# Table of Contents

**DIRECTO KLIENTŲ ASMENS DUOMENŲ TVARKYMO POLITIKA (GDPR)** ..... 1

# DIRECTO KLIENTŲ ASMENS DUOMENŲ TVARKYMO POLITIKA (GDPR)

| Versija – V1<br>Data – 2020-03-01 | Version – V1<br>Date – 1 March 2020 |
|---|---|

## ASMENS DUOMENŲ TVARKYMO POLITIKA (SĄLYGOS)

## ASMENS DUOMENŲ TVARKYMAS NAUDOJANTIS DIRECTO VERSLO VALDYMO SISTEMOMIS

Tuo atveju, kai Klientas arba Valdytojas (kaip jis apibrėžtas šiose Sąlygose žemiau) pradeda naudotis Produktu (kaip jis apibrėžtas šiose Sąlygose žemiau) yra taikomos šiose Sąlygose išdėstytos Asmens duomenų tvarkymo taisyklės. Šios Sąlygos sudaro naudojimosi Produktu sąlygų (atitinkamos Sutarties) neatskiriamą dalį. Jos yra skelbiamos http://wiki.directo.ee/lt/gdpr_priedas

### 1. Terminai ir apibrėžimai

1.1. Šiose Sąlygose, įskaitant preambulę bei priedus, didžiąja raide rašomų terminų reikšmės yra šios:

## POLICY (CONDITIONS) OF PERSONAL DATA PROCESSING

## PERSONAL DATA PROCESSING USING DIRECTO BUSINESS MANAGEMENT SYSTEMS

In case the Client or Data Controller (as defined in these Conditions below) starts using the product (as defined in these Conditions below), the rules of Personal Data processing, which are set out in these Conditions, shall be applicable. These Conditions is inseparable part of conditions of using the Product (of relevant agreement). They are published http://wiki.directo.ee/lt/gdpr_priedas

### 1. Terms and definitions

1.1. In these Conditions, including preamble thereof and annexes thereto, the terms in capital letters shall have the following meanings:

***Duomenų valdytojas arba Klientas arba Valdytojas*** reiškia Klientą, kuris viena arba drauge su kitais nustato Kliento duomenų (įskaitant Asmens duomenis) tvarkymo tikslus ir priemones ir kuris naudojasi Produktu.

***Duomenų tvarkytojas arba Paslaugų teikėjas arba Tvarkytojas arba DIRECTO*** reiškia uždarąją akcinę bendrovę „Directo“, juridinio asmens kodas 125943981, kurios registruota buveinė yra Juozo Balčikonio g. 9, Vilnius, kuri Duomenų valdytojo yra įgaliota tvarkyti Duomenis šiose Sąlygose nustatyta apimtimi.
***Asmens duomenys*** reiškia asmens duomenis, kaip jie yra apibrėžti Reglamente, ir kurie sudaro Kliento duomenų dalį.
***Duomenų subjektas*** reiškia fizinį asmenį, kurio Asmens duomenys sudaro Kliento duomenų dalį.
***Trečiasis asmuo*** reiškia juridinį ar fizinį asmenį, išskyrus Duomenų subjektą, Valdytoją, Tvarkytoją ir asmenis, kurie yra tiesiogiai Valdytojo ar Tvarkytojo įgalioti tvarkyti Asmens duomenis.
***TO Priemonės*** reiškia Tvarkytojo taikomas technines organizacines TO Priemones, kurios yra aiškiai įvardintos 1 priedėlyje.
***Paslaugų sutartis*** reiškia sutartį tarp Duomenų tvarkytojo ir Duomenų valdytojo dėl naudojimosi Produktu, nepriklausomai nuo jos sudarymo formos ar būdo.
***Produktas*** reiškia Sistemą ir Paslaugas, kaip jos apibrėžtos Paslaugų sutartyje.
***Reglamentas arba BDAR*** reiškia Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
***Sąlygos*** Reiškia šias duomenų tvarkymo sąlygas.
***Šalis*** reiškia Duomenų valdytoją arba Duomenų tvarkytoją.
***Šalys*** reiškia Duomenų valdytoją ir Duomenų tvarkytoją kartu.

1.2. Kitos šiose Sąlygose naudojamos sąvokos atitinka Reglamente pateiktas apibrėžtis, taip pat Paslaugų sutartyje nustatytas sąvokas.

***Data Controller or Client or Controller*** means Client which, either alone or in association with others, establishes the purposes and measures of Client’s data (including personal Data) processing and which is using the Product.

***Data Processor or Supplier or Processor or DIRECTO*** means Directo UAB, legal entity code 125943981, registered office at Juozo Balčikonio str. 9, Vilnius, which is authorized by Data Controller to process Data to the extent specified in these Conditions.
***Personal Data*** means the personal data as defined in the Regulation, which form part of the Client's data.
***Data Subject*** means a natural person whose Personal Data forms part of the Client's data.
***Third person*** means a legal entity or a natural person, other than the Data Subject, the Controller, the Processor and persons who are directly authorized by the Controller or Processor to process the Personal Data.
***TO Measures*** means the technical and organizational TO Measures applied by the Processor, which are expressly listed in Schedule 1.
***Service Contract*** means agreement between the Data Processor and the Data Controller on using the Product, irrespective of form and method of conclusion.
***Product*** means the System and the Services, as they defined in the Agreement.
***Regulation or GDPR*** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
***Conditions*** Means these Conditions of Personal Data Processing.
***Party*** means the Data Controller or the Data Processor.
***Parties*** means both the Data Controller and the Data Processor.

