

KLIENTŲ IR TIEKĖJŲ DUOMENŲ TVARKYMO IR APSAUGOS POLITIKA

CUSTOMERS' AND SUPPLIERS' DATA PROCESSING AND PROTECTION POLICY

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ДАНЫХ КЛИЕНТОВ И ПОСТАВЩИКОВ

I. ĮVADAS	I. INTRODUCTION	I. ВВЕДЕНИЕ
<p>1.1. Tiek UAB „Baltic Fresh Fruit“ (toliau – BFF), tiek jos klientai ir verslo partneriai susiduria su sutartine būtinybe priėti prie tam tikrų asmens duomenų, susijusių su klientais ir tiekėjais kaip fiziniaisiais asmenimis, taip pat klientų ir tiekėjų (juridinių asmenų) darbuotojais.</p> <p>1.2. Duomenų apsaugos reikalavimų nesilaikymas tvarkant asmens duomenis pažeidžia įstatymą. Asmens duomenų pažeidimai taip pat gali neigiamai įtakoti asmenis bei pakenkti BFF reputacijai.</p> <p>1.3 Už šios duomenų apsaugos politikos tinkamą įgyvendinimą atsako visi darbuotojai ar kiti asmenys, kurie prieina ar naudojami BFF valdomais asmens duomenimis.</p> <p>1.4. Ši duomenų apsaugos politika taikoma BFF ir bet kuriam BFF verslo partneriui (fiziniam ir juridiniam asmeniui) (toliau - PARTNERIS) (toliau</p>	<p>1.1 Both JSC “Baltic fresh fruit” (hereinafter – BFF) and its business partners face contractual necessity to access certain personal data relating to the clients and suppliers as natural persons as well as clients’ and suppliers’ (legal persons) employees, assigned by the parties.</p> <p>1.2 Failure to comply with data protection requirements when handling personal data is breaking the law. Data breaches can also cause significant distress to individuals and have an adverse impact upon BFF reputation.</p> <p>1.3 It is the responsibility of all staff or others, who access or use personal information at BFF, to adhere to this Data Protection Policy.</p> <p>1.4. This Data Protection Policy applies to BFF, on one side, and to any business partner (natural and legal person) of BFF (hereinafter – PARTNER), on</p>	<p>1.1. Как ЗАО “Baltic Fresh Fruit” (далее - BFF), так и ее клиенты и деловые партнеры сталкиваются с контрактной необходимостью доступа к определенным персональным данным, связанным с клиентами и поставщиками как с физическими лицами, а также с сотрудниками клиентов и поставщиков (юридических лиц).</p> <p>1.2. Несоблюдение требований защиты данных при обработке персональных данных нарушает закон. Нарушения, связанные с персональными данными, также могут негативно повлиять на отдельных лиц и нанести ущерб репутации BFF.</p> <p>1.3 Надлежащее осуществление настоящей политики защиты данных является обязанностью всех сотрудников или других лиц, которые получают доступ или используют персональные данные, которыми управляет BFF.</p> <p>1.4. Настоящая политика защиты данных применяется к BFF, а также к любому деловому партнеру BFF (физическому и юридическому</p>

<p>visi kartu - Šalys), kai jie turi dalytis ir tvarkyti tam tikrus asmens duomenis pagal sutartinę būtinybę, t.y. norint sudaryti ar vykdyti sutartį, ir jie abu veikia kaip nepriklausomi duomenų valdytojai dėl asmens duomenų, kuriuos reikia bendrinti (duomenų valdytojo ir gavėjo santykiai).</p> <p>1.5 Duomenų apsaugos politika netaikoma tais atvejais, kai BFF ir jos PARTNERIAI sudaro duomenų valdytojo-procesoriaus (arba atvirkščiai) santykius (pvz., IT paslaugas, darbo užmokesčio paslaugas, teisinės paslaugas).</p> <p>II. SĄVOKOS</p> <p>2.1. Sutarti tikslai: reiškia tikslus, nurodytus šios Duomenų apsaugos politikos 3.2 punkte.</p> <p>2.2. Darbo dienos: diena, išskyrus Šeštadienį, Sekmadienį ar šventinę dieną toje teritorijoje, kurioje Šalys įsikūrusios.</p> <p>2.3. Verslo partneris: bet kuris BFF esamas ar būsimas verslo partneris, kuris sudarė arba siekia sudaryti sutartį su BFF.</p> <p>2.4. Duomenų davėjas: bet kuri iš Šalių, perduodanti asmens duomenis kitai Šaliai, kuri to prašo kaip duomenų gavėja.</p>	<p>the other side (hereinafter – the Parties), when they need to share and process certain Personal Data due to contractual necessity, i.e. in order to enter into or perform a contract, and they both act as independent Data Controllers in respect of the Personal Data to be shared (controller-recipient relationship).</p> <p>1.5. The Data Protection Policy does not apply where BFF and its PARTNER enter into a controller – processor (or vice versa) relationship (e.g. IT services, payroll services, legal services).</p> <p>II. DEFINITIONS</p> <p>2.1. Agreed Purposes: shall mean those purposes set out in clause 3.2 of this Data Protection Policy.</p> <p>2.2. Business Days: a day other than a Saturday, Sunday or public holiday in the territories where the Parties are established.</p> <p>2.3. Business partner: any business partner of BFF, present or potential, who has entered or is seeking to enter into a Contract with BFF.</p> <p>2.4. Data Discloser: either Party transferring the Personal Data to the other Party asking as the Data Recipient.</p>	<p>лицу) (далее - «ПАРТНЕР») (далее все вместе - Стороны), когда они должны обмениваться и обрабатывать определенные персональные данные в соответствии с договорной потребностью, т.е. с целью заключения или исполнения договора, и они оба выступают в качестве независимых владельцев личных данных, подлежащих обмену (отношения между владельцем и получателем).</p> <p>1.5 Политика защиты данных не применяется в тех случаях, когда BFF и ее ПАРТНЕРЫ образуют отношения владелец-процессор (или наоборот) (например, ИТ-услуги, услуги заработной платы, юридические услуги).</p> <p>II. ОПРЕДЕЛЕНИЯ</p> <p>2.1. Согласованные цели: означает цели, изложенные в пункте 3.2 настоящей Политики защиты данных.</p> <p>2.2. Рабочие дни: день, за исключением Субботы, Воскресенья или дня государственного праздника на территории, где учреждены Стороны.</p> <p>2.3. Деловой партнер: любой существующий или будущий деловой партнер BFF, который заключил или стремится заключить договор с BFF.</p> <p>2.4. Поставщик данных: любая из Сторон, передающая персональные данные другой Стороне, которая запрашивает их в качестве</p>
---	--	---

