



STOPIŅU NOVADA DOME

ULBROKAS VIDUSSKOLA

Reģistrācijas Nr.4313901107

Vālodzes, Stopiņu novadā, LV- 2130, tālrunis: 67910372, 25144588,
fakss: 67910372, e-pasts: ulbrokas.skola@u-vsk.lv; www.ulbrokas-vsk.lv

Stopiņu novadā,
31.08. 2018.

APSTIPRINU

Ulbrokas vidusskolas direktors

N. Balabka

2018. gada 31. augusts

Datu apstrādes noteikumi

Pārzinis -Stopiņu Novada Dome

Izdots pamatojoties uz Stopiņu Novada Domes apstiprinātajiem noteikumiem

Apstiprināja – Ulbrokas vidusskola,
izglītības iestādes reģistrācijas apliecības numurs 4313901107,
juridiskā adrese: “Ulbrokas vidusskola”, Vālodzes, Stopiņu novads, LV - 2130
direktors Normunds Balabka

Stājas spēkā _____.2018.

Pārskatīšanas datums, ne vēlāk kā _____.

ŅEMOT VĒRĀ, KA:

Ulbrokas vidusskola, turpmāk tekstā –“Skola”, savā ikdienas darbā veic fiziskas personas datu apstrādi, tai skaitā, bet ne tikai veic datu vākšanu, reģistrāciju, organizēšanu, strukturēšanu, glabāšanu, pielāgošanu vai pārveidošanu, atgūšanu, aplūkošanu, izmantošanu, izpaušanu, nosūtīt, izplatīt vai citādi darīt tos pieejamus, saskaņošanu vai kombinēšanu, ierobežošanu, dzēšanu vai iznīcināšanu, Skola ir apstiprinājuši šos noteikumus.

Datu apstrādes normatīvais regulējums

Datu apstrādē ir jāievēro Eiropas Parlamenta un Padomes regulas (ES) 2016/679, kas pieņemta 2016. gada 27. aprīlī par fizisku personu aizsardzību attiecībā uz personas datu

apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) noteiktās prasības u.c.

Datu apstrādes principi

Datu apstrāde ir jāveic ievērojot Vispārīgajā datu aizsardzības regulā noteiktos principus:

1. Likumīgums, godprātība un sekojošus pārredzamība
2. Nolūka ierobežojumi
3. Datu minimizēšana
4. Precizitāte
5. Glabāšanas ierobežojums
6. Integritāte un konfidencialitāte
7. Pārskatatbildība

2.1. Likumīgums, godprātība un pārredzamība

Lai īstenotu šos principus Skolas ikdienas darbībā, Skola nodrošina pret datu subjektu godprātīgu attieksmi attiecībā uz viņa datu apstrādi jeb veic datu subjektu datu apstrādi labā ticībā. Godprātības princips pēc būtības ietver arī visus pārējos principus, jo visi principi pamatā ir vērsti, lai realizētu Skolas godīgu attieksmi pret datu subjektu, tai skaitā, bet ne tikai, informējot viņu par datu apstrādi, neizmantojot datus citiem nolūkiem kādiem tie tikuši ievākti.

Godprātīga attieksme izpaužas Skolas rīcībā, respektējot datu subjekta intereses aizsargāt savu privātumu, kā arī veicinot un atvieglojot datu subjektam tā tiesību realizēšanu, piemēram, nodrošinot vienkāršotu datu subjekta piekļuvi informācijai par tā datu apstrādi, droši glabājot datu subjekta datus, ļaujot labot neprecīzus datu subjekta datus un citu tiesību īstenošanu.

Skola, veicot datu apstrādi, ņem vērā datu subjektu briedumu, vecumu un citus personības aspektus un neizmanto personas trūkumus un nezināšanu, lai sasniegtu savus nolūkus.