1.2. The other definitions used in these Conditions are in accordance with the definitions given in the Regulation as well as the terms set out in the Service Contract.

**2. Dalykas**

2.1. Atsižvelgiant į tai, kad Šalys yra sudarę Paslaugų sutartį, pagal kurią Paslaugų teikėjas teikia Klientui tam tikras paslaugas, dėl kurių Kliento duomenys ar tam tikros jų dalys gali būti prieinami Paslaugų sutartyje įvardintais tikslais Paslaugų teikėjui. Kliento duomenys ar jų dalis gali apimti ir Asmens duomenis, tad šios Sąlygos nustato Šalių teises ir pareigas Asmens duomenų tvarkymo klausimais, kaip to reikalauja BDAR.

2.2. Tvarkytojas atlieka Asmens duomenų tvarkymo veiksmus tik pagal Duomenų valdytojo pateiktus teisėtus nurodymus. Duomenų tvarkytojas nedelsdamas informuoja Duomenų valdytoją , jei, jo nuomone, nurodymas pažeidžia Reglamentą ar kitus taikytinus teisės aktus.

**3. Tvarkymo apimtis ir tikslas**

3.1. Asmens duomenų tvarkymas apima tik tuos tvarkymo veiksmus, kurie reikalingi paslaugoms pagal Paslaugų sutartį atlikti.

3.2. Duomenų subjektų, kurių Asmens duomenys gali būti įtraukti į Kliento duomenis, grupės gali būti: darbuotojai, Kliento klientų – juridinių asmenų darbuotojai, Kliento klientai – fiziniai asmenys.

3.3. Tvarkytojo tvarkymo veiksmų tikslas yra tinkamas paslaugų teikimui pagal Paslaugų sutartį.

3.4. Valdytojas patvirtina, kad Valdytojo vykdomas Asmens duomenų tvarkymas (įskaitant naudojimąsi Tvarkytojo paslaugomis) yra atliekamas vadovaujantis atitinkamų Asmens duomenų perdavimo metu galiojančių teisės aktų reikalavimų.

3.5. Pradėdamas naudotis ir tęsdamas naudojimąsi Produktu Valdytojas patvirtina, kad Asmens duomenų tvarkymo sąlygos, nustatytos šiose Sąlygose, jam yra tinkamos ir priimtinos siekiant užtikrinti tinkamą Asmens duomenų apsaugos lygį, atitinkantį jo vykdomą tvarkymą (jo pobūdį), su juo susijusias rizikas, Asmens duomenų rūšį, aprėptį, kontekstą ir tikslus.

**4. Terminas**

4.1. Tvarkytojo atliekamas Asmens duomenų tvarkymas gali tęstis tol, kol galioja Paslaugų sutartis. Jai pasibaigus Tvarkytojas nutraukia tvarkymo veiksmus per Paslaugų sutartyje nurodytą terminą.

**2. Subject matter**

2.1. Taking into account the fact that the Parties have concluded a Service Contract under which the Service Provider is providing certain services to the Client, as a result of which the Client's data or certain parts thereof may be made available to the Service Provider for the purposes specified in the Service Contract. The Client's data or parts thereof may include the Personal Data, these Conditions establish rights and obligations of the Parties as regards to the processing of the Personal Data as required by the GDPR.

2.2. The Data Processor carries out the Personal Data processing exclusively in line with the lawful instructions provided by the Data Controller. The Data Processor shall immediately inform the Controller if, in its opinion, the instructions are contrary to the Regulation or other applicable legislation.

**3. Scope and purpose of processing**

3.1. The processing of Personal Data covers only the processing operations which are required for provision of the service under the Service Contract.

3.2. The following groups of the Data Subjects whose Personal Data may be included in the Client's data: employees, employees of the Client's clients – legal entities, and clients of the Client – natural persons.

3.3. The purpose of the processing operations carried out by the Processor is to ensure proper provision of services under the Service Contract.

3.4. The Controller warrants that the Controller's processing of the Personal Data (including the use of the Processor's services) is carried out in accordance with the requirements of the legal acts applicable as of the time of transfer of the Personal Data.

3.5. By starting and continuing using the Product, the Data Controller confirms that conditions of the Personal Data processing established in these Conditions, are proper and acceptable for it to ensure an adequate level of the Personal Data protection, appropriate to the processing carried out by it (its nature), the risks involved, the nature, scope, context and purposes of the Personal Data.

**4. Time limit for Processing Operations**

4.1. Processing of the Personal Data carried out by the Processor may continue throughout the validity term of the Service Contract. Upon its expiration, the Processor terminates processing operations within the time limit specified in the Service Contract.