<p>2.5. Duomenų apsaugos institucija: institucija, atsakinga už duomenų apsaugą toje teritorijoje, kurioje Šalys įsikūrusios.</p> <p>2.6. Duomenų gavėjas: bet kuri iš Šalių, gaunanti asmens duomenis iš Duomenų davėjo.</p> <p>2.7. Duomenų apsaugos pažeidimas: pažeidimas, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, keičiami, neteisėtai atskleidžiami ar tampa prieinami asmens duomenys.</p> <p>2.8. BDAR: Bendrasis duomenų apsaugos reglamentas (2016/679), Elektroninių ryšių duomenų apsaugos direktyva (2002/58/EB), Privatumo ir elektroninių ryšių (EK direktyva) reglamentai 2003 (SI 2426/2003) (su pakeitimais) ir visi taikytini įstatymai ir kiti teisės aktai, susiję su asmens duomenų tvarkymu ir privatumu, įskaitant, jei taikytina, nacionalinės duomenų apsaugos išduotas gaires ir praktikos kodeksus, ir bet kurios iš aukščiau išvardytų dalykų atitikmuo bet kurioje atitinkamoje jurisdikcijoje.</p> <p>2.9. Teisinis pagrindas: teisėta priežastis Šalims dalintis ir tvarkyti asmens duomenis, nurodytus</p>	<p>2.5. Data Protection Authority: the relevant data protection authority in the territories where the Parties the Contract are established.</p> <p>2.6. Data Recipient: either Party receiving the Personal Data from the other Party acting as, the Data Discloser.</p> <p>2.7. Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Shared Personal Data.</p> <p>2.8. GDPR: the General Data Protection Regulation (2016/679) (GDPR), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) (as amended) and all applicable laws and regulations relating to the processing of the Personal Data and privacy, including where applicable the guidance and codes of practice issued the national data protection authority, and the equivalent of any of the foregoing in any relevant jurisdiction.</p> <p>2.9. Legal Ground: shall mean the legal basis for the Parties to share and process the Personal Data</p>	<p>получателя данных.</p> <p>2.5. Орган по защите данных: орган, отвечающий за защиту данных на территории, где учреждены Стороны.</p> <p>2.6. Получатель данных: любая из Сторон, получающая персональные данные от Поставщика данных.</p> <p>2.7. Нарушение защиты данных: нарушение, которое вызывает случайное или незаконное уничтожение, потерю, изменение, несанкционированное разглашение или доступ к персональным данным.</p> <p>2.8. ОРЗД: Общий регламент по защите данных (2016/679), Директива о защите данных в секторе электронных коммуникаций (2002/58/EC), регламенты от 2003 года о конфиденциальности и электронных коммуникациях (директива ЕС) (SI 2426/2003) (с изменениями) и все применимые законы и другие правовые акты, касающиеся обработки и конфиденциальности персональных данных, включая, где это применимо, и установленные национальные принципы защиты данных, и практические кодексы, а также эквивалент любого из вышеперечисленных документов в любой соответствующей юрисдикции.</p> <p>2.9. Правовая основа: законное основание для обмена и обработки Сторонами персональных</p>
--	--	---

