4. **Data Controller** is Baltic RED UAB, which, in processing the personal data of natural persons, determines the methods and means of using that data.
- 1.5. **Data Subjects** are natural persons whose data is processed by UAB Baltic RED.
- 1.6. **Data Processor** means entities that process personal data controlled by UAB Baltic RED according to the instructions of UAB Baltic RED.
- 1.7. **Provision of data** – disclosure of personal data by transmission or making them available by any other means (with the exception of publishing them in mass media).
- 1.8. Other terms used in the Privacy Policy shall be understood as defined in the Republic of Lithuania Law on Legal Protection of Personal Data (LPPD) and/or the General Data Protection Regulation (GDPR).

2. Protection of personal data of natural persons

- 2.1. The Company treats personal data responsibly. Technical and organisational security measures are used for data protection. Data is stored securely and is accessible to a limited

number of individuals. Personal data is processed within the boundaries of the European Union/European Economic Area.

- 2.2. Without the prior consent of the Data Subject, the Company does not disclose personal data to unrelated third parties. The Company may provide personal data it processes to tax institutions, law enforcement, judicial, or pre-judicial institutions for their investigations or in other cases provided for by law, without the separate consent of the Data Subject.
- 2.3. Employees responsible for the conclusion or execution of contracts may receive the personal data processed by the Company for their activities. For its operations, the Company also utilizes services provided by third parties, access to personal data may be necessary for the proper provision of such services. In this case, the Company ensures that data processors adhere to confidentiality and ensure proper protection of personal data.

3. Principles and purposes of processing personal data

- 3.1. Employees, in performing their duties and processing personal data, must:
 - a) Process personal data lawfully, transparently and fairly;
 - b) Collect data for specified, clearly defined and for legitimate purposes, and not further process in a way incompatible with those purposes;
 - c) Adhere to the principles of purposefulness, proportionality, and data minimization when collecting and processing personal data, not demand the submission of unnecessary data, and avoid collecting and processing excessive data;
 - d) Ensure the accuracy of personal data and, if necessary for the processing of personal data, continuously update them; correct, supplement, destroy inaccurate or incomplete data, or suspend their processing.
 - e) Personal data shall be kept in a form which permits identification of the Data Subjects for no longer than it is necessary for the purposes for which the data were collected and processed;
 - f) Personal data must be managed in such a way as to ensure the adequate protection of personal data, including the protection against unauthorized processing or processing of unauthorised data and unintentional loss, destruction or damage by appropriate technical or organisational measures (the principle of integrity and confidentiality).

4. Personal data sources

- 4.1. **Personal data are provided by the Data Subject himself.** Data Subjects contact the Company, use the services provided by the Company, purchase goods and/or services, leave comments, ask questions, and contact the Company to request information, among other things.
- 4.2. **Personal data are obtained from other sources.** Data are obtained from other institutions or companies, publicly accessible registers, etc.

5. Personal data processing

- 5.1. **The Company processes personal data for the following purposes:**
 - 5.1.1. **Ensuring the operation and continuity of the Company's activities. For this purpose, the following data are processed:**
 - ✓ For the purpose of concluding and executing contracts, personal data of suppliers (natural persons) may be processed: Personal data processed for these

purposes may include name(s), surname(s), personal code or date of birth, place of residence (address), phone number, email address, workplace, position, signature, data in the business license (type of activity, group, code, name, periods of activity, issuance date, amount), individual activity certificate number, data related to whether the Data Subject is a VAT payer, bank account and bank, service/goods amount, currency, and other data provided by the individual, as well as data received by the Company in accordance with the law while conducting its activities and/or data that the Company is obliged to process by laws and/or other legal acts.

- ✓ For the purpose of contract formation and execution, the data of supplier representatives are processed, including: name(s), surname(s), telephone number, email address, company name, address, position, authorisation details (number, date, authorised person's date of birth, signature).
- *Contracts, VAT invoices and other related documents shall be stored in accordance with the time limits set out in the General Index of Document Storage approved by Order of the Chief Archivist of Lithuania.*
- *The legal basis for data processing is the necessity to fulfil a contract, where the client acts as the Data Subject, or to take actions at the client's request before entering into a contract (Article 6(1)(b) of the GDPR), when certain personal data are required by legal regulations (Article 6 (1) (c) of the GDPR).*

