Rekomendācija

Ceļvedis datu apstrādē maziem un vidējiem uzņēmējiem

Datu valsts inspekcija

Projekts tiek finansēts no Eiropas Savienības tiesību, vienlīdzības un pilsonības programmas (2014.-2020. gads)

Ievads

Sākot ar 2016. gada 27. aprīli ir stājusies spēkā Vispārīgā datu aizsardzības regula[1] (turpmāk tekstā – Regula). Latvijā, tāpat kā visā Eiropas Savienībā, to piemēro no 2018. gada 25. maija. Ko nosaka Regula, un kas jāņem vērā uzņēmējiem?

Regula noteic, ka personas datus drīkst vākt un apstrādāt tikai tad, ja tam ir tiesisks pamatojums, dati tiek vākti tikai nepieciešamajā apjomā. Savāktajiem datiem ir jābūt precīziem, aktuāliem, tie jāvāc konkrētos, skaidros un leģitīmos nolūkos, tie jāapstrādā likumīgi, godprātīgi un datu subjektam pārredzamā veidā, jāpieļauj datu subjekta identifikācija un tiem jāatrodas drošībā (Regulas 5. pants). Tas nozīmē, ka pirms datu apstrādes (vākšanas, glabāšanas, izmantošanas), Tavam uzņēmumam ir nopietni jāizvērtē savas datu apstrādes iespējas un, ja ir konstatētas nepilnības, tās jānovērš atbilstoši Regulas prasībām.

Regula nosaka ne tikai personas datu apstrādes kārtību, bet arī datu apstrādes pārziņa un apstrādātāja atbildību. Regulas mērķis ir dot datu subjektam iespēju pārvaldīt savus datus (personisko informāciju), lai kur arī tie neatrastos, savukārt uzņēmumam jānodrošina datu subjekta tiesību ievērošana. Regulā ietvertie personas datu aizsardzības principi, papildus iedzīvotāju tiesību aizsardzībai, palīdzēs arī Tava uzņēmuma informācijas sistēmu un līdz ar to arī Tavu komercinterešu efektīvākai un drošākai funkcionēšanai.

Personas datu apstrāde nav tikai digitālās ekonomikas virzītājs, par personas datu principiem atbilstošu datu apstrādi ir jārūpējas ne tikai informācijas un komunikācijas tehnoloģiju uzņēmumiem. Katra funkcionējoša uzņēmuma rīcībā ir personas dati. Tie ir veikaliem, sociālajiem medijiem, mazajām aptiekām un pat picu cepējiem – uzņēmumi tos kārto, analizē un glabā, gan lai izpildītu normatīvo aktu prasības, gan lai sasniegtu savus komerciālos mērķus, nodrošinot labāka pakalpojuma pieejamību saviem klientiem. Visām fiziskām personām - gan darbiniekiem, gan klientiem ir tiesības zināt datu apstrādes mērķi un apjomu, tiesības saņemt informāciju par savu datu izmantošanu, mainīt un aktualizēt savu datu informāciju.

Pētījumu centra SIA "SKDS" 2019. gada jūlijā veiktajā apsekojumā "Uzņēmēju informētība par Vispārīgo datu aizsardzības regulu un pieredze ar tās prasību nodrošināšanu" noskaidrots, ka aptuveni puse jeb 48 % uzņēmumu, uz kuriem attiecas Regulas prasības, uzskata, ka šobrīd uzņēmumā ir nodrošināta pilnīga atbilstība Regulas prasībām.

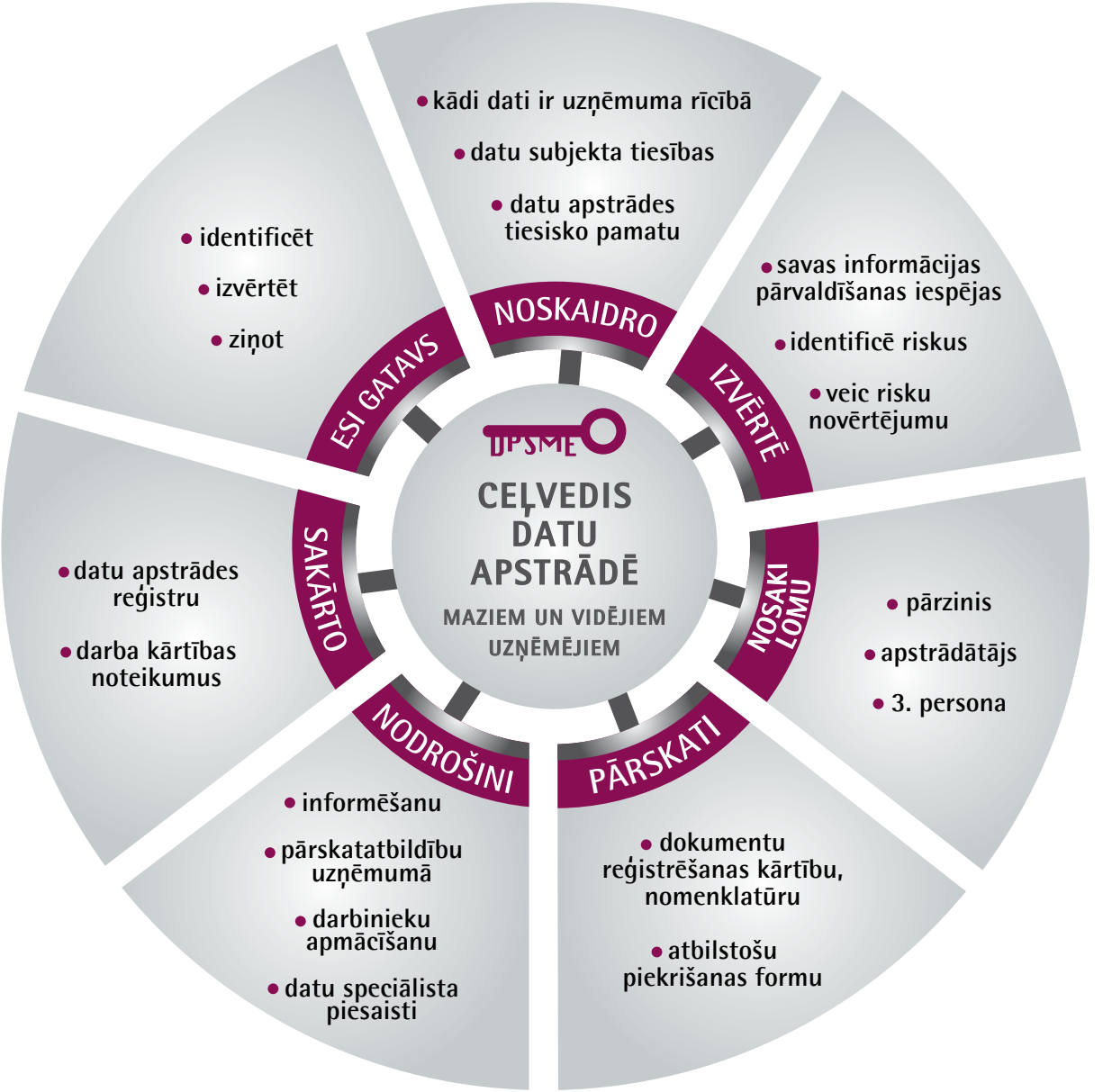
Savukārt, trešdaļā jeb 34 % uzņēmumu vēl ir veicami darbi pilnīgas atbilstības nodrošināšanai. Turpretī pārējā daļā uzņēmumu, uz kuriem attiecas Regula, nekas tās sakarā nav darīts.

Datu valsts inspekcija ir sagatavojusi informatīvu ceļvedi, kas palīdzēs mazajiem un vidējiem uzņēmumiem savā ikdienā efektīvi ieviest organizatoriskus un tehniskus pasākumus, lai nodrošinātu personas datu apstrādes un aizsardzības prasību izpildi.

Šajās rekomendācijās Datu valsts inspekcija sniedz padomus mazo un vidējo uzņēmumu pārstāvjiem par Regulas prasību ievērošanas nodrošināšanu un datu drošības jautājumu izpratni uzņēmumos. Rekomendācijas palīdzēs izprast un pildīt Regulas prasības, sakārtot datu aprites procesus Tavā uzņēmumā un nepieļaut datu drošības pārkāpumus.

---

[1] 2016. gada 27. aprīļa Eiropas Parlamenta un Padomes Regula Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk – Regula)


UPSME
CEĻVEDIS DATU APSTRĀDĒ
MAZIEM UN VIDĒJIEM UZŅĒMĒJIEM
NOSKAIDRO
• kādi dati ir uzņēmuma rīcībā
• datu subjekta tiesības
• datu apstrādes tiesisko pamatu
IZVĒRTĒ
• savas informācijas pārvaldīšanas iespējas
• identificē riskus
• veic risku novērtējumu
NOSAKI LOMU
• pārzinis
• apstrādātājs
• 3. persona
PĀRSKATI
• dokumentu reģistrēšanas kārtību, nomenklatūru
• atbilstošu piekrišanas formu
NODROŠINI
• informēšanu
• pārskatatbildību uzņēmumā
• darbinieku apmācīšanu
• datu speciālista piesaisti
SAKĀRTO
• datu apstrādes reģistru
• darba kārtības noteikumus
ESI GATAVS
• identificēt
• izvērtēt
• ziņot

Definīcijas

Personas dati – jebkura informācija, kas attiecas uz identificējamu fizisku personu (datu subjektu).

