Paslaugų teikimo sutartis /
Agreement for Providing Services

Dokumento data laikoma paskutinio elektroninio parašo laiko žymos data /
The date of the document is the date of the last attached secure electronic signature time stamp

Valstybės įmonė Registrų centras, juridinio asmens kodas 124110246, (toliau – **Užsakovas**), atstovaujama nės Registrų 2025-01-02	The State Enterprise Centre of Registers, legal entity code 124110246, (hereinafter referred to as **the Customer**), s, :o ıe ʏy
ir AB Sysarb, juridinio asmens kodas 556681-8828 (toliau – **Tiekėjas**), atstovaujama toliau Užsakovas ir Tiekėjas kartu vadinami **Šalimis**, o kiekvienas atskirai – **Šalimi.**	and Sysarb AB, legal entity code 556681-8828, (hereinafter referred to as **the Provider**), represented by Hereinafter the Customer and the Provider are collectively referred to as **the Parties**, and each individually **as a Party.**
1. Bendrosios sąlygos Šios bendrosios sąlygos sudaro Tiekėjo ir Užsakovo sutartį. Šiose nuostatose sąvoka Užsakovas reiškia fizinį arba juridinį asmenį, kuris užsisakė prekes arba paslaugas iš Tiekėjo su savo veikla susijusiais tikslais. Šiose bendrosiose sąlygose sąvoka „Prekės" arba „Produktas" susijusi su Sysarb programine įranga (toliau - Sistema) ir su ja susijusiomis teisėmis. Užsakovas taip pat gali iš Tiekėjo įsigyti konsultacines paslaugas (toliau - Paslaugos). Jei Tiekėjas ir Užsakovas raštu susitaria dėl konkrečių Sistemos ar Paslaugų teikimo	1. General Terms and Conditions These general terms and conditions constitute an agreement between the Provider and the Customer. In these provisions, the term "Customer" refers to a natural or legal person who has ordered goods or services from the Provider for purposes related to their own business activities. The term "Goods" or "Product" as referred to in these general terms and conditions pertains to the Sysarb software ("the System") and its associated rights. The Customer may also procure consulting services from the Provider ("the Services"). In the event that the Provider and the Customer mutually agree in writing on specific terms for the

sąlygų, toks konkretus susitarimas turi viršenybę prieš šias bendrąsias sąlygas. Šios sąlygos papildo Šalių Sutarties dokumentus, tokius kaip užsakymai, prašymai ir kainoraščiai.	delivery of the System or the Services, such specific agreement shall take precedence over these general terms and conditions. These terms serve as an addition and complement to the parties' contractual documents such as orders, requests, and price lists.
2. Licencijavimas ir teisės Tiekėjas suteikia Užsakovui neišimtinę, neperleidžiamą teisę šios Sutarties galiojimo laikotarpiu įmonės viduje naudotis Sistema Sutartyje nurodytomis sąlygomis. Sistemos nuosavybės teisė niekada neperduodama Užsakovui, nebent Tiekėjas ir Užsakovas dėl to aiškiai susitaria raštu. Užsakovas turi teisę, kaip nurodyta šiose sąlygose ir užsakymo formoje, leisti naudotis Sistema nurodytoje padalinio vietoje. Visos su Sistema susijusios teisės (įskaitant autorių teises ir kitas intelektinės nuosavybės teises) priklauso Tiekėjui arba trečiosioms šalims, su kuriomis Tiekėjas yra sudaręs sutartis. Užsakovas neįgyja jokių teisių į Sistemą, išskyrus tas, kurios aiškiai nurodytos šiose sąlygose. Informaciją apie Sistemos autorių teises ir susijusius dokumentus tvarko Tiekėjas. Tiekėjas turi teisę apdoroti Užsakovo informacinę medžiagą, kad galėtų rengti Tiekėjo užsakovų prašomas atlyginimų statistikos ataskaitas. Tokia informacinė medžiaga bus nuasmeninta, kad nebūtų galimybės identifikuoti Užsakovo darbuotojų tapatybės.	2. Licensing and Rights The Provider grants the Customer a nonexclusive, non-transferable right, during the term of this agreement, to internally use the System in accordance with the terms specified herein. Ownership of the System never transfers to the Customer unless explicitly agreed upon in writing between the Provider and the Customer. The Customer has the right, as specified in these terms and on the order form, to make the System available at a designated business location. All rights associated with the System (including copyright and other intellectual property rights) belong to the Provider or third parties with whom the Provider has entered into agreements. The Customer does not acquire any rights to the System beyond what is explicitly stated in these terms. Information regarding copyright in the System and related documentation shall be maintained by the Provider. The Provider has the right to process customer materials to generate reports on salary statistics requested by the Provider's customers. Such material will be anonymized to prevent identification of the Customer’s employees.

3. Užsakovo atsakomybė Užsakovas privalo susipažinti su šiomis sąlygomis ir kitais su Sistema susijusiais dokumentais. Laikoma, kad Užsakovas aiškiai suprato sąlygas ir Sistemą bei Paslaugas. Jei Užsakovas sudaro sutartį su kitu paslaugų teikėju dėl integracijos su kitu duomenų šaltiniu (pvz., darbo užmokesčio sistema), Užsakovas atsako už integruotų duomenų funkcionalumo ir kokybės palaikymą. Užsakovas užtikrina, kad jo pateiktuose užsakymuose būtų nurodyti visi reikalavimai ir pageidavimai, susiję su Sistemos pristatymu ir Paslaugų teikimu. Jei užsakyme konkrečiai nenurodytas tam tikras komponentas, Tiekėjas turi teisę savo nuožiūra suprojektuoti ir nuspręsti dėl komponento. Užsakovas taip pat turi turėti Sistemos naudojimui reikalingą įrangą, pavyzdžiui, kompiuterius ir interneto ryšį. Užsisakydamas konsultavimo paslaugas, Užsakovas privalo pateikti Tiekėjui būtiną Paslaugoms suteikti informaciją ir medžiagą, už kurios įsigijimą ar parengimą konsultantas neatsako, kaip nurodyta užduoties aprašyme ar atsižvelgiant į įprastą praktiką. Jei Užsakovas suplanuoja susitikimą su Tiekėjo konsultantu ir pats jį atšaukia likus mažiau nei 14 dienų iki numatytos datos, Tiekėjas turi teisę gauti kompensaciją už susitikimui skirtą laiką.	3. Customer Responsibilities The Customer is responsible for having read through these terms and other documents related to the System. The Customer is accountable for understanding the terms and the System and Services. If the Customer enters into an agreement with another provider for integration with another data source (e.g., payroll system), it is the Customer's responsibility to maintain the functionality and quality of the integrated data. The Customer is responsible for ensuring that their orders contain all requirements and preferences for the delivery of the System and Services. If an order does not specifically specify a particular component, the Provider has the right to design and decide on the component at its discretion. The Customer is also responsible for possessing the necessary equipment for using the System, such as computers and internet connectivity. When ordering consulting services, the Customer must provide the Provider with the necessary information and materials required to perform the Services, which are not the responsibility of the consultant to acquire or develop, as defined by the task description or common practice. If the Customer schedules a meeting with a consultant from the Provider and cancels the meeting at the Customer's request less than 14 days before the scheduled date, the Provider is entitled to compensation for the allocated meeting time.

4. Atitiktis teisės aktams ir kt. Nors Sistema užtikrina tam tikras funkcijas ir supratimą, pateikia įžvalgas, kurie palengvins Užsakovo darbo užmokesčio struktūros suvokimą pagal ES darbo užmokesčio skaidrumo direktyvos (ES 2023/970) (toliau – ES direktyva) reikalavimus, Tiekėjas negali garantuoti, kad Sistema užtikrins visas funkcijas, supratimą ir pateiks įžvalgas, kurios būtinos, kad Užsakovas visiškai atitiktų minėtos ES direktyvos reikalavimus. Be to, Užsakovas pats atsako už visų būtinų veiksmų įgyvendinimą, kad atitiktų ES direktyvą ir teisės aktus, kurie ją perkelia į nacionalinę teisę.	4. Compliance with Laws etc. While the System will provide certain features, understandings, and insights that facilitate the Customer's understanding of its pay structure as required by the EU Pay Transparency Directive (EU 2023/970) (the "EU Directive"), the Provider cannot ensure that the System will provide every feature, understanding, and insight required for the Customer to comply with said EU Directive. Further, it is the Customer's obligation to implement any required actions to comply with the EU Directive and any local implementations thereof.
5. Sistemos naudojimas Sistema gali naudotis tik Užsakovas. Jis negali naudotis Sistema kitaip, nei nurodyta paskirtoje naudojimo srityje arba aprašyta šiose sąlygose. Naudodamasis Sistema, Užsakovas privalo laikytis pridedamuose dokumentuose pateiktų nurodymų ir kitų Tiekėjo periodiškai išleidžiamų instrukcijų. Užsakovas negali kitiems asmenims perduoti, suteikti ar kitaip platinti Tiekėjo suteiktus naudotojo leidimus, išskyrus kiek tai būtina Užsakovo poreikiams, susijusiems su Sistemos naudojimu, užtikrinti. Užsakovas negali perduoti, perleisti ar suteikti savo teisės naudotis Sistema ar jos dalimis be raštiško Tiekėjo sutikimo. Bet kokio perdavimo	5. Use of the System The System may only be used by the Customer. The Customer is not allowed to dispose of the System other than as specified in the designated usage area or as outlined in these terms. When using the System, the Customer must adhere to the instructions in the accompanying documentation and other instructions issued by the Provider from time to time. The Customer may not transfer, assign, or otherwise distribute user permissions granted by the Provider beyond what is necessary for the Customer's own use of the System. The Customer may not transfer, assign, or make available their right to the System or its parts without written consent from the Provider. In case of any transfer, the new party must confirm their