4.2. Tuo atveju, jei pagal taikomus teisės aktus Tvarkytojas turi atlikti šiose Sąlygose numatytus tvarkymo veiksmus net ir po Paslaugų sutarties pasibaigimo, aukščiau esančiame punkte nurodyta nuostata netaikoma ta apimtimi ir laikotarpiu, kuria Tvarkytojas turi vykdyti teisės aktų nustatytą pareigą.

**5. Konfidencialumas bei TO Priemonės**

5.1. Tvarkytojas atsako už tvarkomų Asmens duomenų konfidencialumą ir saugumą. Šis nuostata netaikoma tais atvejais, kai Tvarkytojas privalo atskleisti Asmens duomenis vykdydamas teisės aktuose nustatytas pareigas.

5.2. Tvarkytojas užtikrina, kad visi su Kliento duomenų tvarkymu susiję asmenys būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikoma atitinkama įstatymais nustatyta konfidencialumo prievolė.

5.3. Valdytojui atskirai nurodžius ir jei teisės aktai Tvarkytojo neįpareigoja kitaip, Tvarkytojas privalo saugiai ir neatkuriamai sunaikinti tvarkomus Asmens duomenis, jų kopijas ir jų sunaikinimo faktą patvirtinti Valdytojui.

5.4. Tvarkytojas atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei tvarkymo pobūdį, duomenų saugumui, vientisumui, nepakeičiamumui užtikrinti taiko tik tas TO Priemones, kurios įvardintos 1 priede.

5.5. Aukščiau nurodytos TO Priemonės nėra pritaikytos konkrečiai Valdytojui, o yra standartizuotos ir vienodai taikomos visoms tokio paties pobūdžio Tvarkytojo paslaugoms bei klientams. Valdytojas patvirtina, kad tokios TO Priemonėmis jam yra pakankamos ir tinkamos siekiant užtikrinti tinkamą Asmens duomenų apsaugos lygį, atitinkantį jo vykdomą tvarkymą (jo pobūdį), su juo susijusias rizikas, Asmens duomenų rūšį, aprėptį, kontekstą ir tikslus.

5.6. Tvarkytojas savo nuožiūra gali keisti / atnaujinti TO Priemones apie tai atskirai neinformuodamas Valdytojo. Toks keitimas ar atnaujinimas negali suteikti mažesnio apsaugos lygio, nei šių Sąlygų sudarymo (paskelbimo) metu suteikia TO Priemonės.

4.2. In the event that the Processor is required by the applicable legal acts to carry out the processing operations provided for in these Conditions even after the termination of the Service Contract, the provision referred to hereinabove shall not apply to the extent and for the period during which the Processor is required to comply with the statutory obligation.

**5. Confidentiality and TO Measures**

5.1. The Processor shall be responsible for maintaining the confidentiality and security of the Personal Data being processed. This provision does not apply in cases where the Processor is required to disclose Personal Data when complying with statutory obligations.

5.2. The Processor shall ensure that all the persons involved in the processing of the Client's data are bound by the obligation of confidentiality or subject to the applicable statutory obligation of confidentiality.

5.3. Upon separate Controller’s instruction and if the law does not impose any obligation to the contrary on the Processor, the Processor must securely and irreversibly destroy the Personal Data being processed as well as copies thereof and certify the fact of their destruction to the Controller.

5.4. The Processor, having regard to the level of advancement of technical capabilities, the implementation costs and the nature of the processing, shall apply, for the purpose of ensuring security, integrity, irreversibility of the data, only those TO Measures listed in Annex 1.

5.5. The said TO Measures are not specific to the Controller, but are standardized and applied equally to all the Processor's services of the same kind, as well as to clients. The Controller warrants that such TO Measures are sufficient and appropriate for it to ensure an adequate level of Personal Data protection, appropriate to the processing carried out by it (its nature), the risks involved, the nature, scope, context and purposes of the Personal Data.

5.6. The Processor may, at its discretion, modify / update the TO Measures without notifying the Controller individually. Such modification or updating may not result in a lower level of protection than provided by the TO Measures at the time of the conclusion of these Conditions (making them available).

5.7. Bet kokių techninių organizacinių TO Priemonių, kurių neapima TO Priemonės, įgyvendinimas pagal Valdytojo nurodymą gali būti atliekamas tik Valdytojo sąskaita.

### 6. Informacijos teikimas ir auditas

6.1. Tvarkytojas suteiks Valdytojui informaciją, būtiną įrodyti, kaip vykdomos Tvarkytojo prievolės pagal šias Sąlygas. Tokia informacija pateikiama per protingą Šalių suderintą laikotarpį.

6.2. Tvarkytojas suteiks galimybę ir sudarys sąlygas Valdytojui reguliariai (ne dažniau kaip vieną kartą per metus) Šalių suderintu laiku Valdytojo sąskaita patikrinti (atlikti auditą), kaip vykdomi šiose Sąlygose numatyti reikalavimai. Tokio patikrinimo (audito) apimtis ir sudaromos sąlygos bus tokios:

(a) atsakymai į Valdytojo raštu pateiktus klausimus; bei
(b) galimybė apklausti atitinkamą Tvarkytojo specialistą Tvarkytojo patalpose.