<p>šios Duomenų apsaugos politikos 5.1 punkte.</p> <p>2.10. Bendrieji asmens duomenys: asmens duomenys, kuriais pasidalino tarpusavyje Šalys, kaip tai numatyta 4-ame Duomenų apsaugos politikos straipsnyje.</p> <p>2.11. Darbuotojai: darbuotojai, dirbantys bet kuriai Šaliai ar jos subrangovams, kuriuos Šalis paskiria arba įdarbina dalyvauti sudarant ar vykdant Sutartį.</p> <p>2.12. Sutartis: bet kokia žodinė ar rašytinė verslo sutartis, kurią Šalys siekia vykdyti arba sudaryti.</p> <p>2.13. Subjekto prieigos prašymas: turi tą pačią reikšmę, kaip ir BDAR 15 skyriuje "Duomenų subjekto teisė susipažinti su asmens duomenimis".</p> <p>2.14. Duomenų valdytojas, Duomenų tvarkytojas, Duomenų subjektas ir Asmens duomenys, apdorojimas, teisė į objektą ir atitinkamos techninės bei organizacinės priemonės turi tą pačią reikšmę, kaip ir BDAR.</p>	<p>set out in clause 5.1 of this Data Protection Policy.</p> <p>2.10. Shared Personal Data: the Personal Data to be shared between the Parties under clause 4 of this Data Protection Policy.</p> <p>2.11. Employees: shall mean employees working for any of the Parties or their subcontractors, who are assigned or engaged by the Parties to participate in entering into or performing a Contract.</p> <p>2.12. Contract: any business agreement, either verbal or written, which the Parties are seeking to perform or enter into.</p> <p>2.13. Subject Access Request: has the same meaning as "Right of access by the data subject" in Article 15 of the GDPR.</p> <p>2.14. Data Controller, Data Processor, Data Subject and Personal Data, processing, Right to Object and appropriate technical and organizational measures shall have the meanings given to them in the GDPR.</p>	<p>данных, указанных в пункте 5.1 настоящей Политики защиты данных.</p> <p>2.10. Общие персональные данные: персональные данные, которыми между собой поделились Стороны, как это предусмотрено в статье 4 Политики защиты данных.</p> <p>2.11. Сотрудники: сотрудники, работающие на любую из Сторон или ее субподрядчиков, которых Сторона назначает или нанимает для участия в принятии или выполнении Договора.</p> <p>2.12. Договор: любое устное или письменное деловое соглашение, которое Стороны стремятся исполнить или заключить.</p> <p>2.13. Запрос Субъекта на доступ: имеет то же значение, что и в разделе 15 «Право субъекта данных на доступ к персональным данным».</p> <p>2.14. Владелец данных, Распорядитель данными, Субъект данных и Персональные данные, обработка, право на объект и соответствующие технические и организационные меры имеют то же значение, что и ОРЗД.</p>
<p>III. DUOMENŲ APSAUGOS POLITIKOS TIKSLAS</p> <p>3.1. Ši Duomenų apsaugos politika nustato Asmens duomenų perdavimo tarp Šalių, kaip Duomenų valdytojų, sistemą ir apibrėžia Šalių tarpusavio</p>	<p>III. PURPOSE OF THE DATA PROTECTION POLICY</p> <p>3.1. This Data Protection Policy sets out the framework for the sharing of Personal Data between the Parties as Data Controllers and</p>	<p>III. ЦЕЛЬ ПОЛИТИКИ ЗАЩИТЫ ДАННЫХ</p> <p>3.1. Настоящая Политика защиты данных устанавливает систему передачи Персональных данных между Сторонами, как Владельцами</p>

<p>pareigas, principus bei procedūras, kurių Šalys turi laikytis.</p> <p>3.2. Dalijimasis asmens duomenimis yra būtinas siekiant įgyvendinti šiuos abiejų Šalių Sutartus tikslus: <i>tam, kad šalys galėtų sudaryti ar vykdyti Sutartį.</i></p> <p>3.3. Šalys netvarkys Bendrų asmens duomenų tokiu būdu, kuris nesuderinamas su Sutartais tikslais.</p> <p>3.4. Kaip Duomenų valdytoja kiekviena Šalis yra atsakinga už tai, kad visi Bendrųjų asmens duomenų naudojimo būdai atitiktų visus taikomus duomenų apsaugos ir privatumo įstatymus bei reglamentus.</p> <p>IV. BENDRIEJI ASMENS DUOMENYS</p> <p>4.1. Šios Duomenų apsaugos politikos 3.2 punkte Sutartims tikslams, Bendrieji asmens duomenys gali apimti šiuos asmens duomenis:</p> <p><i>Pirmas vardas; vidurinis (-iai) vardas (-ai); pavardė; darbdavys; pareigos; darbo el. pašto adresas; darbo telefono numeris; viber vartotojo vardas, WhatsApp vartotojo vardas, Skype vartotojo vardas; transporto priemonės registracijos numeris.</i></p>	<p>defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.</p> <p>3.2. The sharing of Personal Data is necessary to support the following Agreed Purposes of both Parties: <i>In order for the Parties to enter into or perform a Contract.</i></p> <p>3.3. The Parties shall not process Shared Personal Data in a way that is incompatible with the Agreed Purposes.</p> <p>3.4. As a Data Controller, each Party remains responsible for ensuring that all uses of the Shared Personal Data are in compliance with all applicable Data Protection and Privacy laws and regulations.</p> <p>IV. SHARED PERSONAL DATA</p> <p>4.1. For the Agreed Purposes listed in clause 3.2 of this Data Protection Policy, the Shared Personal Data may include the following types of Personal Data:</p> <p><i>first name; middle name(s); surname; employer; job title; office email address; office phone number; viber account name; WhatsApp account name; skype account name; vehicle registration number. If the client or supplier is a natural person then</i></p>	<p>данных, и определяет взаимные обязанности, принципы и процедуры, которые должны соблюдаться Сторонами.</p> <p>3.2. Обмен персональными данными является необходимым для достижения следующих Согласованных целей обеих Сторон: <i>для того, чтобы стороны могли заключить или выполнить Договор.</i></p> <p>3.3. Стороны не будут обрабатывать Общие персональные данные способом, несовместимым с Согласованными целями.</p> <p>3.4. Как Владелец данных, каждая Сторона несет ответственность за обеспечение того, чтобы все способы использования Общих персональных данных соответствовали всем применимым законам и регламентам о защите данных и конфиденциальности.</p> <p>IV. ОБЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ</p> <p>4.1. В целях, указанных в пункте 3.2 настоящей Политики защиты данных, Общие персональные данные могут включать такие персональные данные:</p> <p><i>Первое имя; второе имя (имена); фамилия; работодатель; должность; адрес рабочей эл.почты; номер рабочего телефона; имя пользователя viber, имя пользователя WhatsApp, имя пользователя Skype;</i></p>
--	--	--

