TINKAMŲ ORGANIZACINIŲ IR TECHNINIŲ DUOMENŲ SAUGUMO PRIEMONIŲ ĮGYVENDINIMO GAIRĖS ASMENS DUOMENŲ VALDYTOJAMS IR TVARKYTOJAMS

2018-10-31

Šios gairės parengtos remiantis Europos Sąjungos tinklų ir informacijos saugos agentūros (ENISA, angl. *European Union Agency for Network and Information Security*) rekomendacijomis „Handbook on Security of Personal Data Processing, February 2018“, gairėmis „Guidelines for SMEs on the security of personal data processing, December 2017“ ir „ISO27k Forum“ pranešimu „Mapping between GDPR (the EU General Data Protection Regulation) and ISO27k, November 2016“.

Dėl gairių taikymo organizacijoje

Prie visų šiose gairėse išvardytų reikalavimų pateikta nuoroda į susijusį saugumo valdymo **standarto** (Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai. LST EN ISO/IEC 27001:2017) reikalavimą ir pateikti paaiškinimai, atsižvelgiant į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos **reglamentą** (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR).

Šiose gairėse išdėstyti **minimalūs organizaciniai** ir **techniniai** duomenų saugumo reikalavimai gali būti laikytini pakankamais tik tose organizacijose, kurių tvarkomų asmens duomenų saugumo **rizika**, susijusi su pavojais fizinių asmenų teisėms ir laisvėms, **yra žema**.

Atkreipiame dėmesį, kad kuriant (diegiant) ar vertinant turimas organizacines ir technines saugumo priemones, organizacijos turi visapusiškai atsižvelgti į „pobūdį, aprėptį, kontekstą bei tikslus“ ir riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms. BDAR 24 ir 32 straipsniai organizacijas įpareigoja **visais atvejais atlikti rizikos vertinimą**.

Minimalūs reikalavimai duomenų valdytojams ir tvarkytojams dėl tinkamų organizacinių duomenų saugumo priemonių

Eil. Nr.	Reikalavimas	Atitikmuo ISO 27001:2017 A priede	Atitikmuo BDAR ir paaiškinimai
Asmens duomenų saugumo politika ir procedūros			
1.	Asmens duomenų ir jų tvarkymo saugumas organizacijoje turi būti dokumentuotas kaip informacijos saugumo politikos dalis.	**A.5 Informacijos saugumo politika**	Saugumo politika yra svarbus dokumentas, nustatantis pagrindinius informacijos saugumo ir asmens duomenų apsaugos principus organizacijoje. Tai yra visų konkrečių techninių ir organizacinių priemonių įgyvendinimo pagrindas pagal BDAR 32 straipsnį ir jį papildantį 24 straipsnį dėl duomenų valdytojo įgyvendinamos atitinkamos duomenų apsaugos politikos. Remiantis saugumo politika, konkrečios techninės ir organizacinės priemonės aprašomos detalesnėse politikose (pvz., prieigos kontrolės, įrenginių valdymo, išteklių valdymo ir kt.). Saugumo politika nustato bendrą organizacijos informacijos saugos valdymą ir gali būti dalis bendros organizacijos IT saugos politikos. Bet kuriuo atveju saugumo politikoje turi būti aiškiai išskirta asmens duomenų apsauga.
2.	Saugumo politika turi būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.		
Vaidmenys ir atsakomybės			
3.	Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką.	**A.6.1.1 Su informacijos saugumu susiję vaidmenys ir atsakomybės**	BDAR 32 straipsnio 4 dalis numato, kad duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas

4.	Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu).		duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Europos Sąjungos arba valstybės narės teisę. Pagrindinė asmens duomenų saugumo priemonė organizacijos personalui, turinčiam prieigą prie asmens duomenų – aiškiai apibrėžta ir dokumentuota atsakomybė bei vaidmenys, taip pat darbo su asmens duomenimis kompetencijos. Ypač svarbus vaidmuo tenka saugos specialistui (ar įgaliotiniui), kuris yra atsakingas už tinkamos saugumo politikos įgyvendinimą. Kitas svarbus vaidmuo tenka duomenų apsaugos pareigūnui (toliau – DAP), kuris prižiūri, kaip laikomasi BDAR. Šie asmenys turi glaudžiai bendradarbiauti. Reikėtų pažymėti, kad tam tikrais atvejais pagal BDAR 37 straipsnį DAP paskyrimas yra privalomas.
Prieigos valdymo politika			
5.	Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. *need to know*) principu.	**A.9.1.1 Prieigos valdymo politika**	Būtina nustatyti prieigos kontrolės politiką sistemoms, naudojamoms tvarkant asmens duomenis. Kontrolė turi būti grindžiama principu „būtina žinoti“, t. y. kiekvienam vaidmeniui ar naudotojui turėtų būti suteiktas tik toks asmens duomenų prieinamumo lygis, kuris yra būtinas jo užduotims atlikti. Šis reikalavimas glaudžiai susijęs su duomenų kiekio mažinimo principu (BDAR 5 straipsnio 1 dalies c punktas). Prieigos kontrolės politika turi būti įgyvendinama taikant technines priemones (taip pat žiūrėti šių gairių 18–21 punktus „Prieigų kontrolė ir autentifikavimas“).