atveju naujoji šalis privalo raštu patvirtinti, kad sutinka su šios sutarties sąlygomis. Užsakovas atsakingas už naudotojo prisijungimo duomenų saugojimą, kad būtų išvengta neautorizuotos prieigos.	acceptance of the terms in this agreement in writing. The Customer is responsible for storing user credentials securely to prevent unauthorized access.
6. Pristatymas, atsarginė kopija ir palaikymas Naudotojo prisijungimo duomenys, įskaitant žiniatinklio adresą, naudotojo vardą ir slaptažodį, pateikiami per vieną savaitę po to, kai Tiekėjas gauna užsakymą. Sistema laikoma pristatyta, kai prisijungimo duomenys el. paštu išsiunčiami Užsakovo nurodytu el. pašto adresu. Tiekėjas tvarko informaciją pagal ISO/IEC 27001:2017 standarto reikalavimus, kurie apima administracinį, fizinį ir IT saugumą. Techninė pagalba teikiama darbo dienomis Tiekėjo darbo valandomis. Ji apima patarimus Užsakovui ir konsultacijas, kurios padeda nustatyti ir ištaisyti klaidas siekiant užtikrinti suderintą Sistemos funkcionalumą ir veikimą, klaidų diagnostinę analizę bei informaciją apie suteiktas ar vykdomas paslaugas. Techninė pagalba apibrėžiama kaip Užsakovo problemos sprendimas telefonu, nors Tiekėjas pasilieka teisę bendrauti el. paštu, per pokalbius internetu ar pateikti vedlius. Dėl pagalbos galima kreiptis naudojantis Tiekėjo svetainėje nurodytais susisiekimo būdais arba įrankiais, esančiais pačioje Sistemoje.	6. Delivery, Backup, and Support User credentials, including web address, username, and password, are provided within one week after the Provider receives the order. The System shall be considered delivered when user credentials are delivered via email to the email address provided by the Customer. The Provider operates with information security based on the requirements of ISO/IEC 27001:2017, covering administrative security, physical security, and IT security. Technical support is provided by the Provider on business days during office hours. Technical support entails advice and guidance to the Customer for identifying and rectifying errors to maintain the agreed-upon functionality and performance of the System, diagnostic analysis of errors, and information about delivery or ongoing Services. Technical support is defined as an issue where the Customer's problem can be solved through a telephone call, even if the Provider reserves the right to communicate through e-mail, chat or guides. Support can be accessed through the contact methods provided on the Provider's website or within the System.

7. Mokėjimai Sutarties galiojimo laikotarpiu Užsakovui netaikomi jokie mokesčiai už naudojimąsi Sistema. Sutarties galiojimo laikotarpiu paslaugos teikiamos neatlygintinai, o Užsakovas neturi jokių finansinių įsipareigojimų Tiekėjui. Pasibaigus sutarties galiojimo laikotarpiui, jeigu Užsakovas nuspręstų tęsti naudojimąsi Sistema ar kitomis Tiekėjo teikiamomis paslaugomis, Užsakovas inicijuotų naują viešąjį pirkimą pagal galiojančius teisės aktus. Tolesni veiksmai dėl Sistemos naudojimo ar paslaugų pirkimo bus atliekami tik įvykdžius šį naują pirkimo procesą ir sudarius naują sutartį su Tiekėju.	7. Payment During the validity period of the contract, the Customer is not charged any fees for using the System. During the term of the contract, the services are provided free of charge, and the Customer has no financial obligations to the Provider. After the contract expires, if the Customer decides to continue using the System or other services provided by the Provider, the Customer will initiate a new public procurement in accordance with the applicable legislation. Further actions regarding the use of the System or the purchase of services will be carried out only after completing this new purchase process and concluding a new contract with the Provider.
8. Defektai ir klaidos Jeigu Sistemoje yra defektų ar trūkumų ir Tiekėjas per 14 (keturiolika) dienų nuo raštiško Užsakovo skundo pateikimo dienos nepašalina šių defektų arba nesiima priemonių esminiams trūkumams ištaisyti, Užsakovas turi teisę nedelsiant nutraukti šią sutartį. Ši nutraukimo teisė gali būti įgyvendinama tik tuo atveju, jei nustatytas trūkumas turi esminės reikšmės Užsakovo naudojimuisi Sistema ir Užsakovas, naudodamasis Sistema, laikėsi visų pridėtoje dokumentacijoje ir kitose pateiktose instrukcijose nustatytų reikalavimų. Skundai arba pranešimai apie klaidas turi būti pateikti kai Užsakovas sužinojo arba turėjo sužinoti apie defektus. Šioje Sutartyje	8. Defects and Bugs If defects or deficiencies exist in the System and the Provider does not remedy such defects or take measures to correct serious deficiencies within 14 days from the Customer's written complaint, the Customer has the right to terminate this agreement immediately. However, this termination right assumes that the deviation is of significant importance to the Customer's use of the System and that the Customer has utilized the System in accordance with the accompanying documentation and other specified instructions. Complaints or bug reports must be submitted after the Customer has discovered or should have discovered the defect. The term "bug" in this context does not include errors that arise after the

terminas „klaida“ neapima klaidų, kurios atsirado dėl Užsakovo atliktų Sistemos modifikacijų ar papildymų.	Customer's modifications or additions to the delivery.
9. Klaidų taisymas Klaidų taisymas reiškia, kad Tiekėjas atsako už Sistemos veikimą pagal sutartas specifikacijas. Atsiradus programinės įrangos klaidai, Tiekėjas privalo profesionaliai ištaisyti klaidą arba pasiūlyti keitimą. Užsakovui reikšmingos klaidos turi būti pašalintos nedelsiant, tačiau ne vėliau kaip per vieną mėnesį nuo skundo pateikimo. Klaidų taisymas turi būti pradėtas per 24 valandas nuo pagalbos prašymo ir skundo iš Užsakovo gavimo, bet nebūtinai užbaigtas.	9. Error Rectification Error rectification means that the Provider is responsible for ensuring that the System functions according to the agreed specifications. In the event of a program error, the Provider is responsible for rectifying the error professionally through correction or offer of replacement. Errors that are significant to the Customer must be rectified promptly, but no later than one month from the complaint. Error rectification must be initiated, but need not be completed, within 24 hours of receiving a support request and complaint from the Customer.
10. Atsakomybės apribojimas Tiekėjas nėra atsakingas už žalą, kurią sukėlė: 1. netinkamas Sistemos naudojimas arba netinkami Užsakovo veiksmai; 2. Užsakovo atlikti Sistemos pakeitimai ar įsikišimai į Sistemą; 3. Užsakovo techninės įrangos gedimai arba gedimai, atsiradę dėl Užsakovo IT aplinkos; 4. kenksmingos programinės ar kibernetinės atakos Užsakovo IT aplinkoje, darančios įtaką Sistemos prieinamumui. Tiekėjas atsako ir kompensuoja Užsakovui už klaidas ar trūkumus tik taip: ištaiso klaidas ar pašalina trūkumus. Tiekėjas neatsako už gamybos nuostolius, negautą pelną, žalą tretiesiems asmenims ar kitus netiesioginius nuostolius.	10. Limitation of Liability The Provider is not liable for any damages caused by: 1. improper use of the System or Customer mishandling; 2. alterations or interventions in the System by the Customer; 3. faults in equipment provided by the Customer or faults caused by the Customer's IT environment; 4. virus attacks or hacker attacks in the Customer's IT environment affecting the System's availability. The Provider's liability and the Customer's sole compensation for errors or deficiencies shall be: rectification of errors or deficiencies, or in the case of significant errors or deficiencies. The Provider is not liable for production losses, lost profits, third-party damage, or other indirect losses.

11. Tiekėjo teisė sustabdyti Užsakovo prieigą ir susigrąžinti Sistemą Tiekėjas turi teisę sustabdyti Užsakovo prieigą prie Sistemos arba sustabdyti Paslaugų teikimą ir susigrąžinti Sistemą, jei Užsakovas netinkamai naudoja Paslaugas / Sistemą ir tai gali pakenkti Tiekėjui, iš esmės pažeidžia Tiekėjo politiką ar vertybes, arba kitaip reikšmingai kenkia Tiekėjo interesams. Ši teisė gali būti įgyvendinama tik tuo atveju, jei Tiekėjas raštu informuoja Užsakovą apie būtinybę ištaisyti situaciją ir įspėja, kad prieiga bus sustabdyta, jei problema nebus išspręsta per 14 (keturiolika) kalendorinių dienų. Tiekėjas taip pat pasilieka teisę sustabdyti arba visiškai nutraukti paslaugų teikimą, dėl aukščiau šiame punkte nurodytų priežasčių.	11. The Provider's Right to Suspend the Customer and Retrieve the System The Provider has the right to suspend the Customer's access to the System or halt the provision of Services and retrieve the System if the Customer misuses the Services/System in a manner that could harm the Provider, materially breaches the Provider's policy or values, or otherwise seriously conflicts with the Provider's interests. This right is subject to the Provider notifying the Customer to rectify the situation in writing and providing a warning that suspension will occur if the issue is not rectified within 14 calendar days, and if the Customer does not rectify the issue within the specified time frame. The Provider also reserves the right to pause or entirely discontinue work for the same reasons as stated above.
12. Konfidencialumas Tiekėjas įsipareigoja laikytis kiekvieno Užsakovo pateiktų konfidencialumo nuostatų. Kitais atvejais Šalys įsipareigoja neribotą laiką neatskleisti pašaliniams asmenims jokios konfidencialios informacijos apie kiekvienos Šalies veiklą ir neskelbtinos informacijos apie Sistemą, kuri galėtų pakenkti Tiekėjui. Šiame kontekste „konfidenciali informacija“ apibrėžiama kaip bet kokia dokumentuota ar nedokumentuota techninė, komercinė ar kitokio pobūdžio informacija, išskyrus informaciją, kuri yra viešai žinoma ar tampa viešai žinoma kitais būdais nepažeidžiant šios nuostatos.	12. Confidentiality The Provider commits to following the confidentiality provisions communicated by each Customer. Otherwise, the parties undertake, without limitation in time, not to disclose to outsiders any confidential information regarding each party's operations and sensitive information about the System that could harm the Provider. "Confidential information" in this context refers to any information - technical, commercial, or of another nature - whether documented or not, except for information that is or becomes publicly known or is otherwise known through means other than a breach of this provision.

