REKOMENDACIJA Nr.1

DĖL TINKAMŲ ORGANIZACINIŲ IR TECHNINIŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ ĮGYVENDINIMO.

2023 m. liepos 07 d.

Siekiant užtikrinti 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB *(toliau – BDAR)*, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo *(toliau – ADTAĮ)* ir kitų Europos Sąjungos ir Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą Vilniaus darželyje-mokykloje „Saulutė" *(toliau - Darželis)* parengta ši rekomendacija, kurioje išdėstyti minimalūs organizaciniai ir techniniai asmens duomenų saugumo reikalavimai. Kuriant (diegiant) ar vertinant Darželyje turimas organizacines ir technines asmens duomenų saugumo priemones, rekomenduojama visapusiškai atsižvelgti į asmens duomenų tvarkymo tikslus ir riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms bei atlikti rizikos vertinimą.

MINIMALŪS REIKALAVIMAI DĖL TINKAMŲ ORGANIZACINIŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ.

1. Asmens duomenų saugumo politika ir procedūros.

Asmens duomenų ir jų tvarkymo saugumas Darželyje turi būti aiškiai apibrėžti Privatumo ir asmens duomenų tvarkymo ir jų saugumo politikoje. Privatumo ir asmens duomenų tvarkymo ir jų saugumo politika yra svarbus dokumentas, nustatantis pagrindinius informacijos saugumo, fizinių asmenų *(toliau – Duomenų subjektas*) asmens duomenų apsaugos ir jų tvarkymo principus Darželyje. Tai yra visų konkrečių techninių ir organizacinių priemonių įgyvendinimo pagrindas pagal BDAR 32 straipsnį ir jį papildantį 24 straipsnį. Privatumo ir asmens duomenų tvarkymo ir jų saugumo politika nustato bendrą informacijos ir asmens duomenų apsauga Darželyje. Remiantis Privatumo ir asmens duomenų tvarkymo ir jų saugumo politika, konkrečios techninės ir organizacinės priemonės Darželyje aprašomos detalesnėse taisyklėse. Privatumo ir asmens duomenų tvarkymo ir jų saugumo politika turi būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.

2. Vaidmenys ir atsakomybės.

Su Duomenų subjektų asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės Darželyje turi būti aiškiai apibrėžti ir paskirstyti Darželio taisyklėse. Turi būti nustatytas ir aiškiai apibrėžtas Darželio darbuotojų teisių ir pareigų suteikimas ir atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras *(Pvz., Darželio vidaus tvarkos instrukcijų ar taisyklių pertvarkymo, darbuotojų atleidimo arba jų funkcijų pasikeitimo metu)*
BDAR 32 straipsnio 4 dalis reikalauja, kad Darželis (kaip Duomenų valdytojas ir/ar duomenų tvarkytojas) imasi priemonių, siekdami užtikrinti, kad bet kuris Darželiui (duomenų valdytojui arba duomenų tvarkytojui) pavaldus darbuotojas (fizinis asmuo), galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai Darželio (duomenų valdytojo) vadovas duoda nurodymus juos tvarkyti arba tas Darželio darbuotojas (darbuotoja) privalo tai daryti pagal Lietuvos Respublikos ar Europos Sąjungos teisę. Pagrindinė asmens duomenų saugumo priemonė Darželio personalui, turinčiam prieigą prie Duomenų subjektų asmens duomenų, jų atsakomybė bei vaidmenys, taip pat darbo su Duomenų subjektų asmens duomenimis kompetencijos turi būti aiškiai apibrėžtos ir dokumentuotos atskiruose Darželio taisyklėse (instrukcijose). Ypač svarbus vaidmuo tenka Darželio specialistui (ar įgaliotiniui), kuris yra atsakingas už tinkamos Darželio Privatumo ir asmens duomenų tvarkymo ir jų saugumo politikos įgyvendinimą. Darželio duomenų apsaugos pareigūnas *(toliau – DAP)* prižiūri, kaip laikomasi BDAR. Šie asmenys turi glaudžiai bendradarbiauti.

