

VDAI gairs dl pritaikytosios ir standartizuotosios asmens duomen apsaugos: k atkreipia dmes?

Duomen apsaugos pareignas Allaw® supažindina

Valstybin duomen apsaugos inspekcija (toliau - VDAI) paskelb gaires dl pritaikytosios ir standartizuotosios duomen apsaugos informacins sistemos gyvavimo cikle (toliau - gairs). Šios gairs, tikimasi, pads duomen valdytojams ir duomen tvarkytojams gyvendinant Bendrojo duomen apsaugos reglamento (toliau - BDAR) 25 str. tvirtintus reikalavimus. [Duomen apsaugos pareignas Allaw](#) atkreipia dmes ir supažindina su **svarbiausiais VDAI gairi aspektais, kurie turt bti taikomi kiekvieno duomen valdytojo ir duomen tvarkytojo duomen tvarkymo veikloje.**

Kam gairs gali labiausiai padti?

Kaip nurodoma paiose gairse, jos turt padti [duomen valdytojams](#) ir duomen tvarkytojams, o vis pirma jos skirtos duomen valdytojo ar duomen tvarkytojo informacini sistem ar atskiros programins, technins rangos krjams:

Gairs vis pirma skirtos:

- IT projekt vadovams,
- IT architektams,
- programuotojams,
- testuotojams,
- duomen apsaugos pareignams
- ir kitiems asmenims, kurie dalyvauja informacini sistem, kuriose tvarkomi asmens duomenys krime.

Informacins sistemos gyvavimo ciklas apima visus sistemos bsenos pokylius nuo jos steigimo pagrindo nustatymo iki veikimo pabaigos, t.y., informacins sistemos inicijavimas, krimas, eksploatavimas, modernizavimas, likvidavimas. Gairse pateikta gyvavimo ciklo koncepcija taip pat taikytina atskiram programins ar technins rangos vystymui. Gairse pateikia informacija kokijs aspektus kiekviename iš sistemos gyvavimo etap reikalinga atkreipti dmes. [Duomen apsaugos pareignas Allaw](#) atkreipia dmes **svarbiausius aspektus ne tik mintuose etapuose, bet ir kasdienje duomen tvarkymo veikloje.**

Svarbu ...

[Pasitikrinti, kad taikomos duomen saugumo priemonis atitinka rizikos lyg](#)

[sitikinti, kad darbuotojai yra praj BDAR mokymus](#)

[Pasitikrinti, ar BDAR mokym programa atitinka reikalavimus](#)

Nepamiršti

Mokymai turi bti reguliars ir vykdomi bei

VDAI paskelb gaires dl pritaikytosios ir standartizuotosios asmens duomen apsaugos

Darbuotoj mokym svarba

Kaip ne kart yra pažymjusi VDAI, mokymai yra viena pagrindini organizacini asmens duomen saugumo priemoni, padedanti užtikrinti bet kokios organizacijos atitikt BDAR 24, 25, 28, 32 str. ir 39 str. 1 d. b) punkto reikalavimams. Juo rengti pareigoja ir BDAR 37, 43 str. Jie ypatingai svarbs ir sistemos inicijavimo procese, kai nustatomos asmens duomen tvarkymo operacijos, asmens duomen ir duomen subjekt kategorijos, duomen teikjai ir duomen gavjai bei identifikuojamas poreikis gyti papildomas žinias ar kompetencijas.

Vadovaujantis VDAI gairmis, mokymai ir kompetencijos pagal profesines grupes turt apimti bent žemiau nurodytas temas.

Mokymai ir kompetencijos turt apimti bent šias temas:

- su asmens duomen tvarkymu susij principai, asmens duomen teisto tvarkymo slygos, specialij kategorij asmens duomen, asmens duomen apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas (BDAR 5–10 straipsniai);
- duomen subjekto teiss (BDAR 12–23 straipsniai);
- duomen valdytojai ir duomen tvarkytojai, j atsakomybs, asmens duomen saugumo principai (BDAR 24–43);
- informacijos saugumo valdymo sistem pagrindai (pvz., ISO 27001, ISF Standard of Good Practice for Information Security);
- programins rangos krimo standartai (pvz., ISO 27034, SDL);
- saugumo testavimas (pvz., OWASP Testing Guide, OWASP ASVS, OWASP Top 10);
- kibernetini grsmi rizikos vertinimas (pvz., STRIDE, DREAD);
- vidins organizacijos privatumo, saugos procedros ir dokumentacija.

darbuotoj žinios
atnaujinamos ne
reiau kaip kart
per metus.



Susisiekt i

Teirautis dl prieigos
prie BDAR mokym
e-medžiagos

Sužinoti apie
inovatyvi
paslaug duomen
apsaugos
pareignas Allaw®

Palikti žinut
duomen apsaugos
pareignui Allaw®

Telefonu: 8-616
02000

k atkreipti dmes, nustatant duomen saugumo priemonės?

