



DUK. AKREDITAVIMAS PAGAL BDAR. Kokie reikalavimai taikomi siekiant teikti sertifikavimo paslaugas pagal BDAR?

2024-12-11

Valstybinė duomenų apsaugos inspekcija (toliau – VDAI), patvirtinusi fizinių ir juridinių asmenų, siekiančių teikti sertifikavimo paslaugas, akreditavimo procedūrą, parengė šį atsakymą į kelis iš dažnai užduodamų klausimų dėl Bendrojo duomenų apsaugos reglamento¹ (toliau – BDAR) 42 ir 43 straipsnių taikymo.

1. Kada organizacijos gali kreiptis dėl jų asmens duomenų tvarkymo veiklų sertifikavimo?

VDAI pabrėžia, kad **sertifikavimasis nėra privalomas**. Kitaip tariant asmens duomenų tvarkymas gali būti atliekamas ir neturint sertifikato pagal BDAR. Vis dėlto, sertifikuotis **gali būti naudinga pačioms organizacijoms** ar tam tikras asmens duomenų tvarkymo paslaugas teikiantiems fiziniams asmenims.

Sertifikatus galės išduoti **tik VDAI akredituotos sertifikavimo įstaigos**, kurios teiks sertifikavimo paslaugas **pagal sertifikavimo kriterijus**, kurie pagal BDAR įtvirtintą nuoseklumo užtikrinimo procedūrą turės būti **įvertinti visų asmens duomenų apsaugos priežiūros institucijų** ir dėl kurių Europos duomenų apsaugos valdyba (toliau – EDAV) bus priėmusi nuomonę. Tai reiškia, kad **sertifikatus pagal BDAR turintys asmenys** galės **jais naudotis** siekiant jų paslaugų gavėjams papildomai **pagrįsti**, kad tam tikra jų atliekama asmens duomenų tvarkymo veikla **atitinka BDAR** reikalavimus.

Pastaba. BDAR nustatytas sertifikavimo mechanizmas skirtas sertifikuoti **ne konkretų produktą** (prekę, įrangą, kt.), bet **asmens duomenų tvarkymo veiklą**.

Asmens duomenų tvarkymo veikla – asmens duomenų tvarkymo veiksmų (etapų) rinkinys, siekiant **konkretaus asmens duomenų tvarkymo tikslo**.

2. Kas gali teikti sertifikavimo paslaugas?

Sertifikavimo paslaugas galės teikti tik tokios sertifikavimo įstaigos, kurios (**taikomos visos sąlygos**):

¹ [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 95/46/EB \(Bendras duomenų apsaugos reglamentas\).](#)

- Turi teisę **naudotis sertifikavimo kriterijais** (dėl kurių gauta EDAV nuomonė, žr. [sąrašą](#)), t. y. yra gavę šių kriterijų savininko sutikimą sertifikavimo kriterijus naudoti, **arba yra tokių sertifikavimo kriterijų savininkės** (dėl tokių sertifikavimo kriterijų EDAV nuomonė taip pat turi būti gauta, žr. [Sertifikavimo kriterijų patvirtinimo tvarkos aprašą](#)).
- **Kurias akreditavo VDAI** (žr. [Sertifikavimo įstaigų akreditavimo tvarkos aprašą](#) (toliau – Akreditavimo aprašas)).

Pastebėtina, kad sertifikavimo įstaiga gali būti tiek fizinis, tiek juridinis asmuo, atitinkantis nustatytus akreditavimo kriterijus (žr. Akreditavimo tvarkos aprašo 1 priedą).

3. Ką svarbu žinoti, siekiant būti akredituotu teikti sertifikavimo paslaugas?

VDAI rekomenduoja, prieš teikiant prašymą akredituoti teikti sertifikavimo paslaugas, įvertinti, ar esate pasiruošę jas teikti (įvertinant ir tai, kad akreditavimo paslaugų teikimas yra mokamas). **Jeį neturite reglamentuotų būtinų procedūrų ar personalo**, rekomenduojame, visų pirma, imtis priemonių šiems reikalavimams užtikrinti, nes priešingu atveju Jūsų akreditavimas gali ilgai užtrukti arba gali būti atsisakyta Jus akredituoti.

Jeį nesate tikri, ar esate pasiruošę teikti sertifikavimo paslaugas, siūlytume atitiktis nustatytiems reikalavimams vertinimą, **visų pirma**, atlikti patiems. Pavyzdžiui, norėdami atitikti reikalavimą dėl susitarimo dėl sertifikavimo paslaugų teikimo, turite įvertinti, ar Jūsų parengtame susitarimo projekte yra aptarti visi reikalavimai, nustatyti Akreditavimo aprašo 1 priedo 4.1.2 skiltyje (įskaitant atitinkamą skiltį ISO 17065 standarte²).