3. Prieigos valdymo politika.

Būtina nustatyti prieigos kontrolė prie Darželio IT sistemų, naudojamų Duomenų subjektų asmens duomenų tvarkymui. Prieigos kontrolė prie Darželio IT sistemų turi būti įgyvendinama taikant technines priemones. Kiekvienam vaidmeniui, susijusiam su Duomenų subjektų asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės. Kiekvienam vaidmeniui, susijusiam su Duomenų subjektų asmens duomenų tvarkymu ar naudotojui turėtų būti suteiktas tik toks prieinamumo lygis prie Duomenų subjektų asmens duomenų, kuris yra būtinas jo užduotims atlikti. Darželyje turi būti tvarkomi adekvatūs, tinkami ir tik tokie Duomenų subjektų asmens duomenis, kurių reikia siekiant tikslų, dėl kurių jie Darželyje tvarkomi. Šis reikalavimas glaudžiai susijęs su duomenų kiekio mažinimo principu *(BDAR 5 straipsnio 1 dalies c punktas)*.

4. Išteklių ir turto valdymas.

Darželis turi turėti IT išteklių, naudojamų Duomenų subjektų asmens duomenimis tvarkyti ir techninės, programinės ir tinklo įrangos registrą, o registro tvarkymas turi būti priskirtas konkrečiam Darželio darbuotojui *(Pvz., IT specialistui)*. Registras turi apimti IT išteklių tipą *(pvz., tarnybinę stotį, kompiuterinę darbo vietą)*, vietą *(fizinę ar elektroninę)*. IT ištekliai turi būti reguliariai peržiūrimi ir atnaujinami. Rekomenduojamas peržiūros dažnumas: kartą per 3 mėnesius. Darželio techninės, programinės ir tinklo įrangos valdymas yra būtinas Duomenų subjektų asmens duomenų saugumui ir vientisumui, nes tai leidžia kontroliuoti duomenų apdorojimo priemones. Darželio išteklių valdymas būtinai turi apimti IT išteklių ir tinklo topologijos, kuri yra naudojama tvarkant Duomenų subjektų asmens duomenis, registravimą. Duomenų subjektų asmens duomenis Darželyje turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas Duomenų subjektų asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo. Vientisumo ir konfidencialumo principas apibrėžtas BDAR 5 straipsnio 1 dalies f punkte.

5. Pakeitimų valdymas.

Darželis turi užtikrinti, kad visi IT sistemų pakeitimai būtų stebimi ir registruojami registre konkretaus Darželio IT specialisto. Pakeitimų valdymo tikslas – sinchronizuoti ir kontroliuoti visus Darželio IT sistemose, naudojamose tvarkant asmens duomenis, atliekamus pakeitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas pakeitimų įgyvendinimas gali sukelti neteisėtą Duomenų subjektų asmens duomenų atskleidimą, pakeitimą ar sunaikinimą. Pakeitimų valdymas Darželyje yra būtinas duomenų tvarkymo vientisumui užtikrinti *(BDAR 5 straipsnio 1 dalies f punktas)* ir Darželio (duomenų valytojo) atskaitomybės principui įgyvendinti *(BDAR 5 straipsnio 2 dalis).* Darželio (duomenų valytojo) programinės įrangos kūrimas turėtų būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie Darželio (duomenų valytojo) IT sistemų, naudojamų tvarkant Duomenų subjektų asmens duomenis. Testuojant Darželio (duomenų valytojo) sistemas, reikia naudoti tęstinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros.

