PERSONAS DATU AIZSARDZĪBAS AKTUALITĀTES PAŠVALDĪBU IESTĀDĒS COVID-19 LAIKĀ

DATU AIZSARDZĪBAS SPECIĀLISTS LAURIS KLAGIŠS

2021

PAR LEKTORU

- Zvērināts advokāts kopš 2006.gada
- Sertificēts datu aizsardzības speciālists kopš 2009.gada
- SIA «Datu aizsardzības speciālists» valdes loceklis

PAR SIA «DATU AIZSARDZĪBAS SPECIĀLISTS»

Uzņēmums dibināts 2006. gadā un ir specializējies personas datu aizsardzībā un datu aizsardzības speciālistu nodrošināšanā valsts un pašvaldību iestādēm.

Mūsu klientu vidū ir: Rīgas centrāltirgus, Latvijas televīzija, SIA "ZAAO", Latvijas Jūras administrācija, Valsts valodas centrs, Vidzemes augstskola, Liepājas universitāte, kā arī vairākas pašvaldību kapitālsabiedrības, kas sniedz atkritumu apsaimniekošanas, transporta, siltumapgādes, ūdensapgādes, dzīvojamo ēku apsaimniekošanas un citus pakalpojumus, kas izriet no pašvaldību funkcijām.

SEMINĀRA MĒRĶIS:

Iepazīstināt klausītājus ar aktualitātēm, kas skar personas datu aizsardzību.

- Datu valsts inspekcijas aktualitātes
- Citu valstu pieredze
- Biežāk pieļautās kļūdas personas datu aizsardzībā
- Datu nodošana uz Lielbritāniju
- Tiešsaistes platformu lietošana
- Covid-19 ietekme uz personas datu aizsardzību

DATU VALSTS INSPEKCIJAS AKTUALITĀTES

I E V A D S

2020.gadā Datu valsts inspekcijai (turpmāk tekstā arī - DVI) bija piešķirtas papildu **piecas amata vietas** un **finansējums – 577 980 EUR**.

Inspekcijā gada laikā tiek saņemtas vidēji 1200 sūdzības (ap **100 sūdzībām mēnesī**) saistībā ar iespējamiem personu datu apstrādes pārkāpumiem, bet **pamatotas no tām ir tikai aptuveni 10 %.**

Saudzēšanas periods ir beidzies. Administratīvo pārkāpumu lietās piemēroti gan brīdinājumi, gan **naudas sodi - no 300 līdz pat 150 000 EUR**.

2020.gadā **sodus vai aizrādījumus** no Datu valsts inspekcijas ir **saņēmuši** arī **turpat desmit valsts vai pašvaldību uzņēmumi.**

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI LATVIJĀ (1)

Datu valsts inspekcija pašiniciatīvas ietvaros pārbaudīja SIA «HH Invest» interneta vietnes privātuma politikas saturu, secinot, ka datu subjektiem pieejamā **informācija nebija sniegta vieglā uztveramā valodā**. Tā bija **atspoguļota nesistemātiskā veidā**.
Tika secināts, ka par atsevišķiem apstrādes aspektiem, kas atbilstoši Vispārīgās datu aizsardzības regulas 13.pantam bija datu subjektam jāskaidro, **skaidroti netika**.
Par šādu pārkāpumu tika piemērots **15 000 EUR** liels sods.

Veiktās pārbaudes rezultāta ir nodrošināts, ka viens no lielākajiem Latvijas internetveikaliem ir pilnveidojis datu subjektiem sniegto informāciju par personas datu apstrādi.

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI LATVIJĀ (2)

Ievērojot publiskajā telpā izskanējušo informāciju par sabiedrības bažām saistībā ar AS "HAUSMASTER" paziņojumu par iespējamu personas datu aizsardzības pārkāpumu, Datu valsts inspekcija ir uzsākusi lietas apstākļu noskaidrošanu.
AS "HAUSMASTER", ievērojot Vispārīgās datu aizsardzības regulas nosacījumus, ir paziņojis Datu valsts inspekcijai par personas datu aizsardzības pārkāpumu.