² LST EN ISO/IEC 17065:2012 „Atitiktis įvertinimas. Reikalavimai, keliami produktų, procesų ir paslaugų sertifikavimo įstaigoms“ standartas.

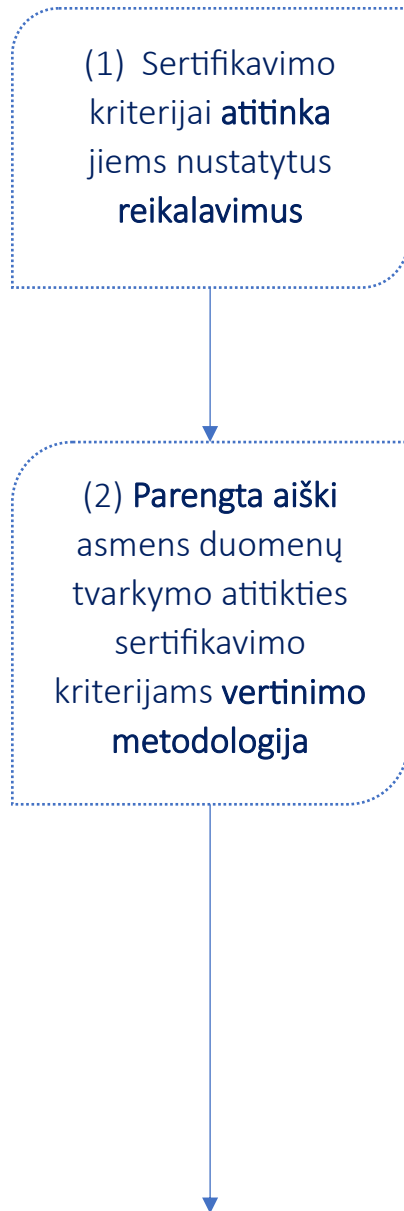


***Pastaba.** VDAI pabrėžia, kad nors sertifikavimo įstaigos turi atitikti tiek Akreditavimo aprašo 1 priede, tiek ISO 17065 standarte nustatytus akreditavimo reikalavimus, **VDAI neakredituoja jų pagal ISO 17065 standartą.**

VDAI vertina atitiktį šiame standarte esantiems reikalavimams tiek, kiek būtina įvertinti sertifikavimo įstaigos galimybes teikti sertifikavimo paslaugas pagal konkrečius sertifikavimo kriterijus (sertifikavimo schemą), vadovaujantis BDAR.

4. Noriu patvirtinti savo sertifikavimo kriterijus, kokia procedūra man taikoma?

Rekomenduotume, visų pirma, įsivertinti, ar esate tinkamai pasiruošę pradėti procedūrą, t. y. ar parengti sertifikavimo kriterijai atitinka jiems nustatytus reikalavimus (1 žingsnis), taip pat ar esate pasiruošę visą sertifikavimo metodologiją ir kitą būtiną medžiagą, sudarančią sąlygas išsamiai įvertinti, kaip turėtų būti atliekamas sertifikavimas pagal šiuos kriterijus (2 žingsnis).