5.1.2. Administration of debtors of a company. For this purpose, the following data are processed:

- ✓ In administering the Company's debtors and transferring debts for recovery, the personal data of clients (debtors, natural persons) may be processed, including: name(s), surname(s), telephone number, email address, outstanding debt amount, information about services provided and/or goods sold, and other data related to the debt.
- *Contracts, VAT invoices and other related documents shall be stored in accordance with the time limits set out in the General Index of Document Storage approved by Order of the Chief Archivist of Lithuania.*
- *Data relating to the administration of the Company's debtors shall be stored for no longer than necessary for the purposes for which the personal data are processed.*
- *The legal basis for data processing is the necessity to fulfil a contract, where the client acts as the Data Subject, or to take actions at the client's request before entering into a contract (Article 6(1)(b) of the GDPR), as certain personal data are required to be processed by legal regulations (Article 6(1)(c) of the GDPR), and the necessity to pursue the legitimate interests of the Company to improve its operations and business performance (Article 6(1)(f) of the GDPR).*

5.1.3. Execution of internship contracts: For this purpose, the following data are processed:

- ✓ For the execution of internship contracts, the following personal data are processed: name(s), surname(s), personal code, or, if not available, date of

birth, signature, phone number, email address, address, educational institution, internship duration, and activities.

- *The personal data of trainees contained in the texts of relevant documents (contracts, orders, applications, etc.) (in cyberspace, in electronic or paper format or other media) , are stored in accordance with the General Guidelines for Document Storage approved by the Chief Archivist of Lithuania, specifying the retention periods.*
- *Legal Basis for Data Processing is the necessity to fulfil a contract, where the trainee acts as the Data Subject, or to take actions at the trainee's request before entering into a contract (Article 6(1)(b)) of the GDPR and when certain personal data are required to be processed by legal regulations (Article 6 (1) (c) of the GDPR).*

5.1.4. Search for new employees for vacant positions in the Company: For this purpose, the following candidate personal data are processed:

- ✓ Name, surname, date of birth, address, telephone number, email address, education, and other data specified in the documents submitted by candidates to the Company, including CV.
- *Candidates' personal data are stored until the completion of the selection for the vacant position. If the candidate agrees to a longer retention period, the personal data are stored for the period specified in the consent for personal data processing.*
- *The legal basis for data processing is consent. Candidates for vacant positions give implicit consent to process their data only until the end of the selection process. After the selection for the vacant position is completed, the data of unsuccessful candidates are deleted, except in cases where candidates provide separate consent for data processing after the selection process (Article 6 (1) (a) of the GDPR).*

5.1.5. Administering of inquiries, comments and complaints. For this purpose, the following data are processed:

- ✓ Name(s), surname(s), email address, telephone number, address, subject of the inquiry, comment, or complaint, text of the inquiry, comment, or complaint.
- *Data related to inquiries, comments, and complaints are stored for 1 (one) month from their submission, unless it is necessary to process personal data for a longer period under another legal basis (e.g., settlement of legal disputes). In such cases, personal data are retained for no longer than is necessary for the purposes for which the personal data are processed.*
- *The legal basis for data processing is the necessity to process the data to achieve the legitimate interests of the Data Controller or a third party, except where such interests or fundamental rights and freedoms of the Data Subject, which require the protection of personal data, are overridden by the legitimate interests of the controller or of a third party, in particular where the Data Subject is a child (Article 6 (1) (f) GDPR), and the consent of the Data Subject (Article 6 (1) (a) of the GDPR).*

5.1.6. Purpose of ensuring the safety of the Company employees, other Data Subjects and property (video surveillance). For this purpose, the following data are processed:

- ✓ Images. Video surveillance systems do not use facial recognition and/or analysis technology, image data captured by these systems are not grouped or profiled by a particular Data Subject (person). The Data Subject is informed about the on-going video surveillance by the information signs with the camera's symbol and the Company's details, which are presented before entering the surveyed area and/or the premises. The video surveillance area may not include the premises where the Data Subject expects absolute personal data protection.
- *The function of recording video footage with video cameras is active 24 hours a day. The surveillance cameras activate based on motion sensors, and the captured personal data (video data) are stored for up to 14 (fourteen) days from the moment of capture. Afterward, they are automatically deleted, except in cases where there is reason to believe that a violation, breach of duties, criminal activity, or other illegal actions have been recorded (until the end of the corresponding investigation and/or case resolution).*
- *Basis for the processing of data processing – the processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular, where the Data Subject is a child (Article 6 (1) (f) of the GDPR).*