<p><i>Jeigu klientas ar tiekėjas yra fizinis asmuo, asmens kodas, registruotos gyvenamosios vietos adresas, individualios veiklos pažymėjimo numeris ir PVM mokėtojo kodas taip pat įeina į Bendruosius asmens duomenis.</i></p> <p>4.2. Bendrieji asmens duomenys apsiriboja asmens duomenimis, aprašytais šios Duomenų apsaugos politikos 4.1 punkte.</p> <p>4.3. Bendrieji asmens duomenys neturi būti nesusiję ar pertekliniai, palyginus su Sutartais tikslais.</p> <p>V. TEISINGAS IR TEISĖTAS TVARKYMAS</p> <p>5.1. Šios Duomenų apsaugos politikos Sutartais tikslais kiekviena Šalis užtikrina, kad ji tvarkys Bendruosius asmens duomenis remdamasi šiais Teisiniais pagrindais:</p> <p><i>tvarkymas yra būtinas teisėtiems duomenų valdytojo ar trečiosios šalies interesams, išskyrus tuos atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni (BDAR 6 str. 1 d. (f) punktas).</i></p>	<p><i>personal code, registered address, individual economic activity certificate number and VAT number are also applicable.</i></p> <p>4.2. The Shared Personal Data shall be limited to the Personal Data described in clause 4.1 of this Data Protection Policy.</p> <p>4.3. The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.</p> <p>V. FAIR AND LAWFUL PROCESSING</p> <p>5.1. For the Agreed Purposes under this Data Protection Policy, each Party shall ensure that it processes Shared Personal Data on the basis of the following Legal Ground:</p> <p><i>processing is necessary for the purposes of the legitimate interests pursued by the 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 (GDPR Art 6. 1 (f)).</i></p>	<p><i>регистрационный номер транспортного средства. Если клиент или поставщик является физическим лицом, личный код, адрес зарегистрированного места жительства, номер сертификата индивидуальной деятельности и код плательщика НДС также включены в Общие персональные данные.</i></p> <p>4.2. Общие персональные данные ограничиваются персональными данными, описанными в пункте 4.1 настоящей Политики защиты данных.</p> <p>4.3. Общие персональные данные не должны быть не связанными или чрезмерными по отношению к Согласованным целям.</p> <p>V. ПРАВИЛЬНАЯ И ЗАКОННАЯ ОБРАБОТКА</p> <p>5.1. В Согласованных целях настоящей Политики о защите данных каждая Сторона обеспечивает обработку Общих персональных данных на следующих Правовых основах:</p> <p><i>обработка необходима для законных интересов владельца или третьей стороны, за исключением тех случаев, когда такие интересы субъекта данных или основные права и свободы, в связи с которыми необходимо обеспечить защиту персональных данных, являются выше их (пункт (f) части 1 статьи 6 ОРЗД).</i></p>
--	--	---

5.2. Abi Šalys dėl Bendrųjų asmens duomenų užtikrina, kad jų pateikiami privatūs pranešimai būtų aiškūs ir kad Duomenų subjektams būtų suteikta pakankamai informacijos tam, kad jie galėtų suprasti, kokiais jų asmeniniais duomenimis Šalys dalijasi, aplinkybes, kuriomis jais bus dalijamasi, duomenų pasidalijimo tikslai ir arba tapatybė, su kuo duomenimis yra dalijamasi, arba organizacijos, kuri gaus asmens duomenis, prašymas (BDAR 14 straipsnis).

5.3. Abi Šalys įsipareigoja informuoti Duomenų subjektus apie tikslus, dėl kurių jos tvarkys savo valdomus asmens duomenis, taip pat suteiks Duomenų subjektui visą informaciją, kurią ji turi pateikti pagal BDAR ir savo taikomus įstatymus tam, kad Duomenų subjektas suprastų kaip jo asmeninius duomenis tvarkys Duomenų valdytojas.

VI. DUOMENŲ KOKYBĖ

6.1. Duomenų davėjas užtikrina, kad Bendrieji asmens duomenys būtų tikslūs.

6.2. Jei kuri nors Šalis sužino apie netikslius Bendruosius asmens duomenis, ji apie tai praneša

5.2. Both Parties shall, in respect of Shared Personal Data, ensure that their privacy notices are clear and provide sufficient information to Data Subjects in order for them to understand what of their Personal Data the Parties are sharing, the circumstances in which it will be shared, the purposes for the data sharing and either the identity with whom the data is shared or a description of the type of organization that will receive the Personal Data (GDPR Art 14).

5.3. Both Parties undertake to inform Data Subjects of the purposes for which it will process their Personal Data and provide all of the information that it must provide in accordance with GDPR and its own applicable laws, to ensure that the Data Subjects understand how their Personal Data will be processed by the Data Controller.

VI. DATA QUALITY

6.1. The Data Discloser shall ensure that Shared Personal Data is accurate.

6.2. Where either Party becomes aware of inaccuracies in Shared Personal Data, they will

5.2. В отношении Общих персональных данных обе Стороны гарантируют, что предъявляемые ими личные сообщения будут ясными и что Субъекты данных будут получать достаточную информацию, позволяющую им понимать, какими их персональными данными Стороны делятся, обстоятельства, при которых такие данные будут передаваться, цели обмена данными, а также описание личности, получающей персональные данные, либо организации, которая получит персональные данные (статья 14 ОРЗД).