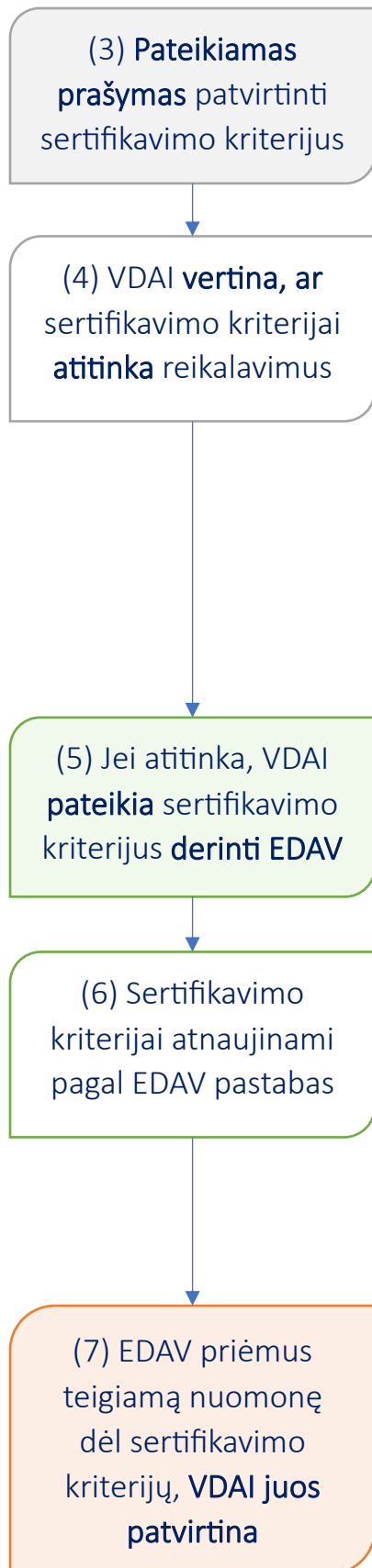


(1 žingsnis) Sertifikavimo kriterijai turi būti:

- › nuoseklūs ir atitikti jais siekiamus tikslus;
- › svarbūs ir tinkami, siekiant įrodyti konkrečių subjektų, kuriuos siekiama sertifikuoti, atitiktį BDAR (ir pritaikomi organizacijos, įvertinant ir jų dydį, sektorių ir kt.);
- › suformuluoti nuosekliai, aiškiai, suprantamai ir taip, kad juos būtų galima patikrinti ir taikyti praktiškai;
- › *kai taikoma*, suderinami su kitais teisės aktais ir standartais
- › Suderinami su BDAR ir EDAV gairėmis (žr. „Naudinga informacija“ žemiau).

(2 žingsnis) Be sertifikavimo kriterijų taip pat būtina pateikti:

- › Sertifikavimo **mechanizmo aprašymą** (Europos duomenų apsaugos ženklo atveju, papildomai paaiškinama, kaip šis mechanizmas bus pritaikomas išduodant sertifikatus organizacijoms, veikiančioms kitose ES valstybėse);
- › Sertifikavimo **kriterijų ryšį su BDAR straipsniais** (kokių BDAR straipsnių atitiktį kiekvienas iš sertifikavimo kriterijų užtikrins);
- › **Atitikties sertifikavimo kriterijams vertinimo aprašymą** (vertinimo metodologiją);
- › (*sertifikavimo pagal BDAR 46 straipsnį atveju, jei taikoma*) kaip bus užtikrinama, kad **asmens duomenų importuotojai** (trečiosiose valstybėse), kuriems netaikomas BDAR ir kurie nori sertifikuotis pagal BDAR 46 straipsnį, **taikys sertifikavimo mechanizmu numatytas tinkamas apsaugos priemones**;
- › (*Europos duomenų apsaugos ženklo atveju, jei taikoma*) taikytinų **nacionalinių teisės aktų sąrašą** ir paaiškinimą, kaip jis buvo sudarytas, kaip bus užtikrinamas jo aktualumas.



(3, 4 žingsniai) Visi aukščiau nurodyti dokumentai ir informacija (lietuvių ir anglų kalbomis), pridedami prie laisvos formos prašymo, **pateikiami vertinti VDAI**.

VDAI vertina nurodytą sertifikavimo mechanizmą, sertifikavimo kriterijų taikymo sritį (sritis), tinkamumą sertifikavimo funkcijai atlikti.

Atliekant šį vertinimą atsižvelgiama į [BDAR](#), [EDAV gairių Nr. 1/2018](#) 47 ir 67 punktus ir jų 2 priede nustatytas kriterijų vertinimo gaires, [EDAV gairių Nr. 07/2022](#) 3 skyrių ir [EDAV dokumentą dėl Europos duomenų apsaugos ženklo](#).

Sertifikavimo kriterijų vertinimas atliekamas **per 8 savaites** (terminas pradedamas skaičiuoti nuo paskutinių dokumentų VDAI pateikimo, o jei VDAI neprašė pateikti papildomų dokumentų, nuo tos dienos, kai pateiktas tinkamas prašymas). Šis terminas **gali būti pratęstas 6 savaitėms** (įvertinant pateiktos informacijos apimtį ir sudėtingumą ar kitas svarbias aplinkybes).

(5, 6 žingsniai) Tuo atveju, **jei sertifikavimo kriterijai atitinka** jiems nustatytus reikalavimus, VDAI parengia sprendimo projektą ir **pateikia** jį su sertifikavimo kriterijais (ir visai kartu pateiktais dokumentais) **EDAV**.

