

## NFR (nefunkciniai) reikalavimai informacijos saugai ir BDAR

Eil. Nr.	Reikalavimo tipas	Reikalavimas
1	Saugos valdymas	Tiekėjas paslaugų teikimo metu privalo užtikrinti, kad jis, jo tiekiamą įrangą ir jo pasitelkiami kiti ūkio subjektai (ūkio subjektai, kurių pajėgumais remiamasi kvalifikacijai pagrįsti, subtiekejai ir kita) atitinka Lietuvos Respublikos Vyriausybės 2018-08-13 nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ patvirtintame Kibernetinio saugumo reikalavimų apraše (toliau – Aprašas) esminiams kibernetinio saugumo subjektams nustatytus kibernetinio saugumo reikalavimus. Perkančiajai organizacijai paprašius, per abiejų šalių suderintą terminą, Tiekėjas privalo pateikti paaiškinimus ir (ar) kitus įrodymus (pvz., sertifikatus ir (ar) politikas, ir (ar) procesų aprašus, ir (ar) išorinio audito išvadas), kurie patvirtintų, kad Tiekėjas užtikrins atitiktį Aprašo reikalavimams.
2	Saugos valdymas	Perduodamas Sistemos programinę įrangą, Tiekėjas turi sugeneruoti ir pateikti šios programinės įrangos komponentų (angl. Software Bill of Material, SBOM) ataskaitą: CyclonDX standarto JSON formato faile su vientisumo patikra (angl. integrity verification). Atnaujinus programinę įrangą, turi būti sugeneruota ir pateikta nauja SBOM ataskaita.
3	Saugos valdymas	Tiekėjas turi užtikrinti galimybę Pirkėjui ar jo įgaliotam partneriui ne rečiau kaip vieną kartą per metus arba įvykus dideliame (pagal Kibernetinio saugumo įstatymo nuostatas) kibernetiniam incidentui atlikti Sistemos palaikymo ir vystymo veiklos auditą ar patikrą, siekiant įvertinti taikomas Pirkėjo duomenų saugos užtikrinimo organizacines bei technines priemones.
4	Saugos valdymas	Sistemoje turi būti užtikrinama, kad Pirkėjo duomenys (data at rest), jų perdavimas (data in transit) ir jų atsarginės kopijos (data backups) yra šifruojami, parenkant naujausias NIST, EISA ar BSI organizacijų rekomendacijas atitinkančius šifravimo algoritmus, šifravimo raktų ilgus ir t.t., o naudojamų šifravimo priemonių detalus sąrašas ir (arba) raktai turi būti pateikti Pirkėjui.
5	Saugos valdymas	Sistemos naudotojų paskyros turi būti valdomos per Pirkėjo valdomą aktyvaus katalogo (angl. Active Directory (AD)) arba Entra ID sistemas, užtikrinant vieno prisijungimo (angl. Single Sign On (SSO)) principus ir autentikavimui naudojant bent vieną iš šių protokolų: Open ID Connect, SAML 2.0, WS-Fed. Sistemos vidinės (default, built-in) naudotojų paskyros turi būti užblokuotos ir galės būti naudojamos tik išskirtiniais atvejais (pvz. sistemos atnaujinimas ar atstatymas).