6.3. Valdytojas gali pasitelkti trečiąją šalį – nepriklausomą auditorių, atlikti tokiam patikrinimui su sąlyga, kad tokios šalies atžvilgiu Tvarkytojas neturi pagrįstų prieštaravimų.

6.4. Tvarkytojas nesuteiks nei Valdytojui, nei jo pasitelktai trečiajai šaliai prieigos prie Tvarkytojo sistemų ir/ar IT infrastruktūros.

6.5. Bet kokiai tokio audito metu Valdytojo sužinotai informacijai taikomos Paslaugų sutarties nuostatos (įskaitant dėl konfidencialumo, kt.).

6.6. Šalys susitaria, kad bet koks informacijos teikimas ir pagalba atliekant auditą negali trukdyti įprastinės Tvarkytojo veiklos bei sąlygoti nepagrįstų Tvarkytojo kaštų.

### 7. Pagalba Valdytojui

7.1. Atsižvelgiant į Tvarkytojo atliekamus Asmens duomenų tvarkymo veiksmus ir jų apimtį bei pobūdį, Tvarkytojas:

7.1.1. suteiks Valdytojui pagalbą, kad būtų įvykdyta Valdytojo prievolė atsakyti į prašymus pasinaudoti teisės aktuose numatytomis Duomenų subjekto teisėmis.

5.7. Implementation of any technical organizational TO Measures, not covered by the TO Measures, may be possible only at the expense of the Controller and according to the Controller's instruction.

### 6. Provision of information and auditing

6.1. The Processor will provide the Controller with the information necessary to demonstrate how the Processor's obligations under these Conditions are being performed. Such information shall be provided within a reasonable period agreed by the Parties.

6.2. The Processor will provide the opportunity and conditions for the Controller to regularly (no more often than once a year) inspect (perform an audit), at the time agreed between the Parties and at the Controller's expense, compliance with the requirements established in these Conditions. The scope and conditions for such an inspection (audit) will be as follows:

(a) answers to questions submitted by the Controller in writing; and
(b) the possibility of interviewing the appropriate Processor's officer at the Processor's premises.

6.3. The Controller may invoke a third party, an independent auditor, to perform such inspection, provided that the Processor does not have any reasonable objections with respect to such a party.

6.4. The Processor will not give the Controller, or the third party invoked thereby, access to the Processor’s systems and/or IT infrastructure.

6.5. The provisions of the Service Contract (including related to confidentiality, etc.) shall apply to the information obtained by the Controller in the course of such an audit.

6.6. The Parties agree that any provision of information and assistance in conducting audits may not interfere with the normal activities of the Processor and result in unreasonable costs for the Processor.

### 7. Assisting the Data Controller

7.1. Taking into account the Personal Data processing operations carried out by the Processor, the scope and nature thereof, the Processor:

7.1.1. will provide the Controller with assistance in fulfilling the Controller's obligation to respond to requests for access to the rights of the Data Subject as stipulated by the applicable legislations.

7.1.2. įsipareigoja bendradarbiauti su Valdytoju bei pateikti Valdytojo prašomą informaciją ir (ar) dokumentus, reikalingus priežiūros institucijai vykdant Valdytojo patikrinimą ir kuriuos Tvarkytojas gali pateikti.

7.1.3. gavęs bet kokį valstybinės valdžios institucijų prašymą ar reikalavimą, susijusį su Asmens duomenų tvarkymu, susijusį su Tvarkytojo veiksmais pagal šias Sąlygas, ar Asmens duomenimis, privalo apie tai nedelsiant informuoti Valdytoją raštu, nebent tai nebūtų leidžiama pagal taikomus teisės aktus.

7.1.4. Tvarkytojas įsipareigoja informuoti Valdytoją apie saugumo pažeidimą tik tuo atveju, jei toks pažeidimas yra susijęs su Kliento duomenimis. Tokiu atveju Tvarkytojas informuoja Valdytoją per protingą terminą, bet ne vėliau kaip per 24 valandas.

7.1.5. padeda Valdytojui įvykdyti jam tenkančias prievoles dėl poveikio duomenų apsaugai vertinimo ir išankstinių konsultacijų su priežiūros institucija, teikdamas konsultacijas ar kitokią pagalbą Valdytojui.

7.2. Šalys susitaria, kad bet kokia pagalba pagal šias Sąlygas,jei ji atskirai neįvardinta/neaptarta Paslaugų sutartyje kaip paslaugų pagal ją dalis ar viršija Paslaugų sutartyje numatytus Paslaugų teikėjo įsipareigojimus, bus apmokama pagal Paslaugos teikėjo tuo metu galiojančius paslaugų teikimo įkainius arba Šalių suderintus įkainius.

**8. Sub-tvarkytojai**

8.1. Tvarkytojas turi teisę pasitelkti kitus tvarkytojus (sub-tvarkytojus) be išankstinio Valdytojo sutikimo išlikdamas už juos visiškai atsakingu. Tokie pasitelkti duomenų tvarkytojai užtikrins šiose Sąlygose nustatytų Tvarkytojui taikomų reikalavimų įgyvendinimą tiek, kiek tai susiję su jiems patikėtais Asmens duomenų tvarkymo veiksmais.