13. Sąlygų pakeitimai Tiekėjas pasilieka teisę bet kuriuo metu vienašališkai keisti šias bendrąsias sąlygas. Apie tokius pakeitimus Užsakovas informuojamas raštu, siunčiant pranešimą paštu arba el. paštu, likus ne mažiau kaip dviem mėnesiams iki pakeistų sąlygų įsigaliojimo. Jei Užsakovas pateikia raštišką pranešimą apie nesutikimą su bendrųjų sąlygų pakeitimais iki jų įsigaliojimo, Šalių sudaryta sutartis laikoma nutraukta praėjus 1 mėnesiui nuo raštiško Užsakovo pranešimo apie nesutikimą pateikimo. Įspėjimo laikotarpiu galioja ankstesnė bendrųjų sąlygų redakcija. Jei Užsakovas raštu nepateikia pranešimo dėl nesutikimo su pakeitimais, laikoma, kad Užsakovas sutinka su naujomis bendrosiomis sąlygomis, ir jos įsigalioja nuo Tiekėjo nurodytos datos.	13. Changes to the Terms The Provider unilaterally reserves the right to modify these general terms and conditions at any time. Such changes shall be communicated in writing to the Customer by mail or email at least two months before the amended terms take effect. In the event that the Customer opposes the adjustments to the general terms and conditions in writing before the changes take effect, the agreement between the parties shall instead terminate with a notice period of one month from the Customer's written statement of non-acceptance. During the notice period, the previous version of the general terms and conditions shall apply. If the Customer does not oppose the adjustment in writing, the new general terms and conditions shall be deemed accepted and effective from the date specified by the Provider.
14. Sutarties galiojimo trukmė ir nutraukimas Ši sutartis ir jos sąlygos įsigalioja, kai Užsakovas pasirašo ir pateikia užsakymą arba bet kokio kito tipo susitarimą, kuriame nurodytos šios bendrosios sąlygos. Sutartis galioja 3 (tris) mėnesius nuo jos įsigaliojimo dienos ir yra skirta bandomajam laikotarpiui. Pasibaigus bandomajam laikotarpiui, ši sutartis automatiškai netenka galios. Licencijos nutraukimo atveju turi būti suplanuotas bendras susitikimas, skirtas Užsakovo asmens duomenų tvarkymo klausimams spręsti nutraukimo proceso metu.	14. Duration of Agreement and Termination This agreement and terms become effective when the Customer signs and submits an order or any other type of agreement referring to these general terms and conditions. Unless otherwise agreed, the agreement is valid for 3 (three) months from the date of its entry into force and shall be for a trial period. Upon the expiration of the trial period, this Agreement shall automatically terminate. To terminate the license, a joint meeting for handling Customer's personal data shall be scheduled in connection with the termination.

Be to, kas nurodyta šioje sutartyje, kiekviena Šalis turi teisę nedelsiant nutraukti šią sutartį, jei kita Šalis: a) padaro esminį sutarties pažeidimą ir nepašalina jo per 10 (dešimt) dienų nuo kitos šalies pateikto rašytinio pranešimo apie pažeidimą arba b) inicijuoja likvidavimo procedūras, pateikia prašymą dėl bankroto, yra paskelbiama bankrutavusia, sustabdo mokėjimus arba bet kokiu kitu būdu tampa akivaizdžiai nemoki. Nutraukus sutartį, Užsakovas privalo nedelsdamas nustoti naudotis Sistema. Jei sutarties galiojimo laikotarpiu buvo pateikta medžiaga ar dokumentai, kuriuose yra konfidencialios informacijos, tokia medžiaga ar dokumentai turi būti grąžinti kitai Šaliai nedelsiant po sutarties nutraukimo.	In addition to what is stated in this agreement, each party has the right to terminate this agreement with immediate effect if the counterparty: a) commits a material breach of the agreement and fails to rectify it within 10 days from the other party's written notice of the breach, or b) initiates liquidation proceedings, applies for or is declared bankrupt, suspends payments, or in any other way is likely to be insolvent. Upon termination of the agreement, the Customer must immediately cease using the System. If materials or documentation containing confidential information have been provided during the agreement period, such material or documentation must be returned to the counterparty immediately after termination.
15. Perdavimas Šalys neturi teisės perduoti sutarties ar iš jos kylančių teisių ar įsipareigojimų be raštiško kitos Šalies sutikimo.	15. Assignment The parties do not have the right to assign the agreement or any rights or obligations arising therefrom without the written consent of the other party.
16. Nenugalima jėga (*Force Majeure*) Šalis atleidžiama nuo atsakomybės dėl netinkamo šioje Sutartyje numatytų įsipareigojimų vykdymo ar visiško jų nevykdymo, jeigu jie neįvykdomi dėl nuo Šalies nepriklausančių aplinkybių (force majeure). Kai tik tokios aplinkybės išnyksta, įsipareigojimai turi būti įvykdyti pagal sutartas sąlygas. Nenugalimos jėgos aplinkybėmis laikomi karas, karo veiksmai, valdžios institucijų veiksmai ar neveikimas, nauji arba	16. Force Majeure A party is exempt from the consequences of failing to fulfill certain obligations under this agreement if the failure is due to circumstances beyond the party's control that prevent performance thereof. As soon as the obstacle ceases, the obligation shall be fulfilled in accordance with the agreed-upon manner. War, acts of war, governmental actions or omissions, new or changed legislation, labor conflicts, natural disasters, pandemics, third-party actions or omissions or other deficiencies

pakeisti teisės aktai, darbo konfliktai, gamtos stichijos, pandemijos, trečiųjų šalių veiksmai ar neveikimas, įskaitant, bet neapsiribojant, energijos tiekimo trūkumais, duomenų komunikacijos sutrikimais arba ribota interneto prieiga, atsirandančiais dėl virusų ar programišių atakų, ar panašių įvykių, taip pat kitos lygiavertės aplinkybės. Šalis, ketinanti pasinaudoti aukščiau nurodytu atleidimu nuo atsakomybės dėl nenugalimos jėgos (force majeure) aplinkybių, privalo nedelsdama raštu informuoti kitą Šalį apie tokių aplinkybių buvimą ir jų įtaką įsipareigojimų vykdymui. Nepaisant aukščiau išdėstytų nuostatų dėl atleidimo nuo atsakomybės, kiekviena Šalis turi teisę nedelsiant nutraukti sutartį, jei konkretų įsipareigojimą vėluojama vykdyti daugiau kaip tris mėnesius.	attributable to third parties, including but not limited to lack of energy supplies, data communication deficiencies, or other deficiencies in internet availability due to virus or hacker attacks or similar events, or equivalent circumstances, are considered exempting circumstances. A party wishing to claim exemption under the first paragraph above shall promptly notify the other party thereof. Regardless of what is stated above regarding exemption from consequences, a party has the right to terminate the agreement with immediate effect if the fulfillment of a specific obligation is delayed by more than three months.
17. Asmens duomenys Tam tikrų asmens duomenų, kuriuos Tiekėjas tvarko vykdydamas šią sutartį, atveju Užsakovas yra duomenų valdytojas, o Tiekėjas – duomenų tvarkytojas. Tokiam duomenų tvarkymui taikomas Šalių sudarytas atskiras duomenų tvarkymo susitarimas.	17. Personal Data For certain personal data that the Provider processes in connection with the performance of this agreement, the Customer is the data controller and the Provider is the data processor. In relation to such processing, the separate data processing agreement entered into by the parties applies.
18. Ginčai Iš šios sutarties kylančius ginčus galutinai sprendžia abi Šalys derybų keliu.	18. Dispute Any disputes and disagreements arising out of or related to this Agreement shall be resolved by negotiation between the Parties.
19. PRIEDAI 19.1. Priedas Nr. 1 Techninė specifikacija;	19. ANNEXES TO THE CONTRACT 19.1. Annex 1 “Technical Specification”;

19.2. Priedas Nr. 2 Asmens duomenų tvarkymo susitarimas; 19.3. Priedas Nr. 3 Susitarimas dėl taikomų organizacinių ir techninių kibernetinio saugumo reikalavimų.	19.2. Annex 2 "Arrangement on processing of personal data"; 19.3. Annex 3 Arrangement on applicable organisational and technical cybersecurity requirements.

Paslaugų viešojo pirkimo–pardavimo
sutarties specialiosios dalies
Priedas Nr. 1

TECHNINĖ SPECIFIKACIJA			
1.	**Sąvokos**		
1.1. **Užsakovas** – Valstybės įmonė Registrų centras (toliau – Registrų centras; Perkančioji organizacija). 1.2. **Tiekėjas** – ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Perkančioji organizacija sudaro sutartį.			
2.	**Bendrosios nuostatos**		
Jeigu šioje techninėje specifikacijoje nurodomas konkretus modelis ar tiekimo šaltinis, konkretus procesas, būdingas konkretaus tiekėjo tiekiamoms prekėms ar teikiamoms paslaugoms, ar prekių ženklas, patentas, tipai, konkreti kilmė ar gamyba, standartai, sertifikatai dėl kurių tam tikriems subjektams ar tam tikriems produktams būtų sudarytos palankesnės sąlygos arba jie būtų atmesti, gali būti pateikiamas lygiavertis objektas nurodytajam. Pateikti minimalūs reikalavimai. Tiekėjai gali siūlyti geresnių charakteristikų pirkimo objektą.			
3.	**Pirkimo objektas**	Prieiga prie Sysarb platformos	
4.	**Pirkimo objekto apimtys (kiekiai)**	1	komplektas
5.	**Techniniai reikalavimai pirkimo objektui**		
	5.1. Turi būti suteikta prieiga prie Sysarb platformos, skirtos darbo užmokesčio skaidrumui ir lygybei užtikrinti. 5.2. Galimybė sukelti Registrų centro darbuotojų atlygio duomenis į SYSARB platformą (duomenis sukels Registrų centro darbuotojai). 5.3. Galimybė dirbtinio intelekto įrankio pagalba atlikti detalią įmonės atlygio duomenų analizę, vadovaujantis pareigybių lygiais, žemėlapiu ir aprašymais, siekiant užtikrinti vienodą atlyginimą už vienodą darbą. 5.4. Platformoje turi būti prieinamos vidinio teisingumo analizei skirtos ataskaitos. 5.5. Tiekėjas privalo užtikrinti atitiktį tarptautiniams duomenų apsaugos ir kibernetinio saugumo standartams.		
6.	**Paslaugų teikimo vieta**	Nuotoliniu	
7.	**Paslaugų teikimo terminas**	Paslaugos turi būti suteiktos ne vėliau kaip per 3 mėnesius nuo sutarties įsigaliojimo dienos.	
8	**Paslaugų teikimo termino pratęsimas ir sąlygos**	-	
9.	**Atsiskaitymo tvarka**	Paslaugos teikiamos neatlygintinai	
10.	**Kokybė ir trūkumų pašalinimas**	Paslaugų kokybė turi atitikti tokio pobūdžio paslaugoms taikomus teisės aktų reikalavimus.	
11.	**Garantija**	-	
12.	**Žalieji reikalavimai**	12.1. Perkamos nematerialaus pobūdžio paslaugos, nesusijusios su materialaus objekto sukūrimu, kurių teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos.	
13.	**Paslaugų teikimo metu pateikiami dokumentai**	-	

Annex No 1
to the Special Part of the Contract for the
Public Procurement-Sale of services