6. Duomenų tvarkytojai.

Prieš pradedant Duomenų subjektų asmens duomenų tvarkymo veiklą, Darželis (duomenų valytojas) ir jo samdomi duomenų tvarkytojai turėtų sutartyje aiškiai apibrėžti, dokumentuoti ir suderinti tarpusavio visus formalumus ir procedūras, taikomas duomenų tvarkytojams (rangovams ar užsakomosioms paslaugoms) dėl Duomenų subjektų asmens duomenų tvarkymo. Procedūros turi nustatyti tokį patį Duomenų subjektų asmens duomenų saugumo lygį, koks yra numatytas Darželio (duomenų valdytojo) Privatumo ir asmens duomenų tvarkymo ir jų saugumo politikoje. BDAR 28 straipsnis numato, kad Darželis (duomenų valytojas) pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad Duomenų subjektų asmens duomenų tvarkymas atitiktų BDAR reikalavimus ir būtų užtikrinta Duomenų subjekto teisių apsauga. Tame pačiame straipsnyje teigiama, kad duomenų tvarkytojas turi veikti pagal sutartį ar kitą teisės aktą. Darželis (duomenų valdytojas) ir jo samdomi duomenų tvarkytojai turi oficialiai susitarti dėl formalių reikalavimų ir prievolių. Duomenų tvarkytojas turi pateikti Darželio (duomenų valdytojo) vadovei dokumentais pagrįstus įrodymus dėl jo atitikties keliamiems reikalavimams. Duomenų

tvarkytojas turi veikti tik pagal sutartį ir privalo nedelsdamas pranešti Darželio (duomenų valdytojo) vadovei apie nustatytus asmens duomenų saugumo pažeidimus.

7. Asmens duomenų saugumo pažeidimai ir incidentai.

Darželis (duomenų valdytojas) turi nustatyti reagavimo į asmens duomenų saugumo pažeidimus (incidentus) taisykles. Taisyklėse turi būti aiškiai nustatytas reagavimo į incidentus planas, kad būtų užtikrintas veiksmingas incidentų, susijusių su asmens duomenimis, valdymas, pranešimo apie asmens duomenų saugumo pažeidimus Darželio (duomenų valdytojo) vadovei, Valstybinei duomenų apsaugos inspekcijai, bei duomenų subjektams tvarka vadovaujantis BDAR 33 ir 34 straipsniais.
Duomenų saugumo pažeidimo atveju Darželis (duomenų valdytojas) turi įvertinti, ar tai turės įtakos asmens duomenų tvarkymui (*Pvz.; atsitiktiniam ar neteisėtam perduodamų, saugomų ar kitaip tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, neteisėtam atskleidimui ar prieigai prie jų)*.
Darželis (duomenų valdytojas) turi užtikrinti, kad jis laikosi savo įsipareigojimų pagal BDAR 33 ir 34 straipsnius, susijusius su pranešimu apie asmens duomenų saugumo pažeidimus priežiūros institucijai (VDAI) ir Duomenų subjektams. Duomenų tvarkytojai taip pat turi užtikrinti, kad jie laikosi savo įsipareigojimų pagal BDAR 33 straipsnį ir galės nedelsdami pranešti Darželio (duomenų valdytojo) vadovei apie minėtus pažeidimus. Bet kuriuo atveju, tiek Darželis (duomenų valdytojas), tiek jo samdomi duomenų tvarkytojai turi turėti tinkamas procedūras ne tik pranešti apie asmens duomenų pažeidimus, bet ir juos suvaldyti.

8. Veiklos tęstinumas.

Darželis (duomenų valdytojas) turi nustatyti pagrindines procedūras, kurių reikia laikytis incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas Duomenų subjektų asmens duomenų tvarkymo Darželio IT sistemomis tęstinumas ir prieinamumas. Darželio (duomenų valdytojo) veiklos tęstinumo planas ir pagrindines procedūras yra būtinas nustatant procesus ir technines priemones, kurių Darželis (duomenų valdytojas) turėtų laikytis incidento ar Duomenų subjektų asmens duomenų pažeidimo atveju. Šis planas papildo Darželio (duomenų valdytojo) Privatumo ir asmens duomenų tvarkymo ir jų saugumo politiką. Ši priemonė aiškiai susijusi su BDAR 32 straipsnio 1 dalies c punktu, kuris įpareigoja Darželi (duomenų valdytoją) ir jo samdoma duomenų tvarkytoją laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju.