6	Saugos valdymas	Sistemos naudotojų paskyroms priskiriamos privilegijos ir (arba) rolės bei kiti saugos parametrai turi būti valdomos per Pirkėjo valdomą aktyvaus katalogo (angl. Active Directory (AD)) ir (arba) per Pirkėjo valdomą tapatybių ir prieigų (angl. Identity and Access Management (IAM)) sistemą.
7	Saugos valdymas	Sistemos įvykių žurnaluose turi būti registruojami ir ne mažiau kaip 6 mėnesius saugomi visų naudotojų (esamų/aktyvių, de-aktyvuotų ir ištrintų) visi atlikti veiksmai kartu su veiksmų turiniu (angl. user activity logging), visi naudotojų paskyrų ir privilegijų/rolių keitimo veiksmai kartu su veiksmų turiniu (angl. security change logging).
8	Saugos valdymas	Jei paslaugų teikimo metu Tiekėjui reikalinga gauti Pirkėjo neskelbtinos informacijos (vidinės informacijos, konfidencialios informacijos ar komercinių (gamybinių) paslapčių) turi būti pasirašomas informacijos perdavimo susitarimas. Šiame susitarime turi būti nurodyta: <ul style="list-style-type: none"> <li>- perduotina informacija ir jos konfidencialumo lygis;</li> <li>- informacijos gavėjai;</li> <li>- informacijos perdavimo būdas;</li> <li>- techniniai ir organizaciniai informacijos saugumo reikalavimai, kuriuos turi užtikrinti Tiekėjas, apsaugodamas neskelbtiną Pirkėjo informaciją.</li> </ul>
9	Saugos valdymas  Incidentai / saugumo pažeidimai (BDAR 28 str. 3 d. f p., BDAR 33 str. 2 d., NIS 2 23 str.)	Pirkėjas turi būti nedelsiant informuojamas apie Sistemos informacijos ir kibernetinės saugos įvykius ir incidentus ar asmens duomenų saugumo pažeidimus, jų įtaką Pirkėjo informacijos ir duomenų saugumui bei jų valdymo būklę. Per 24 valandas LTG skaitmeninio saugumo komandai arba kompetentingai institucijai turėtų būti perduotas išankstinis įspėjimas ir keletas pirmųjų prielaidų apie incidento pobūdį. Po 72 valandų turi būti perduota išsami pranešimo ataskaita, kurioje pateikiamas incidento įvertinimas, sunkumas ir poveikis bei kompromitavimo rodikliai. Po 1 mėnesio turi būti pateikta galutinė ataskaita. Pirkėjas turi turėti galimybę susisiekti su saugos įvykius ir incidentus valdančiais asmenimis, kad įsitikinti valdymo proceso efektyvumu.
10	Saugos valdymas  Asmens duomenų saugumas (BDAR 32 str.) ir Pritaikytoji / standartizuotoji asmens duomenų apsauga (BDAR 25 str.)	Sistemos veikimui, kūrimui ir palaikymui, Tiekėjas ir (arba) kitos Šalys, veikiančios kaip duomenų tvarkytojai ir tvarkantys Pirkėjo valdomus asmens duomenis, turi įgyvendinti technines ir organizacines priemones, kad apsaugotų Pirkėjo duomenis pagal BDAR reikalavimus, užtikrinant, be kita ko, atitikimą pritaikytosios duomenų apsaugos (data protection by design) ir standartizuotosios duomenų apsaugos (data protection by default) (BDAR 25 str.) įskaitant, bet neapsiribojant saugojimo terminų nustatymą, asmens duomenų nuasmeninimą ar trynimą automatizuotomis priemonėmis. Tiekėjas turi pateikti visų Šalių, tvarkančių Pirkėjo valdomus asmens duomenis, aukščiau nurodytų reikalavimų įgyvendinimo įrodymus Pirkėjui.

11	<p>Saugos valdymas</p> <p>Duomenų tvarkymo susitarimas (BDAR 28 str.)</p>	<p>Tiekėjas turi su Pirkėju sudaryti duomenų tvarkymo susitarimą (DTS) pagal Pirkėjo pateiktą DTS formą. Tais atvejais, kai Pirkėjo asmens duomenis tvarkys kita Šalis, Tiekėjas turi užtikrinti, kad kita Šalis su Pirkėju sudarys DTS pagal Pirkėjo pateiktą DTS formą. Tais atvejais, kai Tiekėjas yra tik pirkimo objektą sudarančias ir su asmens duomenų tvarkymu susijusias paslaugas teikiančio ūkio subjekto įgaliotas atstovas ir / ar tarpininkas, dėl ko asmens duomenų tvarkymą Sutarties vykdymo metu atliks ne pats Tiekėjas, o jo atstovaujamas paslaugų teikėjas, Tiekėjas privalo užtikrinti, kad šis jo atstovaujamas paslaugų teikėjas pasirašys nurodytą DTS su Pirkėju pagal Pirkėjo pateiktą DTS formą. Pagrįstais atvejais, kai nėra galimybės sudaryti DTS pagal Pirkėjo pateiktą formą, Tiekėjas turi užtikrinti, kad duomenų tvarkytojo paslaugų teikimo sąlygose, be kita ko, būtų įtrauktos BDAR 28 straipsnio reikalavimus atitinkančios nuostatos, kurių įgyvendinimas neturi būti papildomai apmokestinamas.</p>
12	<p>Saugos valdymas</p> <p>Duomenų subjektų teisių įgyvendinimas (BDAR III skyrius, BDAR 28 str. 3 d. e p.)</p>	<p>Produktai (sistemos) ir (arba) paslaugos turi būti sukonfigūruotos taip, kad leistų Pirkėjui įgyvendinti BDAR numatytas duomenų subjektų teises: teisę būti informuotam apie duomenų tvarkymą, teisę susipažinti su asmens duomenimis, teisę reikalauti ištaisyti duomenis, teisę būti pamirštam, teisę apriboti duomenų tvarkymą, teisę nesutikti su duomenų tvarkymu, teisę į duomenų perkeliamumą (BDAR III skyrius). Visų Pirkėjo Tiekėjui perduotų duomenų subjektų prašymų įgyvendinimas neturi būti papildomai apmokestinamas.</p>
13	<p>Saugos valdymas</p> <p>Duomenų perdavimas į trečiąsias šalis (BDAR V skyrius)</p>	<p>Tiekėjas turi užtikrinti, kad Pirkėjo valdomi asmens duomenys nebus perduodami už Europos ekonominės erdvės ribų, nebent egzistuotų bent viena iš BDAR V skyriuje numatytų perdavimo už Europos ekonominės erdvės ribojimo išimčių.</p>
14	<p>Saugos valdymas</p>	<p>Tiekėjas privalo užtikrinti, kad nurodyti reikalavimai būtų taikomi jo partneriams, subrangovams, Sistemos gamintojams ir (arba) kitoms Šalims, dalyvaujančioms Sistemos kūrimo, vystymo ir palaikymo veikloje.</p>