7.1.2. undertakes to cooperate with the Controller and provide the information and/or the documents requested by the Controller, which are required by the supervisory authority in the course of the Controller's inspection and which may be provided by the Processor.

7.1.3. upon receipt of any request or demand from public authorities, relating to the processing of Personal Data, to the actions of the Processor under these Conditions or to the Personal Data, must immediately notify the Controller in writing, unless prescribed to the contrary by the applicable legislations.

7.1.4. The Processor undertakes to notify the Controller of a security breach only if such a breach is related to the Client's data. In this case, the Processor will notify the Controller within a reasonable time, but no later than within 24 hours.

7.1.5. Shall assist the Controller in fulfilling its obligations, regarding the data protection impact assessment and the prior consultations with the supervisory authority, by providing consultations or other assistance to the Controller.

7.2. The Parties agree that any assistance under these Conditions, if not individually named/covered by the Service Contract as part of the services thereunder or exceeding the obligations of the Service Provider provided for in the Service Contract, will be paid at the service rates currently applied by the Service Provider at the time or at the rates agreed upon by the Parties.

**8. Sub-processors**

8.1. The Processor has a right to subcontract other processors (sub-processors) without the prior consent of the Controller. The Processor remains fully liable for them. Such data processors invoked by the Processor will ensure the compliance with the requirements imposed by these Conditions to the Processor as far as the Personal Data processing operations entrusted to them are concerned.

**9. Atsakomybė**

9.1. Tvarkytojas už dėl Asmens duomenų tvarkymo sukeltą žalą atsako tik tuo atveju, jei jis nesilaikė Reglamente konkrečiai Tvarkytojams nustatytų prievolių arba jei jis veikė nepaisydamas teisėtų Valdytojo nurodymų arba juos pažeisdamas (įskaitant šių Sąlygų pažeidimus). Tokiu atveju Tvarkytojas atsako tik už tą žalą, kurią tiesiogiai sąlygojo Tvarkytojui nustatytų prievolių pažeidimai. Bet kokiu atveju Tvarkytojo atsakomybei bus taikomos Paslaugų sutartyje nustatytos atsakomybės taikymo sąlygos (įskaitant ribojimus).

9.2. Valdytojas yra atsakingas už Tvarkytojo patirtą žalą, atsiradusius Valdytojui pažeidus šias Sąlygas ir (ar) Lietuvos Respublikos teisės aktų reikalavimus.

**10. Sąlygų taikymas**

10.1. Šios Sąlygos pradedamos taikyti nuo tada, kada Valdytojas pradeda naudotis Produktu.

10.2. Šalies kylančios teisės ir (ar) pareigos Šalies negali būti perleistos tretiesiems asmenims be išankstinio kitos Šalies rašytinio pritarimo.

**11. Keitimas**

11.1. Šias Sąlygas Tvarkytojas gali keisti, pildyti ar kitaip modifikuoti vienašališkai apie bet kokį pakeitimą, papildymą ar modifikavimą informuodamas Valdytoją paskelbdamas tai tinklapyje (aukščiau pateiktoje nuorodoje).

11.2. Valdytojo naudojimasis Produktu po šių Sąlygų pakeitimo, papildymo ar kitokio modifikavimo reiškia, kad Valdytojas sutinka su tokiais pakeitimais, papildymais ar kitokiais modifikavimais.

**12. Baigiamosios nuostatos**

12.1. Šioms Sąlygoms taikoma Lietuvos Respublikos teisė.

12.2. Šioms Sąlygoms taikomos Paslaugų sutarties nuostatos tiek, kiek suderinama su šių Sąlygų nuostatomis.

12.3. Šalys susitaria, kad bet koks ginčas ir (ar) reikalavimas, kylantis iš šių Sąlygų ar susijęs su jomis, ar kylantis iš šių Sąlygų pažeidimo, nutraukimo ar negaliojimo, bus sprendžiamas Paslaugų sutartyje numatyta tvarka.

12.4. Visi pranešimai teikiami Paslaugų sutartyje numatytais būdais ir forma.

**9. Liability**

9.1. The Processor shall only be liable for the damages caused by the processing of Personal Data, if it has not complied with the obligations imposed specifically on the Processors by the Regulation or if it has acted contrary to or in violation of the lawful instructions of the Controller (including violations of these Conditions). In this case, the Processor shall only be liable for the direct damage caused by the violation of the obligations imposed on the Processor. In any case, the terms and conditions for the arising of liability of the Processor (including limitations) set forth in the Service Contract shall apply to the liability of the Processor.

9.2. The Controller shall be liable for the damage incurred by the Processor as a result of the breach of these Conditions and/or requirements of legal acts of the Republic of Lithuania committed by the Controller.

**10. Application of these Conditions**

10.1. These Conditions shall become applicable when the Controller starts using the Product.

10.2. The rights and/or obligations of a Party may not be assigned to third parties without prior written consent of the other Party.

**11. Changes**

11.1. These Conditions may be changed, supplemented or otherwise modified unilaterally by the Processor by informing the Controller about any change, supplementation or modification of these Conditions by publishing it at the website (as specified above in these Conditions).