Datu subjekts – identificēta vai identificējama fiziska persona.

Biometriskie dati – personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskās personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm un ļauj veikt vai apstiprina šīs fiziskās personas viennozīmīgu identifikāciju.

Ģenētiskie dati – personas dati, kas attiecas uz fiziskas personas pārmantotām vai iegūtām ģenētiskajām pazīmēm, sniedz unikālu informāciju par šīs fiziskās personas fizioloģiju vai veselību un izriet no šīs fiziskās personas bioloģiskā parauga analīzes.

Veselības dati – personas dati, kas saistīti ar fiziskas personas fizisko vai garīgo veselību, tostarp veselības aprūpes pakalpojumu sniegšanu un, atspoguļo informāciju par tās veselības stāvokli.

Īpašu kategoriju[2] personas dati – rase, etniskā piederība, politiskie uzskati, reliģiskā vai filozofiskā pārliecība, dalība arodbiedrībās, ģenētiskie dati, biometriskie dati, veselības dati, dati par dzimumdzīvi, seksuālo orientāciju.

Personas datu aizsardzības pārkāpums – drošības pārkāpums, kura rezultāts ir nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

Pārzinis – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus.

Apstrādātājs – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas pārziņa vārdā apstrādā personas datus.

Pārskatatbildība – pārzinis pārskatāmi, ar attiecīgiem dokumentiem (dokumentu kopumu), pierāda un pamato, ka datu apstrāde notiek atbilstoši Regulas prasībām.

Leģitīms – likumīgs, likumīgi atzīts.

Sīkdatnes (cookies) – neliels teksta fails, ko mājaslapa saglabā Tavā datorā vai mobilajā ierīcē, kad Tu to apmeklē. Tās ļauj mājaslapai atcerēties Tavas izvēles (piemēram, valodu, burtu lielumu utt.), tāpēc Tev tās nav atkārtoti jāiestata katru reizi, kad atgriezies mājaslapā vai pārlūko dažādas lapas.

Pseidonimizācija – personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu.

Trešā persona – fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus.

Saīsinājumi:

DVI – Datu valsts inspekcija.

ES – Eiropas Savienība.

MVU – Mazie un vidējie uzņēmumi.

NIDA – Novērtējums par ietekmi uz datu aizsardzību.

Regula - Vispārīgā datu aizsardzības regula.

Piemērs.

Negatīvais piemērs.

Atceries, pievērs uzmanību!

[2] Pirms Regulas piemērošanas tika izmantots termins "sensitīvie dati"

PAŠNOVĒRTĒJUMA TESTS

Pirms uzsāc rekomendācijās ietverto pasākumu (ieteikumu) ieviešanu savā uzņēmumā, Datu valsts inspekcija aicina aizpildīt kontroljautājumu sarakstu par personas datu apstrādi Tavā uzņēmumā, lai izvērtētu vai līdzšinējā prakse, kādā tiek iegūti un apstrādāti personas dati Tavā uzņēmumā, ir atbilstoši normatīvajam regulējumam.

Lai pārliecinātos, ka uzņēmuma rīcībā esošās informācijas pārvaldīšana, kontrole un datu plūsma atbilst normatīvajiem aktiem un, lai noskaidrotu, kas tieši datu apstrādes un aizsardzības procesā ir jāuzlabo, Lielbritānijas uzraudzības iestāde ir izstrādājusi pašnovērtējuma testu, ņemot vērā tieši MVU vajadzības[3].

Atbildi uz šiem jautājumiem un noskaidro, vai Tava uzņēmuma rīcībā esošās informācijas pārvaldīšana, kontrole un datu plūsma ir atbilstoša normatīvajiem aktiem.

1. **Vai Tavā uzņēmumā ir izveidots uzņēmuma rīcībā esošo personas datu apstrādes reģistrs? Vai Tavam uzņēmumam ir zināms to izmantošanas nolūks?**
   - ☐ JĀ
   - ☐ NĒ

- Vai esi domājis par to, kādu informāciju Tavs uzņēmums iegūst un nodod uzņēmējdarbības aktivitāšu ietvaros?
- Vai šī informācija iekļauj fizisku personu datus par klientiem? Tie var būt personu vārdi, uzvārdi un adreses, kam tiek piegādātas preces, kā arī mārketinga aktivitāšu ietvaros izmantotā kontaktinformācija un citi dati.
- Vai zini, kāpēc Tavs uzņēmums ievāc un glabā fiziskos personu datus?
- Vai Tavam uzņēmumam ir izveidots personas datu reģistrs par to, kādi dati ir tā rīcībā, kā uzņēmums ar tiem rīkojas un kāpēc tos glabā?
- Vai uzņēmuma datu apstrādes reģistrs iekļauj šādu informāciju:
  - Datu kategorijas, piemēram, personu vārdi un e-pasta adreses.
  - Kā tika iegūti dati? Piemēram, papīra formātā vai caur uzņēmuma tīmekļa vietni.
  - Kāpēc tieši šie dati?
  - Cik ilgi Tava uzņēmuma rīcībā bija un cik ilgi tie tiks glabāti?
  - Vai Tavs uzņēmums šos datus kādam nodod?
  - Vai šie dati ir īpašo kategoriju dati, piemēram, medicīniskie dati?

Ieteicamās darbības:

- Izveido sarakstu, kurā fiksē uzņēmuma rīcībā esošos personas datus, piemēram, vārds, uzvārds, e-pasts, adrese.
- Kādēļ Tavam uzņēmumam ir nepieciešami šie dati?
- Norādiet kā konkrētos personas datus apstrādājat (glabājat, nododat, analizējat).
- Norādiet kāds ir tiesiskais pamats šīm datu apstrādēm.

[3] Information Commissioner's Office "How well do you comply with data protection law: an assessment for small business owners and sole traders" *https://ico.org.uk/for-organisations/data-protection-self-assessment/assessment-for-small-business-owners-and-sole-traders/*

Tev nav jāpārraksta visi Tava uzņēmuma rīcībā esošie e-pasti, vārdi, uzvārdi, bet gan jāapzina, kādi tieši dati Uzņēmumā tiek iegūti un kāds ir to apstrādes tiesiskais pamatojums. Lai uzzinātu kādos gadījumos ir nepieciešams veidot datu apstrādes reģistru lasi sadaļu "SAKĀRTO" (28.lpp)

Tava uzņēmuma rīcībā esošo personas datu glabāšanai nepieciešams nodrošināt atbilstību vienam no sešiem datu apstrādes tiesiskajiem pamatiem. Lai noteiktu personas datu apstrādes tiesisko pamatu savā uzņēmu lasi sadaļā "NOSKAIDRO" ➔ "Kāds ir datu apstrādes tiesiskais pamats Tavā uzņēmumā?" (11.lpp)

2. **Vai cilvēki zina, ka Tava uzņēmuma rīcībā ir viņa personas dati? Vai viņi saprot kā tie tiek izmantoti?**

   ☐ JĀ

   ☐ NĒ

- Vai Tavs uzņēmums informē datu subjektus par to kā tiek izmantoti viņu personas dati?
- Vai uzņēmums informē cilvēkus tad, ja viņu personas dati tiek nodoti?
- Vai skaidrojat cilvēkiem, ko plānojat darīt ar viņu personas datiem, papīra formā, piemēram, izmantojot skrejlapas vai plakātus, vai tiešsaistē, izmantojot privātuma politiku?
- Ja tā, vai šajā privātuma politikā ir ietverta visa tālāk sniegtā informācija:
  - Tava uzņēmuma nosaukums un par datu aizsardzību atbildīgā persona.
  - Kāpēc Tavs uzņēmums glabā personas datus (tiesiskais pamats) un ko ar tiem dara?
  - no kurienes Tavs uzņēmums saņēma datus?
  - Kam dati tiek nodoti un kādā veidā, ieskaitot jebkādu nodošanu ārpus Latvijas?
  - Cik ilgi tiek glabāti dati?
  - Kā cilvēki var pieprasīt piekļuvi saviem datiem, to labošanu vai dzēšanu?
  - Kā iesniegt sūdzību DVI?
  - Vai pieņemat automatizētus lēmumus, vai tiek veikta profilēšana?

Ieteicamās darbības:

Ja Tavs uzņēmums pašlaik nesniedz nekādu informāciju par Tavā uzņēmumā veikto personas datu apstrādi, tad ir jāizveido privātuma politika un tajā jāiekļauj turpmāk minētā informācija.

Ja Tavs uzņēmums sniedz informāciju par Tavā uzņēmumā veikto personas datu apstrādi, ir jāpārbauda, vai privātuma politikā ir iekļauta turpmāk minētā informācija:

- Tava uzņēmuma nosaukums un persona, kas atbild par datu aizsardzību;
- Kāpēc Tavs uzņēmums glabā personas datus (tiesiskais pamats) un kā dati tiek apstrādāti?
- Kur personas dati iegūti?
- Personas, kurām nododat datus, un kā to darāt (ieskaitot jebkuru nodošanu ārpus ES)
- Cik ilgi glabājat datus?
- Kā var pieprasīt piekļuvi saviem datiem, to labošanu vai dzēšanu?
- Kā iesniegt sūdzību Datu valsts inspekcijai?
- Vai tiek pieņemti automatizēti lēmumi vai veikta profilēšana, pamatojoties uz Tava uzņēmuma rīcībā esošajiem datiem?
- Vai šo informāciju publicējat uzņēmuma iekšējās instrukcijās vai interneta vietnēs?