5.3. Обе Стороны обязуются информировать Субъектов данных о целях, в связи с которыми они будут обрабатывать персональные данные, находящиеся в их управлении, а также предоставлять Субъекту данных всю информацию, которую она должна предоставить в соответствии с ОРЗД и применяемыми ею законами, чтобы Субъект данных понимал, как его персональные данные будут обрабатываться Владелец данных.

VI. КАЧЕСТВО ДАННЫХ

6.1. Поставщик данных обеспечивает точность Общих персональных данных.

6.2. Если какая-либо из Сторон узнает о неточных Общих персональных данных, она информирует

<p>kitai Šaliai.</p> <p>VII. DUOMENŲ SUBJEKTŲ TEISĖS</p> <p>7.1. Duomenų subjektai turi teisę gauti konkrečią informaciją apie jų asmens duomenų tvarkymą pateikiant Subjektų prieigos prašymą. Duomenų subjektai taip pat gali prašyti ištaisyti, ištrinti ar užblokuoti savo asmeninius duomenis.</p> <p>7.2. Šalys tvarko Subjekto prieigos prašymus, priimtus sprendimus ir visą informaciją, kuria buvo apsikeista. Įrašai turi apimti prašymo pateikti informaciją kopijas, išsamią informaciją apie prieinamus duomenis ir, jei reikia, visų su prašymu susijusių susitikimų, susirašinėjimų ar skambučių pastabas.</p> <p>7.3. Šalys susitaria, kad atsakomybė už Subjekto prieigos prašymo įvykdymą tenka Šaliai, gaunančiai Subjekto prieigos prašymą dėl tos Šalies turimų asmens duomenų.</p> <p>7.4. Šalys susitaria teikti pagrįstą ir greitą pagalbą (per 5 Darbo dienas nuo tokio pagalbos prašymo) tam, kad jos galėtų patenkinti Subjektų prieigos prašymus ir atsakyti į visus kitus duomenų subjektų klausimus ar skundus.</p>	<p>notify the other Party.</p> <p>VII. DATA SUBJECTS' RIGHTS</p> <p>7.1. Data Subjects have the right to obtain certain information about the processing of their Personal Data through a Subject Access Request. Data Subjects may also request rectification, erasure or blocking of their Personal Data.</p> <p>7.2. The Parties shall maintain a record of Subject Access Requests, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.</p> <p>7.3. The Parties agree that the responsibility for complying with a Subject Access Request falls to Party receiving the Subject Access Request in respect of the Personal Data held by that Party.</p> <p>7.4. The Parties agree to provide reasonable and prompt assistance (within 5 Business Days of such a request for assistance) as is necessary to each other to enable them to comply with Subject Access Requests and to respond to any other queries or complaints from Data Subjects.</p>	<p>об этом другую Сторону.</p> <p>VII. ПРАВА СУБЪЕКТОВ ДАННЫХ</p> <p>7.1. Субъекты данных имеют право получать конкретную информацию об обработке своих персональных данных, представляя запрос Субъектов на доступ. Субъекты данных могут также просить исправить, удалить или заблокировать свои персональные данные.</p> <p>7.2. Стороны обрабатывают запросы Субъектов на доступ, принимаемые решения и всю информацию, которой было обменено. Записи должны включать копии запроса на предоставление информации, подробную информацию о доступных данных и, при необходимости, все комментарии к встречам, переписке или звонкам, связанным с запросом.</p> <p>7.3. Стороны договариваются, что ответственность за выполнение запроса Субъекта на доступ лежит на Стороне, получающей запрос Субъекта на доступ относительно персональных данных, находящихся у этой Стороны.</p> <p>7.4. Стороны соглашаются предоставить разумную и быструю помощь (в течение 5 рабочих дней с момента подачи такой просьбы об оказании помощи), с тем, чтобы они могли удовлетворить запросы Субъектов на доступ и ответить на любые другие вопросы или жалобы субъектов данных.</p>
---	--	---

VIII. DUOMENŲ SAUGOJIMAS IR IŠTRYNIMAS

8.1. Duomenų gavėjas negali išsaugoti ar tvarkyti Bendrųjų asmens duomenų ilgiau, nei būtina Sutartiems tikslams įgyvendinti. Duomenų gavėjas užtikrina, kad visi Bendrieji asmens duomenys būtų grąžinti Duomenų davėjui arba sunaikinti tuomet, kai Bendrųjų asmens duomenų tvarkymas nebėra būtinas Sutartų tikslų įgyvendinimui.

8.2. Nepaisant 8.1 punkto, Šalys pratęsia Bendrųjų asmens duomenų saugojimo laikotarpį vadovaudamosi savo šalies taikomais teisės aktais ir/arba pramonės šakos duomenų saugojimo standartiniais reikalavimais.

IX. PERDAVIMAI

9.1. Duomenų gavėjas negali perduoti trečiajai šaliai Bendrųjų asmens duomenų be aiškaus rašytinio Duomenų davėjo sutikimo, išskyrus atvejus, kai trečioji šalis turi teisinį pagrindą reikalauti tokių asmens duomenų pagal BDAR ir Šalis yra įpareigota perduoti prašomus asmeninius duomenis.

9.2. Jeigu pagal 9.1 punktą buvo suteiktas aiškus raštiškas leidimas ar nurodymas, Duomenų gavėjas

VIII. DATA RETENTION AND DELETION

8.1. The Data Recipient shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes. The Data Recipient shall ensure that any Shared Personal Data are returned to the Data Discloser or destroyed once processing of the Shared Personal Data is no longer necessary for the Agreed Purposes it were originally shared for.