Viena no godprātības principa izpausmēm ir datu pārredzamības principa nodrošināšana, ar to saprotot, ka Skola nodrošina pilnīgu, precīzu un pārliedcinošu datu subjektu informēšanu par sagaidāmo datu apstrādi un tās sekām, ja nav ierobežojumu šādas informācijas izpaušanai. Turklāt, lai šo principu īstenotu, datu subjektam informācija ir jānodrošina kodolīgā, saprotamā (ņemot vērā datu subjekta briedumu un citas īpašības, piemēram, bērni u.c.), viegli pārskatāmā un viegli pieejamā veidā. Tādējādi datu subjekts tiks pienācīgi informēts, apzinoties savu datu apstrādes būtību un iespējamās sekas, un šāda datu apstrāde neradīs nepamatotu ietekmi uz datu subjekta privātumu.

Likumīga datu apstrāde paredz, ka Skola atbildīgi izvēlas nolūkus, kādiem tā datus plāno apstrādāt, nepieļaujot tādu nolūku rašanos un īstenošanu, kuri var nepamatoti ietekmēt datu subjekta privātumu. Par likumīgiem nolūkiem viennozīmīgi atzīstami tādi nolūki, kas Skolā un normatīvajos aktos ir atzīti par samērīgiem un pieļaujamiem.

Otrs būtisks likumības principa aspekts ir datu apstrādes uzsākšana tikai atbilstoša tiesiskā pamata esamības gadījumā. Pirms jebkuru datu ievākšanas, izpaušanas trešajām personām, kā arī pirms ievāktu datu apstrādes nolūka maiņas ir jāizvērtē, vai šādi datu apstrādei ir piemērojams kāds no Regulā minētajiem tiesiskiem pamatiem.

Savukārt gadījumā, ja tiek apstrādāti Īpašu kategoriju dati (piemēram, dati par veselību, tautību, reliģisko pārliecību, biometriskie dati) ir jānodrošina, ka attiecīgai datu apstrādei ir piemērojami īpašie Regulā noteiktie tiesiskie pamati šādu datu apstrādei.

2.2. Nolūka ierobežojums

Lai ievērotu nolūka ierobežojuma principu, Skolai ir kritiski jāizvērtē katras plānotās un esošās datu apstrādes nepieciešamība. Šī principa realizācija nepieļauj datu ievākšanu un apstrādi bezmērķīgi (bez konkrēta nolūka) jeb neesot acīmredzamai un pastāvošai nepieciešamībai šādu datu apstrādei. Skola neveic datu apstrādi, nezinot kādiem nolūkiem un kad ievāktie dati tiktu izmantoti, kā arī neievāc datus un neuzglabā tos nekonkrētiem nākotnes nolūkiem, kuru vajadzība nav izvērtēta un realizācijas uzsākšana nav apstiprināta ar normatīvajiem aktiem, attiecīgiem Novada Domes un Skolas vadības lēmumiem vai iekšējiem normatīviem dokumentiem (piemēram, procedūrām, instrukcijām).

Šis princips arī nosaka, ka svarīgi ir konstatēt datu ievākšanas sākotnējo nolūku, un, ja datu izmantošanas nolūks tiek mainīts un nav saderīgs ar šo sākotnējo nolūku, tad šādi datu apstrādei ir jāpārvērtē tiesiskais pamats.

2.3. Datu minimizēšana

Šī principa īstenošanas būtība ir apstrādāt tikai attiecīgā nolūka sasniegšanai nepieciešamos datus, tādējādi samazinot apstrādāto datu apjomu. Datu minimizēšanas principa ieviešana Skolas ikdienas procesos, piemēram, pārskatot esošos risinājumus un procesos, organizējot piekļuvi datiem tikai attiecīgām struktūrvienībām, kurām tas nepieciešams pienākumu izpildei, ļauj Skolai identificēt datus, kuru apstrādes nepieciešamība attiecīgu Skolas pakalpojumu nodrošināšanai ir pārvērtējama, un novērst datu pārmērīgu apstrādi.