<table>
<tr><th colspan="4">TECHNICAL SPECIFICATION</th></tr>
<tr><td>1.</td><td colspan="3">Definitions</td></tr>
<tr><td colspan="4">1.3. The Customer – The State Enterprise Centre of Registers (hereinafter referred to as the Customer).
1.4. The Provider – private legal entity, public legal entity, other organizations and their divisions, or a group of such persons, with whom the Contracting Authority enters into a public procurement contract.</td></tr>
<tr><td>2.</td><td colspan="3">General provisions</td></tr>
<tr><td colspan="4">If this technical specification indicates a specific model or source of supply, a specific process characteristic of goods or services provided by a particular supplier, or a trademark, patent, types, specific origin or production, standards, or certificates, which may favor certain entities or products or exclude others, an equivalent object to the one specified may be offered. The minimum requirements are provided. Suppliers may propose a procurement object with better characteristics.</td></tr>
<tr><td>3.</td><td>Procurement object</td><td colspan="2">Access to the Sysarb platform</td></tr>
<tr><td>4.</td><td>Scope (quantities) of the procurement object</td><td>1</td><td>unit</td></tr>
<tr><td>5.</td><td colspan="3">Technical requirements for the procurement object</td></tr>
<tr><td></td><td colspan="3">5.1. Access to the Sysarb platform must be provided, aimed at ensuring pay transparency and equality.
5.2. The ability to upload the Centre of Registers’ employee remuneration data to the Sysarb platform (data will be uploaded by the Centre of Registers’ employees).
5.3. The ability to perform a detailed analysis of the company’s remuneration data, based on job levels, mapping, and descriptions, to ensure equal pay for equal work.
5.4. The platform must include reports dedicated to internal fairness analysis.
5.5. The Provider shall ensure compliance with international data protection and cybersecurity standards.</td></tr>
<tr><td>6.</td><td>Service provision location</td><td colspan="2">Remotely</td></tr>
<tr><td>7.</td><td>Service provision period</td><td colspan="2">The Agreement shall be valid for a period of three (3) months from the date of its entry into force and shall be for a trial period.</td></tr>
<tr><td>8</td><td>Extension of the period of service and conditions</td><td colspan="2">-</td></tr>
<tr><td>9.</td><td>Payment terms</td><td colspan="2">The services are provided free of charge</td></tr>
<tr><td>10.</td><td>Quality and defect elimination</td><td colspan="2">The quality of the service must comply with the legal requirements applicable to this type of service.</td></tr>
<tr><td>11.</td><td>Warranty</td><td colspan="2">-</td></tr>
<tr><td>12.</td><td>The green requirements</td><td colspan="2">12.1. The procured services are of a non-material nature, unrelated to the creation of a physical object, during which no significant negative impact on the environment is anticipated, no sources of pollution are created, and no waste is generated.</td></tr>
</table>

Paslaugų viešojo pirkimo-pardavimo sutarties
specialiosios dalies
Priedas Nr. 2

SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO

BENDROJI DALIS

1. SĄVOKOS

1.1. **Asmens duomenys** – Specialiojoje dalyje nurodyti asmens duomenys, kuriuos Duomenų valdytojas suteikia teisę tvarkyti Duomenų tvarkytojui Specialiojoje dalyje nustatytu tikslu ir terminu.

1.2. **Duomenų tvarkytojas** – Specialiojoje dalyje nurodytas paslaugas teikiantis fizinis arba juridinis asmuo.

1.3. **Duomenų valdytojas** – valstybės įmonė Registrų centras, veikiantis kaip duomenų valdytojas arba duomenų valdytoją, nurodytą Specialiojoje dalyje, atstovaujantis duomenų tvarkytojas.

1.4. **JIRA** – programinis įrankis, skirtas projekto, produkto bei programinės įrangos kūrimo, priežiūros užduotims ir resursams valdyti.

1.5. **Konfidencialumo pasižadėjimas** – Duomenų valdytojo nustatytos formos pasižadėjimas saugoti valstybės įmonės Registrų centro tvarkomų duomenų paslaptį ir laikytis duomenų saugos reikalavimų, kurį pasirašo Duomenų tvarkytojo įgalioti asmenys, prieš pradedant tvarkyti asmens duomenis.

1.6. **Reglamentas (ES) 2016/679** – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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).

1.7. **Paslaugų teikimo sutartis** – Specialiojoje dalyje nurodyta tarp Paslaugos teikėjo ir Paslaugos gavėjo pasirašyta sutartis dėl paslaugų teikimo, kurios pagrindu yra sudarytas Susitarimas, kaip sudėtinė jos dalis.

1.8. **Paslaugos gavėjas** – valstybės įmonė Registrų centras.

1.9. **Paslaugos teikėjas** – Specialiojoje dalyje nurodytas paslaugas teikiantis fizinis arba juridinis asmuo.

1.10. **Susitarimas** – sudėtinė Paslaugų teikimo sutarties dalis, sudaryta iš Bendrosios ir Specialios dalies, kuriame vadovaujantis Reglamento (ES) 2016/679 28 straipsniu, nustatomos duomenų valdytojo ir duomenų tvarkytojo teisės bei pareigos, duomenų valdytojo vardu tvarkant asmens duomenis.

1.11. **Bendroji dalis** – Susitarimo dalis, kuri nustato bendrąsias asmens duomenų tvarkymo sąlygas, taikomas Susitarimo Šalims.

1.12. **Specialioji dalis** – Susitarimo dalis, kurioje nustatomos konkrečiam Duomenų tvarkytojui taikomos specialios asmens duomenų tvarkymo sąlygos.

1.13. **Šalys** – Duomenų valdytojas ir Duomenų tvarkytojas abu kartu.

2. SUSITARIMO DALYKAS

2.1. Duomenų valdytojas paveda Duomenų tvarkytojui tvarkyti asmens duomenis Susitarime nustatytomis sąlygomis.

3. ŠALIŲ TEISĖS IR PAREIGOS

3.1. Duomenų valdytojas:

3.1.1. privalo užtikrinti, kad asmens duomenų tvarkymas, kurį Duomenų tvarkytojui pavesta atlikti, turėtų teisinį pagrindą;

3.1.2. be Susitarimu nustatytų nurodymų dėl asmens duomenų tvarkymo, turi teisę teikti dokumentais įformintus nurodymus viso asmens duomenų tvarkymo metu. Tokie nurodymai gali būti teikiami raštu Specialiosios dalies 2 punkte nurodytu Duomenų tvarkytojo buveinės adresu, arba elektroniniu paštu, arba registruojami JIRA (kai yra suteiktos prieigos teisės Duomenų tvarkytojo įgaliotiems asmenims);

3.1.3. turi teisę papildomai ir (ar) kitomis nei 3.2.9 papunktyje nurodytomis priemonėmis patikrinti, kaip Duomenų tvarkytojas tvarko asmens duomenis ir (arba) vykdo savo įsipareigojimus pagal šį Susitarimą, toks patikrinimas gali būti atliekamas Šalims susitarus dėl patikrinimo apimties, būdo, kainos ir laiko. Duomenų valdytojas turi teisę papildomam patikrinimui atlikti pasitelkti nepriklausomą auditorių. Bet kuriuo atveju, jeigu Šalys susitaria dėl tokio papildomo patikrinimo, jis turės atitikti šiuos reikalavimus:

3.1.3.1. patikrinimas privalo būti susijęs tik su asmens duomenų tvarkymu pagal Susitarimą;

3.1.3.2. Duomenų valdytojas privalo informuoti Duomenų tvarkytoją apie pageidavimą atlikti papildomą patikrinimą per protingą laiką, kuris privalo būti ne trumpesnis nei 5 darbo dienos;

3.1.3.3. papildomas patikrinimas turi būti atliekamas taip, kad netrukdytų įprastinei Duomenų tvarkytojo veiklai;

3.1.3.4. tuo atveju, jei patikrinimo metu gali būti susipažinta su Duomenų tvarkytojo konfidencialia informacija, Duomenų tvarkytojui pareikalavus, Duomenų valdytojas įsipareigoja saugoti Duomenų tvarkytojo konfidencialią informaciją.

3.2. Duomenų tvarkytojas:

3.2.1. tvarko asmens duomenis pagal Duomenų valdytojo nurodymus, išdėstytus Susitarime, ir kitus raštu (įskaitant elektronine forma) Duomenų valdytojo įformintus nurodymus, išskyrus atvejus, kai duomenis tvarkyti reikalaujama pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurie yra taikomi Duomenų tvarkytojui (tokiais atvejais Duomenų tvarkytojas informuoja Duomenų valdytoją apie šiuos reikalavimus, išskyrus atvejus, kai teisės aktais draudžiama minėtą informaciją pateikti dėl svarbaus viešojo intereso);

3.2.2. užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą ir būtų pasirašę Registrų centro pateiktos formos Konfidencialumo pasižadėjimą;

3.2.3. imasi visų priemonių, kurių reikalaujama pagal Reglamento (ES) 2016/679 32 straipsnį, t. y. techninėmis ir organizacinėmis priemonėmis užtikrina Duomenų valdytojo vardu tvarkomų asmens duomenų saugą, konfidencialumą, vientisumą ir prieinamumą, apsaugą nuo netyčinio arba neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų ir nuo bet kokio kito neteisėto tvarkymo, taip pat saugų duomenų perdavimą kompiuteriniais tinklais. Saugumo priemonės, kurias privalo įgyvendinti Duomenų tvarkytojas, nurodytos Susitarimo Specialiosios dalies 6 punkte „Nurodymai dėl asmens duomenų tvarkymo saugumo“, o taip pat, priklausomai nuo jų tinkamumo pagal asmens duomenų tvarkymo pobūdį, įskaitant bet neapsiribojant, saugumo priemonės turi būti šios:

3.2.3.1. asmens duomenų pseudonimizavimas ir (ar) šifravimas;

3.2.3.2. galimybė užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

3.2.3.3. galimybė laiku atkurti prieinamumą ir prieigą prie asmens duomenų, įvykus fiziniam ar techniniam incidentui;

3.2.3.4. techninių ir organizacinių priemonių, užtikrinančių duomenų tvarkymo saugumą, reguliaraus testavimo, tikrinimo ir įvertinimo procesas;

3.2.4. užtikrina, kad konkrečiai duomenų tvarkymo veiklai Duomenų valdytojo vardu atlikti pasitelks pagalbinį duomenų tvarkytoją tik turėdamas Specialiojoje dalyje įvardintą Duomenų valdytojo leidimą, o pasitelktam pagalbiniam duomenų tvarkytojui bus nustatytos tos pačios duomenų apsaugos prievolės, nurodytos šiame Susitarime;

