Pirkimo sąlygų 1 priedas

TECHNINĖ SPECIFIKACIJA
DUOMENŲ APSAUGOS PAREIGŪNO FUNKCIJŲ VYKDYMO PASLAUGOMS

1. PIRKIMO OBJEKTAS

1.1. Duomenų apsaugos pareigūno funkcijų vykdymo paslaugos, aprašytos techninės specifikacijos 3 dalyje (toliau – Paslaugos).

1.2. planuojama Paslaugų teikimo trukmė 24 (dvidešimt keturi) mėnesiai.

1.4. SĮ Vilniaus atliekų sistemos administratorius (toliau – Įmonė) neįsipareigoja išpirkti visos 1.2. papunktyje nurodytos sutarties vertės.

2. PIRKIMO OBJEKTO PRITAIKYMO SRITIS

2.1. Sutartis bus skirta vykdyti 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 95/36/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas) numatytas Duomenų apsaugos pareigūno funkcijas Įmonė pagal sutartyje nustatytus įkainius ir su Įmone suderintą planą.

2.2. Įgyvendindama Bendrąjį duomenų apsaugos reglamentą, Įmonė yra pasirengusi daugumą reikalingų lokalių teisės aktų (įskaitant Asmens duomenų tvarkymo taisykles, Privatumo ir asmens duomenų tvarkymo politiką, Reagavimo į asmens duomenų saugumo pažeidimus procedūros aprašą ir kt.). Taip pat Įmonė yra įdiegusi arba šiuo metu diegia IT saugos priemones bei kitus saugos valdymo instrumentus, siekiant užtikrinti tinkamą asmens duomenų apsaugos lygį Įmonėje. Šiuo metu Įmonė tvarko apie 400 000 fizinių asmenų ir daugiau nei 50 Įmonės darbuotojų asmens duomenis, todėl Duomenų apsaugos pareigūnas yra būtinas Įmonės veikloje.

3. REIKALAVIMAI PERKAMOMS PASLAUGOMS

Įmonė pirkimu siekia įsigyti šias paslaugas:

3.1. Pagal poreikį atlikti Įmonės lokalių teisės aktų, sutarčių ar raštų su trečiosiomis šalimis peržiūrą ir jų atitikties Reglamento reikalavimams vertinimą, teikti pasiūlymus dėl jų tobulinimo, arba parengti ir suderinti su Įmone atitinkamų dokumentų projektus.

3.2. Pagal poreikį teikti duomenų teikimo ar gavimo sutarčių bei susitarimų, asmens duomenų bendravaldytojų sutarčių ar susitarimų įvertinimus ir planuojamų sudaryti sutarčių su duomenų tvarkytojais, duomenų gavėjais ir kitais asmenimis sąlygų įvertinimus, išvadas ir siūlymus pagal Duomenų apsaugos pareigūno kompetenciją.

3.3. Dalyvauti Įmonės lokalių teisės aktų projektų rengime, derinime ir vizavime teikiant pasiūlymus dėl jų tobulinimo, arba parengti ir suderinti su Įmone atitinkamų dokumentų projektus, bei konsultacijas įmonės darbuotojams rengiantiems lokalių teisės aktų projektus.

3.4. Pagal poreikį parengti (atnaujinti) tipines asmens duomenų tvarkymo formas (informavimo pagal Reglamento 13 / 14 straipsnius tekstų formas, incidentų (pažeidimų) registro, duomenų subjektų prašymų įgyvendinti teises registrų ir kitų registrų formas, atsakymų į duomenų subjektų teisių įgyvendinimo formas, poveikio duomenų apsaugai vertinimo formas, teisėto intereso vertinimo formas ir kitos asmens duomenų tvarkymo dokumentacijos formas).

3.5. Stebėti, kaip laikomasi Reglamento ir kitų duomenų apsaugą reglamentuojančių teisės aktų, ir, esant poreikiui, teikti siūlymus Įmonei dėl reikalingų veiksmų, procesų atnaujinimo, tobulinimo ir (ar) naujų priemonių įgyvendinimo.