1. Datu valsts inspekcijas aktualitātes

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI LATVIJĀ (3)

Atbilstoši AS "HAUSMASTER" sniegtajam paziņojumam 2021.gada 22.janvārī apstrādātājs, kurš AS "HAUSMASTER" vārdā apstrādā personas datus, ir konstatējis, ka ir notikusi **patvaļīga piekļūšana serveriem**, kā rezultātā **dati tika nesankcionēti šifrēti un zuda iespēja tos kontrolēt**. Ņemot vērā minēto, pastāv iespēja, ka trešā persona, izmantojot tehniskos rīkus, ir veikusi prettiesiskas darbības, mēģinot piekļūt uzņēmuma datu apstrādes sistēmai un iegūt personas datus, kas saskaņā ar Krimināllikumu tiek kvalificēts, kā noziedzīgs nodarījums, par kuru **ir paredzēta kriminālatbildība.**

Aptuvenais personu skaits, uz kurām attiecas notikušais incidents (piekļuve apstrādātāja serveriem), ir **vairāk nekā 30 000 datu subjekti**.

1. Datu valsts inspekcijas aktualitātes

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI LATVIJĀ (4)

Datu valsts inspekcija 2020.gada nogalē uzlika **65 000 EUR** sodu SIA "LURSOFT IT" par prettiesisku personas datu apstrādi, **publiskojot** tīmekļa vietnē www.lursoft.lv **personas datus saturošus dokumentus**, kuri ir iekļauti Uzņēmumu reģistra reģistrācijas lietas nepubliskajā daļā.

SIA "LURSOFT IT", neievērojot Maksātnespējas likumā noteikto termiņu, tīmekļa vietnes www.lursoft.lv Maksātnespējas reģistra datu bāzē publicēja informāciju par vēsturiskajiem fiziskās personas maksātnespējas procesiem **ilgāk, nekā vienu gadu pēc ieraksta** - par fiziskās personas maksātnespējas procesa izbeigšanu - izdarīšanas dienas, t.i. tīmekļa vietnē informācija par vēsturiskajiem fiziskās personas maksātnespējas procesiem bija pieejama piecus gadus pēc ieraksta - par fiziskās personas maksātnespējas procesa izbeigšanu - izdarīšanas dienas.

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI LATVIJĀ (5)

Datu valsts inspekcija saņēma sūdzību par darba devēja rīcību - informējot citus nodarbinātos, **nosūtot tiem e-pastu**, kurā bija ietverta informācija par cietušās personas vārdu, uzvārdu un **veselības stāvokli (infekcijas slimības diagnozi).**
Izmeklējot notikušā apstākļus, Datu valsts inspekcija konstatēja, ka cietušā personas dati apstrādāti neatbilstoši, jo šāda apstrāde nebija vajadzīga darba devēja mērķu sasniegšanai un tai nebija nodrošināts atbilstošs tiesiskais pamats.

Darba devējam tika piemērots naudas sods – **6250 EUR**.

CITU VALSTU PIEREDZE

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI CITĀS VALSTĪS (1)

Portugāle.
400 000 EUR sods piemērots Portugāles slimnīcai par to, ka tā **neievēroja datu minimizācijas prasības**. Tajā visiem ārstiem tika nodrošināta piekļuve visiem pacientu datiem. Tāpat arī netika ieviesti tehniskie un organizatoriskie līdzekļi, lai ierobežotu nelikumīgu piekļuvi, kur dati bija pieejami 985 ārstiem, no kuriem 296 vairs nestrādāja šajā slimnīcā.

Secinājumi, ko no šī gadījuma varam mācīties:
1. ierobežot piekļuvi;
2. atslēgt piekļuvi bijušajiem darbiniekiem;
3. izvērtēt izmantoto sistēmu drošību.

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI CITĀS VALSTĪS (2)

Austrija.
Piemērots **4800 EUR sods** kādam uzņēmumam par to, ka tas bija izvēlējies **pārāk plašu videonovērošanas kameras leņķis**, kā arī norādījis **nepietiekamu informāciju par videonovērošanu**.

Secinājumi, ko no šī gadījuma varam mācīties:
1. izvērtēt kameru novietojumu;
2. informēt datu subjektu pirms tiek apstrādāti tā dati;
3. norādīt nepieciešamo informāciju par videonovērošanas veikšanu.

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI CITĀS VALSTĪS (3)

Francija.
50 000 000 EUR sods - Google pārkāpj pārredzamības un informācijas sniegšanas pienākumu:
-nav viegli pieejama informācija;
-nav skaidra informācija par datu apstrādi;
-nav norādīti datu glabāšanas termiņi;
-nepareiza piekrišanas iegūšana.