Ja Tava uzņēmuma privātuma politika nesatur iepriekš minēto informāciju, atjaunini to!

3. Vai tiek apstrādāti tikai tie dati, kas ir nepieciešami?

☐ JĀ

☐ NĒ

- Vai Tavs uzņēmums apstrādā datus, kas nepieciešami darbam?
- Vai uzņēmums nodrošina personu, kuru dati tiek apstrādāti (iegūti, glabāti u.tml.), informēšanu par to, kādi dati sniedzami obligāti un to kādu datu sniegšana nav obligāta?

Ieteicamās darbības:

Pārskati visus Tavā uzņēmumā esošos personas datus un izlem, kas ir nepieciešams apstrādei un kas nav obligāts.

Iznīcini tos personas datus, kas tiek pārmērīgi apstrādāti un kas Tavam uzņēmuma nav nepieciešami. legūstot personas datus, informē datu subjektu par to, kāda informācija ir sniedzama un kāda nav obligāti sniedzama. Regulāri pārbaudi Tava uzņēmuma rīcībā esošos personas datus un droši iznīcini visu, kas ir pārmērīgs vai kas Tavam uzņēmumam nav jāizmanto, jāuzglabā vai citādi jāapstrādā.

Lai nodrošinātu, ka Tavā uzņēmumā tiek apstrādāti tikai tie dati, kas ir nepieciešami lasi sadaļu "NOSKAIDRO" (9.lpp).

Personas datus ir jāapstrādā tikai atbilstoši noteiktajam apstrādes nolūkam, lai apstrāde ir atbilstoša tās nolūkam. Tavs uzņēmums neglabā vairāk personas datus kā tas ir nepieciešams apstrādes nolūkam.

4. Vai dati tiek glabāti tik ilgi, cik nepieciešams?

☐ JĀ

☐ NĒ

- Vai uzņēmums ir noteicis un dokumentējis, cik ilgi personas dati tiks glabāti?
- Vai pēc noteikta laika dati tiks atjaunoti vai dzēsti?
- Vai pēc datu glabāšanas termiņa notecējuma Tavs uzņēmums tos atjauno vai dzēš uzreiz, tiklīdz tie vairs nav nepieciešami?

Ieteicamās darbības:

Izvērtē, cik ilgi Tavam uzņēmuma vajadzētu glabāt iegūtos personas datus. Glabāšanas termiņš var mainīties atkarībā no iegūtajiem personas datu veidiem un to izmantošanas nolūkiem.

Iznīcini informāciju, ko Tavs uzņēmums turējis ilgāk, nekā nepieciešams.

Regulāri pārbaudi, vai personas dati netiek glabāti ilgāk, nekā Tavam uzņēmumam nepieciešams.

Lai nodrošinātu atbilstošus datu glabāšanas termiņus datu apstrādes nolūkam izstrādā uzņēmuma nomenklatūru un darba kārtības noteikumus. Par uzņēmuma nomenklatūru un darba kārtības noteikumiem lasi sadaļā "PĀRSKATI" un "SAKĀRTO" (21., 28.lpp).

5. Vai personas dati tiek uzturēti precīzi un atjaunināti?

☐ JĀ

☐ NĒ

- Vai tiek veiktas regulāras pārbaudes, lai konstatētu, ka Tava uzņēmuma rīcībā esošie personas dati ir precīzi un atjaunināti?

Ieteicamās darbības:

Pārliecinies, ka Tavs uzņēmums viegli un ātri var atjaunināt visus uzņēmumā pieejamos personas datus.

Regulas 5.panta "d" apakšpunkts nosaka, ka personas dati ir precīzi un, ja vajadzīgs, atjaunināti; ir jāveic visi saprātīgi pasākumi, lai nodrošinātu, ka neprecīzi personas dati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti ("precizitāte");

Lai nodrošinātu, ka Tava uzņēmuma rīcībā esošie personas dati ir precīzi un nepieciešamības gadījumā tiek atjaunināti, lasi sadaļu "NOSKAIDRO", "NODROŠINI" un "SAKĀRTO" (9., 24., 28. lpp.)

6. Vai Tava uzņēmuma personas dati ir drošībā?

☐ JĀ
☐ NĒ

- Vai personas dati tiek glabāti drošībā, piemēram, birojā izmantojot aizslēdzamus dokumentu skapjus, izslēdzot vai bloķējot datorus, kad darbinieki neatrodas savās darba vietās?
- Vai uzņēmumā tiek veikti konkrēti pasākumi, lai glabātu datus drošībā? Piemēram, vai strādājat tikai ar tiem dokumentiem, kas konkrētajā brīdī ir nepieciešami?
- Vai uzņēmumā glabājat papīra dokumentus drošībā? Piemēram, izmantojot drošu papīra dokumentu glabāšanu (seifs) un iznīcināšanu (papīra smalcinātājs)?
- Vai uzņēmumā glabājat elektroniskos datus drošībā, piemēram, šifrējot mobilās ierīces, izmantojot paroles un dublējot datus?

Ieteicamās darbības:

Pārskati un nepieciešamības gadījumā uzlabo pašreizējos drošības pasākumus Tava uzņēmuma darba vidē.

Kā to izdarīt?

- Izmanto datora paroles. Nesaki nevienam, kādas ir Tavas paroles, nomaini tās ik pa laikam.
- Pirms dodies prom no sava darba galda, datorā aktivizē snaudas režīmu vai izslēdz to.
- Iznīcini konfidenciālos papīra atkritumus, tos sasmalcinot.
- Pārliecinies, ka IT cietajos diskos nepaliek personas dati, kad atbrīvojies no tehnikas.
- Esi piesardzīgs, atverot aizdomīgus e-pastus un to pielikumus.
- Pārliecinieties, ka personas datu papīra kopijas tiek droši glabātas, kad tās netiek izmantotas.
- Izmantojiet tikai drošu WI-FI.
- Šifrējiet personas datus, it īpaši, ja tie var atrasties ārpus biroja un nozaudēšanas vai zādzības gadījumā var radīt kaitējumu datu subjektiem.
- Pievērs uzmanību savai apkārtnei, strādājot ārpus biroja, piemēram kafejnīcā vai vilcienā. Pārliecinieties, ka blakus esošie cilvēki nevar redzēt personas datus, pie kuriem Tu strādā.
- Samaziniet papīra informācijas apjomu, ja nepieciešams strādāt ārpus biroja.

Lai būtu pārliecināts, ka ievēro tehniskos un organizatoriskos pasākumus, kas nodrošina Tava uzņēmuma rīcībā esošo datu drošību, lasi sadaļu "PĀRSKATI" (21. lpp) ➔ "Kāda ir dokumentu reģistrēšanas kārtība un nomenklatūra Tavā uzņēmumā?", sadaļu "IZVĒRTĒ" un sadaļu "NODROŠINI" (16. un 24. lpp).

7. Vai Tavā uzņēmumā ir kāds veids, kā cilvēki var izmantot savas tiesības attiecībā uz uzņēmuma rīcībā esošajiem personas datiem?

☐ JĀ

☐ NĒ

- Vai zini kādas tiesības ir datu subjektiem?

Kopumā šādas:

- Tiesības būt informētam - tiek paziņots, kādi datu subjekta dati uzņēmumā ir un ko ar tiem dara (kā apstrādā).
- Piekļuves tiesības - iespēja pieprasīt uzņēmuma rīcībā esošos datus.
- Tiesības uz labošanu - kļūdainu datu labošana.
- Tiesības dzēst - iespēja lūgt izdzēst / iznīcināt uzņēmuma rīcībā esošos datus.
- Tiesības ierobežot apstrādi - spēja ierobežot izmantoto datu daudzumu vai veidu.
- Tiesības uz datu pārnesamību - pieprasījums pārvietot savus datus elektroniski uz citu uzņēmumu.
- Tiesības iebilst - iespēja pieprasīt pārtraukt viņu datu izmantošanu.

- Vai Tavā uzņēmumā ir plāns, kā izskatīt datu subjektu pieprasījumus?

Lai spētu identificēt un nodrošināt datu subjekta tiesību ievērošanu, lasi sadaļu "NOSKAIDRO" ➔ "Vai esi informēts, kādas ir datu subjekta tiesības?" (10. lpp.).

8. Vai Tava uzņēmuma personāls zina savus pienākumus datu aizsardzības jomā?

☐ JĀ

☐ NĒ

- Vai visi uzņēmuma darbinieki, kuri apstrādā personas datus, ir apmācīti par datu aizsardzības jautājumiem un darbinieku pienākumiem datu aizsardzības jomā?
- Vai zini kā rīkoties, ja notiek personas datu pārkāpums?

Personas datu pārkāpums nozīmē drošības pārkāpumu, kas noved pie nejaušas vai nelikumīgas personas datu iznīcināšanas, pazaudēšanas, mainīšanas, neatļautas izpaušanas vai piekļuves tiem.

Tas ietver pārkāpumus, kas radušies gan nejaušu, gan apzinātu iemeslu dēļ. Tas arī nozīmē, ka pārkāpums ir kas vairāk nekā tikai personas datu nozaudēšana.

- Vai zini par kādiem pārkāpumiem ir jāziņo DVI?