8.2. Notwithstanding clause 8.1, the Parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and/or industry.

IX. TRANSFERS

9.1. The Data Recipient shall not share the Shared Personal Data with a third party without the express written permission or order of the Data Discloser, unless the third party has a Legal Ground to require such Personal data in accordance with GDPR and the Party has an obligation to transfer the Personal Data requested.

9.2. Where express written permission or order has been granted further to clause 9.1, the Data

VIII. ХРАНЕНИЕ И УДАЛЕНИЕ ДАННЫХ

8.1. Получатель данных не может хранить или обрабатывать Общие персональные данные дольше, чем это необходимо для достижения Согласованных целей. Получатель данных обеспечивает, чтобы все Общие персональные данные были возвращены Поставщику данных или уничтожены, когда обработка Общих персональных данных больше не требуется для достижения Согласованных целей.

8.2. Несмотря на пункт 8.1, Стороны продлевают срок хранения Общих персональных данных в соответствии с законодательными и / или стандартными требованиями хранения данных, применимыми в их стране и/или отрасли.

IX. ПЕРЕДАЧА

9.1. Получатель данных не может передавать третьим лицам Общие персональные данные без четкого письменного согласия Поставщика данных, за исключением случаев, когда третье лицо имеет законные основания требовать такие персональные данные в соответствии с ОРЗД и Сторона обязана передать запрошенные персональные данные.

9.2. Если в соответствии с пунктом 9.1 было выдано четкое письменное разрешение или

<p>neatskleis ir neperduos Bendrųjų asmens duomenų už EEE ribų prieš tai neužtikrinęs, kad Bendrųjų asmens duomenų apsaugai bus suteikta tinkama ir lygiavertė apsauga.</p> <p>X. SAUGUMAS IR MOKYMAS</p> <p>10.1. Duomenų davėjas yra atsakingas už bet kokių Bendrųjų asmens duomenų, perduodamų Duomenų gavėjui, saugaus perdavimo užtikrinimą naudojant atitinkamus techninius metodus.</p> <p>10.2. Šalys susitaria įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti jų turimus Bendruosius asmens duomenis nuo neįgaloto ar neteisėto duomenų tvarkymo ir atsitiktinio praradimo, sunaikinimo, sugadinimo, pakeitimo ar atskleidimo, įskaitant, bet neapsiribojant:</p> <ul style="list-style-type: none"> • užtikrinti, kad IT įranga, įskaitant nešiojamą įrangą, būtų laikoma užrakinamose vietose tuomet, kai jos nėra prižiūrimos; • nepalikti nešiojamųjų įrenginių, kuriuose yra asmens duomenų, be priežiūros; • užtikrinti, kad darbuotojai naudotų 	<p>Recipient shall not disclose or transfer Shared Personal Data outside the EEA without ensuring that adequate and equivalent protections will be afforded to the Shared Personal Data.</p> <p>X. SECURITY AND TRAINING</p> <p>10.1. The Data Discloser shall be responsible for the security of transmission of any Shared Personal Data in transmission to the Data Recipient by using appropriate technical methods.</p> <p>10.2. The Parties agree to implement appropriate technical and organizational measures to protect the Shared Personal Data in their possession against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:</p> <ul style="list-style-type: none"> • Ensuring IT equipment, including portable equipment is kept in lockable areas when unattended; • not leaving portable equipment containing the Personal Data unattended; • ensuring that staff use appropriate secure 	<p>указание, Получатель данных не будет разглашать или передавать Общие персональные данные за пределами ЕЭЗ, предварительно не обеспечив адекватную и эквивалентную защиту для защиты Общих персональных данных.</p> <p>X. БЕЗОПАСНОСТЬ И ОБУЧЕНИЕ</p> <p>10.1. Поставщик данных несет ответственность за обеспечение безопасной передачи любых Общих персональных данных, передаваемых Получателю данных, с использованием соответствующих технических методов.</p> <p>10.2. Стороны договариваются принять соответствующие технические и организационные меры для защиты имеющихся у них Общих персональных данных от несанкционированной или незаконной обработки и случайной потери, уничтожения, повреждения, изменения или разглашения данных, включая, но не ограничиваясь:</p> <ul style="list-style-type: none"> • гарантировать, что ИТ-оборудование, включая портативное оборудование, хранится в запираемых местах тогда, когда оно не находится под присмотром; • не оставлять портативные устройства, содержащие персональные данные, без присмотра; • гарантировать, что сотрудники используют
--	---	--