Secinājumi, ko no šī gadījuma varam mācīties:
1. jāsniedz pilnīga informācija saprotamā valodā (atbilstoši GDPR 13.pantam);
2. jāiegūst likumīga piekrišana;
3. jāizstrādā un jāpublicē privātuma politika.

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI CITĀS VALSTĪS (4)

Rumānija.
Piemērots **15 000 EUR sods** viesnīcai Pullman par to, ka tā **atstājusi "nepieskatītus" izdrukātus 46 viesu brokastu sarakstus**, kā rezultātā nepilnvarota persona tos nofotografējusi un ievietojusi internetā.

Secinājumi, ko no šī gadījuma varam mācīties:
1. jāievēro «tīrā galda» princips;
2. jānodrošina piekļuves tiesību kontrole.

PĀRKĀPUMI DATU AIZSARDZĪBĀ UN PIEMĒROTIE NAUDAS SODI CITĀS VALSTĪS (5)

Zviedrija.
Inspekcija piemēro **20 000 EUR sodu** kādai Zviedrijas izglītības iestādi **par sejas atpazīšanas tehnoloģijas izmantošanu**, lai uzraudzītu skolēnu klātbūtni skolā. Minētā iestāde ir prettiesiski apstrādājusi sensitīvus biometriskos datus.

Secinājumi, ko no šī gadījuma varam mācīties:
1. jāievēro datu minimizācijas princips;
2. jāsaņem datu subjektu piekrišana.

BIEŽĀK PIEĻAUTĀS KĻŪDAS PERSONAS DATU AIZSARDZĪBĀ

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (1)

1. Lielākajai daļai auditēto uzņēmumu mājaslapās un sociālo tīklu profilos **bez tiesiska pamata tiek izvietota** ne tikai **darbinieku kontaktinformācija** (vārds, uzvārds, amats, tālrunis, e-pasts), bet arī šo **darbinieku fotogrāfijas**.

2. Mājaslapās nereti tiek vākti mājaslapu apmeklētāju dati, bet **nav izvietota privātuma politika**.

3. Pirms publisku pasākumu organizēšanas tās apmeklētāji **netiek** pienācīgi **informēti**, **ka** šis **pasākums tiks fotografēts un/vai filmēts**.

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (2)

4. Mēdz būt situācijas, kad personām **nav iespējas atteikties no jaunumu saņemšanas** e-pasta vai sms formā.

5. Mājaslapas bieži vien ir **bez derīga SSL sertifikāta**, līdz ar to pastāv iespēja, ka dati, ko datu subjekts mājaslapā nodod uzņēmumam, var nešifrētā veidā nonākt trešo personu rīcībā.

6. Bieži vien uzņēmumi ārpakalpojumu sniedzējiem **datus nodod, neatrunājot pušu pienākumus un tiesības attiecībā uz datu apstrādi**.

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (3)

7. Nereti mēdz būt situācijas, ka personas datus saturoši **dokumenti** (piemēram, līgumi) **glabājas neslēdzamās telpās un neslēdzamos skapjos**.

8. Lai piekļūtu datu apstrādes sistēmai, piemēram, grāmatvedības programmai, **divas vai vairākas personas lieto vienus un tos pašus piekļuves rekvizītus vai arī piekļuves rekvizītus nelieto vispār.**

9. Bieži vien lietvedības datorprogrammās ievadītie **personas dati glabājas mūžīgi vai daudz ilgāk**, kā tas ir nepieciešams.

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (4)

10. Darba tiesisko attiecību ietvaros darbinieku lietās **tiek glabāti** dati un dokumenti, kurus glabāt nebūtu tiesiska pamata (piemēram, **dati par ģimenes stāvokli, tautību vai pilsonību**, kā arī **personas apliecinošu dokumentu, bērnu dzimšanas apliecību**, kā arī **laulības apliecību kopijas).**

11. Ja personas dati tiek nodoti uz valsti, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstis, vai starptautiskajai organizācijai, bieži vien **nav izstrādāti iekšējie noteikumi un skaidra kārtība šo datu nodošanai.**

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (5)

12. Uzņēmumu un iestāžu **darbinieki** nereti **netiek** rakstveidā vai kādā citā veidā **informēti par pienākumu - neizpaust personas datus** (tostarp pēc darba, dienesta vai citu tiesisko attiecību izbeigšanās).

13. **Darbā nepieņemto darbinieku CV** parasti **tiek glabāti bez termiņa ierobežojuma**, kas nav nepieciešams personas datu apstrādes mērķa (darba līguma izpilde) sasniegšanai, jo beidzoties darbinieku atlasei un pārbaudes laikam, šādu dokumentu glabāšanai nav tiesiska pamata.