EDAV pateikia gautą medžiagą vertinti visoms asmens duomenų apsaugos priežiūros institucijoms ir jų gautos pastabos aptariamos EDAV posėdyje. Suderintos pastabos pateikiamos prašymą patvirtinti sertifikavimo kriterijus pateikusiam asmeniui (t. y. Jums). Sertifikavimo kriterijai turi būti atnaujinti pagal gautas pastabas. **Pastaba.** EDAV pastabas dėl sertifikavimo kriterijų gali teikti kelis kartus.

Atnaujinti sertifikavimo kriterijai pateikiami vertinti EDAV. Įvertinus gautą medžiagą ir pagal pastabas atnaujintus sertifikavimo kriterijus, EDAV dėl jų priima nuomonę.

(7 žingsnis) EDAV priėmus nuomonę, kurioje pritariama sertifikavimo kriterijams, VDAI šiuos kriterijus patvirtina. Tuo atveju, jei EDAV priims nuomonę, kad sertifikavimo kriterijai neatitinka BDAR, VDAI priims sprendimą atsisakyti tvirtinti sertifikavimo kriterijus.

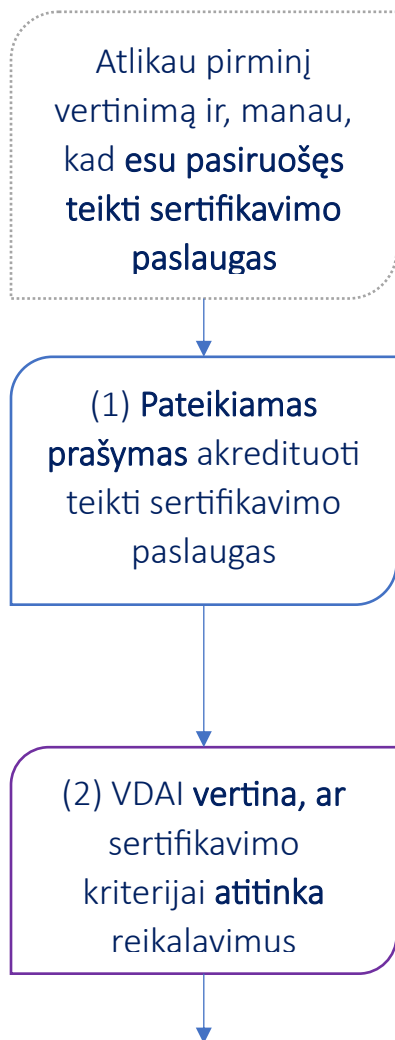
Sertifikavimo kriterijai **paskelbiami** VDAI ir [EDAV interneto svetainėse](#). Juos savo interneto svetainėje turės paskelbti ir akredituota sertifikavimo įstaiga, kuri pagal juos teiks sertifikavimo paslaugas.

Naudinga informacija:

- [Sertifikavimo kriterijų patvirtinimo tvarkos aprašas](#);
- [EDAV gairės 1/2018](#) dėl sertifikavimo kriterijų ir papildomas [priedas](#) dėl sertifikavimo kriterijų vertinimo;
- [EDAV gairės 07/2022](#) dėl sertifikavimo kriterijų kaip asmens duomenų perdavimo į trečiąsias valstybės įrankio;
- [EDAV dokumentas dėl Europos duomenų apsaugos ženklo](#);
- [EDAV nuomonės dėl sertifikavimo kriterijų](#) ir [patvirtintų sertifikavimo kriterijų registras](#).

5. Noriu akredituotis teikti sertifikavimo paslaugas, kokia procedūra man taikoma?

VDAI atkreipia dėmesį, kad teikiant prašymą akredituoti teikti sertifikavimo paslaugas **būtina turėti patvirtintus sertifikavimo kriterijus**. Asmenys, norintys teikti sertifikavimo paslaugas, gali arba patys parengti sertifikavimo kriterijus ir juos pateikti tvirtinti VDAI, arba gali įgyti teisę naudotis sertifikavimo kriterijais, kurių savininkais yra kitos organizacijos (tokios organizacijos nustatytomis sąlygomis).



Prieš teikiant prašymą akredituoti teikti sertifikavimo paslaugas VDAI **rekomenduoja įsivertinti**, ar tikrai esate pasiruošę tokias paslaugas teikti (taip pat žr. atsakymą į trečiąjį klausimą). Atitiktis akreditavimo reikalavimams procesas yra **mokamas** ([apie taikomas valstybės rinkliavas skaitykite čia](#)). Jei dėl Jūsų prašymo bus priimtas neigiamas sprendimas ir norėsite kreiptis su nauju prašymu akredituoti teikti sertifikavimo paslaugas (ištaisę nustatytus trūkumus), nustatytą mokestį **turėsite mokėti dar kartą**.