3.6. Atlikti kontaktinių asmens funkcijų atlikimą, kuomet duomenų subjektai ir priežiūros institucija kreipiasi į Įmonę su duomenų tvarkymu susijusiais klausimais.

3.7. Esant poreikiui bendradarbiauti su priežiūros institucijos funkcijas vykdančia Valstybine duomenų apsaugos inspekcija.

3.8. Užtikrinti asmens duomenų tvarkymo veiklos vykdymą ir prašymų, susijusių su įrašų tvarkymu, pateikimo priežiūros institucijai atlikimą.

3.9. Paaiškėjus faktui, kuris gali įtakoti duomenų saugumo incidento/pažeidimo atsiradimą, identifikuoti ar yra/buvo duomenų saugumo pažeidimas, apie kurį turėtų būti pranešama priežiūros institucijoms.

3.10. Identifikavus asmens duomenų saugumo pažeidimą, kai nėra pavojų fizinių asmenų teisėms ir laisvėms (nėra būtina informuoti priežiūros instituciją) pagal kompetenciją teikti asmens duomenų saugumo pažeidimų tyrimo išvadą Įmonės atsakingiems asmenims, ir teikti sprendimų būdus pažeidimams nutraukti, nepasikartoti.

3.11. Teikti pranešimą (-us) priežiūros institucijoms arba duomenų subjektams apie duomenų saugumo incidento/pažeidimo keliamą pavojų fizinių asmenų teisėms ir laisvėms, ne vėliau kaip per 72 val. nuo momento, kai Įmonė sužinojo apie įvykusį duomenų saugumo incidentą/pažeidimą, kuriems gali kilti pavojus dėl duomenų praradimo.

3.12. Įgyvendinti asmens duomenų tvarkymo veiklos įrašų registro priežiūrą, kontrolę ir atnaujinimą.

3.13. Atlikti duomenų tvarkymo ir priežiūros veiksmų, apie kuriuos jam buvo pranešta, vertinimus bei teikti su Įmone iš anksto suderintos formos ataskaitas apie atliktus darbus.

3.14. Dalyvauti Įmonės vidaus / išorės duomenų apsaugos audituose, pažeidimų valdyme ir tyrimuose.

3.15. Atlikti reguliarų ne mažiau kaip du kartus per metus Asmens duomenis tvarkančių Įmonės darbuotojų informavimą ir mokymą apie jų prievoles pagal Reglamentą ir kitus duomenų apsaugą reglamentuojančius teisės aktus, bei atlikti darbuotojų testavimą. Darbuotojų mokymams ir testavimui turi turėti naudojamą mokymų ir testavimo platformą, kurioje butų galimybė apmokyti ir testuoti ne mažiau kaip 60 asmenų ir kuri užtikrintų neribotą sistemos naudojimą darbuotojų mokymui, testavimui ir įvertinimui. Mokymų platformoje turi būti galimybė gauti ataskaitas (duomenis) apie testavimuose dalyvavusius, testus išlaikiusius darbuotojus. Informaciją apie turimą testavimo platformą tiekėjas turi pateikti kartu su pasiūlymu.

3.16. Teikti išvadas dėl poreikio atlikti poveikio duomenų apsaugai vertinimą ir konsultacijas dėl poveikio duomenų apsaugai vertinimo (įskaitant bet neapsiribojant teikti susijusius siūlymus dėl Įmonės vidinių teisės aktų rengimo, keitimo, konsultuoti dėl taikytinų duomenų tvarkymo sprendinių ir priemonių, rizikų bei pavojų (poveikio) identifikavimo ir atlikti visus kitus veiksmus, būtinus poveikio duomenų apsaugos vertinimo dokumentacijos parengimui ir suderinimui su Įmone, kad Įmonė galėtų pasitvirtinti atliktus poveikio duomenų apsaugos vertinimus, vadovaujantis Reglamento 35 straipsniu ir kitais taikytinais Asmens duomenų apsaugos teisės aktais, ir išvadų dėl poveikio asmens duomenų apsaugai vertinimo teikimas.