11.2. Use of the Product by the Controller after changes, supplementations or modifications of these Conditions means that the Controller agrees with these changes, supplementations or other modifications.

**12. Miscellaneous**

12.1. The laws of the Republic of Lithuania apply to these Conditions.

12.2. The provisions of the Service Contract apply to these Conditions as much as compatible with the provisions of these Conditions.

12.3. The Parties agree that any dispute and/or claim arising out of these Conditions or in relation thereto, or arising out of the breach, termination or invalidity thereof will be resolved in a procedure set forth by the Service Contract.

12.4. All notices shall be provided in the manner and form established in the Service Contract.

| **1 priedėlis prie** | **Schedule 1 to** |
|---|---|

## ASMENS DUOMENŲ TVARKYMO SĄLYGŲ

### 1. Informacijos Saugumo Politika

1.1. DIRECTO turi plėtoti, administruoti ir išlaikyti tinkamą politiką, kad apsaugotų DIRECTO informacijos sistemas nuo nuostolių, žalos, neteisėto atskleidimo ar verslo sutrikimo, kuris apima fizinę apsaugą ir loginį informacijos sistemų suskaidymą įskaitant bet kuriuos Kliento duomenis ir Asmens duomenis pateiktus DIRECTO atlikti Paslaugas, kurios turi būti tvarkomos ar perduodamos.

### 2. Informacijos saugumo organizavimas

2.1. DIRECTO turi išlaikyti tinkamai kvalifikuotą personalą, su aiškiai apibrėžtais vaidmenimis ir atsakomybėmis savo informacijos saugumo organizavime, koordinuoti saugumo įgyvendinimą DIRECTO organizavime.

2.2. DIRECTO turi nustatyti reikalavimus informacijos jautrumui, apsaugai ir atskleidimui, ir peržiūrėti tokius reikalavimas kasmet.

2.3. DIRECTO turi efektyviai atskirti pareigas, vaidmenis ir atsakomybes, siekiant užkirsti kelią neteisėtam DIRECTO verslo kritinės informacijos lėšų naudojimui.

### 3. Turto valdymas

3.1. DIRECTO turi prižiūrėti procedūras, nustatyti, kontroliuoti ir išlaikyti pagrindinio DIRECTO turto nuosavybės ir apsaugos klasifikaciją ir Kliento duomenis ir Asmens duomenis esančius DIRECTO duomenų centro infrastruktūroje.

3.2. DIRECTO turi sukurti politiką apibrėžiančią priimtiną informacijos ir turto naudojimą, ir skelbti ją visiems tinkamiems DIRECTO turto ir informacijos naudotojams.

### 4. Žmogiškųjų išteklių saugumas

4.1. DIRECTO turi plėtoti ir įgyvendinti politiką ir procedūras, kurios užtikrina DIRECTO personalo ir 3-ųjų šalių tinkamumą atsižvelgiant į jų vaidmenis ir atsakomybę.

4.2. DIRECTO turi teikti tinkamą informuotumo ugdymą ir prieigą prie informacijos, kad DIRECTO naudotojai ir 3-osios šalys suprastų jų IT saugumo įsipareigojimus atižvelgiant į Kliento duomenis ir Asmens duomenis.

4.3. DIRECTO turi užtikrinti, kad visos būtinos procedūros yra atliekamos DIRECTO darbuotojams pasikeitus vaidmeniui, pasibaigus užduočiai, nutraukus darbą, sutartį, susitarimą.

## CONDITIONS OF PERSONAL DATA PROCESSING

### 1. Information Security Policy

1.1. DIRECTO shall develop, administer and maintain appropriate policies that protect DIRECTO’s information systems from loss, damage, unauthorized disclosure or disruption of business, which includes the physical protection and logical segmentation of information systems including any Customer Data and Personal Data, provided to DIRECTO to perform the Services, to be processed or transmitted.

### 2. Organization of Information Security

2.1. DIRECTO shall retain suitably qualified personnel, with clearly defined roles and responsibilities, within their information security organization, to coordinate the implementation of security for the DIRECTO organization.

2.2. DIRECTO shall determine requirements for sensitivity, protection and disclosure of information, and shall review such requirements annually.

2.3. DIRECTO shall effectively segregate duties, roles and responsibilities, to prevent unauthorized use of DIRECTO’s business critical information assets.

### 3. Asset Management

3.1. DIRECTO shall maintain procedures to identify, control and maintain the ownership and security classification of key DIRECTO assets and Customer Data and Personal Data held within the DIRECTO data center infrastructure.

3.2. DIRECTO shall create policies defining the acceptable use of information and assets, and promulgate these to all appropriate users of DIRECTO assets and information.

### 4. Human Resources Security

4.1. DIRECTO shall develop and implement policies and procedures that ensure the suitability of DIRECTO personnel and 3rd parties in relation to their roles and responsibilities.

4.2. DIRECTO shall provide appropriate awareness training and access to information, so that DIRECTO users and 3rd parties understand their IT Security responsibilities, in relation to Customer Data and Personal Data.

4.3. DIRECTO shall ensure that all necessary procedures are performed for DIRECTO employees upon change of role, end of engagement, termination of employment, contract or agreement.