3.2.5. atsižvelgdamas į duomenų tvarkymo pobūdį, padeda Duomenų valdytojui taikydamas tinkamas technines ir organizacines priemones, kiek tai įmanoma, kad būtų įvykdyta Duomenų valdytojo prievolė atsakyti į prašymus pasinaudoti Reglamente (ES) 2016/679 nustatytomis duomenų subjekto teisėmis. Jeigu Duomenų tvarkytojas gauna duomenų subjekto prašymą dėl Reglamento (ES) 2016/679 12-22 straipsniuose nustatytų duomenų subjekto teisių įgyvendinimo, privalo šį prašymą nedelsiant, bet ne vėliau kaip per 3 darbo dienas persiųsti Duomenų valdytojui elektroniniu paštu nurodytu Specialiosios dalies 7 punkte;

3.2.6. padeda Duomenų valdytojui užtikrinti Reglamento (ES) 2016/679 32–36 straipsniuose nustatytų prievolių laikymąsi, atsižvelgdamas į duomenų tvarkymo pobūdį ir turimą informaciją:

3.2.6.1. ne vėliau kaip per 24 valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento raštu Specialiosios dalies 7 punkte nurodytais adresais, informuoja Duomenų valdytoją apie įvykusį tvarkomų asmens duomenų saugumo pažeidimą ir pateikia pranešimą, jame nurodydamas Reglamento (ES) 2016/679 33 straipsnio 3 dalyje išvardytą informaciją bei imasi priemonių pažeidimui nedelsiant sustabdyti ir užkertančių kelią tolesnei žalai dėl įvykusio asmens duomenų saugumo pažeidimo bei mažinančių įvykusio asmens duomenų saugumo pažeidimo padarinius. Jeigu visos informacijos neįmanoma pateikti tuo pačiu metu, informacija toliau nedelsiant turi būti teikiama etapais. Duomenų valdytojo prašymu per nurodytą laikotarpį Duomenų tvarkytojas pateikia papildomą informaciją, reikalingą Duomenų valdytojui vertinant asmens duomenų saugumo pažeidimo aplinkybes, įskaitant, bet neapsiribojant, Duomenų tvarkytojo asmens duomenų saugumo pažeidimų žurnalo išrašą;

3.2.6.2. gavęs Duomenų valdytojo prašymą, per Duomenų valdytojo nurodytą terminą pateikia informaciją, kuri Duomenų valdytojui būtina atliekant poveikio duomenų apsaugai vertinimą, vadovaujantis Reglamento (ES) 2016/679 35 straipsniu, įskaitant informacijos pateikimą, kai Duomenų valdytojas priima sprendimą kreiptis į Valstybinę duomenų apsaugos inspekciją dėl išankstinių konsultacijų;

3.2.7. užbaigęs teikti su duomenų tvarkymu susijusias paslaugas, atsižvelgdamas į asmens Duomenų valdytojo nurodymus, pateiktus Specialiojoje dalyje, ištrina arba grąžina Duomenų valdytojui visus asmens duomenis ir ištrina esamas jų kopijas, išskyrus atvejus, kai Europos Sąjungos ar Lietuvos Respublikos teisės aktai nustato Duomenų tvarkytojo pareigą asmens duomenis saugoti. Jei Duomenų tvarkytojui taikoma prievolė pagal teisės aktus saugoti asmens duomenis, Duomenų tvarkytojas, prieš pradėdamas tvarkyti asmens duomenis Duomenų valdytojo vardu, Specialiojoje dalyje privalo nurodyti jam taikomus teisės aktus, kuriais jis yra įpareigotas saugoti asmens duomenis;

3.2.8. įsipareigoja nekopijuoti, neperkelti, nesaugoti ir kitaip netvarkyti asmens duomenų Duomenų tvarkytojo IT infrastruktūroje, kai pagal Duomenų valdytojo Specialiojoje dalyje pateiktus nurodymus nustatyta, kad asmens duomenys tvarkomi tik Duomenų valdytojo IT infrastruktūroje;

3.2.9. įsipareigoja periodiškai savo iniciatyva ir sąskaita tikrinti, ar atitinkamos techninės ir organizacinės priemonės atitinka duomenų tvarkymo pobūdį, apimtį, kontekstą ir tikslus, o taip pat riziką, susijusią su duomenų tvarkymu, fizinių asmenų teisių ir laisvių atžvilgiu. Duomenų tvarkytojas šį tikrinimą gali atlikti pats arba pasitelkti nepriklausomą auditorių. Duomenų valdytojo rašytiniu

prašymu tikrinimo ataskaitą arba jos ištrauką, Duomenų tvarkytojas privalo pateikti Duomenų valdytojui;

3.2.10. jei Duomenų valdytojas nenurodo Susitarime arba vėliau nepateikia dokumentais pagrįstų nurodymų dėl asmens duomenų perdavimo į trečiąją valstybę ar tarptautinėms organizacijoms, Duomenų tvarkytojas neturi teisės atlikti tokį perdavimą pagal šį Susitarimą, išskyrus, jei asmens duomenis trečiosioms valstybėms ar tarptautinėms organizacijoms reikia perduoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurių turi laikytis Duomenų tvarkytojas, nors Duomenų valdytojas nedavė nurodymų Duomenų tvarkytojui tai atlikti. Tokiu atveju, apie šį teisinį reikalavimą Duomenų tvarkytojas informuoja Duomenų valdytoją, Specialiojoje dalyje nurodydamas jam taikomus teisės aktus, kuriais jis yra įpareigotas perduoti asmens duomenis į trečiąją valstybę ar tarptautinėms organizacijoms, nebent tas teisės aktas draudžia perduoti tokią informaciją;

3.2.11. turėdamas pagrįstų įrodymų, kad Duomenų valdytojo nurodymu gali būti pažeidžiami teisės aktai, turi teisę sustabdyti tokio nurodymo vykdymą prieš tai raštu Specialiosios dalies 7 punkte nurodytais adresais informavęs Duomenų valdytoją. Duomenų valdytojui įrodžius nurodymo atitiktį teisės aktams arba iš dalies jį pakeitus, nurodymas turi būti vykdomas.

4. ATSAKOMYBĖ

4.1. Duomenų valdytojas yra atsakingas už tai, kad jo duodami nurodymai Duomenų tvarkytojui dėl asmens duomenų tvarkymo atitiktų Reglamento (ES) 2016/679 reikalavimus.

4.2. Duomenų tvarkytojas yra atsakingas už tai, kad tvarkytų Duomenų valdytojo pateiktus asmens duomenis, laikydamasis šio Susitarimo ir Duomenų valdytojo nurodymų.

4.3. Jei pasitelktas kitas duomenų tvarkytojas nevykdo arba netinkamai vykdo asmens duomenų apsaugos prievoles, Duomenų tvarkytojas išlieka visiškai atsakingas Duomenų valdytojui už pasitelkto kito duomenų tvarkytojo prievolių vykdymą.

4.4. Susitarimo sąlygos neatleidžia Šalių nuo kitų pareigų, kurios joms taikomos pagal Reglamentą (ES) 2016/679 ar kitus teisės aktus.

5. BAIGIAMOSIOS NUOSTATOS

5.1. Susitarimas įsigalioja nuo jo pasirašymo dienos ir galioja iki Paslaugų teikimo sutarties galiojimo dienos.

5.2. Bet kokie nesutarimai ar ginčai, kylantys tarp Šalių dėl Susitarimo, sprendžiami derybų būdu, o jeigu tokiu būdu ginčų išspręsti nepavyksta, jie sprendžiami Lietuvos Respublikos teisme pagal Duomenų valdytojo registruotos buveinės vietą, vadovaujantis Lietuvos Respublikoje galiojančiais įstatymais ar kitais teisės aktais.

SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO

SPECIALIOJI DALIS

1. Duomenų valdytojas (Paslaugos gavėjas):

Valstybės įmonė Registrų centras, juridinio asmens kodas 124110246, kurios registruota buveinė yra Studentų g. 39, Vilnius, telefono ryšio numeris +370 5 268 8262, elektroninio pašto adresas info@registrucentras.lt

2. Duomenų tvarkytojas (Paslaugos teikėjas):

Sysarb AB, juridinio asmens kodas 556681-8828, Järntorget 12 C, 732 30 Arboga, Sweden, +46 589-501 60, support@sysarb.com

3. Paslaugų teikimo sutartis:

Prieiga prie Sysarb platformos

4. Nuostatos apie asmens duomenų tvarkymą:

Asmens duomenų tvarkymo tikslas	Galimybė atlikti detalią įmonės atlygio duomenų analizę dirbtinio intelekto įrankio pagalba
Asmens duomenų tvarkymo pobūdis ir duomenų tvarkymo operacijos	Darbo užmokesčio lygybės platformos testavimas; operacijos - duomenų įvedimas, ištrynimas, struktūrizavimas, keitimas.
Asmens duomenų subjektų kategorijos	Darbuotojai
Tvarkomų asmens duomenų rūšys	Darbuotojo vardas ir pavardė, padalinys, pareigybės pavadinimas, pareigybės lygis, darbo užmokestis
Asmens duomenų tvarkymo vieta	Sysarb’s serveriai yra patalpinti Glesys AB: Kanslistvägen 12, 311 39 Falkenberg, Sweden
Asmens duomenų tvarkymo trukmė	Iki paslaugų sutarties pabaigos
Leidimas pasitelkti kitą duomenų tvarkytoją, kuris bus pasitelkiamas po Susitarimo pasirašymo	Duomenų tvarkytojas gali pasitelkti kitą duomenų tvarkytoją tik turėdamas išankstinį konkretų Duomenų valdytojo leidimą. Apie planuojamą pasitelkti kitą duomenų tvarkytoją Duomenų tvarkytojas informuoja Duomenų valdytoją oficialiu raštu Specialiosios dalies 7 punkte nurodytu adresu, ne vėliau kaip prieš 20 darbo dienų iki planuojamo pasitelkimo, o Duomenų valdytojas per 10 darbo dienų raštu Specialiosios dalies 2 punkte nurodytais kontaktais (raštas siunčiamas paštu arba elektroniniu paštu) pateikia Duomenų tvarkytojui leidimą arba nesutikimą.