Išteklių ir turto valdymas			
6.	Organizacija turi turėti IT išteklių, naudojamų asmens duomenims tvarkyti, registrą (techninės, programinės ir tinklo įrangos). Registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). Registro tvarkymas turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui.	**A.8 Turto tvarkymas**	Tinkamas techninės, programinės ir tinklo įrangos valdymas yra būtinas asmens duomenų saugumui ir vientisumui, nes tai leidžia kontroliuoti duomenų apdorojimo priemones. Išteklių valdymas būtinai turi apimti IT išteklių ir tinklo topologijos, kuri yra naudojama tvarkant asmens duomenis, registravimą. Vientisumo ir konfidencialumo principas apibrėžtas BDAR 5 straipsnio 1 dalies f punkte.
7.	IT ištekliai turi būti reguliariai peržiūrimi ir atnaujinami. Siūlomas peržiūros dažnumas: kartą per 3 mėnesius.		
Pakeitimų valdymas			
8.	Organizacija turi užtikrinti, kad visi IT sistemų pakeitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto (ar įgaliotinio)).	**A. 12.1 Darbo procedūros ir atsakomybės**	Pakeitimų valdymo tikslas – sinchronizuoti ir kontroliuoti visus IT sistemose, naudojamose tvarkant asmens duomenis, atliekamus pakeitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas pakeitimų įgyvendinimas gali sukelti neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą. Pakeitimų valdymas yra būtinas duomenų tvarkymo vientisumui užtikrinti (BDAR 5 straipsnio 1 dalies f punktas) ir duomenų valytojo atskaitomybės principui įgyvendinti (BDAR 5 straipsnio 2 dalis).
9.	Programinės įrangos kūrimas turėtų būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų,		

	naudojamų tvarkant asmens duomenis. Testuojant sistemas, reikia naudoti testinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros.		
Duomenų tvarkytojai			
10.	Prieš pradedant asmens duomenų tvarkymo veiklą, duomenų valdytojai ir duomenų tvarkytojai turėtų apibrėžti, dokumentuoti ir suderinti formalias gaires ir procedūras, taikomas duomenų tvarkytojams (rangovams ar užsakomosioms paslaugoms) dėl asmens duomenų tvarkymo. Šios gairės ir procedūros turi nustatyti tokį patį asmens duomenų saugumo lygį, koks yra numatytas organizacijos saugumo politikoje.	**A.15 Santykiai su tiekėjais**	BDAR 28 straipsnis numato, kad „duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.“ Tame pačiame straipsnyje teigiama, kad duomenų tvarkytojas turi veikti pagal sutartį ar kitą teisės aktą.
11.	Duomenų tvarkytojas privalo nedelsdamas pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus.		
12.	Duomenų valdytojas ir duomenų tvarkytojas turi oficialiai susitarti dėl formalių reikalavimų ir prievolių. Duomenų tvarkytojas turi pateikti		

	dokumentais pagrįstus įrodymus dėl atitikties keliamiems reikalavimams.		
Asmens duomenų saugumo pažeidimai ir incidentai			
13.	Turi būti nustatytas reagavimo į incidentus planas su išsamia tvarka, kad būtų užtikrintas veiksmingas incidentų, susijusių su asmens duomenimis, valdymas.	**A.16 Informacijos saugumo incidentų valdymas**	Duomenų saugumo pažeidimo atveju organizacija turi įvertinti, ar tai turės įtakos „atsitiktiniam ar neteisėtam perduodamų, saugomų ar kitaip tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, neteisėtam atskleidimui ar prieigai prie jų“ (BDAR 4 straipsnio 12 dalis). Duomenų valdytojai turi būti tikri, kad jie laikosi savo įsipareigojimų pagal BDAR 33 ir 34 straipsnius, susijusius su pranešimu apie asmens duomenų saugumo pažeidimus priežiūros institucijai ir duomenų subjektams. Duomenų tvarkytojai taip pat turi būti tikri, kad jie laikosi savo įsipareigojimų pagal BDAR 33 straipsnį ir galės nedelsdami pranešti duomenų valdytojui apie minėtus pažeidimus. Bet kuriuo atveju, tiek duomenų valdytojai, tiek ir tvarkytojai turi turėti tinkamas procedūras ne tik pranešti apie asmens duomenų pažeidimus, bet ir juos suvaldyti.
14.	Apie asmens duomenų pažeidimus turi būti nedelsiant pranešama vadovybei. Turi būti nustatyta pranešimo apie pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka, vadovaujantis BDAR 33 ir 34 straipsniais.		
Veiklos tęstinumas			
15.	Organizacija turi nustatyti pagrindines procedūras, kurių reikia laikytis incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.	**A. 17 Veiklos tęstinumo valdymo informacijos saugumo aspektai**	Veiklos ar paslaugų tęstinumo planas yra būtinas nustatant procesus ir technines priemones, kurių organizacija turėtų laikytis incidento ar asmens duomenų pažeidimo atveju. Šis planas papildo organizacijos saugumo politiką. Ši priemonė aiškiai susijusi su BDAR 32 straipsnio 1 dalies c punktu, kuris įpareigoja duomenų valdytoją ir tvarkytoją „laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“.