(1 žingsnis) Siekiant akredituotis teikti sertifikavimo paslaugas, **būtina VDAI pateikti**:

- › Nustatytos formos **prašymą** (Akreditavimo aprašo 2 priedas)
- › Dokumentus, **įrodančius, kad atitinkate** akreditavimo reikalavimus (nustatytus Akreditavimo aprašo 1 priede)
- › **Valstybės rinkliavos sumokėjimą** patvirtinantį dokumentą
- › **Sertifikavimo kriterijus**, pagal kuriuos teiksite sertifikavimo paslaugas (jei juos patvirtino VDAI - priimto sprendimo datą ir numerį)

(2 žingsnis) VDAI **vertina** asmens, siekiančio teikti sertifikavimo paslaugas, **atitiktį akreditavimo reikalavimams** pagal pateiktus dokumentus (ir kitą pateiktą informaciją). Pateikta informacija tikrinama ir atliekant patikrinimą vietoje ar auditą.

Vertinimas atliekamas **per 8 savaites** (terminas pradedamas skaičiuoti nuo paskutinių dokumentų VDAI pateikimo, o jei VDAI neprašė pateikti



papildomų dokumentų, nuo tos dienos, kai pateiktas tinkamas prašymas su priedais). Šis terminas **gali būti pratęstas 6 savaitėms** (įvertinant pateiktos informacijos apimtį ir sudėtingumą ar kitas svarbias aplinkybes).

(3 žingsnis) Nustačius, kad asmuo **atitinka** akreditavimo reikalavimus ir turi sertifikavimo kriterijus, pagal kuriuos teiks sertifikavimo paslaugas, VDAI **priima sprendimą akredituoti** pareiškėją, o jei akreditavimo kriterijų neatitinka ar neturi sertifikavimo kriterijų - priima sprendimą atsisakyti akredituoti pareiškėją.

Sertifikavimo įstaigos **akreditacija teikti sertifikavimo paslaugas galioja 5 metus**.

Pastaba. VDAI gali **panaikinti** sprendimą akredituoti sertifikavimo įstaigą nustačiusi, kad ši įstaiga **nesilaiko BDAR ar Akreditavimo tvarkos reikalavimų**, turinčių įtaką Sertifikavimo įstaigos atitikties Akreditavimo kriterijams vertinimui. VDAI taip pat gali **sustabdyti** sertifikavimo įstaigos akreditaciją, kai **būtina atlikti papildomą jos atitikties vertinimą**.

(4 žingsnis) Sprendimas akredituoti sertifikavimo įstaigą (taip pat panaikinti ar stabdyti jos akreditaciją) paskelbiamas VDAI interneto svetainėje, nurodant:

- › Sertifikavimo įstaigos (juridinio asmens) pavadinimą ir įmonės kodą arba (fizinio asmens) vardą, pavardę verslo liudijimo arba individualios veiklos pažymos numerį; ir
- › VDAI sprendimo priėmimo datą, numerį ir nuorodą į Sertifikavimo kriterijus, pagal kuriuos bus teikiamos sertifikavimo paslaugos.

Naudinga informacija:

- [Sertifikavimo įstaigų akreditavimo tvarkos aprašas](#) (su akreditavimo reikalavimais ir prašymo forma);
- [EDAV gairės 4/2018](#) dėl sertifikavimo įstaigų akreditavimo;
- [Lietuvos Respublikos Vyriausybės nutarimas dėl valstybės rinkliavų už akreditavimo paslaugas](#).