**5. Fizinis ir aplinkos saugojimas**

5.1. DIRECTO turi įvesti efektyvią fizinę ir aplinkos kontrolę ir apsaugos priemones, siekiant išsaugoti DIRECTO informacinių sistemų ir Kliento duomenų / Asmens duomenų vientisumą ir prieinamumą.

5.2. DIRECTO turi teikti priemones, skirtas užtikrinti ir palaikyti pagalbinę informacijos ir informacijos sistemų infrastruktūrą, įskaitant bet kokios įrangos, susijusios su bet kokiu klientų įtraukimu, fizinę apsaugą.

**6. Ryšių ir operacijų saugumas**

6.1. DIRECTO turi apibrėžti tinkamą procesų ir procedūrų rinkinį efektyviam ryšių tinklo sistemų valdymui ir informacijos apdorojimo įrenginius, kuriuose yra Kliento duomenų ir Asmens duomenų įskaitant:

• Pakeitimų valdymas
• Trečiosios šalies paslaugų teikimo valdymas
• Sistemos planavimas ir pakeitimas
• Apsauga nuo kenksmingo kodo
• Reguliari informacijos ir programinės įrangos atsarginė kopija
• Tinklo saugumo valdymas įskaitant saugią nuotolinę prieigą, įsilaužimo aptikimą, tinklo protokolą ir perimetro apsaugą, priemones skirtas neleistinai veiklai aptikti, saugoti ir tvarkyti skaitmeninę mediją
• Keitimasis informacija taikant tarpusavyje suderintus metodus ir tinkamą šifravimo naudojimą
• Stebėsena ir audito registravimas
• Informacinių sistemų eksploatavimo nutraukimas
• Verslo kritinių sistemų ir komponentų pajėgumų valdymas
• Plėtros ir išankstinės gamybos aplinka
• Valdymo procedūros, tvarkant ir saugant laikmeną

**7. Prieigos kontrolė**

7.1. DIRECTO turi įdiegti procedūras, skirtas kontroliuoti prieigą prie informacijos sistemų ir Kliento duomenų/Asmens duomenų, įskaitant naudotojo identifikavimo ir prieigos kontrolės teikimą.

**5. Physical and Environmental Security**

5.1. DIRECTO shall institute effective physical and environmental controls and safeguards, to preserve the integrity and availability of DIRECTO information systems and the Customer Data/Personal Data contained thereon, whether they are in use at DIRECTO facilities, client sites or third-party locations.

5.2. DIRECTO shall provide measures for assuring and maintain the supporting infrastructure of information and information systems, including the physical protection of any equipment associated with any client engagement.

**6. Communications and Operations Security**

6.1. DIRECTO shall define a suitable set of processes and procedures for the effective management of the communications network systems and information processing facilities which contain Customer Data and Personal Data including:

• Change management
• Third Party service delivery management
• System planning and acceptance
• Protection against malicious code
• Regular backup of information and software
• Network security management including secure remote access, intrusion detection, network protocol and perimeter protection, countermeasures designed to detect unauthorized activity, storage and handling of digital media
• Exchange of information via mutually agreed methods and appropriate use of encryption
• Monitoring and audit logging
• Decommissioning of information systems
• Capacity management of business' critical systems and components
• Development and pre-production environments
• Procedures for management, handling and storage of media

**7. Access Control**

7.1. DIRECTO shall implement procedures designed to control access to information systems and Customer Data/Personal Data, including providing user identification and access controls.

7.2. DIRECTO turi siekti apriboti prieigą prie Kliento konfidencialios informacijos/Asmens duomenų įgaliotiems naudotojams, kurie reikalauja tokios prieigos remiantis verslo reikalavimais.

7.2. DIRECTO shall seek to limit access to Client's Confidential Information/Personal Data to authorized users, who require such access based upon business requirements.

**8. Informacinių sistemų įsigijimas, plėtra ir priežiūra**

8.1. Atsižvelgiant į Informacinių Sistemų specifikaciją, įsigijimą, plėtrą ir priežiūrą, įskaitant tuos, kuriuos įsigyja iš išorės tiekėjų ir pagamintų viduje, DIRECTO turi nustatyti būtinus konfidencialumo, vientisumo ir prieinamumo reikalavimus, ir peržiūrėti juos atsižvelgiant į ilgalaikį rizikos profilį per naudojimo laikotarpį.

**8. Information Systems Acquisition, Development & Maintenance**

8.1. With regard to the specification, acquisition, development and maintenance of Information Systems, including both those procured from external vendors and those internally produced, DIRECTO shall determine the necessary confidentiality, integrity and availability requirements, and continue to review these against an enduring risk profile through the usage lifecycle.

8.2. DIRECTO turi apibrėžti ir išlaikyti principus bet kokiems programinės įrangos plėtros gyvavimo ciklo atitinkamiems saugumo aspektams.

8.2. DIRECTO shall define and maintain principles for the appropriate security aspects of any software development lifecycle.