14. Daudzos uzņēmumos **aizvien tiek lietota operētājsistēma Windows XP**, kurai jau 2015. gadā tika pārtraukts Microsoft drošības atbalsts.

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (6)

15. **Rezerves kopijas** – tās dažkārt vispār **netiek nodrošinātas** vai arī tiek nodrošinātas neregulāri.

16. Ne vienmēr ir noteiktas prasības attiecībā uz **paroles garumu**.

17. Uzņēmumos ļoti reti ir izstrādāti **IS drošības noteikumi**.

18. Nav izstrādāti **personas datu apstrādes aizsardzības noteikumi**.

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (7)

19. Attiecībā uz videonovērošanu biežākais auditos konstatētais pārkāpums jāatzīmē tas, ka vai nu **nebija** nemaz **norādes par to, ka tiek veikta videonovērošana**, vai arī **norādes neatbilda Regulai**. Tāpat pie pārkāpumiem tika atklāta arī **audioieraksta veikšana**, **nesamērīgi plaša publiskās ārtelpas novērošana** un **darbinieku privāto telpu novērošana**.

20. Saskaņā ar Regulas 30. pantu katram pārzinim, pie kura strādā vairāk kā 250 darbinieki, ir jāveido **datu apstrādes reģistrs**, taču **ne vienmēr** šis reģistrs **tiek veidots**.

SECINĀJUMI PĒC 100 UZŅĒMUMU IZVĒRTĒŠANAS (8)

21. Saskaņā ar Regulas 37. pantu ir noteikti gadījumi, kad iestādēm ir **jāieceļ datu aizsardzības speciālists**, piemēram, gadījumā, kad datu apstrādi veic valsts vai pašvaldības iestāde vai pašvaldības kapitālsabiedrība. Liela daļa valsts un pašvaldību iestāžu un kapitālsabiedrību to vēl nav izdarījušas.

Kopsavilkums.
Rezumējot iepriekš minēto, secināms, ka lielākā daļa valsts un pašvaldību kapitālsabiedrību vēl nav pilnībā ieviesuši Regulu, tomēr ir vērojama arī pozitīva tendence – aizvien vairāk uzņēmumu aizdomājas par personas datu aizsardzību un ar saviem vai piesaistīto speciālistu spēkiem veic iekšējos auditos un novērš konstatētās neatbilstības.

DATU NODOŠANA UZ LIELBRITĀNIJU

«ES-AK TIRDZNIECĪBAS UN SADARBĪBAS NOLĪGUMS» PIEMĒROŠANA (1)

Eiropas Komisija 2020.gada 24.decembrī vienojās ar Apvienoto Karalisti, noslēdzot 2020.gada 31.decembrī sadarbības nolīgumu **«ES-AK tirdzniecības un sadarbības nolīgums»**, kas tiek piemērots no 2021.gada 1.janvāra.

Sadarbības nolīgums nosaka pārejas periodu, kas **ļauj turpināt personas datu brīvu plūsmu** no Eiropas Savienības un Eiropas Ekonomikas zonas uz Apvienoto Karalisti pēc pārejas perioda beigām līdz Eiropas Komisijas lēmuma pieņemšanai par aizsardzības līmeņa pietiekamību.

1. Datu nodošana uz Lielbritāniju

«ES-AK TIRDZNIECĪBAS UN SADARBĪBAS NOLĪGUMS» PIEMĒROŠANA (2)

Noteiktajā laika posmā personas datu nosūtīšanu no Eiropas Savienības un Eiropas Ekonomikas zonas uz Apvienoto Karalisti **neuzskata par datu nosūtīšanu uz trešo valsti.**

Ņemot vērā minēto, **līdz 2021.gada 30.aprīlim** personas **datus uz Apvienoto Karalisti var nosūtīt** līdzīgi kā uz jebkuru citu Eiropas Savienības valsti, nepiemērojot Vispārīgajā datu aizsardzības regulā noteiktos principus un metodes attiecībā uz datu nosūtīšanu uz trešo valsti.

Ja Eiropa neatzīs Lielbritāniju par drošu valsti datu aizsardzībai, tad Lielbritānijas uzņēmumam **Bill.me LTD**, kura pakalpojumus izmanto pašvaldības, **var nākties meklēt risinājumu, glabājot datus ES**.