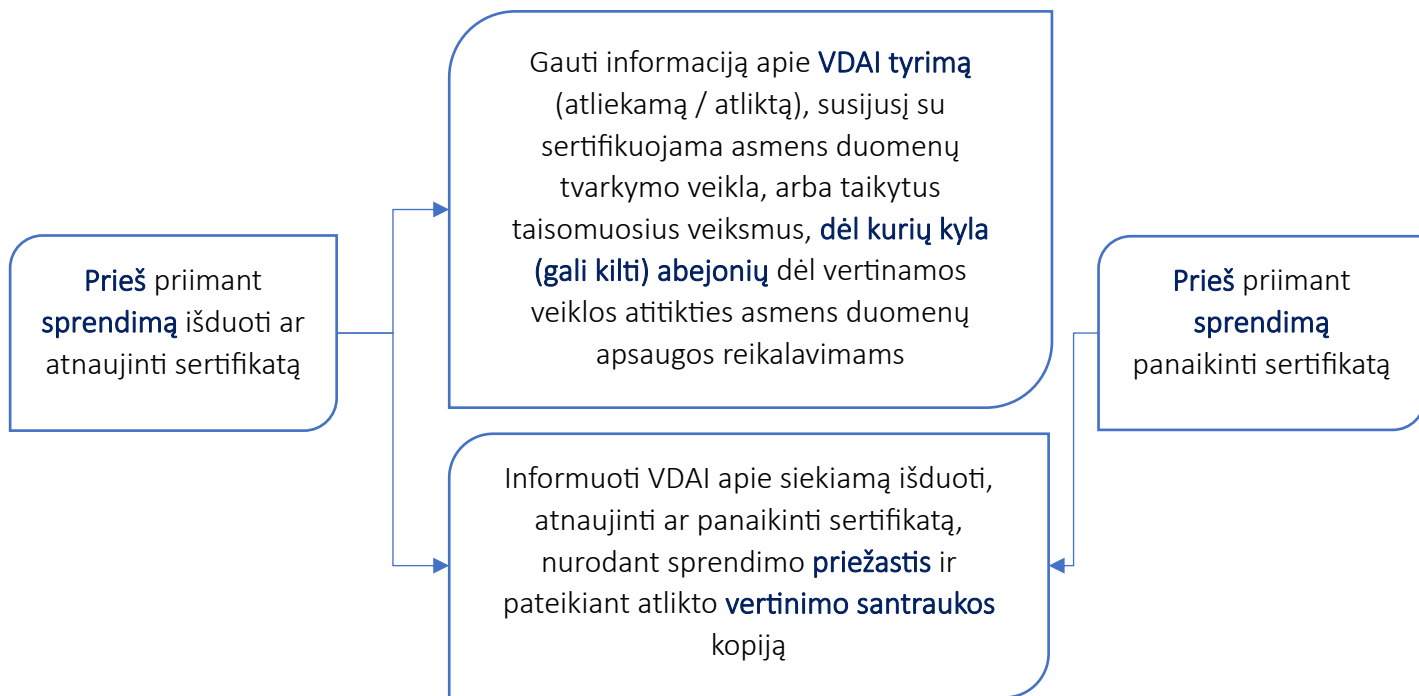
6. Esu akredituotas teikti sertifikavimo paslaugas, į ką papildomai turėčiau atkreipti dėmesį?

Akredituota sertifikavimo įstaiga turi savo interneto svetainėje **paskelbti** (taip, kad būtų lengvai pasiekiami) (žr. Akreditavimo reikalavimus, skiltys 4.6 ir 7.8):

- › visas patvirtintų **sertifikavimo kriterijų** ir **sertifikavimo procedūrų** versijas (esamas ir ankstesnes), nurodant jų galiojimo datas
- › informaciją apie **skundų dėl sertifikavimo ar kitų susijusių pažeidimų procedūras** ir pateiktas apeliacijas
- › **informaciją apie sertifikuotus subjektus**, pateikiant jo pavadinimą, kodą, buveinės adresą,

sertifikuoto asmens duomenų tvarkymo operacijos aprašymą, nuorodą į sertifikavimo kriterijų versiją, atitikties vertinimo rezultatą (ir vertinimo ataskaitos santrauką) ir galiojimo datą, taip pat, kai taikoma, sertifikato galiojimo sustabdymo ar panaikinimo datą.

Akredituotos sertifikavimo įstaigos **pareiga keistis informacija su VDAI** (žr. Akreditavimo reikalavimus, skiltis 7.1):



Pastaba. Nors akredituota sertifikavimo įstaiga turi pareigą informuoti VDAI apie visus siekiamus priimti sprendimus, susijusius su sertifikavimu, tai nereiškia, kad VDAI vertins kiekvieną sprendimą. Tačiau, esant poreikiui, VDAI turi teisę duoti akredituotai sertifikavimo įstaigai nurodymą sertifikato neišduoti (neatnaujinti) arba jį panaikinti.

Akredituotos sertifikavimo įstaigos išduoti **sertifikatai galioja ne ilgiau kaip 3 metus**, o atitikties išduotiems **sertifikatams priežiūrą** tokia įstaiga **atlieka bent kartą per metus** (žr. Akreditavimo reikalavimus, skiltys 7.7 ir 7.9).