

KĄ TURIME ŽINOTI APIE
ASMENS DUOMENŲ TVARKYMĄ NUOTOLINIO MOKYMO/SI IR DARBO METU

1. Duomenų valdytojas (Mokykla):

- asmens duomenis tvarko vadovaudamasi Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – *ADTAI*), Europos Parlamento ir Tarybos reglamentu (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 – *Reglamentas*) ir jo įgyvendinamaisiais teisės aktais ir Mokyklos vidaus dokumentais, nustatančiais darbuotojų, mokinių ir trečiųjų asmenų asmens duomenų tvarkymą;
- paskiria atsakingus už duomenų apsaugą darbuotojus;
- konsultuojasi su Steigėjo duomenų apsaugos pareigūnu nagrinėdama klausimus, susijusius su asmens duomenų apsauga (rengiant mokyklos vidaus dokumentus, reglamentuojančius asmens duomenų tvarkymą ar sprendžiant klausimus dėl nuotolinio mokymo ir kt.).

2. Asmens duomenų saugumo pažeidimu laikomas bet koks saugumo incidentas, dėl kurio įvyksta vienas ar keli žemiau išvardinti pažeidimai:

- **konfidencialumo pažeidimas** – kai netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama (gaunama) prieiga tam teisės neturintiems asmenims: duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio pavišinimas, slaptažodžio praradimas ar atskleidimas kitam darbuotojui, nešiojamojo kompiuterio, kuriame sukaupti duomenys, praradimas, popierinių dokumentų praradimas, vagystė ir t.t.;
- **pasiekiamumo pažeidimas** – kai netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami: tai galėtų būti duomenų bazės ištrynimasis, praradimas (vagystė), sunaikinimas, tarkim gaisro, liūties, kitu ekstremaliu atveju ir nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiekiamumo pažeidimu laikytinas ir įprastinę Mokyklos veiklą sutrikdęs prieigos prie duomenų praradimas;
- **vientisumo pažeidimas** – netyčia ar neteisėtai atlikti asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, atlikti joje esančių įrašų pakeitimai, programinės įrangos ar kitokie procedūrų sutrikimai, dėl kurių atsiranda duomenų netikslumų arba pasikeitimų.
- **nesankcionuotas prisijungimas** prie nuotolinio mokymosi platformos (pavyzdžiui, mokinys prie nuotolinio mokymosi platformos (Zoom, Skype ir kt.) prijungia pašalinius asmenis);
- **nesankcionuotas duomenų kopijavimas** iš nuotolinio mokymosi platformos (pavyzdžiui, mokinys fotografuoja, kopijuoja, įrašo ar pan. asmens duomenis) ir suteikia prieigą pašaliniams asmenims;

- **kiti pažeidimo atvejai**, kurie atitinka aukščiau pateiktus apibrėžimus.

3. Kai įvyksta asmens duomenų saugumo pažeidimas:

- duomenų valdytojas (Mokykla), vos sužinojęs, kad padarytas asmens duomenų saugumo pažeidimas, praneša kompetentingai priežiūros institucijai apie asmens duomenų saugumo pažeidimą, nepagrįstai nedelsdamas ir, jei įmanoma, nuo to laiko, kai apie tai buvo sužinota, praėjus ne daugiau kaip 72 valandoms, nebent duomenų valdytojas (Mokykla) gali pagal atskaitomybės principą įrodyti, kad asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Tai numato Bendrasis duomenų apsaugos reglamentas. Taip pat atliekami kiti vidaus dokumentuose (pvz. Mokyklos asmens duomenų apsaugos politikoje, Sutartyse su mokymosi paslaugų gavėjais, Sutikimuose dėl asmens duomenų tvarkymo ir kt.) numatyti veiksmai.

4. Kokių duomenų apsaugos priemonių duomenų valdytojas (Mokykla) imasi vykdydamas nuotolinį ugdymą?

- informuoja duomenų subjektus (mokinius, jų tėvus (globėjus) apie tvarkomus asmens duomenis, kad jie nuotolinio ugdymo tikslu tvarkomi tik duomenų valdytojo (Mokyklos) vardu;
- informuoja duomenų subjektus (mokinius, jų tėvus (globėjus) ir duomenų tvarkytojus pedagogus, kur jie gali kreiptis įvykus asmens duomenų saugumo pažeidimui (mokinių - techninių (IT) mokymo priemonių specialistė Alė Vilutienė, darbuotojų – raštinės vadovė Vida Peseckienė);
- informuoja duomenų subjektus (mokinius, jų tėvus (globėjus) ir duomenų tvarkytojus pedagogus, kokias saugumo priemones turi užtikrinti nuotolinio mokymo priemonės naudotojai;
- apsvarsto tiesioginių transliacijų, vaizdo įrašų galimybes bei poreikį ir derina su mokinių tėvais;
- Nusprendžia, kurios programos naudojamos, teikia informaciją ir pagalbą apie jas;
- užtikrina, kad ugdymo procese dalyvautų tik autorizuoti mokiniai.
- teikia pasiūlymus, kurie galėtų apriboti neautorizuotą prisijungimą prie pamokų naudojant

Zoom programą, pavyzdžiui:

konferencijose galima dalyvauti tik su savo tikru vardu ir pavarde;

galima naudoti slaptažodžius;

galima naudoti laukimo kambarius (angl. Waiting Room);

prisijungusius mokinius identifikuoti iš vaizdo duomenų;

prasidėjus pamokai (arba kai prisijungia visi mokiniai) užrakinkiti prisijungimo langus.

- svarsto galimybę dėl Microsoft Teams programos įsisavinimo ir pilno naudojimo nuotoliniame ugdyme.