Priedas 4

DUOMENŲ TVARKYMO SUTARTIS

UAB „Ignitis grupės paslaugų centras“, pagal Lietuvos Respublikos įstatymus įsteigta ir veikianti uždaroji akcinė bendrovė, juridinio asmens kodas 303200016, PVM mokėtojo kodas LT 100008194913, registruotos buveinės adresas A. Juozapavičiaus g. 13, LT- 09311 Vilnius, Lietuvos Respublika, apie kurią duomenys kaupiami ir saugomi VĮ Registrų centras, atstovaujama (toliau – **Valdytojas**) ir

Starred B.V., pagal Olandijos įstatymus teisėtai įregistruota ir veikianti įmonė, juridinio asmens kodas 55736452, PVM mokėtojo kodas NL8518.39.885B01, registruotos buveinės adresas Singel 542, 1017 AZ, Amsterdamas, Olandija, atstovaujama (toliau – **Tvarkytojas**),

toliau Valdytojas ir Tvarkytojas kartu vadinami Šalimis, o kiekvienas atskirai – Šalimi, sudarė šią Duomenų tvarkymo sutartį (toliau – **Duomenų tvarkymo sutartis**):

1. Sutartyje naudojamos sąvokos

1.1. **Asmens duomenys** (arba **duomenys**) – bet kuri informacija, susijusi su fiziniu asmeniu (duomenų subjektu), kurio tapatybė yra žinoma arba gali būti nustatyta pasinaudojant šiais duomenimis (pavyzdžiui, vardas, pavardė, asmens kodas, gimimo data, kontaktinė informacija, skaitiklio duomenys, IP adresas ir kt.), vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.

1.2. **Duomenų tvarkymas** – bet kuris su asmens duomenimis atliekamas veiksmas – rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, paskelbimas, grupavimas, keitimas, jungimas, naudojimas, loginės ir (ar) aritmetinės operacijos, paieška, skleidimas, naikinimas, teikimas, kitoks veiksmas ar veiksmų rinkinys.

1.3. **Techninės ir organizacinės saugumo priemonės** – priemonės, kurios skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką.

1.4. **Asmens duomenų apsaugos teisės aktai** – teisės aktai, kurie reglamentuoja asmens duomenų apsaugą ir (ar) nustato reikalavimus duomenų saugumo priemonėms, įskaitant, tačiau neapsiribojant, 2016 m. balandžio 27 d. 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 (toliau - BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą, Lietuvos Respublikos elektroninių ryšių įstatymą bei kitus Europos Sąjungos ir Lietuvos Respublikos teisės aktus, įskaitant jų pakeitimus.

Annex 4

DATA PROCESSING AGREEMENT

UAB „Ignitis grupės paslaugų centras“, a private limited company established and operating in accordance with the laws of the Republic of Lithuania, legal entity code 303200016, VAT code LT 100008194913, registered office address A. Juozapavičiaus str. 13, LT- 09311 Vilnius, The Republic of Lithuania, about which data is collected and stored by (hereinafter referred to as the as the **Controller**), and

Starred B.V., legally registered and operating company according to the laws of the Netherlands, legal entity code 55736452, VAT payer code NL8518.39.885B01, registered office address Singel 542, 1017 AZ, Amsterdam, Netherlands, represented by (hereinafter referred to as the **Processor**),

the Controller and the Processor shall hereinafter be jointly referred to as Parties and each of them individually shall hereinafter be referred to as the Party, have concluded this Data Processing Agreement (hereinafter referred to as the **Data Processing Agreement**):

1 1. Concepts used in the Agreement

1.1. **Personal Data** (or the **Data**) shall mean any information related to a natural person (data subject), whose identity is known or could be determined by using this data (for instance, name, surname, personal number, date of birth, contact information, meter data, IP address, etc.), one or several characteristics of a physical, physiological, psychological, economic, cultural, or social nature typical to the person.

1.2. **Data Processing** shall mean any action involving the Personal Data: collection, recording, accumulation, storage, classification, publication, grouping, changing, combination, use, logic and (or) arithmetic operations, search, dissemination, destruction, provision, other action or a set of actions.

1.3. **Technical and Organizational Security Measures** shall mean measures designed for protection of the Personal Data against accidental or unlawful destruction, changing, disclosure as well as against any other unlawful processing. The aforementioned measures shall ensure such a level of security, which would correspond to the nature of the Personal Data subject to protection and the risks associated with processing thereof.

1.4. **Legislation on the Protection of Personal Data** shall mean legislation regulating protection of the Personal Data and/or establishing the requirements applicable to data security measures, including, but not limited to, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (hereinafter – the GDPR), Law on Legal Protection of Personal Data of the Republic of Lithuania, Law on Electronic Communications of the Republic of Lithuania as well as other legislations of the European Union and the Republic of Lithuania, including amendments thereof.

1.5. Other concepts used in the Data Processing Agreement shall be construed based on the definitions thereof given in the Legislation on the Protection of Personal Data.

1.5. Kitos Duomenų tvarkymo sutartyje naudojamos sąvokos suprantamos taip, kaip apibrėžtos Asmens duomenų apsaugos teisės aktuose.	**2. Basis and purpose for the provision of data**
2. Duomenų teikimo pagrindas ir tikslas	
2.1. Asmens duomenys yra renkami ir tvarkomi turint teisėtą tikslą – • jei Šalys sudariusios/sudaro sutartį dėl kito objekto ir Duomenų tvarkymo sutartis skirta tik užtikrinti tinkamą sudarytos/sudaromos sutarties vykdymą: siekiant užtikrinti tinkamą Tvarkytojo įsipareigojimų pagal Kandidatų patirties matavimo informacinės sistemos „Starred“ nuomos, palaikymo ir konsultavimo paslaugų sutartį (toliau – **Sutartis**) vykdymą.	2.1. Personal Data shall be collected and processed for a lawful purpose: • if the Parties have concluded/ conclude a contract for another object and the only purpose of the Data Processing Agreement is to ensure proper implementation of the contract concluded/ being concluded: in order to ensure proper implementation of the obligations assumed by the Processor under Subscription, Support and Professional services of cloud-based Candidate experience survey System contract (hereinafter referred to as the **Contract**) •
2.2. Šia Duomenų tvarkymo sutartimi Valdytojas paveda Tvarkytojui pagal Valdytojo nurodymus Duomenų tvarkymo sutarties 2.1 punkte nurodytu tikslu tvarkyti Asmens duomenis Duomenų tvarkymo sutartyje ir jos prieduose nurodytomis sąlygomis ir tvarka taip pat vadovaujantis Valdytojo nurodymais.	2.2. By this Data Processing Agreement, the Controller shall assign processing of the Personal Data for the purpose indicated in Paragraph 2.1 of the Data Processing Agreement to the Processor under the conditions and the procedure established in the Data Processing Agreement and the Annexes thereof following instructions given by the Controller.
3. Valdytojo įsipareigojimai	**3. Obligations of the Controller**
3.1. Valdytojas patvirtina, kad Priede Nr. 1 nurodytų Asmens duomenų tvarkymas, kurio pagrindas yra Šalių sudaryta Sutartis ir Duomenų tvarkymo sutartis, yra teisėtas bei atitinka asmens duomenų apsaugos teisės aktus.	3.1. The Controller does hereby confirm that processing of the Personal Data specified in Annex No 1 based on *the Contract and the Data Processing Agreement* concluded by the Parties is lawful and meets the Legislation on the Protection of Personal Data.
3.2. Valdytojas patvirtina, kad Duomenų tvarkymo sutartyje ir jos prieduose pateikė ir Sutarties bei Duomenų tvarkymo sutarties vykdymo laikotarpiu esant poreikiui papildomai pateiks reikiamus nurodymus Tvarkytojui dėl Valdytojo pavedimu atliekamo Asmens duomenų tvarkymo.	3.2. The Controller hereby confirms that it has provided in the Data Processing Agreement and in the annexes thereof, and, if will be required so, will additionally provide during the term of *the Contract and the Data Processing Agreement* necessary instructions to the Processor regarding the processing of Personal Data at the order of the Controller.
3.3. Valdytojas įsipareigoja, gavęs Tvarkytojo prašymą, nedelsiant, bet ne vėliau nei per 5 (darbo) dienas suteikti Tvarkytojui reikiamą informaciją, susijusią su šios Duomenų tvarkymo sutarties pagrindu tvarkomų asmens duomenų tvarkymu pagal šios Duomenų tvarkymo sutarties ir teisės aktų reikalavimus.	3.3. The Controller shall hereby undertake to provide the Processor immediately upon receipt of the Processor's request, but no later than within 5 (business) days, with the required information related to the processing of Personal Data being processed on the basis of this Data Processing Agreement in accordance with the requirements of this Data Processing Agreement and the legislation.
4. Tvarkytojo įsipareigojimai	**4. Obligations of the Processor**
4.1. Tvarkytojas, tvarkydamas Asmens duomenis, įsipareigoja laikytis asmens duomenų apsaugos teisės aktų, Duomenų tvarkymo sutarties ir jos priedų reikalavimų bei kitų Valdytojo pavedimų. Tvarkytojo Valdytojo pavedimu tvarkomi Asmens duomenys, jų tvarkymo tikslas, apimtis ir sąlygos nurodytos Duomenų tvarkymo sutarties Priede Nr. 1.	4.1. The Processor shall hereby undertake to follow the requirements established by the Legislation on the Protection of Personal Data, the Data Processing Agreement and the Annexes thereof as well as other assignments given by the Controller within the course of processing of Personal Data. Personal Data processed at the order given by the Controller, the purpose, scope, and conditions of processing thereof are specified in Annex No 1 to the Data Processing Agreement.
4.2. Tvarkytojas nedelsdamas informuoja duomenų valdytoją, jei Valdytojo nurodymai dėl duomenų tvarkymo pobūdžio, techninių ir organizacinių priemonių, Tvarkytojo nuomone, prieštarauja BDAR arba kitiems ES ar Lietuvos Respublikos teisės aktams, reglamentuojantiems duomenų apsaugą.	4.2. The Processor shall immediately notify the Controller if, in the opinion of the Processor, the instructions given by the Controller on the nature of data processing, technical and organizational measures are in conflict with the GDPR or other EU or Lithuanian legislation governing the data processing.
4.3. Tvarkytojas, tvarkydamas Asmens duomenis įsipareigoja, savo lėšomis užtikrinti tvarkomų Asmens duomenų apsaugą, įgyvendindamas tinkamas technines ir organizacines priemones,	4.3. The Processor shall hereby undertake to ensure at its own cost, in the course of Personal Data processing, protection of the Personal Data being processed through implementing proper technical and organizational measures designed for the protection of Personal Data being processed against accidental or unlawful destruction, corruption, changing, loss,