Kuriant informacinės sistemas / programinį rang asmens duomenims tvarkyti ypatingai svarbu, kad jos atitikt asmens duomen tvarkymo principus (BDAR 5 str.), leist gyvendinti duomen subjekt teises (BDAR 12-22 str.) bei užtikrint atitinakam duomen saugumo lyg (BDAR 24, 25, 32–34 str.). Nustatant duomen saugumo priemonės organizacijoms pirmiausia reikalinga atlikti rizikos vertinim (BDAR 24 ir 32 str.). Vadovaujantis naujausiomis VDAI gairmis atliekant š vertinim verta:

1

Nustatyti priimtinos rizikos lygius duomen apsaugai bent pagal šias kategorijas:

neturi vykti asmens duomen saugumo pažeidimai duomen subjektas privalo kontroliuoti savo asmens duomenis;
negali bti nepagrstai apribotos duomen subjekto teiss ar laisvs;
duomen subjektas negali bti profiliuojamas arba diskriminuojamas;
negali bti pavogta duomen subjekto tapatyb;
duomen subjektas neturi patirti finansini nuostoli;
negali bti paveikta duomen subjekto reputacija;
pseudonim suteikimo atvejais neturi bti manoma atsekti tikrosios tapatybs; neturi vykti asmens duomen saugumo pažeidimai

2

Nustatyti priimtinos rizikos lygius duomen saugumui bent pagal šias kategorijas:

asmens duomenys negali bti netyia ar neteistai pakeisti, prarasti ar sunaikinti;
asmens duomenys negali bti neteistai atskleisti;
asmens duomenys turi bti apsaugoti atsižvelgiant programins rangos konfidencialum, vientisum, prieinamum ir atsparum;
asmens duomenys turi bti pseudonimizuoti ir (ar) užšifruoti;
vykus fiziniam ar techniniam incidentui, turi bti manoma laiku atkurti galimyb tvarkyti asmens duomenis;
turi bti užtikrintas reguliarius duomen tvarkymo saugumo priemoni veiksmingumo vertinimas.

3

Pagal rizikos vertinimo rezultatus numatyti tinkamas organizacines ir technines saugumo priemonės

VDAI rekomenduoja

Pai priemoni nustatymas turt remtis ankstesnėmis VDAI Tvarkom asmens duomen saugumo priemoni ir rizikos vertinimo gairėmis duomen valdytojams ir duomen tvarkytojams bei OWASP programins rangos saugos užtikrinimo standartu (angl. OWASP Application Security Verification Standard 4.0.1).

Taikom priemoni reguliari peržiūra

Atsižvelgiant tai, kad tiek informacini sistem / programins rangos, bei duomen tvarkymo veikla apskritai paprastai yra dinamiška veikla (neretai keičiasi jos apimtis, dalyviai ir pan.) ypatingai svarbu užtikrinti reguliari pasirinkt priemoni BDAR reikalavimams gyvendinti peržiūr ir atnaujinim. VDAI atkreipia dėmesį, kad nuolat vertinant technini ir organizacini saugumo priemoni veiksmingumą turi būti vertinti:

1. pažeidžiamumo analiz ir skverbimosi testai;
2. nuolatiniai automatiniai programins rangos, infrastruktūros ir tinklo bklų patikrinimai;
3. serverio ir kliento programins rangos bei trejų šali komponent taisymas;
4. našumo patobulinimai, laiku atliekami rangos atnaujinimai, pvz., operacini sistem, programins rangos bibliotek, šifravimo algoritmai ir j rakt atnaujinimai ir pan.;
5. sistemos vyki ir vartotojų veiklos registravimas, periodiškų žurnalų peržiūra siekiant nustatyti saugumo pažeidimus;
6. reguliari mokymai, instruktažai ir pan.;
7. asmens duomen apsaugos kultūros laikymasis (pvz., apklausos, testai ir pan.);
8. **incident valdymo plano** reguliari atnaujinimas;
9. vidaus ir išorės auditai ar kitokios formos atitikim taisykloms (teisės aktams, elgesio kodeksams, vidaus taisykloms, saugos politikai ir pan.) dokumentavimas;
10. periodiniai duomen tvarkytojų ir trejų šali patikrinimai dėl susitarimų laikymosi.

Nuorodos

Kur eiti toliau

Kur eiti toliau

<https://allaw.lt/klauskite-teisininko/>
<https://allaw.lt/legalspaces/display/DAPaaS/Allaw+BDAR+atitikties+portalas>
<https://allaw.lt/legalspaces/quiz/learning/view.action?category=1>
<https://allaw.lt/legalspaces/site/duomenu-apsaugos-pareigunas>
<https://teisinerizika.lt/work/bdar-reikalavimai/>
https://vdai.lrv.lt/lt/news/view_item/id.157
https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf
Blog: VDAI gairės dėl pritaikytosios ir standartizuotosios asmens duomen apsaugos: k atkreipia dėmesį?

Panašs straipsniai

Panašs straipsniai

Content by label

There is no content with the specified labels





Naudingi ištekliai

[BDAR e-vedlys](#)

[BDAR e-mokym erdv](#)

[BDAR auditas \(klausimynas\)](#)