Piemērojot šo principu, Skola apzinās, ka datu minimizēšana nav vienreizēji veicams pasākums, bet šī principa īstenošana datu apstrādes ciklā būtu jāveic regulāri, jo darba vide, normatīvo aktu prasības un apkārtējie apstākļi ir mainīgi.

Datu minimizācijas princips vienādi ir piemērojams gan tām datu apstrādēm, ko Skola veic iekšienē, gan arī gadījumos, ja datus ir nepieciešams nodot datu apstrādātājiem (piemēram, samazinot nododamo datu apmēru un/vai pseidonimizējot datus) vai izpaužot datus trešajām personām.

Skola savā slēgtajā vidē saglabā izglītojamā vārdu un uzvārdu lietošanu gan mācību procesa laikā, ārpus tā.

2.4. Precizitāte

Precīzi dati ir viena no Regulas pamatvērtībām, jo tikai precīzi dati var nodrošināt godprātīgu un taisnīgu lēmumu pieņemšanu attiecībā uz datu subjektu. Turklāt jāņem vērā, ka neprecīzi

dati atsevišķās situācijās var radīt būtiskas negatīvās sekas attiecībā uz datu subjektu, kuras nebūs taisnīgas.

Šī principa godprātīga īstenošana ir ne tikai Skolas pienākums, bet ir nepieciešama veiksmīgas pamatdarbības nodrošināšanai, līdz ar to Skola izstrādā mehānismus (piemēram, iekļaujot līgumos datu subjektam pienākumu informēt Sabiedrību par izmaiņām datos).

2.5. Glabāšanas ierobežojums

Glabāšanas ierobežojuma principa būtība ir datus glabāt tikai tik ilgi, cik tas ir nepieciešams nolūka sasniegšanai, un tiklīdz nolūks ir sasniegts dati ir jāizdzēš vai informācijas nesēji, kuros dati ir fiksēti, jāiznīcina.

Tomēr šis princips nebūtu jāapskata virspusēji, jo, beidzoties vienam nolūkam, var rasties jauni leģitīmi nolūki, kas var pamatot nepieciešamību datus glabāt ilgāk – arī pēc pamatnolūka izbeigšanās, piemēram, ja pakalpojuma līgums tiek izbeigts, pamatnolūks – sniegt pakalpojumu klientam – ir sasniegts un dati šim nolūkam vairs nebūtu nepieciešami un apstrādājami, tomēr ir pieļaujams, ka dati tiek apstrādāti papildus nepieciešamiem nolūkiem – izpildīt normatīvo aktu prasības par attaisnojamo grāmatvedības dokumentu glabāšanu vai lai aizsargātu Skolas leģitīmās intereses, ja datu subjekts vēlētos celt jebkādas prasījumu pret Skolu.

Gadījumos, kad mainās datu apstrādes nolūks, ir nepieciešams pārvērtēt datu apstrādes apjomu, kuru nepieciešams apstrādāt, lai sasniegtu jaunus nolūkus, piemēram, ieviešot mehānismus un procedūras, kas noteiktu kārtību, kādā pārskatāms veiktās datu apstrādes apjoms nolūku maiņas gadījumā.

2.6. Integritāte un konfidencialitāte

Ievērojot to, ka mūsdienās datu apstrāde galvenokārt notiek ar elektroniskiem datu apstrādes līdzekļiem, šo līdzekļu izmantošana var radīt gan priekšrocības efektīvā datu apstrādes nodrošināšanā, gan arī trūkumus jeb riskus datu subjektu datu apstrādei. Līdz ar to jāpievērš uzmanību tehnisko un organizatorisko risinājumu ieviešanai Skolā, lai pēc iespējas samazinātu riskus datiem, kurus rada tehnoloģiju izmantošana (piemēram, datu nokļūšana trešo personu rīcībā, datu nepamatota iznīcināšana).