skirtas apsaugoti tvarkomus Asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, sugadinimo, pakeitimo, praradimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Šios priemonės turi užtikrinti reikiamą apsaugos lygį, kuris atitiktų tvarkomų Asmens duomenų pobūdį ir jų tvarkymo keliamą riziką bei teisės aktų reikalavimus.	disclosure as well as against any other unlawful processing. These measures should ensure the required level of protection, which would correspond to the nature of the Personal Data being processed and the risks associated with processing thereof as well as to the requirements of the legislation.
4.4. Tvarkytojas įsipareigoja užtikrinti Asmens duomenų konfidencialumą bei garantuoja, kad prieiga prie Asmens duomenų bus suteikta tik tiems Tvarkytojo darbuotojams ar jo įgaliotiems asmenims, kuriems to reikia jų funkcijoms vykdyti ir su Asmens duomenimis būtų atliekami tik tie veiksmai, kuriems atlikti Tvarkytojui suteiktos teisės, kiek to reikalauja tinkamas šios Duomenų tvarkymo sutarties vykdymas. Tvarkytojas įsipareigoja užtikrinti, kad Asmens duomenis tvarkyti įgalioti asmenys būtų tinkamai informuoti apie Asmens duomenų konfidencialumą, būtų tinkamai apmokyti, kaip vykdyti savo pareigas ir laikytis Asmens duomenų tvarkymui taikomų reikalavimų, numatytų Duomenų tvarkymo sutartyje, Valdytojo pavedimuose ir teisės aktuose bei būtų įsipareigoję užtikrinti Asmens duomenų konfidencialumą.	4.4. The Processor shall hereby undertake to ensure confidentiality of Personal Data and guarantees that access to Personal Data will be granted only to those employees of the Processor or to the persons authorized by the Processor who need it for the implementation of their functions, and that data would only be used for the actions for the performance of which the Processor has been granted rights, only those activities to which the Processor has been granted rights shall be performed with the Personal Data to the extent required for the proper fulfilment of this Data Processing Agreement. The Processor shall hereby undertake to make sure that the persons authorized to process Personal Data would be properly informed about confidentiality of Personal Data, would be properly trained on the implementation of their duties and following the requirements applicable to Personal Data processing provided for in the Data Processing Agreement, in the assignments given by the Controller and in the legislation, and that they are committed to maintaining the confidentiality of Personal Data.
4.5. Tvarkytojas įsipareigoja užtikrinti Saugumo reikalavimuose (Duomenų tvarkymo sutarties Priede Nr. 2) išdėstytas apsaugos priemones. Tvarkytojas įsipareigoja užtikrinti, kad šios apsaugos priemonės būtų įdiegtos prieš pradedant tvarkyti Asmens duomenis bei būtų nuolat peržiūrimos ir, reikalui esant, atnaujinamos, vykdoma jų stebėsena ir kontrolė. Gavęs Valdytojo prašymą, Tvarkytojas nedelsiant, bet ne vėliau nei per 10 (darbo) dienų, informuoja Valdytoją apie tai, kaip Tvarkytojas laikosi ir užtikrina, kad su Tvarkytoju susiję ir jo įgalioti asmenys laikytųsi šių Saugumo reikalavimų ir kokių priemonių Tvarkytojas ėmėsi siekiant užtikrinti Saugumo reikalavimų laikymąsi.	4.5. The Processor shall hereby undertake to ensure the protection measures specified in the Security Requirements (Annex No 2 and 3 to the Data Processing Agreement). The Processor shall hereby undertake to make sure that these protection measures are introduced prior to starting processing of Personal Data and are subject to continuous oversight, and are upgraded, whenever needed, monitored and controlled. Upon receipt of the Controller's request, the Processor shall immediately, but not later than within 10 (business) days notify the Controller on how the Processor complies and how it ensures that the persons related to and authorized by the Processor comply with these Security Requirements, and what steps the Processor has taken to ensure compliance with the Security Requirements.
4.6. Tvarkytojas įsipareigoja užtikrinti, kad visu Duomenų tvarkymo sutarties galiojimo laikotarpiu duomenys nebūtų tvarkomi (įskaitant perdavimą ar saugojimą) už Europos Sąjungos teritorijos ar Europos ekonominės erdvės ribų, išskyrus atvejus, kai buvo gautas išankstinis raštiškas Valdytojo sutikimas. Pasirašydamas Sutartį Valdytojas duoda sutikimą tvarkyti duomenis už ES ribų tik tiems dviems subprocesoriams („Mailchimp“, „Domo, Inc.“), kurie jau nurodyti 3 priede.	4.6. The Processor shall undertake to ensure that, throughout the duration of the Data Processing Agreement, data would not be processed (including transmission or retention thereof) outside the territory of the European Union or the European Economic Area, except with the prior written consent of the Controller. Signing the Agreement Controller gives consent to process data outside EU only for those two Subprocessors (Mailchimp, Domo,Inc.), which are already specified in Annex No. 3.
4.7. Tvarkytojas privalo turėti ir pateikti atnaujintus duomenų tvarkymo veiklos įrašus, įskaitant kiekvieno subjekto, veikiančio kaip subtvarkytojas, pavadinimą, kontaktinius duomenis, atstovą (įskaitant duomenų apsaugos pareigūną, jei paskirtas) ir buveinę.	4.7. The Processor must hold and provide the updated records of data processing activities, including the name, contact details, representative (including the Data Protection Officer, if appointed) and domicile of each entity acting as a sub-processor.
5. Tvarkytojo pagalba Duomenų valdytojui	**5. Processor‘s assistance to the Controller**
5.1. Tuo atveju, kai įgaliotos valstybės institucijos, pareigūnai ar bet kuris kitas asmuo, įskaitant duomenų subjektą, pateikė prašymą, skundą, pretenziją, kuris tiesiogiai susijęs su Duomenų tvarkymo sutarties ir Sutarties pagrindu tvarkomais duomenimis, Tvarkytojas nedelsiant, tačiau ne vėliau kaip per 3 (darbo) dienas Valdytojo kontaktiniu el. paštu turi perduoti tokį prašymą	5.1. In cases where the authorized public authorities, officers or any other person, including the data subject, has filed a request, complaint, claim directly related to the data processed under the Data Processing Agreement and the Contract, the Processor must immediately, but not later than within 3 (business) days, transfer such request to the Controller by sending it to the contact e-mail address of the Controller. If the request/complaint/claim are not

Valdytojui. Jeigu prašymas/skundas/pretenzija nėra susiję išimtinai su Bendrajame duomenų apsaugos reglamente numatytomis duomenų subjektų teisėmis, Valdytojas ir Tvarkytojas priklausomai nuo situacijos ir klausimo pobūdžio susitaria, kad rengia ir pateikia atsakymą duomenų subjektui.	related exclusively with the rights of the data subjects under the General Data Protection Regulation, the Controller and the Processor, depending on the situation and the nature of the matter, shall agree that they shall prepare and submit reply to the data subject.
5.2. Gavęs prašymą pasinaudoti Bendrajame duomenų apsaugos reglamente nustatytomis duomenų subjekto teisėmis Tvarkytojas 5.1. p. nustatytu terminu ir priemonėmis prašymą perduoda Valdytojui.	5.2. Upon receipt of request to exercise the rights of the data subject laid down in the General Data Protection Legislation, the Processor shall, within the deadline and using the measures specified in Clause, transfer the request to the Controller.
5.3. Šalys susitaria, kad Bendrajame duomenų apsaugos reglamente nustatytas duomenų subjektų teises įgyvendina ir atsakymą į subjekto prašymą teikia Valdytojas. Tvarkytojas, atsižvelgdamas į duomenų tvarkymo ir pateikto prašymo pobūdį padeda Valdytojui įgyvendinti duomenų subjektų teises ir atsakyti į pateiktus prašymus pateikdamas reikalingus dokumentus, informaciją, taikydamas tinkamas technines ir organizacines priemones prašymams įgyvendinti.	5.3. The Parties hereby agree that the rights of data subjects laid down in the General Data Protection Legislation shall be implemented and reply to the request of the subject shall be provided by the Controller. The Processor, having regard to the nature of data processing and the request submitted, shall help the Controller in implementing the rights of data subjects and replying to the requests submitted by providing necessary documents, information, using appropriate technical and organizational measures to fulfil the requests.
5.4. Tvarkytojas, atsižvelgdamas į duomenų tvarkymo pobūdį ir duomenų tvarkytojo statusą, padeda Valdytojui užtikrinti Bendrajame duomenų apsaugos reglamento 32-36 str. nustatytų prievolių laikymąsi: a) nedelsiant informuodamas Valdytoją apie įvykusius duomenų saugumo pažeidimus, kad Valdytojas galėtų įvykdyti jam nustatytą pareigą ne vėliau kaip per 72 val. informuoti Valstybinę duomenų apsaugos inspekciją apie pažeidimą; b) padėdamas komunikuoti su duomenų subjektais tais atvejais, kai įvykus duomenų saugumo pažeidimui dėl didelio pavojaus būtina informuoti duomenų subjektus; c) teikdamas konsultacijas ir padėdamas įvertinti galimas rizikas atliekant poveikio duomenų apsaugai vertinimą, tais atvejais, kai duomenų tvarkymas atliekamas pasitelkiant Tvarkytojo sukurtus įrankius, sistemas, procesus ir kai atlikti poveikio duomenų apsaugai vertinimą yra būtina vadovaujantis Asmens duomenų apsaugos teisės aktais; d) esant poreikiui pagal savo kompetenciją kartu su Valdytoju dalyvaudamas išankstinėse konsultacijose su Valstybine duomenų apsaugos inspekcija, kai tokios konsultacijos yra privalomos vadovaujantis Asmens duomenų apsaugos teisės aktais.	5.4. Given the nature of the data processing and the status of the processor, the Processor shall assist the Controller in ensuring compliance with the obligations laid down in Articles 32 through 36 of the General Data Protection Regulation: a) immediately notifying the Controller of any data security breach in order the Controller could fulfil its duty to notify the State Data Protection Inspectorate of the breach not later than within 72 hours; b) assisting in communication with data subjects in case where, following a data security breach, a high risk necessitates the notification of data subjects; c) providing advice and assistance in assessing potential risks in carrying out data protection impact assessment in cases where data processing is done using tools, systems and processes developed by the Controller, and where a data protection impact assessment is necessary under the legislation on the Protection of Personal Data; d) if necessary, within its competence, on participating together with the Controller in prior consultation with the State Data Protection Inspectorate, where such consultation is mandatory in accordance with the legislation on the Protection of Personal Data.
5.5. Tvarkytojas įsipareigoja neatlygintinai pateikti Valdytojui visą informaciją, būtiną siekiant įrodyti, kad vykdomos visos Duomenų tvarkymo sutartyje ir teisės aktuose numatytos prievolės.	5.5. The Processor shall undertake to provide the Controller free of charge with all information that is necessary for proving that all obligations provided for in the Data Processing Agreement and in the legal acts are being fulfilled.
6. Pranešimas apie duomenų saugumo pažeidimą	**6. Notice on data security breach**
6.1. Jei įvyksta arba įtariama, kad įvyko duomenų saugumo pažeidimas arba Tvarkytojo atžvilgiu vykdomi bet kokie kiti Valstybinės duomenų apsaugos inspekcijos procesiniai veiksmai, susiję su Asmens duomenų, tvarkomų pagal Duomenų tvarkymo sutartį ir (arba) Sutartį, tvarkymu, Tvarkytojas nedelsdamas, tačiau bet kuriuo atveju ne vėliau kaip per 24 (dvidešimt keturias) valandas nuo saugumo incidento nustatymo neatlygintinai raštu informuoja apie tai Valdytoją.	6.1. If data security breach occurs or it is suspected to having occurred, or any other procedural actions of the State Data Protection Inspectorate related to the processing of Personal Data processed under the Data Processing Agreement and/or the Contract are being carried out the Processor shall immediately, but in any case not later than within 24 (twenty-four) hours following the identification of the security incident, notify the Controller in writing thereof.
6.2. Tvarkytojas pateikia Valdytojui Pranešimą su visa informacija, kuri pagal Asmens duomenų apsaugos teisės aktus yra reikalinga	6.2. The Processor shall submit to the Controller a Notice 1.1 containing all information which, under the legislation on the Protection of Personal Data, is necessary for the Controller to be able to properly fulfil its obligation to notify the State Data Protection