Pārkāpumam var būt vairākas nelabvēlīgas ietekmes uz indivīdiem, kas ietver emocionālas ciešanas un fiziskus un materiālus zaudējumus. Tev jānosaka no tā izrietošie riski cilvēku tiesībām un brīvībām, to iespējamība un nopietnība. Ja risks ir iespējams, tad pārzinis par to paziņo DVI.

- Vai zini par kādiem pārkāpumiem jāinformē datu subjekti?

Ja pārkāpums varētu radīt lielu risku datu subjekta tiesībām un brīvībām, Regula noteic, ka pārzinis par to informē datu subjektu tieši un bez liekas kavēšanās, cik drīz vien iespējams.

Ieteicamās darbības:

- Pārliecinies, ka visi Tava uzņēmuma darbinieki ir informēti par datu subjekta tiesībām.
- Apmāci darbiniekus - kādi pieprasījumi varētu tikt saņemti no datu subjektiem un kā rīkoties, ja tas notiek.
- Pārliecinies, ka varēsi nodrošināt datu subjekta tiesības atbilstoši to pieprasījumiem. Piemēram, pārliecinies, vai Tava uzņēmuma datorprogrammas ļauj dzēst vai labot informāciju.

Uz datu subjekta pieprasījumu jāatbild viena mēneša laikā.

Lai nodrošinātu, ka Tavā uzņēmumā darbinieki ir informēti un apmācīti ievērot Regulu, lasi sadaļu "NODROŠINI" ➔ "Kā Tavā uzņēmumā darbinieki tiek informēti un apmācīti ievērot Regulas prasības? Vai darbinieki zina savus pienākumus?", "Kādi ir darba kārtības noteikumi Tavā uzņēmumā?" (30. lpp) un sadaļu "ESI GATAVS" (31. lpp).

Paldies, ka aizpildīji testu!

Ja Tavas atbildes ir vairumā JĀ –

Datu aizsardzība Tavā uzņēmumā izskatās labi.

Tomēr, ja ir kādas atbildes, kas rada šaubas, lūdzu, atgriezies pie konkrētā jautājuma skaidrojuma *Ieteicamās darbības* un uzzini ko darīt.

Ja Tavas atbildes ir vairumā NĒ –

Lai gan ir nepieciešams uzlabot datu aizsardzības procesus Tavā uzņēmumā, esam pārliecināti, ka Tavs uzņēmums to spēs. Lūdzu, atgriezies pie konkrētā jautājuma skaidrojuma *Ieteicamās darbības* un uzzini ko darīt, lai sakārtotu datu aizsardzību savā uzņēmumā.

NOSKAIDRO

Vai zini, kādi personas dati ir Tava uzņēmuma rīcībā?

Regula noteic, ka datu subjektam (darbiniekam, sadarbības partnerim vai nejaušam garāmgājējam) ir tiesības zināt, kādi viņa personas dati ir pārziņa (Tava uzņēmuma) rīcībā.

Lai vieglāk varētu identificēt personas datu kategorijas, kas ir Tava uzņēmuma rīcībā, var izmantot vairākas metodes.

Piemēram, tās var iedalīt pēc datu subjektiem:

- **Iekšējie** – darbinieku un darbinieku ģimenes locekļu personas dati;
- **Ārējie** – klientu, piegādātāju un pakalpojumu sniedzēju personas dati.

Iekšējie dati tiek izmantoti darba vajadzībām, to lietošanu regulē spēkā esošie normatīvie akti par darba līgumu slēgšanu, kvalifikācijas un pieredzes noteikšanu, algas izmaksām, utt. Bieži vien, personai stājoties darbā, darba devēja pienākums ir zināt konkrētās personas veselības stāvokli vai kādu citu īpaša rakstura informāciju par potenciālo darba ņēmēju.

Pārzinim ir jāatceras, ka informāciju par:

1. personas veselības stāvokli,
2. personas rasi,
3. etnisko piederību (tautību),
4. politiskajiem uzskatiem,
5. reliģisko vai filozofisko pārliecību,
6. dalību arodbiedrībās,
7. ģenētiskiem datiem,
8. biometriskiem datiem,
9. jebkādu citu informāciju par personas dzimumdzīvi vai seksuālo orientāciju APSTRĀDĀT IR AIZLIEGTS. Regulas 9. pants noteic izņēmuma gadījumus, kad var tikt veikta iepriekš minēto datu apstrāde. Piemēram, darba devējs var apstrādāt informāciju par darbinieka veselības stāvokli, ja šī informācija ir nepieciešama darbinieka nodarbināšanas jautājumos (Regulas 9. panta otrās daļas "b" punkts).

Der atcerēties, ka Regulā noteiktā aizsardzība attiecībā uz personas datu apstrādi attiecas uz fiziskām personām neatkarīgi no to valstspiederības vai dzīvesvietas. Regula neattiecas uz tādu personas datu apstrādi, kas skar juridiskas personas un, jo īpaši, uzņēmumus, kuriem ir juridiskas personas statuss, tostarp juridiskās personas nosaukumu, uzņēmējdarbības formu un kontaktinformāciju. Uzņēmuma valdes locekļi, kā arī amatpersonas, pildot darba uzdevumus, pārstāv juridisku personas iestādes nevis savas kā fiziskas personas intereses. Savukārt, ja šī informācija tiek apstrādāta ārpus profesionālās darbības konteksta, tā būs personas datu apstrāde Regulas tvērumā.

Jānis Bērziņš ir galdnieks, kurš ir nodarbināts kā individuālais komersants "Jānis Bērziņš". Šajā gadījumā personas dati "Jānis Bērziņš", kas attiecas uz individuālo komersantu kā komercdarbības juridisko formu, nav fiziskas personas dati Regulas izpratnē, piemēram, gadījumos, kad klients (esošs vai potenciāls) sazinās ar Jāni Bērziņu par vienošanās izpildi/noslēgšanu. Ja šo informāciju izmanto cits uzņēmējs, lai informētu Jāni Bērziņu, ka pašlaik tiek piedāvāta akcija visiem Jāņiem Bērziņiem ceļojumam uz kādu ārvalsti, tā būs uzskatāma par Jāņa Bērziņa personas datu apstrādi, jo notiks ārpus Jāņa Bērziņa profesionālās darbības konteksta.

Vai esi informēts, kādas ir datu subjekta tiesības?

Tavam uzņēmumam ir pienākums zināt un nodrošināt Regulā noteikto datu subjekta tiesību ievērošanu:

- **Tiesības būt informētam pirms personas datu vākšanas.** Datu subjektam ir jāzina un jāsaprot, ka un kā viņa dati tiek apstrādāti - vākti, glabāti un dzēsti (Regulas 13. un 14. pants).
- **Tiesības prasīt piekļuvi personas datiem** (Regulas 15. pants) un zināt kādam mērķim dati tiek izmantoti. Tavam uzņēmumam ir jāzina, kādi personas dati kur atrodas, jāspēj sniegt personas datus, ja datu subjekts to pieprasa.
- **Tiesības uz informācijas labošanu** (Regulas 16. pants). Iespēja labot un aktualizēt personas datus, kas glabājas Tavā uzņēmumā. Savukārt Tavam uzņēmumam ir jāreģistrē datu labošanas brīdis un turpmāk jāizmanto tikai aktuālie dati.
- Ja persona vairs nav Tavs klients un nevēlas, lai Tu izmantotu viņa datus, datu **subjektam ir tiesības pieprasīt datu dzēšanu,** ja datu apstrādes tiesiskais pamats ir personas piekrišana un nav cita likumīga pamata to apstrādei, ja personas dati vairs nav nepieciešami saistībā ar nolūkiem, kādos tie tika vākti vai citādi apstrādāti; personas dati ir apstrādāti nelikumīgi u.c. (Regulas 17. pants). Tas nozīmē ne tikai to, ka Tavam uzņēmumam ir jāzina, kādi dati un uz kāda pamata tiek apstrādāti, bet arī jānodrošina tādu sistēmu izmantošana, kas ļauj īstenot šīs datu subjekta tiesības.
- **Tiesības pieprasīt, lai tiktu ierobežota personas datu apstrāde** (izņemot glabāšanu) (Regulas 18. pants).
- **Tiesības lūgt saņemt savus personas datus**, ko viņš sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā un ir tiesības minētos datus nosūtīt citam pārzinim, ja tie apstrādāti uz piekrišanas vai līguma pamata un apstrādi veic ar automatizētiem līdzekļiem (Regulas 20. pants).
- **Tiesības būt informētam**, ja ir noticis personas datu aizsardzības pārkāpums, kas būtiski varētu apdraudēt datu subjekta intereses. Tavā uzņēmumā ir jābūt izstrādātam rīcības plānam, lai varētu operatīvi paziņot par datu aizsardzības pārkāpumu. (Regulas 33. panta 5. punkts).

Atbilde uz datu subjekta pieprasījumu ir jāsniedz viena mēneša laikā, bez maksas.

Datu subjekti ir jāinformē par plānotajām personas datu apstrādēm pirms apstrādes uzsākšanas (privātuma politika, videonovērošanas zīmes).

Tavam uzņēmumam jāspēj identificēt konkrētais datu subjekts, veicot jebkādu viņa personas datu apstrādi – gan iegūstot personas datus, gan atbildot uz jebkuru datu subjekta pieprasījumu izsniegt, labot vai dzēst datus. Šīs darbības, kas veiktas ar datiem, ieteicams dokumentēt, lai varētu pamatot veikto apstrādi.