5.1.7. Administration of the Company's initiatives, surveys, competitions and other public engagement activities. For this purpose, the following personal data are processed:

- ✓ First name(s), surname(s), telephone number, email address, proposals, comments, ideas or other information submitted by the Data Subject, as well as information regarding the consents and acknowledgements provided by the Data Subject.
- *Personal data shall be retained for the duration of the initiative and for 3 (three) years following its completion, except where the submitted proposal gives rise to another purpose of personal data processing or another legal relationship. Where the retention of personal data is necessary for the establishment, exercise or defence of legal claims, the personal data may be retained until such claims have been finally resolved.*
- *Legal basis for processing – the processing of personal data is necessary for the purposes of the legitimate interests pursued by the Company in administering its initiatives, surveys, competitions and other public engagement activities, evaluating submitted proposals, ensuring the Company's right to use the submitted proposals, and establishing, exercising or defending legal claims (Article 6(1)(f) of the GDPR).*

5.1.8. For other purposes for which the Company has the right to process the personal data of the Data Subject, when the Data Subject has given consent, when data need to be processed for the legitimate interests of the Company, or when processing data is required by applicable laws.

6. Using social networks

- 6.1. Any information you provide via social media (including messages, use of the Like and Follow fields and other communications) is controlled by the operator of the social network concerned.
- 6.2. Our Company currently has an account on the social network LinkedIn, whose privacy policy is available at the address <https://www.linkedin.com/legal/privacy-policy>.
- 6.3. We encourage you to read third-party privacy notices and contact service providers directly if you have any questions about how they use your personal data.

7. Data Protection Officer

- 7.1. Pursuant to Article 37(1)(b) of the GDPR, the Data Controller and data processor are obliged to appoint a data protection officer when the activities of the Data Controller and data processor meet all of these criteria.
 - Main activity – processing of personal data;
 - Regular and systematic monitoring of Data Subjects;
 - Monitoring of Data Subjects is carried out on a large scale.
- 7.1. Considering the specific nature of the Company's operations, it can be concluded that the Company's core activity is not the processing of personal data, and the Company does not conduct extensive monitoring of subjects. This means that the first and third criteria are not met, so the appointment of a Data Protection Officer is not necessary.
- 7.2. Following the recommendations of the data protection working group of Article 29, even when not mandatory under the GDPR, appointing a Data Protection Officer may sometimes be beneficial for companies and is encouraged as a voluntary practice. The Article 29 Data Protection Working Party encourages this voluntary practice.
- 7.3. Taking this into account, the Company appoints a Data Protection Officer. The Officer can be appointed from among the existing Company employees, a new employee, or a person with whom a service contract would be concluded.
- 7.4. The Data Protection Officer will assist in ensuring compliance with accountability measures (e.g., conducting impact assessments on data protection and performing or assisting in audits). The Data Protection Officer acts as an intermediary between various stakeholders (e.g., supervisory authorities, Data Subjects, and business units within the organization).
- 7.5. The Data Protection Officer is not personally responsible for improper data processing. The Data Controller or Data Processor must ensure and be able to prove that data processing complies with the provisions of the General Data Protection Regulation (GDPR). Therefore, the Data Controller or Data Processor is responsible for ensuring the compliance of data processing with the requirements.
- 7.6. The Data Protection Officer performs the following functions:
 - **Informs** the Company and employees involved in data processing about their obligations under the GDPR and other European Union or member state data protection regulations, providing consultation on these matters.
 - **Monitors** the compliance of the Company with the GDPR, other European Union or national data protection regulations, and internal company documents in the field of data protection, including issuing directives, increasing awareness and training of employees involved in data processing, and conducting related audits.

- **Provides consultation** on impact assessments and monitors their execution in accordance with Article 35 of the GDPR.
- **Liaisons** with the supervisory authority, namely the State Data Protection Inspectorate.
- Acts as a **point of contact** for the supervisory authority when it comes to inquiries related to data processing, including the preliminary consultations specified in Article 36 of the GDPR, and provides consultation on all other matters if necessary.