Valdytojui, kad jis galėtų tinkamai įvykdyti pareigą pranešti Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams bei pašalinti ir sumažinti duomenų saugumo pažeidimo padarinius.

6.3. Tvarkytojas privalo skubiai imtis priemonių užkirsti kelią tolesnei žalai dėl įvykusio duomenų saugumo pažeidimo, taip pat sumažinti tokio pažeidimo padarinius.

6.4. Tvarkytojas gavęs rekomendacijas ir/ar nurodymus iš Valdytojo dėl duomenų saugumo pažeidimo privalo nedelsiant juos vykdyti.

6.5. Tvarkytojas privalo registruoti visus Duomenų tvarkymo sutarties ir Sutarties pagrindu tvarkomų Asmens duomenų saugumo pažeidimus, įskaitant su pažeidimu susijusius faktus, jų padarinius ir atliktus taisomuosius veiksmus.

7. Asmens duomenų subtvarkymas

7.1. Valdytojas neprieštarauja, kad sutarties vykdymui Tvarkytojas pasitelktų subtvarkytojus.

7.2. Prieš pasitelkdamas naują arba pakeisdamas esamą subtvarkytoją, Tvarkytojas iš anksto apie tai raštu (elektroniniu paštu) informuos Valdytoją, pateikdamas subtvarkytojo rekvizitus ir kitą informaciją susijusią su asmens duomenų tvarkymo veikla.

7.3. Valdytojas turi teisę motyvuodamas ir tik dėl svarbių priežasčių (pvz., dėl to, jog kyla reali grėsmė tvarkomų asmens duomenų saugumui) nesutikti su naujo Subtvarkytojo pasitelkimu ir apie tai informuoti Tvarkytoją per 5 (penkias) darbo dienas nuo Tvarkytojo pranešimo gavimo dienos. Jei Valdytojas prieštarauja dėl Asmens duomenų perdavimo subtvarkytojui, Tvarkytojas privalo toliau vykdyti savo įsipareigojimus pagal Duomenų tvarkymo sutartį be subtvarkytojo pasitelkimo.

7.4. Tvarkytojas yra atsakingas už tai, kad sutartyse su subtvarkytojais būtų numatytos ne mažesnės nei šioje Duomenų tvarkymo sutartyje nurodytos duomenų apsaugos priemonės.

7.5. Valdytojas norėdamas užtikrinti, kad tarp Tvarkytojo ir subtvarkytojo pasirašytoje sutartyje būtų nustatyti tokie patys reikalavimai, kokie taikomi ir Tvarkytojui, turi teisę pareikalauti su subtvarkytoju pasirašytos duomenų tvarkymo sutarties ir/arba jos pakeitimų kopiją.Tvarkytojas privalo pateikti tik tokią sutarties ar jos dalies kopiją, kurioje aptarti tik duomenų tvarkymo klausimai.

7.6. Tvarkytojas privalo užtikrinti, kad jo pasitelkti subtvarkytojai duomenis tvarkytų pagal visas atitinkamas duomenų tvarkymo instrukcijas ir tik tokiu mastu bei tokiu būdu, kiek tai būtina atitinkamų paslaugų teikimui. Tvarkytojas privalo įpareigoti subtvarkytojus, kad pasitelkiant kitus pagalbinius tvarkytojus, sutartyse dėl duomenų tvarkymo būtų nurodytos ne mažesnės asmens duomenų apsaugos priemones, nei nurodyta šioje sutartyje. Tvarkytojas neinformuoja Valdytojo apie subtvarkytojų pasitelktus pagalbinius tvarkytojus.

7.7. Tvarkytojas yra atsakingas už jo pasitelktų subtvarkytojų, įskaitant ir subtvarkytojų pasitelktų asmenų ar darbuotojų, veiksmus ir neveikimą, sąlygojusį asmens duomenų tvarkymą reglamentuojančių teisės aktų reikalavimų nesilaikymą.

Inspectorate and data subjects, and to eliminate and minimize the consequences of data security breach.

6.3. The Processor must take urgent actions to prevent further damage as a result of the data security breach and to minimize the consequences of such breach.

6.4. Upon receipt of recommendations and/or instructions from the Controller in connection with the data security breach, the Processor must immediately implement them.

6.5. The Processor shall register all security violations of the Personal Data being processed on the basis of this Data Processing Agreement and the Contract, including the facts related to the violation, the consequences thereof and the implemented corrective actions.

7. Sub-processing of Personal Data

7.1. The Controller does not object to engagement of sub-processors by the Processor for performance of the contract/agreement.

7.2. Before using a new or replacing the existing sub-processor, the Processor will notify the Controller in advance thereof in writing (by e-mail) by providing details of the sub-processor and other information relating to the personal data processing activities.

7.3. The Controller shall have the right, by giving the arguments and for good reasons only (for example, because of a real threat to the security of the personal data processed), object to the engagement of a new sub-processor, and notify the Processor thereof within 5 (business) days of the date of receipt of the Processor's notice. If the Controller objects to the transfer of Personal Data to the Sub-Processor, the Controller must continue to fulfil its obligations under the Data Processing Agreement without suing the Sub-Processor.

7.4. It is the responsibility of the Processor to ensure that contracts with sub-processors would include data protection measures that are not less than those specified in this Data Processing Agreement.

7.5. For the purpose of ensuring that the contract signed between the Processor and the Sub-processor sets out the same requirements as those applicable to the Processor, the Controller shall have the right to request a copy of the data processing contract signed with the Sub-processor and/or of its amendments. The Processor must only provide such copy of the contract or of its part which only deals with data processing issues.

7.6. It is the responsibility of the Processor to ensure that the sub-processors that it engages would process data in accordance with all relevant data processing instructions and only to the extent and in the manner necessary for the provision of the relevant services. The Processor must oblige the sub-processors that, in invoking other auxiliary processors, the contracts for data processing would include the personal data protection measures that are not less than those specified in this Agreement. The Processor shall not notify the Controller on the auxiliary processors engaged by the sub-processors.

7.7. The Processor shall be responsible for the actions and omission of the sub-processors engaged by it, including persons or employees engaged by the sub-processors, resulting in non-compliance with the requirements of the legislation governing the Processing of Personal Data.