Kāds ir datu apstrādes tiesiskais pamats Tavā uzņēmumā?

Izsniedzot vai citādi apstrādājot personas datus, ir vairāki tiesiskie pamati datu apstrādei, kuru piemērojamība ir jāvērtē katrā konkrētā gadījumā atsevišķi.

Datu apstrādei (personas datu iegūšana, glabāšana, nodošana u.c.) ir jābūt:

- tiesiski pamatotai,
- godprātīgai un pārredzamai,
- ar konkrētu nolūku (mērķi),
- iespējami minimālai – (iegūstam tikai pašus nepieciešamākos datus),
- precīzai,
- drošai – nodrošinot aizsardzību pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu. (Regulas 5. pants)

Pārskati sava uzņēmuma rīcībā esošās datu bāzes un kartotēkas un pārliecinies, ka datu apstrāde atbilst Regulas prasībām. Neglabā tos datus, kuru apstrādei nav tiesiska pamata un tos, kas glabājas pārāk ilgi, ir novecojuši (piemēram, klientam ir mainīts uzvārds, dzīves vietas adrese), kā arī tos datus, kas vairs nav nepieciešami sākotnējam apstrādes nolūkam.

Tiesiskie pamati personas datu apstrādei noteikti Regulas 6. panta 1. punktā. Ņem vērā, ka, apstrādājot īpašas kategorijas personas datus, papildus 6. panta 1. punktā norādītajam tiesiskajam pamatam Tavam uzņēmumam būs nepieciešams atrast tiesisko pamatu arī Regulas 9. panta 2. punktā:

- **Piekrišana.**

Persona (datu subjekts) ir devusi piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem. Gadījumos, kad saskaņā ar piekrišanu tiek apstrādāti īpašo kategoriju dati (Regulas 6. panta 1. punkta "a" apakšpunkts un Regulas 9. panta 2. punkta "a" apakšpunkts) šādai piekrišanai ir jābūt skaidrai (no pārskatatbildības viedokļa tas nozīmē, ka nepieciešama rakstiska piekrišana skaidri formulētam mērķim).

Veikalā klientam (datu subjektam) tiek piedāvāts aizpildīt klientu apmierinātības aptaujas anketu, kurā jānorāda vārds, uzvārds, elektroniskā pasta adrese. Aptaujas mērķis ir piedāvāt personalizētus piedāvājumus konkrētam klientam. Lai saņemtu personas datus šādas aptaujas veikšanai, pārzinim ir jāsaņem klienta piekrišana. Vēlams rakstveidā, lai veikals (pārzinis) varētu uzskatāmi pierādīt, ka šai datu apstrādei ir ieguvis tiesisko pamatu – klienta piekrišanu.

Piekrišana datu apstrādei var arī nebūt rakstiska. Ikdienā mēs bieži sastopamies ar sīkdatņu apstrādi interneta vietnēs, kad pirms vietnes apskates turpināšanas, apstiprinām piekrišanu, nospiežot pogu, ka interneta vietne mūs atcerēsies. Šāda piekrišana tiek sniegta ar konkrētu darbību – nospiežot pogu.

- **Līguma izpilde.**

Datu apstrāde izriet no uzņēmuma (pārziņa) līgumsaistībām ar klientu (datu subjektu) vai, ievērojot personas pieprasījumu, datu apstrāde nepieciešama, lai attiecīgu līgumu noslēgtu.

Jānis ir noslēdzis distances līgumu par preču piegādi savā dzīvesvietā. Lai piegādātu Jāņa pasūtītās preces, preču piegādātājam ir nepieciešami Jāņa personas dati – vārds, uzvārds, adrese. Bez šiem datiem līgums par preču piegādi nevar tikt izpildīts. Preču piegādātājs var arī lūgt uzrādīt personu apliecinošu dokumentu preču piegādes laikā, lai pārliecinātos, ka tieši Jānis ir pasūtījis preces.

Fiziska persona (datu subjekts) vēlas apmeklēt apmācības pie komersanta (pārziņa), kam ir tiesības izdot sertifikātu par apgūto mācību kursu. Lai komersants varētu sniegt šādu pakalpojumu, komersantam ar datu subjektu ir nepieciešams noslēgt līgumu par pakalpojuma sniegšanu/saņemšanu, kas satur noteiktus personas (datu subjekta) datus. Šādā gadījumā bez personas datu apstrādes nav iespējams ne noslēgt līgumu, ne arī izsniegt sertifikātu par kursu apgūšanu. Tādējādi personas datu apstrāde izriet no līgumsaistībām.

- **Juridisks pienākums.**

Personas datu apstrāde ir nepieciešama pārzinim, lai veiktu ES vai valsts tiesību aktā noteiktu pienākumu.

Pieņemot darbinieku, darba devējam ir jāievēro normatīvajos aktos noteiktās prasības.

Darba likums nosaka obligātās veselības pārbaudes darbiniekiem. Darba devējam ir pienākums tādas pieprasīt un apstrādāt atbilstoši Darba likumā noteiktajam. Pretējā gadījumā darba devējs nepilda likumā noteikto pienākumu.

Iepriekš minētai apstrādei ir ne tikai Regulas 6. panta 1. punkta "c" apakšpunktā, bet arī Regulas 9. panta 2. punkta "b" apakšpunktā norādītais tiesiskais pamats. Atceries, ka veselības dati saskaņā ar Regulu ir uzskatāmi par īpašo kategoriju personas datiem.

Darba devējs katru darba ņēmēju reģistrē Valsts ieņēmumu dienestā, sniedzot ziņas par darba ņēmējiem.

- **Sabiedrības intereses.**[4]

Datu apstrāde nepieciešama, lai veiktu sabiedrības interesēs īstenojamu uzdevumu vai īstenotu oficiālas pilnvaras, kas noteiktas ES vai valsts tiesību aktā.

Latvijas Zvērinātu advokātu kolēģijai ir Latvijas Republikas Advokatūras likumā noteiktas pilnvaras veikt disciplināras procedūras pret kolēģijas locekļiem.

- **Vitālo interešu aizsardzība.**

Personas datu apstrāde ir nepieciešama, lai aizsargātu fiziskās personas vitāli svarīgas intereses, tajā skaitā dzīvību un veselību.

4 Ministru kabineta 2010. gada 7. septembra noteikumi Nr. 827 "Noteikumi par valsts sociālās apdrošināšanas obligāto iemaksu veicēju reģistrāciju un ziņojumiem par valsts sociālās apdrošināšanas obligātajām iemaksām un iedzīvotāju ienākuma nodokli"

Autoavārija. Persona tiek nogādāta slimnīcā ar dzīvībai bīstamiem ievainojumiem. Lai aizsargātu šīs personas vitāli svarīgās intereses (dzīvību un veselību), slimnīcai ir tiesisks pamats piekļūt personas slimības vēsturei.

- **Pārziņa vai trešās personas leģitīmo interešu ievērošana.**

Šāds personas datu apstrādes pamats ir pieļaujams tikai tad, ja tādējādi netiek būtiski ietekmētas personas, kuras dati tiek apstrādāti, intereses, pamattiesības un pamatbrīvības jo īpaši, ja datu subjekts ir bērns.

Šo apakšpunktu nepiemēro apstrādei, ko veic publiskas iestādes, pildot savus uzdevumus.

Uzņēmums/organizācija uzrauga, kā tā darbinieki lieto informācijas tehnoloģiju ierīces, lai aizsargātu uzņēmuma iekšējā tīkla drošību.

Uzņēmums/organizācija veic videonovērošanu darba vietā, lai novērstu noziedzīgus nodarījumus pret īpašumu un personu veselību un dzīvību.

Novērtējums, vai uzņēmuma/organizācijas leģitīmās intereses ir svarīgākas par attiecīgās personas, kuras dati tiek apstrādāti, interesēm, ir atkarīgs no situācijas un apstākļiem. Piemēros minētajos gadījumos personas datu apstrāde būtu pieļaujama tikai tad, ja tā uzskatāma par vismazāk ierobežojošo metodi attiecībā uz datu subjektu privātumu.

Ar trešās personas leģitīmo interešu ievērošanu būtu jāsaprot ne tikai konkrētas un identificējamas trešās personas, bet arī personu loks vai sabiedrība kopumā.

Sniedzam nelielu ieskatu par Regulas 6. panta 1. punkta "f" apakšpunktu – **pārziņa vai trešās personas leģitīmo interešu ievērošanas** tiesiskā pamata lietošanu praksē.


KĀDS IR DATU APSTRĀDES TIESISKAIS PAMATS TAVĀ UZŅĒMUMĀ?
Pārziņa vai trešās personas leģitīmo interešu ievērošana
Piekrišana
Līguma izpilde
Juridisks pienākums
Sabiedrības intereses
Vitālo interešu aizsardzība

Kādos gadījumos leģitīmas intereses var būt tiesiskais pamats?