<p>atitinkamus saugius slaptažodžius prisijungdami prie sistemų ar duomenų bazių, kuriose yra asmens duomenys;</p> <ul style="list-style-type: none"> • užtikrinti, kad reikiama IT įranga būtų apsaugota antivirusine programine įranga, užkardomis, slaptažodžiais ir tinkamais šifravimo algoritmais; • apriboti prieigą prie atitinkamų duomenų bazių ir sistemų tik tiems pareigūnams, darbuotojams ir subrangovams, kuriems reikia turėti prieigą prie asmens duomenų, ir užtikrinti, kad slaptažodžiai būtų reguliariai keičiami bei atnaujinami tam, kad būtų išvengta netinkamos prieigos tais atvejais, kai asmenys nebėra susiję su Šalimi; • reguliariai atlikti grėsmių vertinimą arba įsibrovimo bandymus sistemose; • užtikrinti, kad visi darbuotojai, tvarkantys asmeninius duomenis, būtų informuoti apie jų pareigas juos tvarkant; • leisti kitai Šaliai atlikti patikrinimus ir vertinimus, susijusius su taikomomis saugumo priemonėmis, arba pareikalavus pateikti įrodymus apie šias priemones. 	<p>passwords for logging into systems or databases containing the Personal Data;</p> <ul style="list-style-type: none"> • ensuring that necessary IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption algorithms; • limiting access to relevant databases and systems to those of its officers, staff agents and sub-contractors who need to have access to the Personal Data, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged by the Party; • conducting regular threat assessment or penetration testing on systems; • Ensuring all staff handling Personal Data have been made aware of their responsibilities with regards to handling of Personal Data; • Allowing for inspections and assessments to be undertaken by the other Party in respect of the security measures taken, or producing evidence of those measures if requested. 	<p>соответствующие безопасные пароли при входе в системы или базы данных, содержащие персональные данные;</p> <ul style="list-style-type: none"> • гарантировать, что необходимое ИТ-оборудование защищено антивирусным программным обеспечением, межсетевыми экранами, паролями и соответствующими алгоритмы шифрования; • ограничить доступ к соответствующим базам данных и системам только тем должностным лицам, сотрудникам и субподрядчикам, которым необходим доступ к персональным данным, и обеспечить регулярное изменение и обновление паролей для предотвращения несанкционированного доступа в тех случаях, когда лица больше не связаны со Стороной; • проводить систематическую оценку угроз или тестирование на проникновение в системы; • гарантировать, что все сотрудники, работающие с персональными данными, проинформированы о своих обязанностях по их обработке; • разрешить другой Стороне проводить проверки и оценки применяемых мер безопасности или предоставлять доказательства таких мер по запросу.
<p>XI. DUOMENŲ SAUGUMO PAŽEIDIMAI IR PRANEŠIMŲ TVARKA</p>	<p>XI. DATA SECURITY BREACHES AND REPORTING PROCEDURES</p>	<p>XI. НАРУШЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ И ПРОЦЕДУРА УВЕДОМЛЕНИЯ</p>

<p>11.1. Šalys yra griežtai įsipareigojusios kitai Šaliai pranešti apie bet kokius galimus ar faktinius Bendrųjų asmens duomenų praradimus kuo greičiau, bet ne vėliau kaip per 1 Darbo dieną po nustatyto galimo ar faktinio praradimo tam, kad Šalys galėtų nutarti kokių veiksmų, vadovaujantis nacionaliniais duomenų apsaugos įstatymais ir gairėmis, reikia imtis tam, kad problema būtų išspręsta.</p> <p>11.2. 11.1 punktą taip pat taikomas bet kokiems saugumo pažeidimams, kurie gali pakenkti Bendrųjų asmens duomenų saugumui.</p> <p>11.3. Šalys susitaria teikti viena kitai reikalingą pagalbą, tam, kad būtų galima greitai sutvarkyti bet kokį duomenų saugumo pažeidimą.</p> <p>XII. GINČŲ SU DUOMENŲ SUBJEKTAIS ARBA DUOMENŲ APSAUGOS INSTITUCIJA SPRENDIMAS</p> <p>12.1. Jei Duomenų subjektas arba Duomenų apsaugos institucija pradeda ginčą ar pareiškia pretenziją dėl Bendrųjų asmens duomenų tvarkymo prieš vieną ar abi Šalis, Šalys praneša viena kitai apie tai ir susitaria bendradarbiauti tam, kad tokie ginčai ir pretenzijos būtų kuo greičiau</p>	<p>11.1. The Parties are under a strict obligation to notify any potential or actual losses of the Shared Personal Data to the other Party as soon as possible and, in any event, within 1 Business Day of identification of any potential or actual loss to enable the Parties to consider what action is required in order to resolve the issue in accordance with the applicable national data protection laws and guidance.</p> <p>11.2. Clause 11.1 also applies to any breaches of security which may compromise the security of the Shared Personal Data.</p> <p>11.3. The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Data Security Breach in an expeditious and compliant manner.</p> <p>XII. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE DATA PROTECTION AUTHORITY</p> <p>12.1. In the event of a dispute or claim brought by a Data Subject or the Data Protection Authority concerning the processing of Shared Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling</p>	<p>11.1. Стороны имеют строгую обязанность информировать другую Сторону о любой потенциальной или фактической потере Общих персональных данных как можно скорее, но не позднее, чем в течении 1 Рабочего дня после выявления потенциальной или фактической потери для того, чтобы Стороны могли решить, какие действия необходимо предпринять в соответствии с национальными законами и руководящими принципами о защите данных для решения проблемы.</p> <p>11.2. Пункт 11.1 также применяется к любым нарушениям безопасности, которые могут нанести ущерб безопасности Общих персональных данных.</p> <p>11.3. Стороны соглашаются оказывать друг другу необходимую помощь, позволяющую оперативно устранять любые нарушения безопасности данных.</p> <p>XII. РЕШЕНИЕ СПОРОВ С СУБЪЕКТАМИ ДАННЫХ ИЛИ ОРГАНОМ ПО ЗАЩИТЕ ДАННЫХ</p> <p>12.1. Если Субъект данных или Орган по защите данных инициирует спор или предъявляет претензию в отношении обработки Общих персональных данных против одной или обеих Сторон, Стороны уведомляют друг друга об этом и договариваются сотрудничать, чтобы</p>
---	--	--