7.8. Tvarkytojo pasitelkti ir Valdytojui priimtini subtvarkytojai nurodyti šio Susitarimo Priede Nr. 3.	7.8. The Subprocessors engaged by the Processor and acceptable to the Controller are specified in Annex No 3 to this Agreement.
8. Auditas	**8. Audit**
8.1. Valdytojas turi teisę, pateikęs išankstinį pranešimą, nepertraukdamas Tvarkytojo veiklos ir neatlygintinai, Tvarkytojo buveinės patalpose atlikti Tvarkytojo patikrinimus ir (ar) auditą įprastomis darbo valandomis. Tokį auditą ar patikrinimus gali atlikti Valdytojo darbuotojai arba kiti Valdytojo įgalioti tinkamais konfidencialumo įsipareigojimais saistomi asmenys. 8.2. Tvarkytojas įsipareigoja suteikti visą reikalingą informaciją, dokumentus ir suteikti prieigas prie Tvarkytojo valdomų įrenginių, kiek tai reikalinga duomenų tvarkymo auditui atlikti ir taikomoms techninėms bei organizacinėms priemonėms įvertinti, nepažeidžiant Tvarkytojo komercinių paslapčių. 8.3. Šalys susitaria, kad audito ar patikrinimų išlaidas, patirtas Valdytojo, apmoka pats Valdytojas. Tačiau jeigu audito ar patikrinimų metu nustatomas Tvarkytojo, jo įgaliotų ar su juo susijusių asmenų (įskaitant jo pasitelktus subtvarkytojus) įsipareigojimų nevykdymas ar netinkamas vykdymas, teisės aktų ir (ar) Valdytojo nurodymų nesilaikymas, Tvarkytojas privalo padengti Valdytojo audito ir (ar) patikrinimų išlaidas bei nedelsiant ištaisyti nustatytus neatitikimus.	8.1. The Controller shall have the right, after having submitted a prior notice, without interrupting the activities of the Controller and free of charge, to conduct inspections and/or audit of the Processor in the premises of the Processor's office during normal business hours. Such audit or inspections may be carried out by the employees of the Controller or by other persons authorized by the Controller who are bound by appropriate confidentiality obligations. 8.2. The Processor shall undertake to provide all necessary information, documents and access to the facilities operated by the Processor to the extent necessary to carry out the audit of the data processing and to evaluate the technical and organizational measures taken, without prejudice to the trade secrets of the Controller. 8.3. The Parties hereby agree that the costs of audit or inspections incurred by the Controller shall be borne by the Controller itself. However, if the audit or inspection reveals failure to fulfil or improper fulfilment of obligations, failure to comply with the legal acts and/or instructions of the Controller by the Processor, by the persons authorized by or related to it (including the sub-processors engaged by it), the Processor must reimburse the Controller for the costs of the audit and/or inspections, and must immediately remedy any identified inconsistencies.
9. Asmens duomenų tvarkymo pabaiga	**9. End of the processing of Personal Data**
9.1. Kai Asmens duomenų tvarkymas tampa nebūtinu Tvarkytojo įsipareigojimams pagal Sutartį vykdymui arba kai pasibaigia Sutarties galiojimo terminas ar Sutartis yra nutraukiama, Tvarkytojas privalo nedelsiant, bet ne vėliau nei Valdytojo nurodytu terminu, netaikydamas jokio papildomo užmokesčio, pateikti (grąžinti) Valdytojui visus Asmens duomenis bei visus kitus duomenis, kuriuos Tvarkytojas tvarkė Valdytojo pavedimu vykdydamas Sutartį, taip pat visas turimas šių duomenų kopijas. Asmens duomenys, kiti duomenys ir jų kopijos pateikiami (grąžinami) Valdytojo nurodytu būdu ir forma. Jeigu Asmens duomenų, kitų duomenų bei jų kopijų pateikti (grąžinti) neįmanoma arba jeigu tai nurodo Valdytojas, Tvarkytojas privalo nedelsiant sunaikinti Asmens duomenis, kitus duomenis ir jų kopijas bei raštu pateikti Valdytojui patvirtinimą apie duomenų ir jų kopijų sunaikinimą.	9.1. When processing of Personal Data is no longer necessary for fulfilment of the Processor's obligations under the Agreement or when the Agreement expires or is terminated, the Processor must immediately, but not later than the deadline specified by the Controller, without imposing any extra fee, submit (return) to the Controller all Personal Data and any other data processed by the Processor at the order of the Controller in the execution of the Agreement, as well as any available copies of such data. Personal data, other data and copies thereof shall be submitted (returned) in the manner and form specified by the Controller. If it is impossible to submit (return) the Personal Data, other data, and copies thereof, or if instructed so by the Controller, the Processor must immediately destroy Personal Data, other data, and copies thereof, and provide the Controller a written confirmation of the destruction of data and copies thereof.
10. Atsakomybė	**10. Liability**
10.1. Tvarkytojas yra atsakingas už visas ir bet kokias sąnaudas, išlaidas, kompensacijas, žalą ir nuostolius, kuriuos asmens duomenų subjektams, Valdytojui, Valdytojo klientui, bendradarbiavimo partneriui ar trečiajai šaliai padaro Tvarkytojas, jo darbuotojas arba subvarkytojas netinkamai vykdydami ir (ar) pažeisdami Duomenų tvarkymo sutartį, Sutartį, Valdytojo nurodymus ir (ar) asmens duomenų apsaugos teisės aktus. 10.2. Tvarkytojas įsipareigoja atlyginti Valdytojo visus tiesioginius nuostolius, įskaitant, bet neapsiribojant nuostoliais, susijusiais su valstybės institucijų paskirtomis baudomis.	10.1. The Processor shall be liable for all and any expenses, costs, compensations, damages, and losses caused to the subjects of Personal Data, the Controller, the Controller's client, cooperation partner, or the third party by the Processor, its employee or sub-processor as a result of inadequate implementation and/or violation of the Data Processing Agreement, the Contract, the Controller's instructions, and/or the Legislation on the Protection of Personal Data. 10.2. The Processor shall hereby undertake to reimburse the Controller for all direct losses, including, but not limited

10.3. Tvarkytojas pilna apimtimi atsako už savo darbuotojų veiksmus ir Priede Nr. 2 išdėstytų Saugumo reikalavimų laikymąsi.	to, losses related to fines imposed by the public authorities. 10.3. The Processor shall be fully liable for the actions of its employees and compliance with the Security Requirements specified in Annex No 2 and 3. 1.2
11. Kitos sąlygos	**11. Other terms and conditions**
11.1. Šalys susitaria laikyti šią Duomenų tvarkymo sutartį ir visą jos pagrindu viena kitai perduodamą informaciją paslaptyje neterminuotai, neatsižvelgiant į tai, ar ta informacija pateikiama žodžiu ar raštu. Šalys susitaria neatskleisti konfidencialios informacijos jokiai trečiai šaliai be išankstinio raštiško ją pateikusios Šalies sutikimo, išskyrus atvejus, kai tokia informacija turi būti atskleista tinkamam šios sutarties vykdymui, teisės, finansų ar kitos srities specialistui/patarėjui, ar paskolos davėjui. Asmuo, kuriam Šalis atskleidžia konfidencialią informaciją, turi prisiimti konfidencialumo įsipareigojimus pagal šio punkto nuostatą ir naudoti tokią informaciją tik tam tikslui, kuriam ji buvo suteikta. Šio straipsnio nuostatos netaikomos informacijai, kuri yra ar tampa prieinama viešai arba gauta atskleidus ar turi būti atskleista pagal teisės aktų reikalavimus. Šalis, pažeidusi šioje sutartyje numatytus įsipareigojimus – saugoti konfidencialią informaciją ir jos neatskleisti, privalo atlyginti kitai Šaliai šios Sutarties pažeidimu padarytus nuostolius bei imtis visų protingų veiksmų, kad per trumpiausią laikotarpį ištaisytų tokio atskleidimo pasekmes. Šis sutarties punktas galioja ir po jos nutraukimo (neterminuotai).	11.1. The Parties hereby agree to keep confidential this Data Processing Agreement and all information communicated to each other on its basis for an indefinite period, regardless of whether that information is provided orally or in writing. The Parties hereby agree not to disclose confidential information to any third party without the prior written consent of the Party having provided it, unless such information must be disclosed for the proper performance of this Agreement, to a legal, financial or other professional/advisor or lender. The person to whom the Party discloses confidential information must assume the obligation of confidentiality under this clause, and use such information only for the purpose for which it was provided. The provisions of this Article shall not apply to information which is or becomes publicly available, or has been or is to be disclosed in accordance with legal requirements. The Party in breach of its obligations under this Agreement to protect confidential information and not disclose it, must reimburse the other Party for losses resulting from the violation of this Agreement, and must take all reasonable steps to remedy the consequences of such disclosure within the shortest possible period of time. This clause of the Agreement shall continue to apply after its termination (for an indefinite period of time).
11.2. Visi pranešimai pagal Duomenų tvarkymo sutartį turi būti atliekami raštu ir yra laikomi tinkamai gautais: (i) jei praėjo 5 (penkios) darbo dienos po jo išsiuntimo registruotu laišku Šalies buveinės adresu, (ii) įteikiant pasirašytinai – tą dieną, kai gavėjas pasirašo, kad gavo jam pateiktą dokumentą, (iii) siunčiant elektroniniu paštu Šalių Priede Nr. 1 nurodytiems kontaktiniams asmenims – tą pačią siuntimo dieną.	11.2. All communications under the Data Processing Agreement must be made in writing and shall be deemed to have been properly received: (i) if 5 (business) days have passed following mailing thereof via recorded mail to the address of the Party's registered office, (ii) in case of serving against signature: on the day when the recipient affixes his/ her signature confirming receipt of the document submitted to him/ her, (iii) in case of e-mailing to the e-mail addresses of the Parties to the contact persons specified in Annex No 1: on the same day of e-mailing thereof.
11.3. Šalių teisiniams santykiams pagal šią Duomenų tvarkymo sutartį yra taikomi asmens duomenų apsaugos teisės aktai, taip pat tiesiogiai taikomus ES teisės aktus.	11.3. The legal relations of the Parties under this Data Processing Agreement shall be subject to the Legislation on the Protection of Personal Data, applicable EU legislation.
11.4. Visi dėl Duomenų tvarkymo sutarties kylantys ginčai yra sprendžiami šalių tarpusavio susitarimu. Šalims nepavykus susitarti, bet kokie ginčai, nesutarimai ar reikalavimai, kylantys iš šios Duomenų tvarkymo sutarties ar susiję su ja, jos pažeidimu, nutraukimu ar galiojimu, neišspręsti Šalių susitarimu, sprendžiami Lietuvos Respublikos teisme pagal Valdytojo buveinę, jeigu teisės aktuose nenustatyta kitaip.	11.4. All disputes arising in connection with the Data Processing Agreement shall be settled by a mutual consensus between the Parties. In the event of failure by the Parties to reach a consensus, any disputes, disagreements, or claims arising out of this Data Processing Agreement or related to it, violation, termination, or validity thereof, not resolved by a mutual consensus between the Parties, shall be resolved at the court of the Republic of Lithuania based on the location of the Controller's registered office, unless stipulated otherwise by the legal acts.
11.5. Esant prieštaravimų tarp šios Duomenų tvarkymo sutarties ir kitų tarp Šalių sudarytų sutarčių sąlygų, taikomos šios Duomenų tvarkymo sutarties nuostatos.	11.5. In the event of conflict between the terms and conditions of this Data Processing Agreement and of other contracts entered into between the Parties, the provisions of this Data Processing Agreement shall apply.
12. Sutarties galiojimas, keitimas ir nutraukimas	**12. Validity, amendment, and termination of the Agreement**
12.1. Duomenų tvarkymo sutartis įsigalioja nuo jos pasirašymo dienos ir galioja tol, kol, priklausomai kas įvyksta pirmiau	