8. Forms of Disclosure of Personal Data

- 8.1. The Company undertakes to maintain confidentiality regarding Data Subjects. Personal data may only be disclosed to third parties if it is necessary for the conclusion and drawing up of the contract for the benefit of the Data Subject or for other legitimate reasons.
- 8.2. The Company may submit personal data to its data processors, who provide services to the Company and process personal data on behalf of the Company. Data processors have the right to process personal data only in accordance with the instructions of the Company and only to the extent necessary for the proper fulfilment of obligations laid down in the Contract. The Company shall use such processors that provide reasonable assurance that appropriate technical and organizational measures will be implemented in such a way that the processing of data complies with the requirements of the GDPR and will ensure the proper protection of the Data Subject's rights.
- 8.3. The Company may also provide personal data in response to requests from courts or public authorities to the extent necessary to properly enforce existing legislation and instructions from public authorities.
- 8.4. The Company guarantees that personal data will not be sold or leased to third parties.

9. Storage term of personal data

- 9.1. The personal data collected by the Company are stored in printed documents and/or in the Company's information systems. Personal data is processed for no longer than necessary for the purpose of data processing or for no longer than required by Data Subjects and/or provided by law.
- 9.2. Although the Data Subject may terminate the contract and refuse from the Company's services, the Company continues to be obliged to keep the data of the Data Subject for possible future claims or legal claims until the expiration of the data storage periods.

10. Rights of the Data Subject:

- 10.1. **Right to receive information on the processing of data;**
- 10.2. **Right to access the data processed;**
- 10.3. **Right to request the correction of data;**
- 10.4. **Right to request to delete the data (“The right to be forgotten”).** This right does not apply if the personal data requested to be deleted are also processed on other legal grounds, such as the processing necessary for the performance of the contract, or when the obligations according to the applicable law.
- 10.5. **Right to restriction of processing;**
- 10.6. **Right to disagree with data processing;**

10.7. **Right to data portability.** The right to data portability may not adversely affect other rights and freedoms. The Data Subject has no rights to the portability of data in relation to personal data processed in a non-automatic weighed in systematised files, such as paper files;

10.8. **Right to require that only automated data processing, including profiling, is applied;**

10.9. **Right to submit a complaint regarding the processing of personal data to the State Data Protection Inspectorate;**

The Company must ensure the disability for the Data Subject to exercise the rights of the Data Subject specified in the Rules, except in cases established by law, when it is necessary to guarantee state security or defence, public order, prevention, investigation, detection or prosecution of criminal offenses, important economic or financial interests of the state, prevention, investigation and detection of breaches of professional ethics, protection of the rights and freedoms of the Data Subject or other persons.

11. Procedure for the implementation of the Data Subject's rights

11.1. You have the right to apply for the exercise of the rights of the Data Subject orally or in writing by submitting a request (Annex 1) in person, by post or by electronic means using the contacts specified in this Privacy Policy. The request to exercise the rights of the Data Subject must be legible, signed, and must contain the name, surname, address and/or other contact details of the applicant for communication or for which a reply on the exercise of the rights of the Data Subject is requested.

11.2. When a Data Subject contacts the Company regarding the exercise of Data Subject rights, they must verify their identity. Failure to do so will result in the Data Controller being unable to process Data Subject requests, and Data Subject rights will not be implemented. This does not apply if you request information about the processing of personal data in accordance with Articles 13 and 14 of the GDPR.

11.3. If a person decides to address the Data Controller personally regarding the implementation of Data Subject rights, the Data Subject must provide the Data Controller with an identity document. If a person decides to apply to the Data Controller in writing for the exercise of the Data Subject's rights by submitting a request by post, the request shall be accompanied by a copy of the person's identity document certified by a notary public or in accordance with another procedure established by the legislation. In the absence of a copy of an identity document, the Data Subject is requested to come to the Company in person and provide a proof of identity document. If a person decides to submit a request electronically, the request must be signed with a qualified electronic signature.

11.4. If the Company has doubts about the identity of the person submitting the request or the accuracy of the information provided, the Company has the right to request additional information to verify it.