1. Datu nodošana uz Lielbritāniju

TIEŠSAISTES PLATFORMU LIETOŠANA

VIDEOKONFERENČU RĪKI (1)

CERT.LV ir izanalizējis šobrīd **populārākos videokonferenču rīkus**: **Cisco Webex Meetings, Zoom, Microsoft Teams** u.c., pēc tādiem parametriem, kā funkcionalitātes iespējas, privātums un drošība, pēdējie atjauninājumi, bīstamākās ievainojamības, izcelsmes valsts utt.

VIDEOKONFERENČU RĪKI (2)

Svarīgākie secinājumi:
- visiem tirgū pieejamajiem risinājumiem ir konstatētas dažādas ievainojamības un trūkumi;
- neeksistē universāls, absolūti drošs risinājums, kas būtu vienlaicīgi lietotājam draudzīgs, nodrošinātu pilnu konfidencialitāti un operatīvi, un kas būtu ieviešams bez papildu resursiem (finanšu, tehniskajiem un cilvēkresursiem) ārkārtas situācijā;
- izmantojot kādu no minētajiem rīkiem, ir jāsaprot, ka tie nav paredzēti konfidenciālas vai sensitīvas informācijas apmaiņai, bet gan ikdienas darbu nodrošināšanai.

ZOOM PLATFORMAS LIETOŠANAS IETEIKUMI (1)

Lai izvairītos no viltotas programmatūras, izmantojiet tās uzstādīšanai tikai oficiālo saiti: https://zoom.us

Sekojiet līdz Zoom lietošanas ieteikumiem, kas pieejami CERT.LV mājaslapā: https://cert.lv/uploads/ieteikumi/document_Zoom.pdf

Drošāk ir izmantot nevis instalēto programmatūru, bet programmatūras versiju Interneta pārlūkprogrammā.

Izmantojiet jaunāko programmas versiju, regulāri to atjauninot.

ZOOM PLATFORMAS LIETOŠANAS IETEIKUMI (2)

Izmantojiet Zoom platformu tā, lai to neiztraucētu neaicināti dalībnieki.

Koplietojot sapulces/mācību stundas saiti sociālajos medijos vai citā publiskā vietā (piemēram, skolas mājaslapā), tai var pievienoties ikviens, kam ir šī saite.

Lai pievienotos sapulcei/mācību stundai, plānotajiem dalībniekiem var pieprasīt norādīt ne tikai sapulces ID, bet arī paroli. Nosūtot saites uz pasākumu, nevajadzētu iekļaut paroli, bet gan nosūtīt to atsevišķi katram dalībniekam.

ZOOM PLATFORMAS LIETOŠANAS IETEIKUMI (3)

Viens no labākajiem veidiem, kā pasargāt Zoom tiešsaistes pasākumu, ir funkcijas «**uzgaidāmā telpa**» (*Waiting Room*) iespējošana.
«***Waiting Room***» ir virtuāla uzgaidāmā telpa, kas attur viesus no pievienošanās sapulcei/mācību stundai pirms tās organizatora. Tas ir veids, kā pārvaldīt, kurš tiek ielaists virtuālajā pasākumā un kurš nē.

Jūs varat liegt dalību, bloķēt nevēlamos vai traucējošos sanāksmes dalībniekus.

ZOOM PLATFORMAS LIETOŠANAS IETEIKUMI (4)

«*Zoom Bombing*» ir situācija, kad Zoom platformā notiekošai sapulcei vai mācību stundai pievienojas neaicināti dalībnieki un traucē tās norisi. Nelūgtie viesi koplieto savus ekrānus, lai «bombardētu» īstos dalībniekus ar traucējošu, izklaidējošu, reizēm arī nelegālu saturu.

Tieši tāpēc, sagaidot visus dalībniekus, «aizslēdziet» sapulci/mācību stundu, izmantojot opciju «***Lock Meeting***». Līdz ar ko neviens jauns dalībnieks nevarēs tai pievienoties, pat ja tam būs zināms sapulces ID un parole.
Lai to izdarītu, sapulces laikā nepieciešams uzklikšķināt izvēlnei «*Participants*», pēc tam - uz pogas «*Lock Meeting*».

COVID-19 IETEKME UZ PERSONAS DATU AIZSARDZĪBU

IEVADS

Covid-19 pandēmija ir kļuvusi par izaicinājumu ne tikai privātpersonu veselībai, bet arī juridisko personu darbības nepārtrauktībai, kā rezultātā, likumdevējam nepārtraukti nākas balansēt starp sabiedrības interesēm ierobežot Covid-19 un personas datu aizsardzību.