12.1.1. galioja Sutartis; arba 12.1.2. iki atskirame Valdytojo pranešime Tvarkytojui apie Duomenų tvarkymo sutarties nutraukimą nurodyto termino. 12.2. Tvarkytojo konfidencialumo įsipareigojimai lieka galioti ir pasibaigus šiai Duomenų tvarkymo sutarčiai ir (arba) Sutarčiai. 12.3. Visi Duomenų tvarkymo sutarties pakeitimai ir papildymai yra galiojantys jeigu sudaryti raštu ir patvirtinti abiejų Šalių atstovų parašais. 12.4. Šalys patvirtina ir garantuoja, kad jos turi visus reikiamus įgaliojimus sudaryti Duomenų tvarkymo sutartį ir ją vykdyti. 12.5. Duomenų tvarkymo sutartis sudaryta 2 (dviem) vienodą teisinę galią turinčiais egzemplioriais, po vieną kiekvienai iš Šalių. **13. Sutarties priedai** 13.1. Priedai yra neatskiriama Duomenų tvarkymo sutarties dalis ir turi būti aiškinami vadovaujantis Duomenų tvarkymo sutarties nuostatomis. Kiekviena Šalis gauna po 1 (vieną) kiekvieno Duomenų tvarkymo sutarties priedo egzempliorių. 13.2. Prie šios Duomenų tvarkymo sutarties pridedami priedai: 13.2.1. Priedas Nr. 1 – Asmens duomenų tvarkymo sąlygos. 13.2.2. Priedas Nr. 2 – Saugumo reikalavimai. 13.2.3. Priedas Nr. 3 - Duomenų tvarkytojo taikomų techninių ir organizacinių saugumo priemonių aprašymas **14. Šalių rekvizitai ir parašai:** **VALDYTOJAS:** UAB „Ignitis grupės paslaugų centras“ AB „Ignitis grupė“ _____ (Parašas) **TVARKYTOJAS:** Starred B.V.	12.1. The Data Processing Agreement shall enter into force from the date of its signature and shall, depending on whichever comes first, remain in force: 12.1.1. as long as the Agreement is valid; or 12.1.2. until the deadline specified in a separate notification given by the Controller to the Processor on termination of the Data Processing Agreement. 12.2. The Processor's confidentiality obligations shall remain in force after the expiry of this Data Processing Agreement and/or of the Contract. 12.3. All amendments and supplements to the Data Processing Agreement shall be valid if made in writing and confirmed with affixed signatures of the representatives of both Parties. 12.4. The Parties shall hereby confirm and guarantee that they have all authorisations required for concluding and fulfilling the Data Processing Agreement. 12.5. The Data Processing Agreement has been concluded in 2 (two) copies of equal legal power, one copy for each Party. **13. Annexes to the Agreement** 13.1. The Annexes form an integral part of the Data Processing Agreement and shall be construed in accordance with the provisions of the Data Processing Agreement. Each Party to the Agreement is given 1 (one) copy of each Annex to the Data Processing Agreement. 13.2. The Annexes to this Data Processing Agreement: 13.2.1. Annex No 1 – Terms and conditions of personal data processing. 13.2.2. Annex No 2 – Security requirements. 13.2.3. Annex No 3 – Description of the technical and organisational security measures implemented by the data processor. **14. Details and signatures of the Parties:** **CONTROLLER:** UAB „Ignitis grupės paslaugų centras“ AB „Ignitis grupė“ _____ (Signature) **PROCESSOR:** Starred B.V.

Priedas Nr. 1 prie Duomenų tvarkymo sutarties **Asmens duomenų tvarkymo sąlygos** **1. Tvarkytojas**	Annex No 1 to the Data Processing Agreement **Terms and conditions of the processing of Personal Data** **1. Processor**

Tvarkytojas vykdo toliau nurodytą duomenų tvarkymo veiklą Valdytojo pavedimu: *1) Siekiant užtikrint apklausos apie kandidatų, kurie buvo atmesti po telefoninio interviu ar interviu, patirtį, siuntimo bei rezultatų duomenų analizavimo debesies technologijos pagalba Paslaugų teikimą.*	The Processor shall carry out the data processing activities specified below at the order of the Controller: *1) In order to ensure the provision of the Service with the help of a survey on the experience of sending a survey of candidates who were rejected after a telephone interview or interview, and the analysis of the results data.*
2. Duomenų subjektai Tvarkomi Asmens duomenys yra susiję su šiomis duomenų subjektų kategorijomis: *1) Kandidatų, kurie buvo atmesti po telefoninio interviu ir interviu, el. pašto adresai;* *2) Kandidatų, kurie buvo atmesti po telefoninio interviu ir interviu, vardai ir pavardės;* *3) Kandidatų, kurie buvo atmesti po telefoninio interviu ir interviu, savanoriškai palikti komentarai apie jų patirtį;* *4) Kandidatų, kurie buvo atmesti po telefoninio interviu ir interviu, sutikimai gauti apklausą;* *5) Darbdavio įvaizdžio ir talentų pritraukimo funkcinės srities darbuotojų vardai, pavardės, el. pašto adresai;* *6) Darbuotojų ieškančių vadovų vardai ir pavardės.*	**2. Data subjects** The Personal Data being processed is related to the following categories of data subjects: *1) Employees of the Controller;* *2) Applicants for job positions in the Controller's company.* *3) Candidates who were rejected after telephone interviews and interviews voluntarily left comments on their experiences;* *4) Consents of candidates who were rejected after the telephone interview and interview to receive the survey;* *5) Names, surnames, e-mails of employees in the functional area of employer image and talent attraction. postal addresses;* *6) Names of managers looking for employees.*
3. Duomenų kategorijos Tvarkomi Asmens duomenys yra arba gali būti toliau nurodyto tipo Asmens duomenys: *1) Informacija apie kandidatus:* • *Vardas, pavardė;* • *Kontaktiniai duomenys (el. paštas);* • *Kandidatų, kurie buvo atmesti po telefoninio interviu ir interviu, savanoriškai palikti komentarai apie jų patirtį;* • *Pozicijų, į kurias kandidatai kandidatavo ir buvo atmesti po telefoninio interviu ir interviu, pavadinimai;* • *Įmonių, į kurias kandidatai kandidatavo ir buvo atmesti po telefoninio interviu ir interviu, pavadinimai;* • *Kandidatų, kurie buvo atmesti po telefoninio interviu ir interviu, sutikimai gauti apklausą.* *2) Informacija apie darbuotojus:* • *Darbdavio įvaizdžio ir talentų pritraukimo funkcinės srities darbuotojų vardai, pavardės, el. pašto adresai;* • *Darbuotojų ieškančių vadovų vardai ir pavardės.*	**3. Data categories** Personal Data processed is or could be Personal Data of the type indicated below: *1) Information on the candidates:* *•Name surname;* *• Contact details (e-mail);* *• Candidates who were rejected after telephone interviews and interviews voluntarily left comments on their experiences;* *• The names of the positions for which the candidates applied and were rejected after the telephone interview and the interview;* *• The names of the companies to which the candidates applied and were rejected after the telephone interview and interviews;* *• Consents of candidates who were rejected after the telephone interview and interview to receive the survey.* *2) Employee information:* *• Names, surnames, e-mails of employees in the functional area of employer image and talent attraction;* *• Names of managers looking for employees.*
4. Duomenų teikimo būdai: *1) suteikiant prieigą prie Valdytojo sistemos <SmartRecruiters>;* *2) rankiniu būdu sukeliant duomenis apie kandidatus (vardai, pavardės, el. pašto adresai) į <Starred> sistemą.*	**4. Methods of data provision** 1) granting access to the Manager's system <SmartRecruiters>; 2) manually entering data about candidates (names, surnames, e-mail addresses) into the <Starred> system or automatically via the integration.
5. Šalių rekvizitai ir parašai: **VALDYTOJAS:** UAB „Ignitis grupės paslaugų centras“	**5. Details and signatures of the Parties:** **CONTROLLER:** UAB „Ignitis grupės paslaugų centras“