3.17. Teikti kitas konsultacijas Įmonei žodžiu ir/ar raštu dėl asmens duomenų tvarkymo ir asmens duomenų saugumo užtikrinimo (įskaitant, bet neapsiribojant dėl duomenų tvarkymo veiklos įrašų, duomenų apsaugos techninių ir organizacinių priemonių taikymo, informacinės saugos, kitų klausimų, susijusių su Reglamentu, kitų Europos Sąjungos ir Lietuvos Respublikos teisės aktų, reguliuojančių asmens duomenų apsaugą, reikalavimų tinkamo įgyvendinimo). Dalyvauti susitikimuose dėl asmens duomenų tvarkymo ir konsultuoti jų metu. Susitikimai vykdomi nuotoliu būdu, siekiant Duomenų apsaugos pareigūnui geriau suprasti asmens duomenų tvarkymo veiksmus. Dėl atitinkamų susitikimų laiko ir trukmės susiderinama iš anksto.

3.18. Nagrinėti ir tirti gautus raštus, prašymus, skundus, pretenzijas dėl duomenų tvarkymo bei pagal savo kompetenciją dalyvauti rengiant (teikti pasiūlymus dėl jų tobulinimo) arba rengti (pagal Įmonės poreikį) atsakymų projektus į juos.

3.19. Pagal poreikį atnaujinti ir/ar rengti Įmonės norminius dokumentus ir procedūras, susijusias su asmens duomenų apsauga.

3.20. Duomenų subjektų prašymų įgyvendinimas.

3.2.1. Nagrinėti į asmens duomenų saugumo pažeidimų registravimo žurnalą įrašytus pažeidimus, teikti išvadas ir pasiūlymus dėl užregistruoto duomenų saugumo pažeidimo valdymo.

3.2.2 Užtikrinti, kad duomenų subjektai būtų tinkamai informuoti apie jų tvarkomus asmens duomenis, teikiant Įmonei konsultacijas, kaip tai turi būti įgyvendinta pagal Reglamento 13 / 14 straipsnius, kad Įmonės internetinėje svetainėje būtų pateikta aktuali, pagal teisės aktus ir BDAR privaloma pateikti informacija apie tvarkomus asmens duomenis, informuoti Įmonę apie poreikį šią informaciją atnaujinti, pateikti medžiagą, kuri turi būti patalpinta Įmonės internetinėje svetainėje.

3.23. Pagal poreikį parengti teisėtų interesų balanso testus. Preliminarus galimas kiekis – 8 teisėtų interesų balanso testų.

3.24. Atlikti kitus Duomenų apsaugos pareigūno veiksmus, numatytus Reglamente, ir nusistovėjusius įmonių praktikoje.

3.2.5. Konsultuoti įmonės darbuotojus asmens duomenų tvarkymo klausimais.

4. PASLAUGŲ SUTEIKIMO IR SUTARTINIŲ ĮSIPAREIGOJIMŲ VYKDYMO TVARKA

4.1. Tiekėjas įsipareigoja paskirti darbuotoją, kuris būtų lengvai pasiekiamas tiek elektroninėje, tiek telekomunikacinėje erdvėje, bei kurio kontaktiniai duomenys, vadovaujantis Reglamento 37 straipsnio 7 dalimi, būtų paskelbti ir pranešti priežiūros institucijai.

4.2. Paslaugos teikiamos nepertraukiamai ir sistemingai. Paslaugų rezultatai pateikiami el. paštu ar per Įmonės ar tiekėjo duomenų (užduočių) valdymo sistemą– Jira Software.

4.3. Paslaugos pradedamos teikti gavus Įmonės užsakymą el. paštu ar per Įmonės ar tiekėjo duomenų valdymo sistemą – Jira Software.