- Ja nepieciešama datu izmantošana tiesvedībā
- Klientu apmierinātības aptauja
- Uzņēmuma sniegtā pakalpojuma atspoguļojums reklāmas nolūkos
- Loterijas organizēšana, lai popularizētu uzņēmuma pakalpojumus un preces
- Krāpšanas risku novēršana
- Drošība/ īpašumu aizsardzība
- Pierādījumu nodrošināšana
- Sadarbības partneru kontaktpersonu datu apstrāde

Pamatsoļi, lai samērīgi izvērtētu uzņēmuma leģitīmās intereses:

1. **Iespējamā tiesiskā pamata izvēle**
2. **Pārziņa intereses likumības un būtiskuma izvērtējums:**

- Vai tā nav aizliegta/ ir atļauta tiesību aktos?
- Vai interese ir pietiekami konkrēta?

- Vai interese ir pašreizēja un reāla?
- Kādas būtu sekas, ja datu apstrāde netiktu veikta?

3. **Alternatīvu apstrādes veidu identificēšana un izvērtēšana.**
4. **Papildu pasākumi:**

- Vai ir iespējams piešķirt atteikšanās tiesības datu subjektiem?
- Vai ir iespējams nodrošināt pseidonimizāciju?
- Kā tiks nodrošināta datu subjektu informēšana?
- Glabāšanas termiņu noteikšana.
- Izvērtēt, vai nav nepieciešams novērtējums par ietekmi uz datu aizsardzību.
- Vai ir paredzēta rīcība datu subjekta iebildumu saņemšanas gadījumā?

5. **Gala lēmums.**

Regula noteic, ka datu apstrāde ir likumīga, ja tai ir piemērojams vismaz viens tiesiskais pamats datu subjekta datu apstrādei. Līdz ar to, katrā personas datu apstrādes posmā ir jābūt noteiktam datu apstrādes tiesiskajam pamatojumam, kas datu apstrādes dzīvescikla laikā var mainīties (piemēram, sākotnēji personas datu apstrāde tika veikta, lai nodrošinātu līgumsaistību izpildi, pēc tam – lai nodrošinātu juridisku pienākumu, ko uzliek normatīvie akti).

Ja apstrādā datus par sodāmību, iepazīsties ar Regulas 10. pantu. Personas datu par sodāmību apstrādei papildus jau minētajiem tiesiskiem pamatiem jāņem vērā arī Regulas 10. pantā noteiktais.

"Likumīgums, godprātība un pārredzamība" ir drošas personas datu apstrādes pamatā.

IZVĒRTĒ

Vai esi apsvēris riskus personas datu drošībai?

Tu labi zini, ka uzņēmējdarbība ir saistīta ar pastāvīgu risku novērtēšanu, lai cik labi nebūtu veikta tirgus un uzņēmējdarbības vides izpēte, briesmu, neveiksmju vai zaudējumu iespējamība ir jāņem vērā, pieņemot jebkuru lēmumu, kas saistīts ar uzņēmējdarbību.

Datu aizsardzība nav izņēmums, tādēļ veicot vai plānojot veikt personas datu apstrādi, ir jāņem vērā iespējamie riski. Vispārīgos gadījumos iespējamo apdraudējumu novērtējums izriet no veselā saprāta – neviens nevēlas, lai informācija, kas domāta paša uzņēmuma vajadzībām nonāktu pie konkurenta (pat ja runājam par parastu klientu sarakstu). Regulā ir noteikti arī gadījumi, kad riska novērtējuma veikšana ir Tavs pienākums. Novērtējums par ietekmi uz datu aizsardzību veicams katrā gadījumā, kad personas datu apstrāde var radīt augstu risku datu subjekta tiesībām un brīvībām, bet jo īpaši, ja:

a) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;

b) Regulas 9. panta 1. punktā minēto īpašo kategoriju datu vai Regulas 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā; vai

c) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.

Regula noteic, ka uzraudzības iestāde (Latvijā – DVI) izstrādā un publisko sarakstu ar tiem apstrādes darbību veidiem, attiecībā uz kuriem obligāti ir jāveic novērtējums par ietekmi uz datu aizsardzību (turpmāk – NIDA). Tas nozīmē, ka, veicot apstrādi vai plānojot veikt apstrādi, kas atbilst DVI publicētajā sarakstā minētajai, obligāti ir veicams NIDA. Šāds saraksts ir publiskots DVI

mājaslapā un par "novērtējumu par ietekmi uz datu aizsardzību" vairāk izlasīsi *https://www.dvi.gov.lv/lv/datu-aizsardziba/organizacijam/ieteikumi/*.

Ņemot vērā, ka apzināt iespējamos riskus plānotajai personas datu apstrādei ir Tavs pienākums, Tev varētu noderēt izpratne par kritērijiem, no kuriem vismaz diviem sakrītot, ir veicams NIDA.

Kritēriju saraksts ir izveidots, pamatojoties uz 29. panta darba grupas vadlīnijām DG248 "Par Novērtējumu par ietekmi uz datu aizsardzību (NIDA un Regulas 2016/679 vadlīnijām (2017. gada 4. oktobris)" un palīdz noteikt tos apstrādes darbības veidus, kas "var radīt augstu risku fizisku personu tiesībām un brīvībām".

Uzņēmumam ir klientu datu bāze un darbinieku datu bāze, tās abas atrodas vienas programmas sistēmas dažādos piekļuves līmeņos. Apkalpojot klientus, darbinieki kļūdas pēc atver darbinieku datu bāzi. Viņi apskatās algu sarakstus, izprintē tos un sākas apspriešanās visā uzņēmumā par to, kāpēc vienam vai otram lielāka alga nekā citiem. Tātad uzņēmums nav nodrošinājis, ka piekļuve darbinieku datu bāzei ir tikai tām personām, kam tas ir nepieciešams, lai pildītu savus darba pienākumus.

Kritēriji

1. Novērtēšana vai vērtēšana, tostarp profilēšana un prognozēšana, jo īpaši, lai analizētu aspektus saistībā ar datu subjekta sniegumu darbā, ekonomisko stāvokli, veselību, personīgajām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos.
2. Automatizēta lēmumu pieņemšana, kuru pamato ar juridisku vai līdzīgu būtisku ietekmi: apstrāde, kuras rezultātā tiek pieņemti lēmumi par datu subjektiem, kas rada "juridiskas sekas attiecībā uz fizisko personu" vai kas "līdzīgi būtiski ietekmē fizisko personu."
3. Sistemātiska uzraudzība: piemēro, lai novērotu, uzraudzītu vai kontrolētu datu subjektus, tostarp datus, kas iegūti tīmeklī vai "publiski pieejamas zonas sistemātiskas uzraudzības" rezultātā.
4. Sensitīvi dati vai ļoti personiska rakstura dati: attiecas uz īpašas kategorijas personu datiem, kā tas noteikts Regulas 9. pantā (piem., informācija par personas politiskajiem uzskatiem), kā arī uz personas datiem saistībā ar sodāmību vai noziedzīgiem nodarījumiem saskaņā ar VDAR 10. pantā noteikto.
5. Datu apstrāde plašā mērogā: Regulā nav norādīta plaša mēroga apstrādes definīcija, taču Regulas 91. apsvērumā ir dotas dažas norādes. Lai identificētu personas datu apstrādi, kas notiek plašā mērogā, 29. panta darba grupa iesaka ņemt vērā šādus faktorus:
   a) datu subjektu skaits tiek identificēts kā konkrēta skaitliska vienība vai proporcionāla daļa no iedzīvotāju kopējā skaita;
   b) datu apjoms un/vai dažādu veidu apstrādāto datu vienumu klāsts;
   c) datu apstrādes darbības ilgums vai pastāvīgums;
   d) apstrādes darbības teritoriālais tvērums;
6. Datu kopu saskaņošana vai apvienošana.
7. Datu apstrāde attiecībā uz īpaši aizsargājamiem datu subjektiem.
8. Inovatīva jaunu tehnoloģiju vai risinājumu izmantošana vai to pielietošana.
9. Ja apstrāde pati par sevi "liedz datu subjektiem īstenot tiesības vai izmantot pakalpojumu vai līgumu."

Pārzinim pirms datu apstrādes visos gadījumos ir jāņem vērā apstrādes raksturs, apjoms, konteksts un

mērķis, kā arī tas, vai pastāv iespējamība, ka apstrāde radīs lielu risku fizisko personu tiesībām un brīvībām saskaņā ar Regulu, un jāveic NIDA, ja pārzinis uzskata, ka datu apstrāde var radīt lielu risku fizisko personu brīvībām un tiesībām.

Vispārīgos personas datu apstrādes gadījumos Tavs pienākums ir noskaidrot, kādi riski ir saistīti ar personas datu apstrādi Tavā uzņēmumā. Regula paredz, ka izvērtējot riskus, papildus tiešajiem riskiem savai uzņēmējdarbībai, Tev jāpārdomā savu klientu, darbinieku (datu subjektu) interešu nodrošināšana.

- Rūpīgi izvērtē iekšējos procesus, darbības ar personu datiem, un nosaki, vai šajos procesos ir iespējams datu aizsardzības pārkāpums un, ja iespējams, cik lielas nepatikšanas tas var sagādāt datu subjektam.
- Izvērtē, kuriem no Tava uzņēmuma darbiniekiem ir piekļuve personu datiem, izvērtē piekļuves nepieciešamību, apmāci darbiniekus rīkoties ar personas datiem, ievērojot datu aizsardzības principus.
- Pārliecinies, kā uzņēmuma iekšienē notiek datu apmaiņa, apsver vai pašreizējie apmaiņas mehānismi ir uzskatāmi par drošiem.
- Ņem vērā datu atrašanās vietu un piekļuvi tiem, kā dati tiek transportēti – datorā, mapēs, fiziskā veidā (piemēram, analīzes) utt.
- Ievies savu datu aizsardzības sistēmu un noteikumus, ņemot vērā iespējamos riskus datu apstrādes un aizsardzības procesā (piemēram, nesankcionēta piekļuve, dzēšana, u.c.)