2.7. Pārskatatbildība

Lai šo principu īstenotu, Skolai jau pirms datu apstrādes uzsākšanas un Regulas piemērošanas ir jāapsver risinājumi, kā Skola uzskatāmi demonstrēs Regulas ievērošanu, piemēram, datu drošības nodrošināšanā, datu subjekta tiesību realizācijas nodrošināšanā, risku novērtēšanā un novēršanā. Atbilstību demonstrēt var veicot, piemēram, šādas darbības:

- 1) atbilstošu tehnisko un organizatorisko līdzekļu un pasākumu ieviešana (t.sk. iekšējo normatīvo aktu izstrāde, iekšējo datu apstrādes procesu auditu veikšana, darbinieku apmācība);
- 2) aktuālu procedūru/instrukciju attiecībā uz apstrādes darbībām uzturēšana;
- 3) ietekmes novērtējuma veikšana (ja nepieciešams);
- 4) datu apstrādes reģistra ieviešana un uzturēšana (ja nepieciešams);

- 5) datu aizsardzības “pēc noklusējuma” un integrētas datu aizsardzības īstenošana, nodrošinot datu minimizēšanu, pseidonimizāciju, pārredzamību, ļaujot datu subjektam kontrolēt un pārraudzīt savu datu apstrādi, kā arī ieviešot atbilstošus drošības pasākumus;
- 6) pievienošanās rīcības kodeksiem vai veiktās datu apstrādes sertificēšana (ja nepieciešams);
- 7) sadarbības ar uzraudzības iestādi tās uzdevumu izpildē nodrošināšana.

Pieņemtie lēmumi, attiecībā uz datu drošību tiek dokumentēti.

Apstrādājamie datu veidi

Personas dati

- Vārds, uzvārds;
- Personas kods;
- Telefona Nr.,
- E-pasta adrese;
- Deklarētā dzīves vieta;
- Pārstāvības tiesiskais pamats;
- Personas ģimenes stāvoklis;
- Personas digitālais attēls;
- Izglītojamo radošo darbu un mācību rezultāti.

Apstrādājamie īpašu kategoriju dati (sensitīvie dati):

- Veselības dati;

Iespējams - apstrādājamie īpašu kategoriju dati (sensitīvie dati):

- Tautība;
- Etniskā izcelsme;
- Biometrijas dati (pirkstu nospiedumi, sejas digitālais attēls, fizisko īpašību un rādītāju kopums)

Riski, no kuriem var izvairīties aizsargājot datus atbilstoši prasībām

Konfidencialitātes noteikumu pārkāpšana

Datu noplūde

Reputācijas zaudēšana

Datu subjekta tiesību neievērošana

Atbildība un uzdevumi

Katrs Skolas darbinieks ir atbildīgs par to, lai viņa pārziņā esošie dati tiktu pienācīgi apstrādāti.

Katram Skolas darbiniekam ir saistoša šī datu drošības politika.

Galveno atbildību par datu apstrādi Skolā nes:

Skolas direktors – atbildīgs par to, ka Skolā visi darbinieki ievēro spēkā esošo normatīvo aktu prasības.

Novada Domes nozīmētais Datu aizsardzības speciālists - Datu aizsardzības speciālistam ir šādi uzdevumi:

- informēt un konsultēt Sabiedrību un Skolas darbiniekus, kuri veic datu apstrādi, par viņu pienākumiem saskaņā ar Regulu un citiem spēkā esošajiem normatīvajiem aktiem;

- uzraudzīt, vai tiek ievēroti spēkā esošie normatīvie akti, Regula, Skolas politika saistībā ar personas datu aizsardzību, tostarp pienākumu sadali, apstrādes darbībās iesaistīto darbinieku informēšanu un apmācību, un ar to saistītajām revīzijām;
- pēc pieprasījuma sniegt padomus attiecībā uz novērtējumu par ietekmi uz datu aizsardzību un pārraudzīt tā īstenošanu;
- sadarboties ar uzraudzības iestādi (Datu Valsts Inspekcija);
- būt par uzraudzības iestādes kontaktpunktu jautājumos, un attiecīgā gadījumā konsultēt par jebkuru citu jautājumu; Datu aizsardzības speciālists, pildot savus uzdevumus, pienācīgi ņem vērā ar apstrādes darbībām saistīto risku, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūku.