8.3. DIRECTO turi nustatyti ir įvertinti paskelbtas technines pažeidžiamas vietas ir grėsmes, ir įdiegti veiksmingą pažeidimų šalinimo ir pažeidžiamumo valdymo politiką, skirtą išvalyti DIRECTO informacijos sistemas kai būtina.

8.3. DIRECTO shall identify and evaluate notified technical vulnerabilities and threats, and shall deploy an effective patch and vulnerability management policy designed to remediate DIRECTO's Information Systems where necessary.

**9. Informacijos saugumo incidento valdymas**

9.1. DIRECTO turi parengti ir priimti incidento reagavimo planą ir programą, kuriose nurodomos procedūros ir nurodymai, kurių reikia laikytis incidento atveju, susijusios su DIRECTO kompiuterių infrastruktūros saugumu, dokumentais, nurodant būtinus žingsnius ir komunikacijos kanalus.

**9. Information Security Incident Management**

9.1. DIRECTO shall prepare and maintain an incident response plan and program containing procedures and directions to follow in the event of an incident related to the security of DIRECTO's computer infrastructure, documenting the necessary steps and channels of communication to be followed.

9.2. DIRECTO turi užtikrinti, kad nurodymuose būtų numatytos tinkamos procedūros pranešti mūsų Klientams, ir kitiems būtiniems suinteresuotiems asmenims, jei bet kuris saugumo incidentas sukėlė saugumo pažeidimą susijusį su Asmens duomenimis.

9.2. DIRECTO shall ensure that the directions incorporate appropriate procedures for notifying our Clients, and other necessary stakeholders, promptly if any security Incident is determined to have caused a security Breach involving Personal Data.

**10. Verslo tęstinumo valdymo informacijos saugumo aspektai**

10.1. DIRECTO turi vystyti ir palaikyti Verslo tęstinumo poveikio analizę ir Nelaimių atstatymo planus, skirtus palaikyti DIRECTO teikiamas paslaugas su minimaliu pertraukimu. Kiekvienas planas turi detalizuoti priemones, skirtas veikmingam paslaugų atkūrimui paremti, kuo greičiau atnaujinti operacijas po avarinės situacijos.

**10. Information security aspects of business continuity management**

10.1. DIRECTO shall develop and maintain Business Continuity impact analyses and Disaster Recovery plans, designed to maintain DIRECTO's delivery of the Services with minimal interruption. Each plan shall detail measures to support the effective restoration of services, to resume operations as soon as possible after an emergency.

10.2. DIRECTO turi periodiškai tikrinti įmonės labiausiai kritiškas verslo programas, pateikti garantiją, kad jos yra lengvai prieinamos paskelbtos nelaimės atveju.

10.2. DIRECTO shall conduct periodic testing on the firm's most critical business applications, to provide assurance that they are readily available in the event of a declared disaster.

10.3. DIRECTO turi užtikrinti, kad atsarginės kopijos yra pašalintos, remti DIRECTO sistemų atkūrimą nelaimės atveju.

**11. Laikymasis**

11.1. DIRECTO turi teikti garantiją, kad DIRECTO informacijos sistemos laikosi saugumo reikalavimų ir politikos, taikomų įstatymų ir norminių reikalavimų.

11.2. DIRECTO turi įgyvendinti tinkamą audito kontrolę, ribojančią prieigą prie įrankių ir sistemų, taip užkertant kelią netinkamam naudojimui ar kompromisui ir užtikrinti, kad auditai atitiktų DIRECTO visuotinę IT saugumo politiką, Ryšio kodą.

**12. Kriptografinė kontrolė**

12.1. DIRECTO turi plėtoti ir įgyvendinti kriptografinės kontrolės naudojimo politiką ilgalaikei apsaugai, konfidencialumo ir jautrios informacijos ir turto vientisumo išsaugojimui.

**13. Tiekėjo santykiai**

13.1. DIRECTO turi nustatyti ir palaikyti formalius susitarimus su trečiosiomis šalimis įtrauktomis į DIRECTO informacinių sistemų paslaugų teikimo valdymo sritį, prireikus įtraukti būtinus saugumo kontrolės, politikos ir paslaugų lygio susitarimus.

10.3. DIRECTO shall ensure that backups are taken offsite, to support the recoverability of DIRECTO systems in the event of a disaster.

**11. Compliance**

11.1. DIRECTO shall provide assurance that DIRECTO information systems comply with security requirements and policies, applicable laws and regulatory requirements.

11.2. DIRECTO shall implement appropriate audit controls, limiting access to tools and systems thus preventing misuse or compromise, and ensuring that audits comply with the DIRECTO Global IT Security Policy; Code of Connection.

**12. Cryptographic Controls**

12.1. DIRECTO shall develop and implement a policy on the use of cryptographic controls for the enduring protection, confidentiality and preservation of integrity of sensitive information and assets.

**13. Supplier Relationships**

13.1. DIRECTO shall establish and maintain formal agreements with third parties involved in the service delivery management of DIRECTO’s information systems, incorporating where appropriate the necessary security controls, policies and service level agreements.

From:
https://wiki.directo.ee/ - **Directo Help**

Permanent link:
**https://wiki.directo.ee/lt/gdpr_priedas?rev=1584953928**

Last update: **2020/03/23 10:58**