9. Personalo konfidencialumas.

Darželis (duomenų valdytojas) turi užtikrinti, kad visi jo darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su Duomenų subjektų asmens duomenų tvarkymu. Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti Darželio (duomenų valdytojo) darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus. Siekiant užtikrinti Duomenų subjektų asmens duomenų konfidencialumą pagal BDAR 32 straipsnį, Darželis (duomenų valdytojas) turi užtikrinti, kad jos darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu. Be to, BDAR 32 straipsnio 4 dalis (atitinkamai BDAR 29 straipsnis) numato, kad Darželis (duomenų valdytojas) ir jo samdomi duomenų tvarkytojai imasi priemonių, siekdami užtikrinti, kad bet kuris Darželiui (duomenų valdytojui) arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su Duomenų subjektų asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai Darželis (duomenų valdytojas) duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Europos Sąjungos arba Lietuvos Respublikos teisę. Šiuo tikslu turėtų būti nustatytos specialios priemonės, užtikrinančios, kad asmenys, dalyvaujantys tvarkant Duomenų subjektų asmens duomenis Darželio (duomenų valdytojo) vardu, būtų tinkamai informuojami apie savo pareigą laikytis konfidencialumo. Šios pareigos tiri būti apibrėžtos Darželio (duomenų valdytojo)instrukcijose ar taisyklėse.

10. Personalo mokymai.

Darželis (duomenų valdytojas) turi užtikrinti, kad visi jo darbuotojai būtų tinkamai informuoti apie Darželio IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Darželio (duomenų valdytojo) darbuotojai, susiję su Duomenų subjektų asmens duomenų tvarkymu, turi būti mokomi dėl atitinkamų duomenų apsaugos reikalavimų ir teisinių įsipareigojimų rengiant reguliarius mokymus, informavimo renginius ar instruktažus.

Rekomenduojamas mokymų dažnumas: kartą per metus. Darželio (duomenų valdytojo) personalo mokymai apie duomenų apsaugos ir saugumo procedūras *(Pvz.; slaptažodžių naudojimas ir prieiga prie konkrečių IT sistemų)* yra svarbūs tinkamam organizacinių ir techninių saugumo priemonių įgyvendinimui ir prevencijai dėl netyčinio Duomenų subjektų asmens duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų. *(BDAR 32 straipsnio 2 dalis).* Žinios apie konkrečius Duomenų subjektų asmens duomenų apsaugos teisinius įsipareigojimus taip pat yra svarbios Darželio darbuotojams, kurie dalyvauja Duomenų subjektų asmens duomenų tvarkymo procesuose.

MINIMALŪS REIKALAVIMAI DĖL TINKAMŲ TECHNINIŲ DUOMENŲ SAUGUMO PRIEMONIŲ.

1. Prieigų kontrolė ir autentifikavimas.

Darželyje turi būti įdiegta ir įgyvendinta bei visiems Darželio IT sistemos naudotojams taikoma prieigų kontrolės sistema. Darželio (duomenų valdytojo) prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti Darželio IT sistemos naudotojų paskyras. Darželyje turi būti vengiama naudoti bendras Darželio IT sistemos naudotojų paskyras. Vietose, kur bendra Darželio IT sistemos naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi turėti tokias pat teises ir pareigas. Minimalus reikalavimas naudotojui prisijungti prie Darželio (duomenų valdytojo) IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Darželio (duomenų valdytojo) prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. Darželis (duomenų valdytojas) turi užtikrinti, kad visi jo darbuotojai būtų tinkamai informuoti apie Darželio IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie Darželio IT sistemos, kurioje yra apdorojami Duomenų subjektų asmens duomenys. Darželio (duomenų valdytojo) darbuotojai, susiję su Duomenų subjektų asmens duomenų tvarkymu, turi būti mokomi dėl atitinkamų duomenų apsaugos reikalavimų ir teisinių įsipareigojimų rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Rekomenduojamas mokymų dažnumas: kartą per metus.