Duomenų valdytojo nurodymai dėl asmens duomenų ištrynimo arba grąžinimo, pabaigus tvarkyti duomenis	Nutraukus paslaugų teikimą, Duomenų tvarkytojas, kuris tvarkė Duomenų valdytojo jam perduotus asmens duomenis, privalo juos nedelsiant, tačiau ne vėliau kaip per 2 darbo dienas, ištrinti ir, Duomenų valdytojui pareikalavus, patvirtinti tai raštu Specialiosios dalies 7 punkte nurodytu adresu per 5 darbo dienas nuo ištrynimo dienos, išskyrus atvejus, kai duomenis saugoti įpareigoja teisės aktai.
Duomenų tvarkytojo pareiškimai, pagrindžiami Europos Sąjungos ir (ar) Lietuvos Respublikos teisės aktais, dėl privalomo asmens duomenų saugojimo (jei toks taikomas Duomenų tvarkytojui)	-
Duomenų perdavimo į trečiąsias valstybes arba tarptautinėms organizacijoms sąlygos	Nebus perduodama

5. Informacija apie Susitarimo pasirašymo momentu pasitelktus kitus asmens duomenų tvarkytojus: ***(pildo Paslaugos teikėjas (Duomenų tvarkytojas)***

Pavadinimas, vardas, pavardė	Įmonės kodas / gimimo data arba individualios veiklos numeris	Buveinės adresas / gyvenamosios vietos adresas	Duomenų tvarkymo aprašymas
-	-	-	-

6. Nurodymai dėl asmens duomenų tvarkymo saugumo:

Duomenų tvarkymo saugumo priemonės	Duomenų tvarkytojas privalo laikytis Susitarimo dėl taikomų organizacinių ir techninių kibernetinio saugumo reikalavimų, kurie yra pateikti atskirame Paslaugų teikimo sutarties specialiosios dalies priede Nr. 3

7. Duomenų valdytojo kontaktai:

Pranešimas apie asmens duomenų saugumo pažeidimą	

Prašymai dėl Reglamento (ES) 2016/679 12-22 straipsniuose nustatytų duomenų subjekto teisių įgyvendinimo	
Pranešimas dėl leidimo pasitelkti pagalbinį duomenų tvarkytoją	
Kiti klausimai	

Annex No 2
to the Special Part of the Contract for the Public Procurement-Sale of services

ARRANGEMENT ON PROCESSING OF PERSONAL DATA

GENERAL PART

1. CONCEPTS AND DEFINITIONS

3.1. **Personal Data** means the personal data specified in the Special Part, which the Data Controller authorises the Data Processor to process for the purpose and within the time limit set out in the Special Part.

3.2. **Data Processor** means a natural person or legal entity providing the services referred to in the Special Part.

3.3. **Data Controller** means a State Enterprise Centre of Registers acting as a data controller or a data processor representing the data controller referred to in the Special Part.

3.4. **JIRA** means a software tool for managing project, product and software development, maintenance tasks and resources.

3.5. **Confidentiality Commitment** means a commitment in the form prescribed by the Data Controller to protect the secrecy of the data processed by the State Enterprise Centre of Registers and to comply with the data security requirements, which shall be signed by the authorised persons of the Data Processor prior to commencement of the processing of personal data.

3.6. **Regulation (EU) 2016/679** 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).

3.7. **Service Agreement** means an agreement for the provision of services signed between the Service Provider and the Service Recipient as specified in the Special Part, on the basis of which the Arrangement is concluded as an integral part thereof.

3.8. **Service Recipient** means the State Enterprise Centre of Registers.

3.9. **Service Provider** means a natural person or legal entity providing the services referred to in the Special Part.

3.10. **Arrangement** means an integral part of the Service Agreement, consisting of a General and Special Parts, which, in accordance with Article 28 of Regulation (EU) No 2016/679, establishes the rights and obligations of the Data Controller and the Data Processor with regard to the processing of personal data on behalf of the Data Controller.

3.11. **General Part** means the part of the Arrangement, which lays down general terms and conditions for the processing of personal data applicable to the Parties thereto.

3.12. **Special Part** means the part of the Arrangement, which lays down special terms and conditions for the processing of personal data applicable to a particular Data Processor.

3.13. **Parties** means the Data Controller and the Data Processor jointly.

4. SUBJECT-MATTER OF THE ARRANGEMENT

2.1. The Data Controller hereby shall entrust the Data processor with the processing of personal data under the terms and conditions laid down therein.

5. RIGHTS AND OBLIGATIONS OF THE PARTIES

5.3. Data Controller shall:

5.3.1. Be obliged to ensure that the processing of personal data entrusted to the Data Processor has a legal ground;

5.3.2. Have the right to provide documented instructions throughout the period of processing of personal data in addition to the instructions for the processing of personal data set out in the Arrangement. Such instructions may be provided in writing at the address of the registered office of the Data Processor referred to in point 2 of the Special Part, or by e-mail, or recorded in JIRA (where access rights have been granted to authorised persons of the Data Processor);

5.3.3. Have the right to verify, in addition to and/or by other means than those referred to in point 3.2.9, how the Data Processor is processing personal data and/or fulfils its obligations hereunder; such verification may be carried out when the Parties agree on the scope, manner, cost and time thereof. The Data Controller shall have the right to engage an independent auditor to carry out the additional verification. In any case, if the Parties agree on such additional verification, it shall have to meet the following requirements:

5.3.3.1. Verification must be related only to the processing of personal data under the Arrangement;

5.3.3.2. The Data Controller must inform the Data Processor of the request to carry out an additional verification within a reasonable period of time, which must be at least 5 working days;

5.3.3.3. The additional verification must be carried out in such a way that it does not interfere with the normal activities of the Data Processor;

5.3.3.4. In the event that confidential information of the Data Processor may be accessed during verification, the Data Controller undertakes to protect the confidential information of the Data Processor at the request of the Data Processor.

5.4. Data Processor shall:

5.4.1. Process personal data in accordance with the Data Controller's instructions set out hereunder and any other instructions provided in writing (including in an electronic form) by the Data Controller, except where processing of the data is required by the legislation of the European Union or a Member State of the European Union to which the Data Processor is subject (in which case the Data Processor shall inform the Data Controller of these requirements, except in cases where the legislation prohibits the provision of such information on the grounds of an overriding reason of public interest);

5.4.2. Ensure that persons authorised to process personal data are committed to confidentiality and have signed a Confidentiality Commitment in the form provided by the Centre of Registers;

5.4.3. Take all the measures required under Article 32 of Regulation (EU) 2016/679, i.e., ensure by technical and organisational means the security, confidentiality, integrity and accessibility of personal data processed on behalf of the Data Controller, protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access, and against any other unauthorised processing, as well as secure transmission of data over computer networks. The security measures to be implemented by the Data Processor, as set out in point 6 of the Special Part of the Arrangement 'Instructions on the security of the processing of personal data', as well as, depending on their appropriateness to the nature of the processing of personal data, shall be, including but not limited to:

5.4.3.1. Pseudonymisation and/or encryption of personal data;

5.4.3.2. Ability to ensure the continuous confidentiality, integrity, accessibility and resilience of data processing systems and services;

5.4.3.3. Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;

5.4.3.4. Process for regular testing, inspection and evaluation of technical and organisational measures ensuring the security of processing of personal data;

5.4.4. Ensure that it is going to engage a sub-processor to carry out specific processing activities on behalf of the Data Controller only with the permission of the Data Controller as set out in the Special Part, and that the sub-processor engaged is going to be subject to the same data protection obligations as set out in this Arrangement;

5.4.5. Given the nature of data processing, assist the Data Controller to the extent possible by applying appropriate technical and organisational measures to fulfil the obligation of the Data Controller to respond to requests to exercise the rights of the data subject set out in Regulation (EU) 2016/679. If the Data Processor receives a request from a data subject for the exercise of the data subject's rights set out in Articles 12-22 of Regulation (EU) 2016/679, it must forward the request to the Data Controller without delay, but at the latest within 3 working days, by the e-mail address referred to in point 7 of the Special Part;

5.4.6. Assist the Data Controller in ensuring compliance with the obligations laid down in Articles 32-36 of Regulation (EU) 2016/679, taking into account the nature of the data processing and the information available:

5.4.6.1. Not later than within 24 hours after a personal data breach has become apparent, inform the Data Controller in writing at the addresses indicated in point 7 of the Special Part of the personal data breach that has occurred and provide a notification, including the information listed in Article 33(3) of Regulation (EU) 2016/679, and take measures to immediately stop the breach and prevent further damage caused by the personal data breach as well as mitigate the consequences of the personal data breach. If it is not possible to provide all the information at the same time, the information must be provided in phases without delay. Upon request of the Data Controller, the Data Processor shall provide, within the specified period, additional information necessary for the Data Controller to assess the circumstances of the personal data breach, including, but not limited to, an extract from the Data Processor's personal data breach log;

5.4.6.2. Upon request of the Data Controller, provide, within a time limit specified by the Data Controller, the information necessary for the Data Controller to carry out a data protection impact assessment in accordance with Article 35 of Regulation (EU) 2016/679, including provision of information if the Data Controller decides to contact the State Data Protection Inspectorate for prior consultation;

5.4.7. After completing the provision of services related to data processing, and taking into account the instructions of the Data Controller provided for in the Special Part, delete or return to the Data Controller all personal data and delete existing copies thereof, except in cases where legislation of the European Union or the Republic of Lithuania stipulates the Data Processor's obligation to retain personal data. If the Data Processor is subject to a statutory obligation to retain personal data, the Data Processor shall, prior to processing of personal data on behalf of the Data Controller, indicate in the Special Part the applicable legislation under which the Data Processor is obliged to retain personal data;

5.4.8. Undertakes not to copy, transfer, store or otherwise process personal data in the Data Processor's IT infrastructure where, in accordance with the instructions provided by the Data Controller in the Special Part, it has been established that personal data shall be processed only in the Data Controller's IT infrastructure;

5.4.9. Undertakes to verify periodically, at its own initiative and expense, whether the respective technical and organisational measures are appropriate to the nature, scope, context and

purposes of the data processing, as well as to the risks associated with the data processing with respect to the rights and freedoms of natural persons. The Data Processor may carry out this verification itself or engage an independent auditor. Upon a written request of the Data Controller, the Data Processor must provide the Data Controller with an inspection report or an extract thereof;

5.4.10. If the Data Controller does not specify in the Arrangement or does not subsequently provide documented instructions for the transfer of personal data to a third country or to international organisations, the Data Processor shall not be entitled to carry out such transfer under this Arrangement unless the transfer of personal data to third countries or international organisations is required by the laws of the European Union or a Member State thereof, with which the Data Processor must comply, even though the Data Controller has not instructed the Data Processor to do so. In this case, the Data Processor shall inform the Data Controller of this legal requirement, indicating in the Special Part the legislation applicable to it, which obliges it to transfer personal data to a third country or to international organisations unless that legislation prohibits the transfer of such information;

5.4.11. Having reasonable grounds to believe that the Data Controller's instructions may infringe legal acts, shall have the right to suspend the execution of such instructions after having informed the Data Controller in writing at the addresses referred to in point 7 of the Special Part. Once the Data Controller has demonstrated conformity of instructions with the legislation or has amended them, the instructions shall be enforced.