Covid-19 pandēmijas ietekme jūtama ne vien fiziskajā pasaulē, bet arī kibertelpā. Ļaundari valdošo krīzes situāciju un organizāciju pāriešanu attālināta darba režīmā nekautrējas izmantot savā labā - gan peļņas gūšanai, gan spiegošanai.

RAKSTISKU APLIECINĀJUMU PIEPRASĪŠANA (1)

Ņemot vērā epidemioloģisko situāciju valstī, kā arī ievērojot atkārtoti izsludināto ārkārtas situāciju, pakalpojumu sniedzēji ar mērķi - pasargāt savus darbiniekus un klientus -, bieži vien vēlas iegūt informāciju **vai klients/apmeklētājs nerada paaugstinātu infekcijas risku.**

Katra organizācija pielieto savu metodi:
- citi aptaujā klientu pirms pierakstīšanas un pakalpojuma sniegšanas klātienē;
- citi prasa rakstiskus apliecinājumus vai arī apstiprinājumus elektroniskajā sistēmā par personas veselību, līdz ar ko persona paraksta to un norāda savu vārdu, uzvārdu, kā arī citus personas datus, u.tml.

RAKSTISKU APLIECINĀJUMU PIEPRASĪŠANA (2)

Datu valsts inspekcija atgādina, ka **prasīt personām apliecinājumu vai apstiprinājumu** tam, ka viņi nav bijuši ārvalstīs, ka viņi nav uzskatāmi par kontaktpersonām vai nav saslimuši ar Covid-19, **nav tiesiska pamata un nepieciešamība.**

Ja pakalpojuma sniedzējs vēlās un uzskata to par nepieciešamu, tas var sasniegt mērķi – **ierobežot Covid-19 infekcijas izplatību** – nevis, ņemot apliecinājumus no personām, bet informējot personas par viņiem noteiktiem pienākumiem, ņemot vērā Ministru kabineta pieņemtos lēmumus un normatīvo aktu regulējumu.

ATTĀLINĀTAIS MĀCĪBU PROCESS (1)

Inspekcija ņem vērā, ka savstarpējā mijiedarbība - skolotājam ar skolniekiem un skolniekiem savstarpēji - var būt būtisks elements to izglītības procesā.
Klātienē, piedaloties nodarbībā, visi nodarbības dalībnieki gan redz, gan dzird viens otru.
Tiešsaistes nodarbību norises apstākļu pietuvināšana klātienes nodarbībām var ļaut pedagogiem jaunos apstākļos izmantot esošās iestrādnes darbā ar audzēkņiem.

ATTĀLINĀTAIS MĀCĪBU PROCESS (2)

Līdz ar to, lai novērstu Covid-19 infekcijas izplatību sabiedrībā, ievērojot normatīvajā aktā noteiktos pamatprincipus, izglītības iestādes var noteikt kārtību tiešsaistes nodarbību organizēšanai tīmekļa vietnē, tai skaitā, identificējot nepieciešamību, **lūgt audzēkņiem izmantot videokameras**, piedaloties tiešsaistes mācību nodarbībā.

ATTĀLINĀTAIS MĀCĪBU PROCESS (3)

Izglītības iestāde ir tiesīga izvēlēties **veikt mācību procesa ierakstīšanu**. Tomēr tai ir jāspēj pamatot šādas izvēles nepieciešamību kvalitatīva un droša mācību procesa veikšanai.
Mācību iestādei šajā gadījumā iekšēji saistošā dokumentā (kārtībā, rīkojumā u.tml.) **būtu jānosaka:**
- ieraksta glabāšanas termiņi;
- piekļuves tiesības ierakstam (kas var tos skatīties);
- citas tehniskas (drošības) un organizatoriskas prasības, lai novērstu nepiederošo personu piekļuvi ierakstam.

DARBINIEKU APTAUJA PAR GATAVĪBU VAKCINĒTIES PRET COVID-19

Datu valsts inspekcija ir sniegusi viedokli par darba devēju organizētajām aptaujām, saistībā ar darbinieku vakcināciju.

Datu valsts inspekcija nekonstatē, ka darba devēja veiktai personas datu apstrādei, iegūstot darbinieku vārdus un uzvārdus, lai veiktu aptauju par darbinieku attieksmi - par gatavību vakcinēties pret Covid-19 -, pastāv kāds no Regulas 6.panta 1.punktā minētajiem tiesiskajiem pamatiem.