2. Techninių žurnalų įrašai ir stebėsena.

Techninių žurnalų įrašai yra esminis saugos reikalavimas, kuris leidžia identifikuoti ir stebėti, sekti Darželio darbuotojų (naudotojų) veiksmus (kurie susiję su asmens duomenų apdorojimu), taip užtikrinant atskaitingumą (jei įvyktų neautorizuotas Duomenų subjektų asmens duomenų atskleidimas, keitimas ar panaikinimas). Taip pat svarbu nuolat stebėti techninių žurnalų įrašus, kurie leistų identifikuoti potencialius vidinius ar išorinius bandymus pažeisti Darželio IT sistemos saugumą ir integralumą. Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai Darželio naudojamai IT sistemai, taikomajai programai, naudojamai Duomenų subjektų asmens duomenų apdorojimui. Techniniuose žurnaluose turi būti matomi visi įmanomi prieigų prie Duomenų subjektų asmens duomenų įrašų tipai *(Pvz.; data, laikas, peržiūrėjimas, keitimas, panaikinimas)*. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. Darželio (duomenų valdytojo) IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį. Rekomenduojamas techninių žurnalų įrašų saugojimo terminas: ne mažiau kaip 6 mėnesiai.

3. Tarnybinių stočių, duomenų bazių apsauga.

Darželio (duomenų valdytojo) informacinių sistemų pagrindas yra tarnybinės stotys ir Duomenų subjektų asmens duomenų bazės. Jų apsauga privalo būti sustiprinta, siekiant užtikrinti saugią darbo aplinką. Darželio (duomenų valdytojo) Duomenų subjektų asmens duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Darželio (duomenų valdytojo) Duomenų subjektų duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos Duomenų subjektų asmens duomenis, kurie yra reikalingi atitinkančiam asmens duomenų apdorojimo tikslui.

4. Darbo stočių apsauga.

Šis reikalavimas yra susijęs su saugos nustatymais Darželio IT sistemos naudotojų darbo stotyse ar kituose įrenginiuose. Yra svarbu nustatyti specifinę saugos politiką ir apriboti Darželio IT sistemos naudotojų veiksmus, siekiant apsaugoti Darželio (duomenų valdytojo) IT sistemas. Darželio (duomenų valdytojo) IT sistemos antivirusinės programos turi būti atnaujinamos ne rečiau kaip kas savaitę. Darželio (duomenų valdytojo) IT sistemos naudotojai neturi turėti privilegijų diegti, šalinti ir administruoti neautorizuotos programinės įrangos. Darželio (duomenų valdytojo) IT sistemos turi turėti nustatytą sesijos laiką, t. y. Darželio IT sistemos naudotojui esant neaktyviam, neveiksniam Darželio IT sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Rekomenduojamas neaktyvios sesijos laikas: ne daugiau kaip 15 min. Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.

5. Tinklo ir komunikacijos sauga.

Darželio (duomenų valdytojo) tinklo ir komunikacijos sauga yra ypač svarbi, siekiant užtikrinti Duomenų subjektų asmens duomenų saugą (tiek vidinių, tiek išorinių tinklų). Komunikacijai naudojamose susirašinėjimo programose, esant galimybei, rekomenduojama aktyvuoti ištisinio šifravimo (angl. end-to-end encryption) nuostatas. BDAR 32 straipsnis numato, kad atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei Duomenų subjektų asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus Duomenų subjektų (fizinių asmenų) teisėms ir laisvėms, Darželis (duomenų valdytojas) ir jo pagal sutartį pasamdytas duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant jei reikia:

a) pseudonimų suteikimą Duomenų subjektų asmens duomenims ir jų šifravimą;
b) užtikrinti nuolatinį Duomenų subjektų asmens duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą.