11.5. The Company's answer to the Data Subject must be given not later than within one month from the date of receipt of the Data Subject's request, taking into account the specific circumstances of the processing of personal data. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

12. Responsibilities of the Data Subject

12.2. The Data Subject must:

- 12.2.1. To inform the Company about changes in the provided information and data. It is important for the Company to have accurate and valid information about the Data Subject.
- 12.2.2. To provide the necessary information so that at the request of the Data Subject the Company can identify the Data Subject and ascertain that it communicates or co-operates with the specific Data Subject (to provide a personal identity document, or in accordance with the procedure laid down by legal acts or by electronic means of communication that allows the Data Subject to be properly identified). It is necessary for the protection of data of the Data Subject and other persons so that the disclosure of the Data Subject's information is restricted to the Data Subject, without prejudice to the rights of others.

13. Organisational and Technical Measures for Data Protection:

- 13.2. The Company makes maximum efforts to ensure that the organizational and technical data security measures comply with the requirements of the General Data Protection Regulation (GDPR). The following infrastructural, administrative and telecommunication (electronic) measures are in place to protect personal data against accidental or unlawful destruction, alteration, disclosure or any other unauthorised processing.

14. Final provisions

- 14.4. By transferring personal data to the Company, the Data Subject agrees with this Privacy Policy, understands its provisions and agrees to comply with it.
- 14.5. In the course of development and improvement of the Company's operations, the Company reserves the right to unilaterally change this Privacy Policy at any time. The Company has the right to unilaterally, partially, or fully change the Privacy Policy, notifying about it on the website <https://www.balticred.com/>.
- 14.6. Amendments or changes to the Privacy Policy take effect from the day of their publication, i.e., from the day they are posted on the website <https://www.balticred.com/>.

15. Contact details

- 15.1. If you have any questions about the processing of your personal data, or if you have any preferences or comments, please contact us: UAB Baltic RED, company registration number 300582361, address Islandijos pl. 32, Kaunas, tel. +370 37 239 010, e-mail info@balticred.com. Contact details of the Data Protection Officer – duomenuapsauga@balticred.com.

This version was updated on 7 July 2026.

FORM OF THE REQUEST TO EXERCISE THE DATA SUBJECT'S RIGHT(S)

Full name of the Data Subject (natural person)

(Contact details: place of residence, telephone number, e-mail address (to be specified at the request of the Data Subject) or representative and representation basis, if the request is submitted by the Data Subject's representative)

To the manager of UAB Baltic RED

APPLICATION ON THE IMPLEMENTATION OF THE DATA SUBJECT RIGHTS (S) _____20_____

(place of application)

Please implement the right (s) of the Data Subject*:

*Mark the appropriate box with a cross

- ☐ **Right to receive information on the processing of data.**
- ☐ **Right to access the data processed.**
- ☐ **Right to request the correction of data.**
- ☐ **Rights to request to delete the data (“The right to be forgotten”).** This right does not apply if the personal data requested to be deleted are also processed on other legal grounds, such as the processing necessary for the performance of the contract, or when the obligations according to the applicable law.
- ☐ **Right to restrict the data processing.**
- ☐ **Right to object to data processing.**
- ☐ **Right to data portability.** The right to data portability may not adversely affect other rights and freedoms. The Data Subject has no rights to the portability of data in relation to personal data processed in a non-automatic processing of system files, such as paper files.
- ☐ **Right to require that only automated data processing, including profiling, is applied.**

Other information**:

**Indicate what you specifically ask and provide as much information as possible to enable to properly enforce your right (s) (for example, if you want to receive a copy of your personal data, indicate specific data (e.g., dated xxxx xx 2018), a copy of email, video dated xxxx xx 2018 (x h x min. you want to receive; If you want to correct the data, indicate what of your specific personal data is inaccurate; if you disagree to the processing of your personal data, indicate the arguments on which you base your disagreement, indicate to which particular data processing you disagree with; if you are applying for the right to data portability, indicate in respect of which data you wish to implement this right, or if you would like to transfer it to your device or other Data Controller, and if the latter, then specify him):

ENCLOSED***:

***If the application is sent by post, a copy of the personal document confirming the identity, certified by a notary public or other legal acts, must be attached to the application. For requests of correction of inaccurate data, copies of the documents confirming the exact data are provided; if they are sent by post, they must be approved by a notary or according to other procedure established by legal acts. If the personal data of the Data Subject, such as his full name, have changed, copies of documents confirming the change of these data must also be presented; if they are sent by post, they must be approved by a notary or according to other procedure established by legal acts.

(signature)

(Full name)