IT sistēmu administrators (darbam piešķirto resursu robežās) – atbild par to, ka:

- Datu apstrāde iesaistītie informācijas un tehnoloģiskie resursi ir pietiekoši, lai nodrošināt datu drošību;
- Regulāri (ne retāk kā vienu reizi gadā) veic informāciju sistēmu pārbaudi, ar mērķi pārliecināties vai viss strādā nevainojami;
- Analizē vai sadarbībā ar trešajām personām, tiek nodrošināta datu drošība.

Galvenās vadlīnijas darbiniekiem

Datiem ir tiesīgas piekļūt tikai tās personas, kurām ir piešķirta attiecīga piekļuve.

Gadījumā, ja darbiniekam tiešo pienākumu veikšanai ir nepieciešami dati, kuru apstrādei viņa nav piešķirtas attiecīgas tiesības, darbinieks informē savu tiešo priekšnieku, kur pieņem lēmumu kā rīkoties.

Dati tiek glabāti droši (tiek ievērots “tīrā galda” princips, dati tiek glabāti slēgtā telpā / skapī. Parole tiek izstrādāta un mainīta atbilstoši Skolas apstiprinātajiem noteikumiem, paroli nedrīkst nodot nedz trešajām personām, nedz saviem darba kolēģiem.

Dati tiek regulāri pārskatīti, dati, kuru apstrādei nav tiesiska pamata, tiek dzēsti.

Gadījumos, kad darbinieks nezin kā rīkoties attiecībā uz datu apstrādi, darbinieks griežas pie sava tiešā priekšnieka un / vai datu aizsardzības speciālista.

Datu glabāšana

Datu glabāšanas ierīces ir jāglabā tā, lai tās un tajās esošā informācija nenonāk nepiederošu personu rokās.

Dati, kas glabājas uz papīra tiek glabāti slēgtā telpā / skapī.

Darbinieks atstājot savu darba dienu pārlicinās, papīra formātā esošo dati ir ievietoti slēgtā skapī.

Izlietotais papīrs tiek šrēderēts vai nodots makulatūrā tam speciāli ierīkotās kastēs.

Dati, kas glabājas elektroniski tiek aizsargāti ar stingru paroli, kas tiek regulāri mainīta un netiek nodota citiem.

Ja dati tiek glabāti pārvietojamos datu nesējos, šie datu nesēji tiek glabāti slēgt skapī.

Datiem tiek veidotas rezerves kopijas, ne retāk kā _____

Dati netiek iznesti no Skolas telpām.

Datori, kuros atrodas dati ir aprīkoti ar ugunsdrošību un pret vīrusu programmām.

Mobilā telefona lietošana

Pie Skolas tehnikas (datoriem u.c.) drīkst slēgt klāt tikai Skolai piederošas tehniskās ierīces.

Skolas e-pastu instalēt telefonā (savā vai Skolas) var tikai ar tiešā priekšnieka atļauju.

Mobilajam telefonam obligāti ir jāizveido pieejas parole, lai tā nozaudēšana gadījumā telefonā esošie dati nenokļūtu trešo personu rokās. (iespējams jāparedz, ka ja pēc tam, kad pieejas parole nepareizi ievadīta 5x, telefons nobloķējas).

Skolas izsniegtajos mobilajos telefonos nedrīkst fotografēt ar darbu nesaistītas lietas un personas.