<p>išspręstos.</p> <p>XIII. GARANTIJOS</p> <p>13.1. Kiekviena Šalis garantuoja ir įsipareigoja:</p> <p>(a) tvarkyti Bendruosius asmens duomenis pagal BDAR.</p> <p>(b) per pagrįstą laiką atsakyti Duomenų apsaugos institucijoms į paklausimus dėl Bendrųjų asmens duomenų.</p> <p>(c) Atsakyti į Subjekto prieigos prašymą pagal šios Duomenų apsaugos politikos sąlygas ir BDAR.</p> <p>(d) imtis visų reikiamų priemonių tam, kad būtų užtikrinta, jog laikomasi 10 skyriuje nurodytų saugumo priemonių.</p> <p>13.2. Kiekviena Šalis kaip Duomenų davėjas garantuoja ir įsipareigoja užtikrinti, kad Bendrieji asmens duomenys būtų tikslūs.</p> <p>13.3. Kiekviena Šalis kaip Duomenų gavėjas garantuoja ir įsipareigoja neatskleisti ir neperduoti Bendrųjų asmens duomenų trečiosioms šalims nei Europos Ekonominėje Erdvėje (EEE), nei už jos ribų, išskyrus atvejus, kai ji laikosi 9.1 ir 9.2 punktuose nustatytų įsipareigojimų, arba kai tokią teisę suteikia galiojantys teisės aktai.</p>	<p>them amicably in a timely fashion.</p> <p>XIII. WARRANTIES</p> <p>13.1. Each Party warrants and undertakes that it will:</p> <p>(a) Process the Shared Personal Data in compliance with the GDPR.</p> <p>(b) Respond within a reasonable time to enquiries from the relevant Data Protection Authority in relation to the Shared Personal Data.</p> <p>(c) Respond to Subject Access Requests in accordance with the terms of this Data Protection Policy and in accordance with the GDPR.</p> <p>(d) Take all appropriate steps to ensure compliance with the security measures set out in <i>clause 10</i> above.</p> <p>13.2. Each Party as a Data Discloser warrants and undertakes that it will ensure that the Shared Personal Data are accurate.</p> <p>13.3. Each Party as a Data Recipient warrants and undertakes that it will not disclose or transfer Shared Personal Data to third parties either within or outside the European Economic Area (EEA) unless it complies with the obligations set out in clauses 9.1 and 9.2 above or such right is given by valid legal acts.</p>	<p>разрешить такие споры и претензии как можно скорее.</p> <p>XIII. ГАРАНТИИ</p> <p>13.1. Каждая Сторона гарантирует и обязуется:</p> <p>(a) обрабатывать Общие персональные данные в соответствии с ОРЗД.</p> <p>(b) в течение разумного периода времени отвечать органам по защите данных на запросы, касающиеся Общих персональных данных.</p> <p>(c) отвечать на запрос Субъекта на доступ в соответствии с положениями настоящей Политики защиты данных и ОРЗД.</p> <p>(d) принимать все необходимые меры для обеспечения соблюдения мер безопасности, указанных в разделе 10.</p> <p>13.2. Каждая Сторона, как Поставщик данных, гарантирует и обязуется обеспечить, чтобы Общие персональные данные были точными.</p> <p>13.3. Каждая Сторона, как Получатель данных, гарантирует и обязуется не разглашать и не передавать Общие персональные данные третьим сторонам ни на территории Европейского экономического пространства (ЕЭП), ни за его пределами, за исключением тех случаев, когда она выполняет обязательства,</p>
---	---	---

<p>XIV. BAIGIAMOSIOS NUOSTATOS</p> <p>14.1. Visi BFF darbuotojai yra atsakingi už šios Duomenų apsaugos politikos laikymąsi.</p> <p>14.2. Ši Duomenų apsaugos politika peržiūrima kasmet arba, jei reikia, dažniau tam, kad ji atspindėtų atitinkamus teisėkūros, reguliavimo ar organizacinius pokyčius.</p> <p>14.3. Norėdami gauti informacijos apie šią Duomenų apsaugos politiką arba duomenų apsaugą, prašome kreiptis elektroniniu paštu info@bff.lt.</p> <p>14.4. Ši Duomenų apsaugos politika patvirtinta ir įsigalioja 2019-05-15.</p>	<p>XIV. FINAL PROVISIONS</p> <p>14.1. All staff of BFF are responsible for adhering to this Data Protection Policy.</p> <p>14.2. This Data Protection Policy shall be reviewed annually, or more frequently if appropriate, to reflect relevant legislative, regulatory, or organizational developments.</p> <p>14.3. For information about this Data Protection Policy or data protection in general please contact via email info@bff.lt.</p> <p>14.4. This Data Protection Policy is approved and enters into force on 15-05-2019.</p>	<p>изложенные в пунктах 9.1 и 9.2, или когда такое право предоставляют действующие законодательные акты.</p> <p>XIV. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ</p> <p>14.1. Все сотрудники BFF несут ответственность за соблюдение настоящей Политики защиты данных.</p> <p>14.2. Настоящая Политика защиты данных пересматривается ежегодно или, при необходимости, чаще, чтобы она отражала соответствующие законодательные, регулирующие или организационные изменения.</p> <p>14.3. При желании получить информацию о настоящей Политике защиты данных или о защите данных, просим обращаться по эл.адресу info@bff.lt.</p> <p>14.4. Настоящая Политика защиты данных была утверждена и вступает в силу 15 мая 2019 года.</p>
--	---	--