6. RESPONSIBILITY

6.1. The Data Controller shall be responsible for ensuring that the instructions it provides to the Data Processor regarding the processing of personal data comply with the requirements of Regulation (EU) 2016/679.

6.2. The Data Processor shall be responsible for processing the personal data provided by the Data Controller in accordance with this Arrangement and the instructions of the Data Controller.

6.3. If a sub-processor engaged fails to fulfil or inadequately fulfils the personal data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the fulfilment of the obligations of the sub-processor engaged.

6.4. The terms and conditions of the Arrangement shall not exempt the Parties from any other obligations, to which they are subject under Regulation (EU) 2016/679 or other legislation.

7. FINAL PROVISIONS

7.1. The Arrangement shall come into force on the date of its signing and shall be valid until the expiry of the Service Agreement.

7.2. Any disagreements or disputes arising between the Parties in connection with the Arrangement shall be settled by means of negotiations, and if the Parties are unable to reach an agreement, they shall be settled in the court of the Republic of Lithuania according to the location of the registered office of the Data Controller pursuant to the laws or regulations in force in the Republic of Lithuania.

ARRANGEMENT ON PROCESSING OF PERSONAL DATA

SPECIAL PART

8. Data Controller (Service Recipient):

State Enterprise Centre of Registers, legal entity code 124110246, with registered office at Studentų St. 39, Vilnius, phone number +370 5 268 8262, e-mail address info@registrucentras.lt

9. Data Processor (Service Provider):

Sysarb AB, legal entity code 556681-8828, Järntorget 12 C, 732 30 Arboga, Sweden, +46 589-501 60, support@sysarb.com

10. Service Agreement:

Access to the Sysarb platform

11. Provisions on the processing of personal data:

Purpose of the processing of personal data	The ability to perform a detailed analysis of company compensation data using an artificial intelligence tool
Nature of the processing of personal data and processing operations	Testing of the pay equity platform; operations - data entry, deletion, structuring, modification.
Categories of personal data subjects	Employees
Types of personal data processed	Employee's first and last name, department, job title, job level, job family, salary
Place of the processing of personal data	Sysarb's servers are hosted by Glesys AB: Kanslistvägen 12, 311 39 Falkenberg, Sweden
Duration of the processing of personal data	Until the end of the service agreement
Permission to use a sub-processor who will be engaged after the signing of the Arrangement	The Data Processor may engage a sub-processor only with the prior specific permission of the Data Controller. The Data Processor shall inform the Data Controller about a sub-processor to be engaged by sending an official letter to the address specified in point 7 of the Special Part, no later than 20 working days before the planned engagement, and the Data Controller shall give the Data Processor the written permission or objection within 10 working days at the contacts specified in point 2 of the Special Part (the letter shall be sent by post or e-mail).
Instructions of the Data Controller for erasure or	Upon termination of the provision of services, the Data Processor that processed the personal data transferred to it by the Data

return of personal data after the end of processing	Controller, must delete the personal data immediately, but at the latest within 2 working days, and, at the request of the Data Controller, confirm it in writing to the address specified in point 7 of the Special Part, within 5 working days from the date of deletion, except in cases where the retention of data is required by legislation.
Statements by the Data Processor, based on the European Union and/or the Republic of Lithuania legislation regarding mandatory retention of personal data (if applicable to the Data Processor)	-
Conditions for the transfer of data to third countries or international organisations	Will not be transferred

12. Information about sub-processors engaged at the time of signing the Arrangement: ***(To be completed by the Service Provider (Data Processor)***

Company name, name, surname	Company code/date of birth or individual economic activity certificate number	Registered address/address of the place of residence	Description of data processing
-	-	-	-

13. Instructions on the security of personal data processing:

Data processing security measures	The Data Processor shall comply with the Arrangement on Applicable Organisational and Technical Cybersecurity Requirements, which are set out in a separate Annex No 3 to the Special Part of the Service Agreement.

14. Contact details of the Data Controller:

Personal data breach notification	
Requests for the exercise of the data subject's	

rights under Articles 12-22 of Regulation (EU) 2016/679	
Notification of the authorisation to engage a sub-processor	
Other issues	

Paslaugų viešojo pirkimo–pardavimo sutarties
specialiosios dalies
Priedas Nr. 3

SUSITARIMAS DĖL TAIKOMŲ ORGANIZACINIŲ IR TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ

Vykdydamas Paslaugų viešojo pirkimo–pardavimo sutartį (toliau – Sutartis), tiekėjas privalo užtikrinti tinkamą duomenų saugumo lygį, t. y. nuolatinį tvarkomų asmens duomenų konfidencialumą, vientisumą, prieinamumą ir duomenų tvarkymo IT sistemų atsparumą, ir, siekdamas šio tikslo, priimti tinkamus sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo. Jei tiekėjas aptarnauja kritinę informacinių ir ryšių technologijų (toliau – IRT) infrastruktūrą arba teikia kitas esmines Lietuvos Respublikos kibernetinio saugumo įstatymo 1 priede numatytas paslaugas Lietuvoje, jis laikosi Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo", reikalavimų, taikomų kibernetinio saugumo esminiam subjektui. Jeigu tai užsienio tiekėjas, kuris jam perduotus duomenis tvarko ne valstybės įmonės Registrų centro (toliau – Registrų centro) IRT infrastruktūroje, turi būti laikomasi tarptautinių, pavyzdžiui, ISO/IEC 27001, standartų reikalavimų arba kitų lygiaverčių standartų (NIST CSF, SOC 2 ir pan.).

Tiekėjas įsipareigoja užtikrinti toliau išvardintų organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimą:

1. Organizacinės duomenų tvarkymo saugumo priemonės	1.1. Sudarius Sutartį, tiekėjo paskirti darbuotojai, kurie teiks paslaugas pagal šią Sutartį ir jungsis prie Registrų centro IRT infrastruktūros, privalo susipažinti su informacinio ištekliaus valdytojo patvirtinta Kibernetinio saugumo politika ir ją įgyvendinančiais teisės aktais bei laikytis nustatytų reikalavimų. Tais atvejais, kai tiekėjui yra perduodama tvarkyti Registrų centro duomenis savo (tiekėjo) infrastruktūroje, tiekėjui būtina vadovautis tiekėjo organizacijoje patvirtinta informacijos ir (ar) kibernetinio saugumo politika. 1.2. Visą Sutarties galiojimo laikotarpį ir po jo privaloma užtikrinti perduodamos, saugomos ar kitais būdais tvarkomos informacijos konfidencialumą, o iki pradedant tokią informaciją tvarkyti, būtina raštiškai įsipareigoti saugoti tokio pobūdžio informaciją. 1.3. Privaloma užtikrinti gautų prisijungimo duomenų saugumą ir neatskleisti jų trečiosioms šalims. 1.4. Naudotojų teises galima suteikti, keisti ir (ar) panaikinti laikantis principo „Būtina žinoti" arba būtina užtikrinti, kad teisė prieiti prie informacijos būtų suteikta tik konkrečioms funkcijoms įvykdyti (darbui atlikti) ir (ar) konkrečiai apibrėžtam laikotarpiui. 1.5. Tiekėjas turi taikyti atitinkamas ir adekvačias teisių suteikimo ar pareigų atšaukimo, vaidmenų ir atsakomybių perdavimo ar perleidimo darbuotojo atleidimo bei jų funkcijų pasikeitimo atveju procedūras savo organizacijoje. 1.6. Tiekėjas turi užtikrinti, kad jo pasitelkti tiekėjai (subtiekėjai) atitiktų tuos pačius informacijos ir kibernetinio saugumo reikalavimus. 1.7. Tiekėjas turi nedelsiant informuoti Registrų centrą apie nutrūkusius darbo santykius su organizacijos darbuotoju, kuriam buvo suteikta

	prieiga prie Registrų centro IRT infrastruktūroje tvarkomos informacijos. 1.8. Tiekėjo pareiga nedelsiant informuoti apie Sutarties vykdymo metu Registrų centro IRT infrastruktūroje pastebėtus didelius ir (ar) kitus elektroninės informacijos saugos incidentus, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, informacijos saugumo reikalavimų nesilaikymą, nusikalstamos veikos požymius, aptiktas saugumo spragas (pažeidžiamumus), kurie kelia riziką kibernetinio saugumo subjekto tinklams ir informacinėms sistemoms, bei kitus svarbius saugai įvykius telefonu +370 5 268 8262 ar raštu, el. p. pagalba@registrucentras.lt. Taip pat būtina informuoti Registrų centrą, bet ne vėliau kaip per 24 val., kai tiekėjo valdomoje informacinių sistemų infrastruktūroje buvo nustatyti minėti atvejai, kurie turi įtakos Registrų centro tvarkomiems duomenims. Tiekėjas privalo Registrų centrui pateikti kibernetinio incidento tyrimo ataskaitą, kurioje būtų išdėstyta visa turima informacija bei duomenys, susiję su incidentu, kai tyrimas bus užbaigtas. 1.9. Tiekėjo pareiga sudaryti sąlygas kibernetinio saugumo subjektui arba jo įgaliotiems paslaugų teikėjams atlikti tiekėjo atitikties auditą (įskaitant neplaninį) Sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui. 1.10. Būtina vykdyti sutartinius paslaugų teikimo įsipareigojimus (angl. *Service Level Agreement*, SLA). 1.11. Draudžiama diegti, saugoti, naudoti, kopijuoti ar platinti nelegalią, autorines teises pažeidžiančią programinę įrangą.
2. Techninės duomenų tvarkymo saugumo priemonės	2.1. 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. 2.2. 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. 2.3. Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių, slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir pan.). Naudotojo slaptažodis turi būti ne trupesnis kaip 10 simbolių ir keičiamas ne rečiau kaip kas šešis mėnesius. Administratoriaus slaptažodis turi būti ne trumpesnis kaip 15 simbolių ir keičiamas ne rečiau kaip kas šešis mėnesius. Turi būti užtikrintas prisijungimo duomenų saugumas. Turi būti imtasi visų priemonių, kad prisijungimo vardai ir slaptažodžiai netaptų žinomi tretiesiems asmenims. 2.4. Kompiuterinėje darbo vietoje ar taikomojoje programinėje įrangoje slaptažodžių išsaugojimas turi būti draudžiamas. 2.5. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio.

