DUOMENŲ APSAUGOS PAREIGŪNAS
MB „Veiklos sprendimai“
Žalgirio g. 122, Vilnius
El. p. dap@veiklos-sprendimai.lt; Tel. Nr. +370 672 43319

INFORMACIJA DĖL ASMENS DUOMENŲ TVARKYMO NUOTOLINIO MOKYMOSI METU

Kada privaloma kreiptis į duomenų apsaugos pareigūną?

- Nagrinėjami klausimai, kurie yra susiję su asmens duomenų apsauga (pavyzdžiui, rengiami vidaus dokumentai, kurie reglamentuos asmens duomenų tvarkymą, sprendžiami klausimai dėl nuotolinio mokymosi).

Kas yra asmens duomenų saugumo pažeidimas?

Duomenų saugumo pažeidimu laikomas bet koks saugumo incidentas, dėl kurio įvyksta vienas arba keli toliau numatyti pažeidimai:

- **konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama (gaunama) prieiga tam teisės neturintiems asmenims**, pavyzdžiui, duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas, praradimas, atskleidimas kitam darbuotojui, nešiojamojo kompiuterio, kuriame sukaupti duomenys, praradimas, popierinių dokumentų praradimas, vagystė ir pan.;
- pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti laikomas duomenų bazės ištrynimas, praradimas (vagystė), sunaikinimas, pavyzdžiui, gaisro, liūties 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, įvykdyti joje esančių įrašų pakeitimai, taip pat programinės įrangos ar kitokie procedūrų sutrikimai, dėl kurių atsiranda duomenų netikslumų arba pasikeitimų.

Kas turėtų būti laikoma asmens duomenų saugumo pažeidimu?

- Nesankcionuotas prisijungimas prie nuotolinio mokymosi platformos (pavyzdžiui, mokinys prie nuotolinio mokymosi platformos (Zoom, Skype ar pan.) prijungia pašalinius asmenis);
- Nesankcionuotas duomenų kopijavimas iš nuotolinio mokymosi platformos (pavyzdžiui, vaikas fotografuoja, kopijuoja, įrašo ar pan. asmens duomenis) ir suteikia prieiga pašaliniams asmenims;
- Kiti atvejai, kurie atitinka aukščiau pateiktus apibrėžimus.

Ką daryti, jeigu įvyksta asmens duomenų saugumo pažeidimas?

Pagal Bendrąjį duomenų apsaugos reglamentą, vos sužinojęs, kad padarytas asmens duomenų saugumo pažeidimas, duomenų valdytojas turėtų pranešti kompetentingai priežiūros institucijai nepagrįstai

nedelsdamas ir, jei įmanoma, nuo to laiko, kai apie tai buvo sužinota, praėjus ne daugiau kaip 72 valandoms, apie asmens duomenų saugumo pažeidimą, nebent duomenų valdytojas gali pagal atskaitomybės principą įrodyti, kad asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Be to, būtina atlikti kitus vidaus dokumentuose numatytus veiksmus.

Kokių priemonių reikia imtis vykdant nuotolinį ugdymą?

- Informuoti duomenų subjektus apie tvarkomus duomenis nuotolinio ugdymo tikslu;
- Informuoti duomenų subjektus ir darbuotojus kur jie gali kreiptis įvykus asmens duomenų saugumo pažeidimui;
- Informuoti duomenų subjektus ir darbuotojus kokias saugumo priemones turi užtikrinti nuotolinio mokymo priemonės naudotojai.

- Reikėtų apsvarstyti ar nuotolinio ugdymo nebūtų galima dėstyti be tiesioginių vaizdo įrašų (pavyzdžiui, įrašant vaizdo įrašą ir pateikiant jį mokiniams);
- Jeigu yra poreikis daryti tiesiogines transliacijas, reikėtų apsvarstyti galimybę netransliuoti mokinio vaizdo;
- Jaunesniems nei 13 metų mokiniams, nuotolinis ugdymas negali būti vykdomas naudojant socialiniu tikslu „Facebook“, nes neatitinka jų naudojimo sąlygų;
- Standartizuoti naudojamas priemones, t. y. nuspręsti, kurios programos naudojamos ir taisyklėse detaliai aprašyti jų naudojimą;
- Užtikrinti, kad ugdymo procese dalyvautų tik autorizuoti mokiniai.

Zoom programa kritikuojama pasaulyje dėl privatumo pažeidimų, tačiau nemaža dalis švietimo įstaigų ją naudoja, todėl pateikiame pasiūlymus, kurie galėtų apriboti neautorizuotą prisijungimą prie pamokų.

1. Konferencijose galima dalyvauti tik su savo tikru vardu ir pavarde;
2. Naudokite slaptažodžius;
3. Naudokite laukimo kambarius (angl. Waiting Room);
4. Prisijungusius mokinius identifikuokite iš vaizdo duomenų;
5. Prasidėjus pamokai (arba kai prisijungia visi mokiniai) užrakinkite prisijungimo langus.

Apsvarstykite naudojimą Microsoft Teams arba Google Classroom.