4.4. Atsiskaitymas vykdomas kiekvieną mėnesį pagal fiksuotą valandinį Paslaugų įkainį.

4.5. Įmonė įsipareigoja Paslaugų teikimo sutarties nustatyta tvarka laiku atsiskaityti už tinkamai ir laiku suteiktas Paslaugas pagal Paslaugų teikėjo pateiktas sąskaitas, kurios išrašomos tik Įmonės patvirtintų Paslaugų ataskaitų pagrindu.

4.6. Pagal Įmonės poreikį, iš anksto suderintą abiejų šalių laiką ir vietą, tiekėjo darbuotojas turi dalyvauti Įmonės veikloje, susijusioje su asmens duomenų apsauga, arba galinčioje turėti įtakos asmens duomenų apsaugai (įskaitant bet neapsiribojant dokumentų pagal jo kompetenciją vizavimą ir derinimą).

4.7. Tiekėjas įsipareigoja užtikrinti reagavimą į Įmonės prašymus (užklausas), bet ne vėliau kaip per 4 val. nuo prašymo gavimo (išskyrus poilsio ir oficialias šventines dienas). Tuo atveju, jei Tiekėjo paskirtas darbuotojas negali eiti pareigų, turi būti paskirtas pakaitinis darbuotojas.

4.8. Įvykus duomenų saugumo incidentui/pažeidimui, kai gali kilti pavojus dėl duomenų praradimo, tiekėjas įsipareigoja pateikti tyrimo įžvalgas per 30 val. po sužinojimo apie incidentą, o galutinę išvadą - per 70 val. po sužinojimo apie incidentą.

4.9. Atsakymai į duomenų subjektų prašymus turi būti parengti laikantis teisės aktuose numatytų terminų.

4.10. Esant poreikiui, dalis Paslaugų turės būti suteiktos Įmonės buveinėje, adresu Laisvės pr. 10, Vilnius.

4.11. Visa su Paslaugų Įmonei teikimu susijusi informacija, įskaitant ir visa iš Įmonės gauta informacija, Paslaugų rezultatai, yra laikoma konfidencialia informacija (nebent Įmonė raštu aiškiai patvirtins Tiekėjui, kad tam tikra pateikta informacija nėra konfidenciali), už kurios saugojimą ir neatskleidimą tretiesiems asmenims (nebent tam yra gautas išankstinis raštiškas Įmonės sutikimas arba imperatyviai numatyta įstatymų) atsako Tiekėjas, prisiimdamas konfidencialumo įsipareigojimus.

4.12. Tiekėjas įsipareigoja nedelsiant informuoti Įmonę apie nuo Tiekėjo nepriklausančias aplinkybes, keliančias pavojų teikiamų Paslaugų kokybei ir / arba terminų laikymuisi.

4.13. Tiekėjas, teikdamas paslaugas, turi vadovautis Reglamentu ir visais galiojančiais asmens duomenų apsaugą reglamentuojančiais Lietuvos Respublikos ar Įmonės lokaliais teisės aktais.

4.14. Tiekėjas, teikdamas paslaugas, turi padėti užtikrinti Įmonei atskaitomybės principo įgyvendinimą įrodinėjant, kaip Įmonė laikosi Reglamento ir teisės aktų nuostatų (t. y., rinkti Įmonės prašymų, jam suteiktų konsultacijų, kitų paslaugų įrodymus ir kt. bei suteikti Įmonei prie jų prieigą pagal poreikį).

4.15. Tiekėjas užtikrina, kad nepertraukiamai turės pakankamą Duomenų apsaugos pareigūno funkcijų vykdymui reikalingą personalą.

4.16. Tiekėjas, gavęs Įmonės prašymą, įsipareigoja raštu pateikti Įmonei veiklos ataskaitą už atitinkamą ataskaitinį laikotarpį apie Įmonės atitikties Reglamentui ir visiems galiojantiems asmens duomenų apsaugą reglamentuojantiems Lietuvos Respublikos teisės aktams.