	2.6. Vadovaujantis susitarimu, techninių žurnalų įrašai turi būti kuriami 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). Saugojimo terminas – ne trumpesnis kaip 3 mėnesiai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį. 2.7. Kompiuterinių darbo vietų, naudojamų duomenų tvarkymui pagal susitarimą, apsauga: 2.7.1. darbo vietų naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų; 2.7.2. naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos; 2.7.3. baigus darbą arba pasitraukiant iš darbo vietos, turi būti atsijungiama nuo tinklų ir informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu; 2.7.4. kritiniai kompiuterinių darbo vietų operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant; 2.7.5. antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą; 2.7.6. kai prieiga prie naudojamų IT sistemų, susijusių su duomenų tvarkymu pagal susitarimą, yra vykdoma internetu, duomenys turi būti šifruojami taikant virtualaus privataus tinklo (VPN) technologiją su TLS / SSL sertifikatu arba naudojama privataus prieigos taško (angl. *Access Point Name*, APN) per mobiliojo ryšio operatorių technologija, taikant perduodamų duomenų šifravimą sraute su TLS / SSL sertifikatu, kai VPN technologija nėra palaikoma mobiliųjų įrenginių; 2.7.7. belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidis ryšys turi būti šifruojamas pagal gerąją saugumo praktiką rekomenduojamu šifravimo ilgio raktu. Būtina naudoti visuotinai saugiais pripažįstamus raktus ir protokolų versijas. Belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai; 2.7.8. mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti; 2.7.9. mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti. 2.8. Viešaisiais elektroninių ryšių tinklais perduodamos kibernetinio saugumo subjektui jautrios informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą bei turi būti apsaugota slaptažodžiais.

	2.9. Mobiliųjų įrenginių laikmenose ir išorinėse kompiuterinėse laikmenose laikomi tinklų ir informacinių sistemų duomenys turi būti šifruojami. Duomenis būtina šifruoti kietojo disko lygiu. 2.10. 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., USB, DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti, pvz., naudojant tam skirtus smulkintuvus arba kitas mechanines priemones. 2.11. Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

Annex No. 3
To the Special Part of the Contract for the Public Procurement-Sale of *Services*

ARRANGEMENT ON APPLICABLE ORGANISATIONAL AND TECHNICAL CYBER SECURITY REQUIREMENTS

When performing the Contract for the Public Procurement-Sale of *Services* (hereinafter referred to as the Contract), the Supplier/Provider shall be obliged to ensure an adequate level of data security, i.e. the constant confidentiality, integrity, availability of the personal data processed and resilience of the data processing IT systems, and to make appropriate decisions on the use of technical and organisational security measures for this purpose. If the Supplier/Provider serves a critical information and communication technology (hereinafter referred to as the ICT) infrastructure, or provides other essential services in Lithuania provided for in Annex 1 to the Law on Cyber Security of the Republic of Lithuania, it shall comply with the provisions of the Cyber Security Requirements approved by Resolution No 818 of the Government of the Republic of Lithuania of 13 August 2018 On the Implementation of the Law on Cyber Security of the Republic of Lithuania applicable to the central cyber security entity. In the case of a foreign Supplier/Provider who processes the data transferred to it outside the ICT infrastructure of the State Enterprise Centre of Registers (hereinafter referred to as the Centre of Registers), the requirements of international standards such as ISO/IEC 27001 or equivalent standards (NIST CSF, SOC 2, etc.) shall be complied with.

The Supplier/Provider undertakes to ensure the implementation of the following organisational and technical cyber security requirements:

1. Organisational security measures for data processing	1.1. Upon conclusion of the Contract, the employees appointed by the Supplier/Provider who will provide services under this Contract and connect to the ICT infrastructure of the Centre of Registers shall be required to read through the Cyber Security Policy adopted by the Information Resource Manager and the implementing legislation, and to comply with the established requirements. In cases where the Supplier/Provider is transferred to process the data of the Centre of Registers in its (Supplier's/Provider's) infrastructure, the Supplier/Provider must comply with the information and/or cyber security policy adopted by the Supplier's/Provider's organisation. 1.2. Maintain the confidentiality of information transmitted, stored or otherwise processed throughout the term of the Contract and thereafter, and to undertake in writing to protect such information prior to the commencement of such processing. 1.3. Ensure the security of the login data received and not to disclose it to third parties. 1.4. Grant, modify and/or revoke user rights on a need-to-know principle, or ensure that access to information is limited to execution of specific functions (carrying out work) and/or for a specific period. 1.5. The Supplier/Provider shall apply appropriate and adequate procedures for granting of rights or lifting of obligations, transfer or assignment of roles and responsibilities in the event of dismissal and change of their functions within its organisation.

	1.6. The Supplier/Provider must ensure that suppliers/providers (sub-suppliers/sub-providers) involved comply with the same information and cyber security requirements. 1.7. The Supplier/Provider shall immediately inform the Centre of Registers of the termination of employment relationship with the employee of the organisation who has been granted access to the information processed in the ICT infrastructure of the Centre of Registers. 1.8. The Supplier/Provider shall have the obligation to immediately inform about any major and/or other electronic information security incidents observed in the information technology infrastructure of the Centre of Registers during the performance of the Contract, non-functioning or improperly functioning security measures, non-compliance with information security requirements, signs of criminal activity, detected security gaps (vulnerabilities) that pose a risk to the networks and information systems of the cyber security entity and other important safety events. It shall also inform the Centre of Registers, but not later than within 24 hours, when the said cases have been identified in the information systems infrastructure managed by the Supplier/Provider, which affect the data processed by the Centre of Registers. It shall provide the cyber security entity with a report on the investigation of a cyber incident when the investigation is completed. 1.9. The Supplier/Provider shall be responsible for facilitating a cyber security entity or its authorised service providers to carry out a Supplier's/Provider's compliance audit (including an unplanned one) during the Contract period or in the event of a major incident. 1.10. Perform the Service level Agreement, SLA. 1.11. Prohibited install, store, use, copy or distribute illegal, copyright-infringing software.
2. Technical security measures for data processing	2.1. An access control system shall be in place and implemented, which is applicable to all users of the IT system. The access control system must allow the creation, validation, review and deletion of user accounts. 2.2. The use of shared user accounts shall be avoided. Where a shared user account is necessary, all users of the shared account shall have the same rights and obligations. 2.3. An authentication mechanism must be in place allowing access to the IT system. The minimum requirement for the user to log in to the IT system shall be a username and a password. The password shall be created according to a certain level of complexity. The password must consist of letters, numbers and special characters; the personal information (such as date of birth, family names, etc.) must not be used for passwords. The user password must consist of at least 10 characters, which must be changed at least every six months; and the administrator password must consist of at least 15 characters, which must be changed at least every six months. The security of the login

	data must be ensured. All measures must be taken to prevent login names and passwords becoming known to third parties. 2.4. The password must be prohibited from being stored in the computer workstation or its software. 2.5. The access control system must be able to detect and prevent the use of passwords that do not meet a certain level of complexity. 2.6. Technical logs must be implemented for each IT system, which is used to process personal data under the Contract. Technical logs shall contain all possible information on access to personal data (e.g. date, time, review, modification, cancellation). The retention period shall be at least 3 months. Technical logs shall bear time stamps and shall be protected against possible tampering, falsification or unauthorized access. Time-keeping mechanisms used in IT systems shall be synchronised according to the common time reference source. 2.7. Protection of computer workstations used for data processing under the Arrangement: 2.7.1. Users of workplaces may not be able to disable or bypass and avoid IT system security settings. 2.7.2. Users may not have privileges (rights) to install, remove, administer unauthorised software. 2.7.3. After work is completed, or when leaving the workplace, the network and information systems must be disconnected, the screen saver with a password must be activated. 2.7.4. Critical security updates for the operating system of computer workstations must be installed regularly and immediately. 2.7.5. Anti-virus applications and their databases of information about viruses and malware must be updated at least once a day. 2.7.6. Where access to the IT systems used for processing data under the Arrangement is provided via the Internet, data must be encrypted using Virtual Private Network (VPN) technology with TLS/SSL certificate or using Access Point Name (APN) technology and applying streaming data encryption with TLS/SSL certificate when VPN technology is not supported by mobile devices. 2.7.7. Wireless connection to IT systems must be allowed only for certain users and processes. The wireless subnet shall be separated from other subnets. Wireless communication must be encrypted in accordance with the encryption length key recommended by good security practices. One should use keys and protocol versions, which are generally acknowledged as secure. The standard manufacturer keys must be changed in the wireless access point. 2.7.8. Mobile and portable devices to be used for work with information systems must be registered and authorised before their use. 2.7.9. Mobile, portable devices must have a sufficient level of access control procedures, as well as other equipment used to process personal data. 2.8. The confidentiality of sensitive information transmitted to a cyber security entity through public electronic communications networks

	must be ensured through encryption and must be protected by passwords. 2.9. Network and information system data stored on mobile devices and external computer media must be encrypted. One should encrypt data at the hard disk level. 2.10. Before removing any data medium, all data contained therein must be destroyed using a dedicated software that supports reliable data destruction algorithms. If this is not possible (e.g. in case of USB, DVD media), the data media must be destroyed physically without the possibility of restoring it, e.g. using shredders or other mechanical means. 2.11. Physical protection of the environment and premises with IT system infrastructure from unauthorised access must be implemented.

Participants

SYSARB AB 556681-8828 Sweden

Manually signed

Signatory

2025-05-12 00:00:00 UTC

Date

Delivery channel: Email

DETALŪS METADUOMENYS	
Dokumento sudarytojas	Valstybės įmonė Registrų centras
Dokumento pavadinimas (antraštė)	Prieiga prie SYSARB platformos
Dokumento registracijos data ir numeris	2025-05-12 Nr. ST-149 (5.7 Mr)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	PDF-LT-V1.0
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Parašo sukūrimo data ir laikas	2025-05-12 16:14
Parašo formatas	PAdES-T
Laiko žymoje nurodytas laikas	2025-05-12 16:14
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA-2
Sertifikato galiojimo laikas	2024-06-07 08:55 - 2029-06-06 08:55
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20250507.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2025-05-26)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	
Paieškos nuoroda	-
Papildomi metaduomenys	-