Personalo konfidencialumas			
16.	Organizacija turi užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu. Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus.	**A.7 Žmogiškųjų išteklių saugumas**	Siekiant užtikrinti asmens duomenų konfidencialumą pagal BDAR 32 straipsnį, organizacija 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 „duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Sąjungos arba valstybės narės teisę“. Šiuo tikslu turėtų būti nustatytos specialios priemonės, užtikrinančios, kad asmenys, dalyvaujantys tvarkant asmens duomenis, būtų tinkamai informuojami apie savo pareigą laikytis konfidencialumo. Taip pat turi būti užtikrinta, kad šios pareigos būtų pakankamai apibrėžtos organizacijos žmogiškųjų išteklių politikoje.
Mokymai			
17.	Organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi dėl atitinkamų duomenų apsaugos reikalavimų ir teisinių įsipareigojimų rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų dažnumas: kartą per metus.	**A.7.2.2 Informacijos saugumo supratimas, švietimas ir mokymas**	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 sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų“ (BDAR 32 straipsnio 2 dalis). Žinios apie konkrečius duomenų apsaugos teisinius įsipareigojimus taip pat yra svarbios, ypač tiems asmenims, kurie dalyvauja didelės rizikos asmens duomenų tvarkymo procesuose.

Minimalūs reikalavimai duomenų valdytojams ir tvarkytojams dėl tinkamų techninių duomenų saugumo priemonių

	Reikalavimas	Atitikmuo ISO 27001:2017 A priede	Atitikmuo BDAR ir paaiškinimai
	Prieigų kontrolė ir autentifikavimas		
18.	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.	**A.9 Prieigos valdymas**	Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie IT sistemos, kurioje yra apdorojami asmens duomenys. Šie saugos reikalavimai įgyvendina organizacijos prieigų kontrolės politiką (taip pat žiūrėti šių gairių 5 punktą „Prieigos valdymo politika“) techniškai panaudojant specifinius komponentus ir taikomąsias programas.
19.	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.		
20.	Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas		

	atsižvelgiant į tam tikrą kompleksiškumo lygį.		
21.	Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio.		
Techninių žurnalų įrašai ir stebėsena			
22.	Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, taikomajai programai, naudojamai asmens duomenų apdorojimui. Techniniuose žurnaluose turi būti matomi visi įmanomi prieigų prie asmens duomenų įrašų tipai (pvz., data, laikas, peržiūrėjimas, keitimas, panaikinimas). Siūlomas saugojimo terminas: ne mažiau kaip 6 mėnesiai.	**A.12.4 Įvykių registravimas ir stebėsena**	Techninių žurnalų įrašai yra esminis saugos reikalavimas, kuris leidžia identifikuoti ir stebėti, sekti naudotojų veiksmus (kurie susiję su asmens duomenų apdorojimu), taip užtikrinant atskaitingumą (jei įvyktų neautorizuotas asmens duomenų atskleidimas, keitimas ar panaikinimas). Taip pat svarbu nuolat stebėti techninių žurnalų įrašus, kurie leistų identifikuoti potencialius vidinius ar išorinius bandymus pažeisti sistemos saugumą ir integralumą.
23.	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.		