_____ (Parašas) **TVARKYTOJAS:** Starred B.V.	_____ (Signature) **PROCESSOR:** Starred B.V.
Priedas Nr. 2 prie Duomenų tvarkymo sutarties **Saugumo reikalavimai** Valdytojas, Tvarkytojui patikėtų asmens duomenų tvarkymui, nustato organizacines ir technines duomenų tvarkymo priemones. Tvarkytojas, su juo susiję ir jo įgalioti asmenys privalo užtikrinti žemiau nurodytus saugumo reikalavimus. **1. Organizacinės duomenų saugumo priemonės** 1.1. Asmens duomenų saugumo politika ir procedūros: 1.1.1. Asmens duomenų ir jų tvarkymo saugumas turi būti dokumentuotas kaip informacijos saugumo politikos dalis. 1.1.2. Saugumo politika turi būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus. 1.2. Vaidmenys ir atsakomybės: 1.2.1. Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką; 1.2.2. Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu). 1.3. Prieigos valdymo politika: 1.3.1. Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) principu. 1.4. Išteklių ir turto valdymas: 1.4.1. Tvarkytojas turi turėti IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registro tvarkymas turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui. 1.4.2. IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas. 1.5. Keitimų valdymas: 1.5.1. Tvarkytojas turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto); 1.5.2. Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, reikia naudoti testinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros. 1.6. Žmogiškieji ištekliai: 1.6.1. Tvarkytojas užtikrina, kad jo darbuotojai tvarko informaciją laikydamiesi tokio konfidencialumo lygio, kurio reikalaujama pagal Sutartį ir šią Duomenų tvarkymo sutartį. 1.6.2. Tvarkytojas užtikrina, kad atitinkami Tvarkytojo darbuotojai būtų susipažinę su informacijos, įrenginių ir sistemų naudojimo reikalavimais (įskaitant nustatytus naudojimo apribojimus) pagal Sutartį ir Duomenų tvarkymo sutartį. Valdytojas turi teisę pareikalauti Tvarkytojo pateikti įrodymus, kad jo darbuotojai	Annex No 2 to the Data Processing Agreement **Security requirements** The Controller shall determine the organizational and technical means for the processing of data entrusted to the Processor. The Processor, the persons related to and authorised by the Processor must ensure the compliance with the following Security Requirements. **1. Organizational Data Security Measures** 1.1. Personal data security policy and procedures: 1.1.1. The security of personal data and their processing information security policy. 1.1.2. The Security Policy must be reviewed and, where necessary, updated at least once a year. 1.2. Roles and responsibilities: 1.2.1. Roles and responsibilities related to the processing of personal data must be clearly defined and distributed in accordance with security policy. 1.2.2. The cancellation of employees' rights and obligations must be clearly defined through appropriate procedures for the transfer or assignment of roles and responsibilities (during the internal restructuring or layoffs, change of functions). 1.3. Access and control policy: 1.3.1. Each role related to the processing of personal data must have specific access control rights, in accordance with the need to know principle. 1.4. Resource and asset management: 1.4.1. The Processor must have a register of IT resources used to process personal data (a list of hardware, software, and network hardware). The register of IT resources must include at least the following information: type of IT resources (e.g., server, computer workstation), place (physical or electronic). The management of the registry must be assigned to a specific person, for example, IT specialist. 1.4.2. The register of IT resources must be regularly reviewed and updated. 1.5. Change management: 1.5.1. The Processor must ensure that all material changes to the IT systems are monitored and registered by specific person (for example, IT or security specialist); 1.5.2. Software development should be performed in a special environment that is not connected to the IT systems used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing. 1.6. Human resources: 1.6.1. The Processor shall make sure that its employees process information subject to the degree of confidentiality required under the Contract and this Data Processing Agreement. 1.6.2. The Processor shall make sure that respective employees of the Processor are familiar with the requirements applicable to use of information, equipment, and systems (including the established restrictions for use) in accordance with the Contract and this Data Processing Agreement. The Controller shall have the right to require the Processor to provide evidences that its

susipažino su Saugumo reikalavimų turiniu ir sutinka laikytis šių reikalavimų. 1.6.3. Tvarkytojas užtikrina, kad Tvarkytojo darbuotojai, atsakingi už saugumą, yra tinkamai apmokyti vykdyti su saugumu susijusias pareigas; 1.6.4. Tvarkytojas paskiria bent vieną asmenį, turintį tinkamos kompetencijos saugumo srityje, kuris yra atsakingas už Saugumo reikalavimuose numatytų saugumo priemonių įgyvendinimą. 1.6.5. Tvarkytojas turi užtikrinti, kad visi darbuotojai b reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, susiję atitinkamus duomenų saugumo reikalavimus ir atsakomybes, ren instruktažus.	employees have made themselves familiar with the content of security requirements and agree to comply with them. 1.6.3. The Processor shall make sure that the Processor's employees in charge for security have been properly trained to fulfil their security-related duties; 1.6.4. The Processor must ensure that at least one person having adequate competence in the area of security is responsible for the implementation of the security measures indicated in the Security Requirements. 1.6.5. The Processor should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.
2. Techninės duomenų saugumo priemonės	**2. Technical data security measures**
2.1. Prieigų kontrolė ir autentifikavimas: 2.1.1. Turi būti įdiegta, įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. 2.1.2. Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas. 2.1.3. Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. 2.1.4. Slaptažodis turi būti sudaromas iš ne mažiau 8 simbolių, naudojant didžiąsias, mažąsias raides ir skaičius. 2.1.5. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka nustatyto kompleksiškumo lygio. 2.1.6. Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. *hash form*). 2.1.7. Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius.	2.1. Access control and authentication 2.1.1. An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts. 2.1.2. The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities. 2.1.3. An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. 2.1.4. The password must be at least 8 characters long, it must include uppercase, lowercase letters and numbers. 2.1.5. The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity. 2.1.6. User passwords must be stored using a hash form. 2.1.7. A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.
2.2. Techninių žurnalų įrašai ir stebėsena: 2.2.1. Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). 2.2.2. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.	2.2. Technical journal entries and monitoring: 2.2.1. The records of technical journals must be implemented for each IT system, application program used for processing personal data. Technical journals must display all possible types of access to personal data records (such as date, time, review, change, cancellation). 2.2.2. Technical journal entries must be timestamped and protected from possible damage, tampering, or unauthorized access. Time accounting mechanisms used in IT systems must be synchronized with a common time reference source.
2.3. Duomenų bazių apsauga: 2.3.1. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos (OS) privilegijomis. 2.3.2. Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus.	2.3. Protection of servers, databases: 2.3.1. The databases and application server servers must be configured to work properly and use a separate account with the lowest operating system privileges assigned. 2.3.2. Databases and Application Servers must process only those personal data that is required for work that meets the data processing objectives
2.4. Darbo vietų apsauga: 2.4.1. Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų. 2.4.2. Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne	2.4. Workstation protection: 2.4.1. Users should not be able to turn off or bypass, avoid security settings. 2.4.2. Antivirus applications and their virus database information must be updated at least weekly, or, as recommended, once daily or more frequently.

rečiau kaip kas savaitę, rekomenduojama kartą per parą ar dažniau. 2.4.3. Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos. 2.4.4. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Neaktyvios sesijos laikas – ne ilgiau kaip 15 min. 2.4.5. Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant. 2.4.6. Antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą. 2.5. Tinklo ir komunikacijos sauga: 2.5.1. Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL). 2.5.2. Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas. 2.6. Atsarginės kopijos: 2.6.1. Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis; 2.6.2. Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų; 2.6.3. Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą; 2.6.4. Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: kasdien – pridedamoji kopija, kas savaitę – pilna kopija. 2.7. Mobilieji, nešiojamieji įrenginiai: 2.7.1. Mobiliųjų, nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą; 2.7.2. Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti; 2.7.3. Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti; 2.7.4. Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos. 2.8. Programinės įrangos sauga: 2.8.1. Informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. frameworks), standartus (pvz., Agile, OWASP ir kt.). 2.8.2. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos. 2.8.3. Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, jau turi būti laikomasi pagrindinių saugos reikalavimų; 2.8.4. Tais atvejais, kai Tvarkytojas iš Valdytojo gautų asmens duomenų tvarkymui pasitelkia debesijos paslaugas (pvz., talpina ir saugo asmens duomenis debesies saugykloje): 2.8.4.1. Tvarkytojas arba debesijos paslaugas teikiantis paslaugos tiekėjas turi būti sertifikuotas pagal ISO 27001 standartą; 2.8.4.2. paslaugų duomenų centrai turi būti Europos ekonominės erdvės šalyje, o saugomi duomenys negali būti perkelti už Europos ekonominės erdvės ribų 2.9. Duomenų naikinimas, šalinimas: 2.9.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi	2.4.3. Users must not have the privileges (rights) of installing, removing, administering unauthorized software. 2.4.4. IT systems must have a set session time, i.e. outs when the user has not been active for a certain time period. Inactive session time - not more than 15 minutes. 2.4.5. Critical security updates released by the operating system developer should be installed regularly and without delay. 2.4.6. Antivirus applications and their databases of virus and malware information must be updated at least daily. 2.5. Network/Communication security: 2.5.1. Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL). 2.5.2. Any movement of data from/to the IT system must be monitored and controlled using firewalls and intrusion detection and prevention systems. 2.6. Back-ups: 2.6.1. Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities; 2.6.2. Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data; 2.6.3. Execution of backups should be monitored to ensure completeness; 2.6.4. Full backups should be carried out regularly. Recommended backup frequency: daily for attached backup, weekly for full backup. 2.7. Mobile, portable devices: 2.7.1. Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use; 2.7.2. Mobile and portable devices that will be used for work and are allowed to access the information systems should be pre-registered and pre-authorized; 2.7.3. Mobile and portable devices should be subject to the same sufficient levels of access control procedures (to the data processing system) as other equipment used for data processing; 2.7.4. The functions and responsibilities of mobile and portable devices must be clearly defined. 2.8. Software security: 2.8.1. Software used in information systems (for processing personal data) must comply with software security best practices, software development frameworks and standards (for example, Agile, OWASP, etc.); 2.8.2. Programming standards and best practices ensuring data security must be adhered to; 2.8.3. After software development, testing and verification, the basic safety requirements must already be met before the system is installed and operational; 2.8.4. In cases where the Processor uses cloud services to process personal data received from the Controller (for example, storing and retaining personal data in the cloud storage): 2.8.4.1. The Processor or cloud service provider must be ISO 27001 certified; 2.8.4.2. Service Data Centres must be located in a country within the European Economic Area and retained data cannot be transferred outside the European Economic Area. 2.9. Data deletion/disposal: 2.9.1. Before removing any data storage media, all data contained in it must be destroyed using software designed for that purpose, which supports reliable data-erasure algorithms. If this is not possible (for example, DVD media), physical

būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti. 2.9.2. Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis. 2.10. Fizinė prieigos kontrolė: 2.10.1. Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos. **3. Atitiktis** 3.1. Valdytojo prašymu Tvarkytojas nedelsiant pateikia Valdytojui atitikties Saugumo reikalavimams ataskaitą. Ataskaitos formą Valdytojas pateiks Tvarkytojui kartu su prašymu. 3.2. Aukščiau paminėti reikalavimai ne mažesne apimtimi taikomi visiems Tvarkytojo pasitelktiems subtvarkytojams, jeigu Valdytojas neprieštarauja, kad Tvarkytojas pasitelktų subtvarkytojus. 3.3. Valdytojas kaip nurodyta Duomenų tvarkymo sutarties 8 dalyje turi teisę audito būdu įsitikinti, kad Paslaugų teikėjas laikosi šių reikalavimų **4. Šalių rekvizitai ir parašai:** **VALDYTOJAS:** UAB „Ignitis grupės paslaugų centras“ AB „Ignitis grupė“ Starred B.V.	destruction of the data medium must be performed without the possibility of recovery. 2.9.2. Paper and portable data media (for example, DVD media) in which personal data was retained or stored must be destroyed by dedicated shredders or other mechanical means. 2.10. Physical access control: 2.10.1. The physical protection of the environment, premises in which the IT system infrastructure is located, must be implemented from unauthorized access. **3. Compliance** 3.1. At the request of the Controller, the Processor shall immediately submit to the Controller a report on compliance with the Security Requirements. The Controller will submit the report form to the Processor along with the request. 3.2. The aforementioned requirements shall apply at not lesser extent to all Sub-processor engaged by the Processor, provided that the Controller does not object to the engagement of sub-processors by the Processor. 3.3. As stated in Paragraph 8 of the Data Processing Agreement, the Controller shall have the right to make sure, through an audit, that the Service provider complies with these requirements **4. Details and signatures of the Parties:** **CONTROLLER:** UAB „Ignitis grupės paslaugų centras“ AB „Ignitis grupė“ **PROCESSOR:** Starred B.V.