Atdodot (arī utilizējot) telefonu, datoru u.c. ierīci ir jānodrošina, ka visi dati iepriekš ir dzēsti (vislabāk formatēt līdz rūpnīcas standartiem).

Aizliegts

Fiziskas personas datus nav atļauts sūtīt, izmantojot gmail.com, mail.ru vai citus ārpus ES reģistrētus kontus, izņemot gadījumus, ka fiziska persona, attiecīgo e-pastu ir norādījusi, kā savu korespondences e-pastu.

Bez IT Sistēmu administratora kopēt programmas.

Bez IT Sistēmu administratora, instalēt citas programmas.

Lejupielādēt pornogrāfiskus, vardarbīgus un rasistiskus materiālus vai jebkurus materiālus, kas varētu būt nelegāli un/vai nepiedienīgi.

Saglabāt ar darbu Skolā saistītus datus uz savām privātajām ierīcēm.

Precīzi un minimāli dati

Nodrošināt, ka dati ir precīzi.

Darbinieki, bez pamatotas vajadzības nekopē un neglabā datus vairākos eksemplāros/kopijās.

Darbinieki pie pirmās iespējas pārliecinās vai dati ir atbilstoši, neatbilstības gadījumā, tos nekavējoties atjauno.

Skola rada datu subjektam viegli pieejamu vidu savu datu atjaunošanai.

Novecojuši dati ir jādzēš (piemēram, telefona Nr., kurš vairs nav aktuāls).

Informācija, kas jāsniedz datu subjektam, ja personas dati ir iegūti no datu subjekta

Ja datu subjekta personas datus vāc no datu subjekta, Skola personas datu iegūšanas laikā datu subjektam sniedz visu šādu informāciju:

- Skolas un attiecīgā gadījumā Skolas pārstāvja identitāte un kontaktinformācija;
- attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija;
- apstrādes nolūki, kam paredzēti personas dati, kā arī apstrādes juridiskais pamats;
- personas datu saņēmēji vai saņēmēju kategorijas, ja tādi ir;
- u.c. informācija atbilstoši Regulas 13.panta prasībām

Papildus iepriekš minētajai informācijai Skola personas datu iegūšanas laikā datu subjektam sniedz šādu papildu informāciju, kas vajadzīga, lai nodrošinātu godprātīgu un pārredzamu apstrādi:

- laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai;
- tas, ka pastāv tiesības pieprasīt Skolai piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu, vai tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību;
- ja apstrādes pamatā ir piekrišana, tiesības jebkurā brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana;
- tiesības iesniegt sūdzību uzraudzības iestādei;

- informācija, vai personas datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī informācija par to, vai datu subjektam ir pienākums personas datus sniegt un kādas sekas var būt gadījumos, kad šādi dati netiek sniegti;

Ja Skola paredz personas datus turpmāk apstrādāt citā nolūkā, kas nav nolūks, kādā personas dati tika vākti, Skola pirms minētās turpmākās apstrādes informē datu subjektu par minēto citu nolūku un sniedz tam visu attiecīgo papildu informāciju.

Iepriekš minēto var nepiemērot, ja un ciktāl datu subjekta rīcībā jau ir attiecīgā informācija.

Datu subjekta pieprasījumi

Datu subjektam ir sekojošas tiesības:

- Tiesības labot savus datus;
- Tiesības tikt aizmirstam (dzēst);
- Tiesības ierobežot savu datu apstrādi;
- Tiesības uz datu pārnesamību;
- Tiesības saņemt informāciju par to, kādi datu subjekta dati ir apstrādāti

Par datu subjekta tiesībām saņemt informāciju

Datu subjektam ir tiesības saņemt no pārziņa apstiprinājumu par to, vai attiecībā uz datu subjektu tiek vai netiek apstrādāti personas dati, un, ja tiek, datu subjektam ir tiesības piekļūt attiecīgajiem datiem un saņemt šādu informāciju:

- apstrādes nolūki;
- attiecīgo personas datu kategorijas;
- personas datu saņēmēji vai saņēmēju kategorijas, kam personas dati ir izpausti vai kam tos izpaudis, jo īpaši saņēmēji trešās valstīs vai starptautiskās organizācijās;
- ja iespējams, paredzētais laikposms, cik ilgi personas dati tiks glabāti, vai, ja nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai;
- tas, ka pastāv tiesības pieprasīt no pārziņa datu subjekta personas datu labošanu vai dzēšanu, vai personas datu apstrādes ierobežošanu vai tiesības iebilst pret šādu apstrādi;
- tiesības iesniegt sūdzību uzraudzības iestādei;
- visa pieejamā informācija par datu avotu, ja personas dati netiek vākti no datu subjekta;
- tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

Ja personas datus nosūta trešai valstij vai starptautiskai organizācijai, datu subjektam ir tiesības saņemt informāciju par atbilstošām garantijām, ko saistībā ar datu nosūtīšanu piemēro.

Skola nodrošina apstrādē esošo personas datu kopiju. Par visām papildus kopijām, ko pieprasa datu subjekts, pārzinis var iekasēt saprātīgu samaksu, kas balstīta uz administratīvām izmaksām. Ja datu subjekts pieprasījumu iesniedz elektroniskā formā un ja vien datu subjekts nepieprasa citādi, informāciju sniedz plaši izmantotā elektroniskā formātā.

Datu apstrādes pārkāpumi

- **Apdraudējums tehniskajiem resursiem** (elektroenerģijas padeves pārtraukums, šķidrumu vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns iedarbības vai

plūdu rezultātā u.c.);

- **Apdraudējums informācijas resursiem** (trešajām personām kļuvusi zināma pieejas parole, konstatēta nesankcionēta piekļuve, konstatēti darbības pārtraukumi, datu pazaudēšana, informācijas noplūde u.c.).

Datu aizsardzības pārkāpums ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

Par jebkuru personas datu apstrādes pārkāpumu darbiniekam, kas to konstatējis, ir nekavējoties jāpaziņo informācijas resursu un tehnisko resursu turētājam.

Ja ir noticis personas datu aizsardzības pārkāpums, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, pārzinim (Skolai) ir jāpaziņo par to Datu Valsts Inspekcijai, izņemot, ja pārzinis spēj uzskatāmi parādīt, ka personas datu aizsardzības pārkāpums, nerada risku fizisku personu tiesībām un brīvībām.

Ja šādu paziņojumu nevar iesniegt 72 stundu laikā, paziņojumam būtu jāpievieno informācija par kavēšanās iemesliem, un informāciju var sniegt pa posmiem bez nepamatotas turpmākas kavēšanās.

Paziņojuma DVI saturs:

- apraksta personas datu aizsardzības pārkāpuma raksturu, tostarp, ja iespējams, attiecīgo datu subjektu kategorijas un aptuveno skaitu un attiecīgo personas datu ierakstu kategorijas un aptuveno skaitu;
- paziņo datu aizsardzības speciālista vārdu un uzvārdu un kontaktinformāciju vai norāda citu kontaktpersonu, ja nav speciālista;
- apraksta personas datu aizsardzības pārkāpuma iespējamās sekas;
- apraksta pasākumus, ko pārzinis veicis vai ierosinājis veikt, lai novērstu personas datu aizsardzības pārkāpumu, tostarp attiecīgā gadījumā – pasākumus, lai mazinātu tā iespējamās nelabvēlīgās sekas.

Skola dokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības.

Gadījumā, ja datu aizsardzības pārkāpums, noticis ar apstrādātāja kompetencē esošiem datiem, apstrādātājs, nekavējoties ziņo pārzinim.

Incidentu gadījumā darbiniekam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un informācijas resursu drošību līdz attiecīgo resursu turētāja ierašanās brīdim.