Iepriekšminētos apstrādes aspektus Tev palīdzēs novērtēt arī šādi jautājumi:

- Vai Tavas datu sistēmas aizsardzība atbilst tajā apstrādāto datu radītajam riskam?
- Vai Tavs uzņēmums ir sagrupējis apstrādātos personas datus, ņemot vērā to radīto apdraudējumu un lielāku risku radošus datus aizsargā rūpīgāk?
- Kādas ierīces ir savienotas vietējā tīklā (vai pašas ierīces un to savienojumi nerada drošības apdraudējumus, kā tas ticis novērsts)?
- Vai zini, kāda programmatūra tiek izmantota Tava uzņēmuma informācijas sistēmās?
- Vai datori ir aprīkoti ar drošības sistēmām, kaut vai parolēm?
- Vai Tu reģistrē darbinieku piekļuvi konfidenciālai informācijai?
- Vai Tavi darbinieki saprot savu lomu organizācijas aizsardzībā pret informācijas drošības draudiem?
- Vai esi apsvēris ko vēl varētu darīt augstāku drošības standartu sasniegšanā?

Tu izlem klientu identificējošo informāciju, ziņas par pasūtījumiem un finanšu informāciju glabāt kartona kastē - koridorā. Uzkopjot telpas, informāciju par klientiem ieguva apkopējs, kurš iegūtos datus izmantoja, lai klienta vārdā nopirktu sev greznu maltīti. Apkopējam atkarībā no nodarītajiem zaudējumiem var piemērot krimināltiesību. Savukārt, Tev sodu var piemērot DVI, jo neesi ieviesis saprātīgus drošības pasākumus, ņemot vērā personas datu apstrādei atbilstīgos riskus.

NOSAKI LOMU

Kāda ir Tava uzņēmuma, partneru un darbinieku loma datu apstrādē?

Ja MVU ir datu pārzinis, tad tas nosaka datu apstrādes mērķi un apjomu pats, atbilstoši savām uzņēmuma vajadzībām. Ja MVU ir datu apstrādātājs, tad tas saņem datu apstrādes norādījumus (Regulas 28. pants) no pārziņa, kā vārdā dati tiek apstrādāti.

Kas ir **datu pārzinis**?

Tu esi nolēmis pieņemt darbā jaunus darbiniekus – sekretāru un grāmatvedi. Lai pieņemtu darbā šos jaunos darbiniekus, Tu nolem slēgt ar viņiem līgumus. Līdz ar to Tu iegūsti personas datus līgumu slēgšanai. Šajā gadījumā Tu esi pārzinis, jo Tu esi noteicis personas datu iegūšanas nolūku.

Atbilstoši Regulai datu pārzinis iniciē, izsaka vēlmi veikt vienu vai otru datu apstrādi, sasniegt kādu mērķi.

Interneta veikalā klienti katru dienu veic pasūtījumus ar piegādi mājās. Visi pasūtījumi tiek iepakoti un kopā ar piegādi apliecinošiem dokumentiem nodoti licenzētai kurjerpakalpojumu kompānijai. Šajā piemērā kurjera pakalpojumu kompānija arī ir datu pārzinis un atbilstoši Regulas noteikumiem patstāvīgi organizē savu pārziņa pienākumu izpildi.

Kas ir **kopīgi pārziņi**?

Pārzinis var noteikt mērķus un apstrādes līdzekļus arī kopā ar citiem pārziņiem. Regulas 26. panta 1. punkts noteic, ka, ja divi vai vairāki pārziņi kopīgi nosaka apstrādes mērķus un veidus, tie ir kopīgi pārziņi.

Datu pārzinis datus apstrādā pats vai kopā ar citiem pārziņiem, tomēr var būt situācijas, kad nepieciešams izmantot ārpakalpojumu – datu apstrādātāju.

Kas ir **datu apstrādātājs**?

Datu apstrādātājs apstrādā personas datus pārziņa vārdā un uzdevumā. **Datu pārzinis** apstrādātājam nosaka:

- kā vākt, apstrādāt un glabāt personas datus,
- kādus tieši personas datus vākt,
- kā datus sistematizēt,
- kāds ir datu izmantošanas nolūks,
- datu glabāšanas termiņu u.c., kas nepieciešams pārziņa noteikto mērķu sasniegšanai.

Kamēr apstrādātājs ievēro pārziņa dotos norādījumus, tikmēr par apstrādi pilnu atbildību uzņemas pārzinis. Brīdī, kad apstrādātājs apzināti vai neapzināti izlemj pārkāpt pārziņa dotos rakstveida norādījumus, apstrādātājs pats kļūst par pārzini un uzņemas pilnu atbildību, kādu Regula ir paredzējusi pārzinim, tajā skaitā soda naudas maksāšanu par izdarītajiem pārkāpumiem. Protams, tas neatbrīvo no atbildības sākotnējo pārzini, ja tas nebūs rīkojies kā rūpīgs saimnieks un vieglprātīgi attiecies pret apstrādātājam dotajiem uzdevumiem un to apjomu.

Informāciju tehnoloģiju laikmetā gandrīz vienmēr uzņēmumi (datu pārziņi) kādu personas datu apstrādes daļu nodod vai nu citam datu pārzinim vai datu apstrādātājam. Tev, kā datu pārzinim, jānodrošina, lai sadarbības partneris un tā sadarbības partneri (apakšuzņēmēji), kas palīdz izpildīt noslēgto līgumu, zinātu par savām saistībām attiecībā uz Regulu. Savukārt datu apstrādātājam vienmēr jārīkojas savas atbildības robežās.

Tavs uzņēmums ar uzņēmumu X noslēdz līgumu par datubāzes uzturēšanu. Datubāzē uzņēmums X glabā klientu personas datus. Jūsu savstarpēji noslēgtais līgums noteic, ka Tavam uzņēmumam ir jāuztur datubāze un pēc uzņēmuma X sniegtās informācijas jāaktualizē datubāzē esošā informācija. Tavs uzņēmums šajā gadījumā ir datu apstrādātājs, kurš apstrādā personas datus tikai tādā apjomā, kā to noteicis uzņēmums X – uztur datubāzi un aktualizē informāciju.

Apstrādi, ko veic apstrādātājs, reglamentē ar līgumu vai citu juridisku aktu saskaņā ar ES vai dalībvalsts tiesību aktiem, kas ir saistošs apstrādātājam un pārzinim un kurā norāda:

- līguma priekšmetu;
- apstrādes raksturu un nolūku;
- personas datu veidu kategorijas;
- datu subjektu kategorijas;
- pārziņa pienākumus un tiesības.

Kas ir **apakšapstrādātājs**?

Apstrādātājs var vēlēties slēgt apakšuzņēmuma līgumus ar citiem apstrādātājiem. To sauc par "apakšapstrādātāja" piesaisti, lai gan šis termins nav tieši ietverts Regulā.

Apstrādātājs bez iepriekšējas konkrētas vai vispārējas rakstiskas pārziņa atļaujas nepiesaista citu apstrādātāju. (Regulas 28. panta 2. punkts)

Vispārējas rakstiskas atļaujas gadījumā apstrādātājs informē pārzini par jebkādām iecerētām pārmaiņām saistībā ar papildu apstrādātāju vai apstrādātāja aizstāšanu, tādējādi sniedzot pārzinim iespēju iebilst pret šādām izmaiņām.

Kas ir **trešā persona**?

Trešā persona ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus.

Uzņēmums X darbojas ar pašgatavotu vaska sveču tirdzniecību.

Uzņēmums X veic darījumu uzskaiti un saviem klientiem izsniedz darījumu apliecinošu dokumentu – kvīti.

Normatīvie akti paredz, ka kvītī jānorāda konkrēti personas dati – vārds, uzvārds, personas identifikācijas numurs. Šo informāciju uzņēmums X normatīvajos aktos noteiktajā kārtībā nodod Valsts ieņēmumu dienestam, kas nodošanas brīdī ir trešā persona.

PĀRSKATI

Kāda ir dokumentu reģistrēšanas kārtība un nomenklatūra Tavā uzņēmumā?

Pārbaudi sevi:

- Sāc ar to, ka noskaidro, kā Tavā uzņēmumā tiek saņemta un reģistrēta informācija.
- Kādas ir lietvedības sistēmas Tavā uzņēmumā?
- Uz kādiem serveriem atrodas datu sistēma?
- Vai piekļuves tiesības ir dalītas, vai katrs izmanto savu paroli?
- Vai ir zināms, kurš darbinieks datus ievadījis, labojis un dzēsis?
- Pārbaudi, cik operatīvi dati pēc aktīvās lietošanas tiek arhivēti un, attiecīgi pēc glabāšanas laika beigām, dzēsti (atbilstoši nomenklatūrai).
- Pārbaudi, vai tiešām dati tiek dzēsti vai paliek datora logfailos.
- Pārbaudi uzņēmuma līgumus un arhīvu.
- Pārbaudi, cik bieži dati tiek dzēsti. Regula pieprasa datu dzēšanu nekavējoties pēc to apstrādes pabeigšanas. Vai uzņēmuma sistēmas to pieļauj?