Priedas Nr. **3** prie Duomenų tvarkymo sutarties **Duomenų tvarkytojo taikomų techninių ir organizacinių saugumo priemonių aprašymas**	Annex No **3** to the Data Processing Agreement

Starred saugumas ir duomenų apsauga

„Starred“ pažymi, kad duomenų apsauga yra pagrindinis mūsų ISO 27001 reikalavimus atitinkančių saugos priemonių tikslas - apsaugoti privačią ir neskelbtiną informaciją, kurią apdoroja mūsų programa. Šioje apžvalgoje apibūdinamas „Starred“ požiūris į saugumą ir atitikimą, įskaitant išsamią informaciją apie technines ir organizacines priemones, susijusias su tuo, kaip „Starred“ apsaugo jūsų duomenis.

Turinys:

Produkto saugumas

Pagrindinių saugos funkcijų ir praktikos, apsaugančios jūsų duomenis Starred apžvalgą žr. žemiau

Techninė įranga ir infrastruktūra

●„AWS Geo-dispersed“, sertifikuoti pagal ISO 27001 ir SOC audituoti duomenų centrai, esantys keliuose ES regionuose: Airijoje (AWS: eu-west-1), Frankfurte, Vokietijoje (AWS: eu-central-1) ir Paryžiuje, Prancūzijoje (AWS: eu-west-3).

● Saugus duomenų replikavimas ir užšifruotas archyvavimas.

● Kasmetinis verslo tęstinumo planavimo (BCP) ir atkūrimo po nelaimių (DR) testavimas.

● Profesionalios, komercinės klasės užkardos, pasienio maršrutizatoriai ir tinklo valdymo sistemos.

Description of the technical and organisational security measures implemented by the data processor

Starred Security and Data Protection

For Starred, data protection is a primary focus of our ISO 27001 compliant security efforts ensuring that we protect private and sensitive information processed by our application. This overview outlines Starred's approach to security, and compliance, including details on technical and organizational measures regarding how Starred protects your data.

Contents:

Product security

For an overview of key security features and practices that protect your data within Starred, see below.

Hardware and infrastructure

- AWS Geo-dispersed, ISO 27001-certified, and SOC-audited data centers, located across multiple regions in the EU: in Ireland (AWS: eu-west-1), in Frankfurt, Germany (AWS: eu-central-1), and in Paris, France (AWS: eu-west-3).
- Secure data replication and encrypted archival.
- Annual Business Continuity Planning (BCP) and Disaster Recovery (DR) testing.
- Professional, commercial-grade firewalls, border routers, and network management systems.

Sistemos ir veiksmai

● Centralizuota, logiška prieigos valdymo sistema.

● Dviejų veiksnių autentifikavimas, šifruota VPN prieiga.

● „Denial of Service“ (DDoS) sušvelninimas.

● Aktyvus įsilaužimų aptikimas ir prevencija.

● Integruota kenkėjiškų programų programinė įranga, kuri automatiškai įspėja „Starred“ reagavimo į incidentus komandą, jei aptinkamas potencialiai žalingas kodas.

● Trečiųjų šalių skverbimosi testavimas.

Programos ir prieiga

● Oficialus kodo peržiūra ir pažeidžiamumo mažinimas iš trečiųjų šalių.

● Programos lygio „Advanced Encryption Standard“ (AES) 256 bitų šifravimas.

● Raktų valdymo ir šifravimo programa.

● Apsauga nuo kenkėjiškų programų.

● Konfigūruojamos saugos funkcijos.

○ Daugelio veiksnių autentifikavimas suteikia papildomą užtikrinimo lygį, kurį gali pasiekti tik tie asmenys, kuriems suteikta prieiga prie Starred.

○ Įgaliojimas pagal vaidmenį leidžia jums nurodyti prieigą prie konkrečių asmenų.

Perdavimas ir saugojimas

● Duomenys užšifruoti pagal geriausios pramonės praktikos standartus. Starred palaiko visą šifravimą perduodant. Jokie nešifruoti duomenys neišeina iš mūsų duomenų centro. Visos mūsų stebėjimo ir galinės sistemos arba siunčia vietinį srautą per VPC, arba bendraujant su likusiu internetu jos naudoja transporto lygio šifravimą. Visi duomenys šifruojami ramybės būsenoje mūsų AWS EBS diskuose. Atsarginės kopijos, siunčiamos į privačius mūsų S3 segmentus, užšifruojamos naudojant 4096 bitų GPG raktus.

● Prieiga prie duomenų ir jų perdavimas iš Starred / iš jų per HTTPS.

● Skaitmeninių sertifikatų technologija.

● Kliento konfigūruojama duomenų išsaugojimo galimybė.

Žmonės

Informacijos saugumas „Starred“ yra kiekvieno darbas. Mes investuojame į mokymus ir sąmoningumą, siekdami užtikrinti, kad informacijos saugumas išliktų svarbiausias visiems mūsų darbuotojams.

Systems and operations

- Centralized, logical access management system.
- Two-factor authentication, encrypted VPN access.
- Denial of Service (DDoS) mitigation.
- Active intrusion detection and prevention.
- Anti-malware software integration that automatically alerts Starred's incident response team if potentially harmful code is detected.
- Third-party penetration testing.

Applications and access

- Formal code reviews and vulnerability mitigation by third parties.
- Application-level Advanced Encryption Standard (AES) 256-bit encryption.
- Key management and encryption program.
- Malware protection.
- Configurable security features.
    - Multi-factor authentication provides an additional level of assurance that only those authorized to access Starred can access.
    - Role-based authorization enables you to designate access to specific individuals.

Transmission and storage

- Data encrypted in accordance with industry best-practice standards. Starred supports full encryption in transit. No non-encrypted data leaves our data center. All our monitoring and backend systems either send local traffic over the VPC, or they use transport-level encryption when communicating with the rest of the internet. All data is encrypted at rest on our AWS EBS disks. Backups sent to our private S3 buckets are encrypted using 4,096 bit GPG keys.
- Access and transfer of data to/from Starred via HTTPS.
- Digital certificate technology.
- Customer-configurable data retention capability.

People

Information security at Starred is everyone's job. We invest in training and awareness to ensure that information security stays top of mind for all of our employees.

● „Starred“ atlieka visų būsimų darbuotojų foninius patikrinimus. Prieš prisijungdamas prie mūsų darbuotojų, „Stared“ patikrins asmens išsilavinimą ir ankstesnį užimtumą bei atliks informacinius patikrinimus. Šių foninių patikrinimų mastas priklauso nuo norimos padėties. ● „Starred“ dirba saugos pareigūnas, priklausantis mūsų programinės įrangos inžinerijos ir operacijų skyriui. Šiam profesionalui pavesta plėtoti saugumo peržiūros procesus, kurti saugumo infrastruktūrą ir įgyvendinti „Starred“ saugumo politiką. Starred asmuo aktyviai ieško saugumo grėsmių naudodamas komercinius ir pritaikytus įrankius, skverbimosi testus, kokybės užtikrinimo (kokybės užtikrinimo) priemones ir programinės įrangos saugumo apžvalgas. ● Visi Starred pažymėti darbuotojai dalyvauja informacinio saugumo ir privatumo mokymuose, kaip dalis įlaipinimo proceso, ir nuolat mokomi per visą Starred karjerą, bent kartą per metus. Įlaipinimo metu nauji darbuotojai sutinka su mūsų elgesio kodeksu, kuris pabrėžia mūsų įsipareigojimą saugoti klientų informaciją. ● Inžinierių mokymai užtikrinti, kad kodavimas būtų atliekamas saugiai, reguliariai tikrinant kodų bazę.	● Starred conducts background checks for all prospective employees. Before they join our staff, Stared will verify an individual's education and previous employment, and perform reference checks. The extent of these background checks is dependent on the desired position. ● Starred employs a Security Officer who is part of our software engineering and operations division. This professional is tasked with developing security review processes, building security infrastructure and implementing Starred's security policies. Starred actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews. ● All Starred employees undergo information security and privacy training as part of the onboarding process and receive ongoing training throughout their Starred careers, at least annually. During onboarding, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. ● Training for engineers to ensure coding is done securely, with regular security audits of the code base.
<u>Procesas</u> „Starred“ verslo procesuose, įskaitant vidaus politiką, programinės įrangos kūrimą ir programų stebėjimą, atsižvelgiama į mūsų klientų duomenų saugumą. ● Patalpų saugumo politika, pvz., Prieiga prie ženklelių, vieši įėjimai su asmenimis ir fizinės prieigos kontrolė. ● Tik nedidelė Starred darbuotojų grupė turi prieigą prie klientų duomenų. Starred darbuotojų prieigos teisės ir lygiai priklauso nuo jų darbo funkcijos ir vaidmens, naudojant mažiausios privilegijos ir būtinybės žinoti sąvokas, kad prieigos teisės būtų suderintos su apibrėžtomis pareigomis. ● Aktyvus stebėjimas ir perspėjimas. Mūsų infrastruktūra ir paslaugos yra stebimi įvairiais būdais, įskaitant: sistemos ir programų metaduomenis centralizuotai registravimo tarnybai analizuoti ir perspėti, pritaikytus mūsų sistemoms, AWS įspėjimą apie įvykius, pvz., Egzempliorių mastelį ir srauto padidėjimą / programos veikimo pokyčius , AWS „Cloudwatch“ perspėjimas infrastruktūros ir programų lygio stebėjimui. ● Starred programinės įrangos kūrimo gyvavimo ciklo (SDLC) saugos apžvalgos, įskaitant planavimo, projektavimo, diegimo testavimo, pristatymo ir reagavimo etapus. ● Oficialus kodų peržiūra ir trečiųjų šalių pažeidžiamumo mažinimas dėl programų ir prieigos saugumo. ● Kasmet peržiūrima verslo tęstinumo politika ir atkūrimo po nelaimių planas. ● Turime griežtą saugumo įvykių valdymo procesą, kuris gali turėti įtakos sistemų ar duomenų konfidencialumui, vientisumui ar prieinamumui. Jei įvyksta incidentas, saugos pareigūnas registruoja	**Process** Starred's business processes, including internal policies, software development and application monitoring, take into consideration the security of our customer data. ● On-premise security policies, such as badge access, manned public entrances and physical access controls. ● Only a small group of Starred employees have access to customer data. For Starred employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. ● Active monitoring and alerting. Our infrastructure and services are monitored in a variety of ways, including: system and application metadata to a centralised logging service for analysis and alerting, tailored to our systems, AWS alerting of events such as instance scaling and spikes in traffic / changes in application performance, AWS Cloudwatch alerting for infrastructure and application level monitoring. ● Security reviews within the Starred Software Development Life Cycle (SDLC), including the planning, design, implementation testing, shipping and response phases. ● Formal code reviews and vulnerability mitigation by third parties for applications and access security. ● Annually reviewed Business Continuity Policy, and Disaster Recovery Plan. ● We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security officer logs and prioritizes it