Tarnybinių stočių, duomenų bazių apsauga			
24.	Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis.	**A.12 Darbo saugumas**	Informacinių sistemų pagrindas yra tarnybinės stotys ir duomenų bazės. Jų apsauga privalo būti sustiprinta, siekiant užtikrinti saugią darbo aplinką.
25.	Duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos asmens duomenis, kurie yra reikalingi darbui, atitinkančiam duomenų apdorojimo tikslus.		
Darbo stočių apsauga			
26.	Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti saugos nustatymų.	**A.14.1 Informacinių sistemų saugumo reikalavimai**	Šis reikalavimas yra susijęs su saugos nustatymais naudotojų darbo stotyse ar kituose įrenginiuose. Yra svarbu priverstinai nustatyti specifinę saugos politiką ir apriboti naudotojų veiksmus, siekiant apsaugoti IT sistemas (pvz., antivirusinės programinės įrangos išjungimas, neautorizuotos programinės įrangos diegimas).
27.	Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kas savaitę.		
28.	Naudotojams negalima turėti privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos.		

29.	IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam, neveiksniam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Siūlomas neaktyvios sesijos laikas: ne daugiau kaip 15 min.		
30.	Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.		
Tinklo ir komunikacijos sauga			
31.	Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS, SSL).	**A.13 Ryšių saugumas**	Tinklo ir komunikacijos sauga yra ypač svarbi, siekiant užtikrinti 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 tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant *inter alia*, jei reikia: - pseudonimų suteikimą asmens duomenims ir jų šifravimą; - gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą; <...>“.

Atsarginės kopijos			
32.	Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susaistytos su rolėmis ir pareigomis.	**A.12.3 Atsarginės kopijos**	Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis organizacijos darbo ir procesų atstatymą, įvykus duomenų praradimui ar sugadinimui. Duomenų kopijų darymo dažnumas ir poreikis priklauso nuo organizacijos ir joje apdorojamų duomenų. BDAR 32 straipsnis numato „gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“.
33.	Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų.		
34.	Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą, išsamumą.		
35.	Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Siūlomas atsarginių kopijų darymo dažnumas: - kasdien – pridedamoji kopija; - kas savaitę – pilna kopija.		
Mobilieji, nešiojami įrenginiai			
36.	Mobiliųjų ir nešiojamų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimąsi.	**A.6.2 Mobilieji įrenginiai ir nuotolinis darbas**	Mobilieji, nešiojami įrenginiai gali išplėsti paslaugas, kurias teikia duomenų valdytojas, tačiau padidina riziką juose esančių duomenų nutekėjimui. Mobiliuosius įrenginius, tokius kaip išmanieji telefonai ar planšetės, naudotojai gali panaudoti savo asmeninėms reikmėms, todėl reikia užtikrinti, kad

37.	Mobilieji, nešiojami įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.		naudotojų asmeniniai duomenys ir organizacijoje administruojami asmens duomenys nebūtų atskleisti.
38.	Mobilieji įrenginiai turi būti adekvataus prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims apdoroti.		
Programinės įrangos sauga			
39.	Informacinėse sistemose naudojama programinė įranga (asmens duomenims apdoroti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. *frameworks*), standartus.	**A.12.6 Techninio pažeidžiamumo valdymas ir A.14.2 Kūrimo ir priežiūros procesų saugumas**	Visuose programinės įrangos kūrimo ir administravimo etapuose organizacija turi užtikrinti duomenų saugos laikymąsi, asmens duomenų apsaugą. BDAR 25 straipsnyje yra aprašomi duomenų apsaugos principai kuriant programinę įrangą, baziniai programinės įrangos saugumo nustatymai, kurių reikalaujama iš duomenų valdytojų, užtikrinant griežčiausius privatumo nustatymus.
40.	Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.		
41.	Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.		

42.	Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.		
Duomenų naikinimas, šalinimas			
43.	Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Tais atvejais, kai to padaryti neįmanoma (pvz., CD, DVD laikmenos ir pan.), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.	**A.8.3.2 Duomenų laikmenų naikinimas ir A.11.2.7 Saugus įrangos naikinimas arba pakartotinis naudojimas**	Pagrindinis 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, duomenų valdytojas privalo užtikrinti, kad visi prieš tai joje buvę sukaupti duomenys būtų negrįžtamai pašalinti. Pagal BDAR 5 straipsnį asmens duomenys neturi būti saugomi, kaupiamai ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. Kai kuriais atvejais duomenų subjektai turi teisę reikalauti duomenis pašalinti anksčiau, negu yra nustatytas duomenų saugojimo, kaupimo terminas.
44.	Popierius ir nešiojamos duomenų laikmenos, kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinami tam skirtais smulkintuvais.		
Fizinė sauga			
45.	Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.	**A.11 Fizinis ir aplinkos saugumas**	Fizinė apsauga yra ne mažiau svarbi negu technologinės saugumo priemonės, nes tiesioginės fizinės prieigos kontrolė prie IT infrastruktūros yra visos taikomos saugos strategijos pagrindas.