Tāpat Datu valsts inspekcijas ieskatā, **vārda un uzvārda norādīšana aptaujā nav samērīga** ar personas datu apstrādes sasniedzamo nolūku, un līdz ar to nolūku (noskaidrot nodarbināto viedokli par vakcinēšanos pret Covid-19) var sasniegt, neapstrādājot nodarbināto personas datus.

DARBINIEKU SARAKSTS COVID-19 VAKCĪNAS SAŅEMŠANAI

Kopš 2021.gada 5.februāra ikviens Latvijas iedzīvotājs varēja uzsākt pieteikšanos, lai saņemtu vakcīnu pret Covid-19, kas ir katras personas brīva izvēle.

Darba devējs, veidojot darbinieku sarakstu ar nolūku (mērķi) - organizēt kolektīvo vakcinēšanos pret Covid-19 -, tādējādi apstrādājot darbinieka personas datus (vārdu, uzvārdu), kā tiesisko pamatu var piemērot tikai Regulas 6.panta 1.punkta «a» apakšpunktu – katra darbinieka sniegta piekrišana personas datu apstrādei.

Darba devējam ir jāņem vērā, **darbinieks pēc piekrišanas sniegšanas var to jebkurā brīdī atsaukt**, un tas nekādā gadījumā **nevar radīt nelabvēlīgas sekas darbiniekam.**

APLIECINĀJUMS PAR COVID-19 VAKCINĀCIJAS STATUSU

Noteikumi neparedz obligātu vakcināciju pret Covid-19, līdz ar to **darba devējam nav tiesības uzlikt par pienākumu darbiniekam vakcinēties pret Covid-19 vai apstrādāt iepriekšminēto informāciju par vakcinācijas saņemšanu.**

Datu valsts inspekcija šobrīd nekonstatē, ka darba devējam pastāv tiesiskais pamats šādu informāciju apstrādāt, t.sk. iegūt un glabāt. Līdz ar to tiek norādīts, ka **darbiniekam šāda informācija nav jāsniedz darba devējam.**

DARBINIEKU VIDEONOVĒROŠANA ATTĀLINĀTĀ DARBA PROCESA LAIKĀ

Darba vietā un darba laikā darbiniekam ir tiesības uz privātās dzīves neaizskaramību, līdz ar to arī darba laikā **darba devējam ir jārespektē darbinieka privātā dzīve**. Attālinātā darba procesā darba vieta ir darbinieka privātā telpa (mājas).
Veicot darbinieka nepārtrauktu novērošanu attālinātā darba procesā, iejaukšanās darbinieka privātumā ir ievērojami lielāka, kā īstenojot videonovērošanu klātienes darba vietā.
Ja darba devējs lūdz darbinieku turēt nepārtraukti ieslēgtu datora kameru vai datoram piesaistītu kameru, Datu valsts inspekcija nesaskata atbilstošu pamatojumu šādas datu apstrādes veikšanai, kā arī norāda, ka **šāda personas datu apstrāde ir nesamērīga** nolūka (mērķa) sasniegšanai, lai novērtētu darbinieka darba kvalitāti.

KO VĒL DARBA DEVĒJS DRĪKST UN KO NEDRĪKST DARĪT? (1)

Vai darba devējs var lūgt darbiniekiem sniegt informāciju, vai darbinieki nav pēdējo 14 dienu periodā bijuši ārvalstīs un nav bijuši kontaktā ar Covid-19 saslimušajiem vai kontaktpersonām?
- **Jā!** Darba devējs var iegūt no darbiniekiem šādu informāciju.

Vai darba devējs var mērīt darbinieku temperatūru?
- **Jā!** Darba devējs prevencijas nolūkos var mērīt darbiniekiem temperatūru, lai konstatētu vai var/nevar pielaist darbinieku pie darba pienākumu pildīšanas, bet nedrīkst uzkrāt, apkopot, glabāt iegūtos datus vai citādi tos pēc tam izmantot.

KO DARBA DEVĒJS DRĪKST UN KO NEDRĪKST DARĪT? (2)

Vai darba devējs var izpaust darbiniekiem, ka kolēģis ir inficējies ar Covid-19?