žurnalą ir nustato jo prioritetą pagal jo sunkumą. Įvykiams, kurie tiesiogiai veikia klientus, suteikiamas didžiausias prioritetas.	according to its severity. Events that directly impact customers are assigned the highest priority.
Taikymas „Starred“ saugi programa apima aparatinę įrangą ir infrastruktūrą, sistemas ir operacijas, programas ir prieigą bei perdavimą ir saugojimą. ● Komercinio lygio duomenų centrai visuose regionuose, kad svarbiausi klientų duomenys liktų prieinami, jei kiltų bet kokių verslo sutrikimų. ● Saugus, beveik realaus laiko duomenų replikavimas. ● Fiziškai ir logiškai atskirti tinklai sistemoms ir operacijoms. Šiuo metu mes turime valdymo, pastatymo ir gamybos tinklus. Tarp valdymo ir kitų dviejų yra tarpusavio ryšių, kad valdymo paslaugos galėtų naudotis tomis aplinkomis, bet ne tarp pastatymo ir gamybos. ● Mes naudojame EC2 saugumo grupes prieigai tarp potinklių, tinklų ir interneto valdyti. Pagal numatytuosius nustatymus prieiga tarp mašinų nėra suteikiama, prievadai tarp jų atidaromi tik prireikus. ● Mūsų VPN yra apsaugotas naudojant kelių veiksnių autentifikavimą. Pirmasis („turėjimo faktorius“) yra panaikinamas sertifikatas, pridėtas prie vartotojo vardo. Antrasis yra („žinių faktorius“) yra (labai) patikimas slaptažodis tam pažymėjimui. Trečiasis („paveldėjimo faktorius“) yra OTP ženklas, atkuriamas kiekvieną minutę. ● Apsauga nuo kenkėjiškų programų. ● Komercinio lygio užkardos ir pasienio maršrutizatoriai, skirti atsispirti IP aptikimo ir paslaugų atsisakymo atakoms / aptikti jas. ● Skaitmeninių sertifikatų technologija ● Dviejų veiksnių šifruota VPN prieiga	**Application** Starred’s secure application encompasses hardware and infrastructure, systems and operations, applications and access, and transmission and storage. ● Commercial-grade data centers across regions, so that critical customer data remain available in the event of any business disruption. ● Secure, near real-time data replication. ● Physically and logically separated networks for systems and operations. Currently we have networks for management, staging, and production. There are peering links between management and the other two, for the purposes of management services having access to those environments, but not between staging and production. ● We utilise EC2 Security Groups to control access between subnets, networks, and the internet. By default, no access between machines is given, ports are only opened between them when necessary. ● Our VPN is protected with multi factor authentication. The first (the “possession factor”) is a revocable certificate, attached to a username. The second is (the “knowledge factor”) is a (very) strong password for that certificate. And the third (the “inherence factor”) is an OTP token, regenerated every minute. ● Malware protection. ● Commercial-grade firewalls and border routers to resist/detect IP-based and denial-of-service attacks. ● Digital certificate technology ● Two-factor encrypted VPN access
Subtvarkytojai Toliau pateikta informacija pateikiama siekiant parodyti „Starred“ procesą įtraukiant subtvarkytojus ir pateikti subtvarkytojų sąrašą. „Starred“ naudoja tam tikrus subtvarkytojus kad palaikytų „Starred“ paslaugų teikimą. **Kas yra subtvarkytojas?** Subtvarkytojas yra duomenų tvarkytojas, kuris „Starred“ vardu tvarko asmens duomenis. „Starred“ naudoja tam tikrus infrastruktūros subtvarkytojus, kad priglobtų savo programas, ir kitus su konkrečia paslauga susijusius antrinius procesorius, kad teiktų specifines „Starred“ paslaugų funkcijas. Starred asmens duomenys tvarkomi Europos Sąjungos šalyse, kai tik įmanoma, kad būtų kuo mažiau duomenų perduota. Jei „Starred“ tvarko asmens duomenis už Europos Sąjungos ribų, tai deramai atsižvelgiama į galiojančius privatumo įstatymus, kuriuos reglamentuoja standartinės sutarčių sąlygos. SCC yra Europos	**Sub-processors** The information below is provided to illustrate Starred’s engagement process for sub-processors, and to provide a subprocessor list. Starred uses certain sub-processors to support the delivery of the Starred services. **What is a sub-processor?** A sub-processor is a data processor who, on behalf of Starred, processes personal data. Starred uses certain infrastructure sub-processors to host its applications and other service- specific sub-processors to provide specific functionality within the Starred services. Starred processes personal data in countries within the European Union whenever possible to keep data transfer to a minimum. If Starred processes personal data outside the European Union it is with

Komisijos patvirtintų sąlygų rinkinys, leidžiantis saugiai perduoti duomenis.

Subtvarkytojų sąrašas

Žemiau rasite subtvarkytojų sąrašą, jų vaidmenį ir veikimo vietą.

„Amazon Web Service, Inc.“ Duomenų priegloba ES

„Rocket Science Group LLC“ d / b / „Mailchimp“ el. Pašto paslaugų teikėjas JAV

New„Relic, Inc.“ veiklos stebėsena ES

„Logz.io“ AI dirbanti ELK kaip paslauga ES

„Functional Software Inc.“ („Sentry“) programų klaidų stebėjimas ES

„Domo, Inc.“ duomenų ataskaitos ir vizualizacija JAV

<u>Deramas patikrinimas ir apsaugos priemonės</u>

„Starred“ naudojasi komerciškai pagrįstomis pastangomis įvertindama subtvarkytojų, kurie gali turėti prieigą prie asmens duomenų arba juos tvarkyti, duomenų apsaugos praktiką. „Starred“ reikalauja, kad subtvarkytojai užtikrintų bent jau duomenų apsaugos lygį, kurio reikalaujama „Starred“ pagal galiojančius duomenų apsaugos įstatymus ir kitus teisės aktus, įskaitant, bet neapsiribojant, reikalavimus:

● teikdami paslaugas „Starred“, naudokite komerciškai pagrįstas saugumo priemones, kad išsaugotumėte asmens duomenų saugumą, vientisumą ir konfidencialumą bei apsisaugotumėte nuo neteisėtos prieigos ir numatomų grėsmių ar pavojų asmens duomenims;

● Asmens duomenis naudokite tik Starred, kad galėtumėte teikti savo paslaugas (įskaitant būtinas subtvarkytojo paslaugas), o ne tvarkykite asmens duomenis jokiu kitu tikslu;

● tvarkykite ir tvarkykite asmens duomenis laikydamiesi visų galiojančių duomenų privatumo ir apsaugos įstatymų, taisyklių ir nuostatų;

● Laikytis įsipareigojimų, kaip reikalauja visi taikomi duomenų privatumo ir apsaugos įstatymai, taisyklės ir reglamentai;

<u>Pažymėjimai</u>

ISO 27001

„Starred“ yra sertifikuotas aukščiausiu šiandien pasiekiamu pasauliniu informacijos saugumo užtikrinimo lygiu ISO 27001, kuris klientams užtikrina, kad „Starred“ atitinka griežtus tarptautinius saugumo standartus.

due regard for the applicable privacy laws, which is governed by Standard Contractual Clauses (SCCs). The SCCs are a set of terms that have been approved by the European Commission which allow data to be safely transferred.

List of Sub-processors

Please find the list of sub-processors, their role and location of processing below.

Amazon Web Service, Inc. Data hosting EU
The Rocket Science Group LLC d/b/a Mailchimp Email service provider USA
New Relic, Inc. Performance Monitoring EU
Logz.io AI-Powered ELK as a Service EU
Functional Software Inc. (Sentry) Application Error Tracking EU
Domo, Inc. Data Reporting and Visualization US

Due diligence and safeguards

Starred uses commercially reasonable efforts to evaluate the data protection practices of sub-processors that may have access to or process personal data. Starred requires sub-processors to provide, at a minimum, the level of data protection required of Starred under applicable data protection laws and regulations, including, but not limited to, the requirements to:

- Use commercially reasonable security measures in providing services to Starred to preserve the security, integrity, and confidentiality of personal data, and to protect against unauthorized access and anticipated threats or hazards to personal data;
- Use personal data only for Starred to provide its services (including necessary sub-processor services), and not process personal data for any other purpose;
- Handle and maintain personal data in compliance with all applicable data privacy and protection laws, rules, and regulations;
- Comply with obligations as required by all applicable data privacy and protection laws, rules, and regulations;

Certifications

ISO 27001

Starred is certified at the highest level of global information security assurance available today, ISO 27001, which provides customers assurance that Starred meets stringent international standards on security.