Kai prieiga prie Darželio naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus *(Pvz.; TLS, SSL).*

6. Atsarginės kopijos.

Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis Darželio (duomenų valdytojo) darbo ir procesų atstatymą, įvykus Duomenų subjektų asmens duomenų praradimui ar sugadinimui. Kopijų darymo dažnumas ir poreikis priklauso nuo Darželio IT sistemos ir joje apdorojamų Duomenų subjektų asmens duomenų. Atsarginės kopijos ir Duomenų subjektų asmens duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos Darželio instrukcijose ar taisyklėse. Darželio atsarginių kopijų laikmenoms saugumui privalo būti užtikrintas tinkamas fizinis aplinkos ir patalpų saugos lygis. Atsarginių kopijų darymo procesas Darželyje turi būti stebimas, siekiant užtikrinti jo užbaigtumą ir išsamumą. Atsarginės duomenų kopijos privalo būti daromos reguliariai.

7. Mobilieji, nešiojami įrenginiai.

Darželio mobilieji, nešiojami įrenginiai, kurie yra naudojami darbui su Darželio informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti, pagal Darželyje nustatyta tvarka. Darželio mobiliųjų ir nešiojamų įrenginių administravimo procedūros turi būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimąsi.

8. Programinės įrangos sauga.

Visuose programinės įrangos kūrimo ir administravimo etapuose Darželis turi užtikrinti Duomenų subjektų asmens duomenų apsaugą. BDAR 25 straipsnyje yra aprašomi Duomenų subjektų asmens duomenų apsaugos principai kurių reikalaujama iš Darželio užtikrinti tvarkant Duomenų subjektų asmens duomenis.
Darželio (duomenų valdytojo) informacinėse sistemose Duomenų subjektų asmens duomenų tvarkymui naudojama programinė įranga turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus ir turi būti laikomasi Duomenų subjektų asmens duomenų saugą užtikrinančių

programavimo standartų ir gerosios praktikos. Darželio (duomenų valdytojo) specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose. Darželio programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

9. Duomenų naikinimas, šalinimas.

Pagrindinis Darželio Duomenų subjektų asmens duomenų naikinimo tikslas yra negrįžtamas asmens duomenų šalinimas, sunaikinimas be teorinės ir praktinės galimybės juos pakartotinai nuskaityti ar atstatyti. Kai yra šalinama pasenusi, nenaudojama, nebereikalinga techninė įranga, Darželis privalo užtikrinti, kad visi prieš tai joje buvę sukaupti Duomenų subjektų asmens duomenis būtų negrįžtamai pašalinti. Pagal BDAR 5 straipsnį Duomenų subjektų asmens duomenis neturi būti saugomi, kaupiamai ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys yra Darželyje tvarkomi. Kai kuriais atvejais Duomenų subjektai turi teisę reikalauti savo asmens duomenis pašalinti anksčiau, negu yra nustatytas duomenų saugojimo, kaupimo terminas. Prieš pašalinant bet kokią Darželio duomenų laikmeną, turi būti sunaikinti visi joje esantys Duomenų subjektų asmens duomenis, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus asmens duomenų naikinimo algoritmus. Tais atvejais, kai to padaryti neįmanoma, turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti. Popierius ir nešiojamos Darželio asmens duomenų laikmenos, kuriose buvo saugomi, kaupiami Duomenų subjektų asmens duomenis, turi būti naikinami tam skirtais smulkintuvais.

10. Patalpų fizinė sauga.

Darželyje turi būti užtikrinta fizinė patalpų, kuriose yra Darželio IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.
Šių rekomenduojamų reikalavimų įgyvendinimas padės Darželio administracijai užtikrinti valdomų ir tvarkomų Duomenų subjektų asmens duomenų apsauga.

Pagarbiai

EB Law & Consulting
EB Teisė ir konsultacijos

Josifas Lovkys
Teisininkas -konsultantas
UAB „EB teisė ir konsultacijos“
Ukmergės g. 369A, 8 a., LT-12142, Vilnius
Mob. +370 698 11214
El. paštas: dap@eblaw.lt