- **Jā!** Darba devējam ir tiesības informēt darbiniekus, ka kolektīvā ir konstatēta saslimšana ar Covid-19, neizpaužot darbinieka vārdu, uzvārdu vai citu personas identificējošu informāciju, un informēt, ka darbiniekiem ir jāievēro atbildīgo iestāžu noteiktos drošības un veselības aizsardzības pasākumus attiecībā uz Covid-19. Tāpat vajadzētu informēt arī trešās personas, kurām šāda informācija ir nepieciešama, par inficēšanās faktu vai par aizdomām.

Personas datu aizsardzībai nav jābūt šķērslim, kas kavētu efektīvu cīņu ar infekciju slimību, tai skaitā Covid-19 izplatību. Tai ir jānovērš nepamatota un nesamērīga informācijas izplatīšana par konkrētām saslimušām personām vai personām, kuras atrodas riska grupā.

DARBINIEKA PIENĀKUMI (1)

Vai darbiniekam ir jāinformē darba devējs par inficēšanos ar Covid-19?
- **Jā!** Saskaņā ar Darba aizsardzības likumu darbiniekam ir pienākums rūpēties par savu drošību un veselību un to personu drošību un veselību, kuras ietekmē vai var ietekmēt viņa darbs, kā arī nekavējoties ziņot darba devējam par jebkuriem darba vides faktoriem, kuri rada vai var radīt risku personu drošībai un veselībai.
Saskaņā ar Darba likuma 81. pantu darbiniekam ir pienākums rūpēties par to, lai pēc iespējas vairāk novērstu vai mazinātu šķēršļus, kas nelabvēlīgi ietekmē vai var ietekmēt parasto darba gaitu uzņēmumā, kā arī par to, lai pēc iespējas vairāk novērstu vai mazinātu zaudējumus.

IT/KIBERHIGIĒNAS IEVĒROŠANA (1)

Strādājot no mājas un izmantojot savu vai darba devēja datoru, darbiniekiem jāievēro personiskā IT jeb kiberhigiēna.

- Pārliecināties, ka ierīcei ir **nepieciešamie atjauninājumi**, piemēram, operētājsistēmas atjauninājumi (iOS vai Android), programmatūras un pretvīrusu atjauninājumi.
- Uzstādīt **antivīrusa programmatūru** un **ugunsmūri**.
- Lietot **drošas paroles** (vismaz 9 zīmes: lielie, mazie burti, cipari, simboli).
- Pārliecināties, ka dators, klēpjdators vai ierīce, kuru izmanto, tiek lietota **drošā vietā**, piemēram, vietā, kur ierīce vienmēr atrodas tavā redzeslokā un līdz minimumam var samazināt to personu skaitu, kuri var skatīt ierīces ekrānu, it īpaši, ja strādā ar sensitīviem personas datiem.

IT/KIBERHIGIĒNAS IEVĒROŠANA (2)

- Katram resursam izmantot **atšķirīgu paroli**. Ja viena parole tiks uzlauzta, tad pārējie konti un iekārtas joprojām būs drošībā.
- Darba pienākumu veikšanai, kas saistīta ar personas datu apstrādi, izmantot **darba e-pastu**, nevis privāto.
- Nevērt vaļā **nezināmas saites**.
- Izvairīties no dažādu **multivides datņu** (filmas, spēlēs, utt.) **lejupielādes**.
- Visur, kur tas tie piedāvāts, izmantot **divu faktoru autentifikāciju**.
- Nodrošināt, lai darba sakarā apstrādātajiem personas datiem **nevar piekļūt citi ģimenes locekļi**.
-**Bloķēt ierīci**, ja kāda iemesla dēļ tā jāatstāj bez uzraudzības.

DARBINIEKA PIENĀKUMI (4)

Viens no iejaukšanās sarakstē veidiem ir **CEO krāpšana** (*CEO Fraud*), kurā uzbrucējs izpēta organizācijas vai uzņēmuma mājas lapu, lai sagatavotu ticamu **krāpniecisku e-pastu** uzņēmuma vadītāja vārdā par finansēm atbildīgajam personālam, lūdzot veikt **steidzamu pārskaitījumu**. Uzbrukumā izmantotā e-pasta adrese, no kuras tiek sūtīts krāpnieciskais ziņojums, var būt izveidota ļoti līdzīga vadītāja e-pasta adresei.

LAIKS JAUTĀJUMIEM!

PALDIES JUMS PAR UZMANĪBU!

Ar cieņu,

Lauris Klagišs

Valdes loceklis

SIA «Datu aizsardzības speciālists»

+371 29470425

lauris.klagiss@gmail.com

www.datuspecialists.lv