Atceries, ka datu apjomam, veidam, to kopumam un glabāšanas mērķim ir nepieciešams tiesisks pamats. (Regulas 6. panta 1. punkts un 9. pants)

Drošas datu sistēmas izveidošana pasargās Tavu darbinieku un klientu personas datus, neļaus tiem noplūst vai nokļūt citu – nepiederošu personu rokās un dos iespēju izvairīties no iekšējiem konfliktiem.

Nosaki, kura sistēma vairāk jāsargā: izvērtē riskus, kurā sistēmas daļā ir vairāk konfidenciālo datu.

Nemētā nesistematizētus datus pa galdu papīra formātā (piemēram) vai darba mapē uz darba datora ekrāna. Nodrošini, lai tiktu ievērots tīrā galda princips. Pievieno sistēmai. Kartotēkā sakārtotos datus turi drošā vietā, piemēram, seifā.

Darbinieku dati parasti atrodas pie uzņēmuma vadītāja, grāmatveža, personāla vadītāja, dažos gadījumos arī pie biroja vai ražošanas vadītāja.

Nosaki konkrētu personu datu glabāšanas veidu datu sistēmā, izveido pielaides (paroles, kodus) un sadali piekļuves līmeņus personāla datiem pēc nepieciešamības.

Katrs uzņēmums pats nosaka datu dzēšanas kārtību un noteikumus, balstoties uz datu glabāšanas pamatojumu un iekšējās kārtības noteikumiem (nomenklatūru).

Ikvienai personai ir tiesības vērsties uzņēmumā vai iestādē, kas apstrādā personas datus, un lūgt izdzēst savus datus, ja:

- dati vairs nav nepieciešami mērķim, kuram tie tika iegūti;
- datu apstrāde notiek, pamatojoties uz indivīda piekrišanu, un viņš atsauc piekrišanu;
- personas dati ir apstrādāti nelikumīgi;
- dzēšana ir nepieciešama, lai izpildītu juridiskas saistības;
- personas dati attiecas uz bērniem, un tie ir savākti saistībā ar bērnu, izveidojot profilu sociālajā tīklā.

Ja dati tiek dzēsti pēc personas pieprasījuma, uzņēmumam vai iestādei par dzēšanu jāinformē arī tie, kuriem dati tika nodoti.

Vai zini, kā noformēt datu subjekta piekrišanu viņa personas datu apstrādei?

Regulas izpratnē datu subjekta "piekrišana" ir jebkura **brīvi sniegta, konkrēta, apzināta un viennozīmīga** norāde uz datu subjekta vēlmēm, ar kuru viņš **paziņojuma vai skaidri apstiprinošas darbības veidā** sniedz piekrišanu savu personas datu apstrādei. Regula paredz vairākus nosacījumus, lai saņemtā piekrišana tiktu uzskatīta par spēkā esošu.

Brīvi sniegta piekrišana

Piekrišana nav uzskatāma par brīvi sniegtu, ja personai nav īstas vai brīvas izvēles, tā nevar atteikties vai atsaukt savu izvēli bez nelabvēlīgām sekām.

Konkrēta piekrišana

Piekrišanai ir jābūt sniegtai attiecībā uz noteiktu, konkrētu personas datu apstrādes mērķi. Ja no datu subjekta tiek iegūta vispārīga piekrišana apstrādāt personas datus, neizdalot, kādi ir šīs apstrādes mērķi, šādu piekrišanu nevar uzskatīt par konkrētu. Papildu nosacījums konkrētai piekrišanai – tai jābūt saprotamai datu subjektam.

Apzināta piekrišana

Apzinātas piekrišanas nosacījums pārklājas ar nosacījumu piekrišanai būt konkrētai. Lai piekrišana tiktu uzskatīta par likumīgu, datu subjektam ir jābūt informētam par to, kā viņa personas dati tiks izmantoti un kādas varētu būt piekrišanas personas datu apstrādei sekas. Lai datu subjekts varētu pieņemt izvērtētu un apzinātu lēmumu sniegt vai nesniegt piekrišanu savu personas datu apstrādei, jānodrošina pieeja vismaz Regulas 13. pantā norādītajai informācijai.

Piekrišanas pieprasījumā ir jānorāda vismaz šāda informācija par personas datu apstrādi:

1. datu apstrādes veicēja identitāte un kontaktinformācija;
2. attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija;
3. datu apstrādes nolūki;
4. apstrādājamo datu veids;
5. pārziņa vai trešās personas leģitīmās intereses, ja apstrāde pamatojas uz Regulas 6. panta 1. punkta "f" apakšpunktu;
6. personas datu saņēmēji vai saņēmēju kategorijas, ja tādi ir;
7. datu subjekta tiesības atsaukt piekrišanu (piemēram, nosūtot e-pasta ziņojumu, lai atsauktu piekrišanu);
8. informācija par to, vai dati tiks izmantoti vienīgi automatizētā lēmumu pieņemšanā, tostarp profilēšanā;
9. informācija par to, vai piekrišana ir saistīta ar personas datu pārrobežu nosūtīšanu – iespējamie riski, veicot datu pārsūtīšanu uz valstīm ārpus ES, ja uz minētajām valstīm neattiecas Komisijas lēmums par aizsardzības līmeņa pietiekamību un nepastāv atbilstošas garantijas u.c.

Ievēro! Regula noteic, ka pārzinim personas datu iegūšanas laikā datu subjektam ir jāsniedz ne tikai iepriekš minētā informācija, bet gan arī šāda papildu informāciju, kas vajadzīga, lai nodrošinātu godprātīgu un pārredzamu apstrādi:

a) laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai;

b) tas, ka pastāv tiesības pieprasīt pārzinim 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;

c) ja apstrāde pamatojas uz Regulas 6. panta 1. punkta "a" apakšpunktu vai 9. panta 2. punkta "a" apakšpunktu (datu subjekta piekrišana) – tiesības jebkurā

brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana;

d) tiesības iesniegt sūdzību uzraudzības iestādei;

e) 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;

f) tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta Regulas 22. panta 1. un 4. punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

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

Viennozīmīga piekrišana

Piekrišana nevar tikt veidota tā, ka to iespējams interpretēt dažādos veidos, radot pārpratumus par to, kādam tieši nolūkam datu subjekts ir devis savu piekrišanu. Tādējādi viennozīmīga piekrišana nozīmē, ka tā ir skaidra datu subjekta norāde, ka viņš piekrīt, ka attiecīgus viņa personas datus apstrādās konkrēts pārzinis konkrētiem mērķiem.

Paziņojuma vai skaidri apstiprinošas darbības forma

Piekrišana var būt izteikta gan rakstiski, gan mutiski, kā arī tā var būt netieši izteikta, interpretējot to no personas rīcības, kas norāda uz tās vēlmi sniegt piekrišanu datu pārzinim, ja likumā nav noteikts citādi. Regula neizslēdz iespēju, ka piekrišana var tikt sniegta elektroniski, piemēram, veicot tehnisko iestatījumu izvēli, atzīmējot piekrišanu atsevišķā lodziņā. Piekrišanai ir jābūt aktīvai darbībai (piemēram, elektronisks izvēles logs, kurš personai ir nepārprotami jāatzīmē, ka tā piekrīt, vai paraksts uz veidlapas). Piekrišana nevar tikt iegūta, ja elektroniskā pieteikuma formā izvēles lodziņu, kas paredzēts, lai atzīmētu piekrišanu personas datu apstrādei, sistēma aizpilda pēc noklusējuma.

Pierādāma, saprotama, atsaucama

Pārzinim, uzsākot personas datu apstrādi uz piekrišanas pamata, ir jāņem vērā vēl citi nosacījumi, kas uzskaitīti Regulas 7. pantā:

- **piekrišanu jāspēj uzskatāmi pierādīt;**
- **tai jābūt viegli saprotamai un skaidri nošķiramai no citiem jautājumiem;**
- **piekrišanu var atsaukt jebkurā laikā.**

Es, Vārds Uzvārds, piekrītu, ka SIA «XXXs» (reģ.nr. XX; adrese: XX iela; XX@XX.lv) veiks manu personas datu apstrādi komerciālu paziņojumu saņemšanai saskaņā ar man sniegto un SIA «XXXs» privātuma politikā (www.XX.lv/privatums) iekļauto informāciju par komercpaziņojumu nosūtīšanu.

Paraksts _____ / V.Uzvārds /

Datums, laiks

Šāda veida piekrišana būs derīga tikai gadījumā, ja privātuma politikā ir sniegta visa Regulas 13. pantā minētā informācija un ir nodrošināts, ka privātuma politika ir pieejama piekrišanas sniegšanas laikā!

NODROŠINI

Datu subjekta informēšana par personas datu vākšanu, glabāšanu un dzēšanu

Personai ir tiesības saņemt skaidru un saprotamu informāciju par to, kas apstrādā viņas datus, kādi dati tiek apstrādāti, kāds ir apstrādes mērķis, tiesiskais pamats, un citu informāciju skaidrā un saprotamā valodā.

Tas nozīmē, ka uzņēmumam brīdī, kad tas iegūst personas datus, ir kodolīgā, pārredzamā un saprotamā veidā, izmantojot vienkāršu valodu, jāsniedz Regulas 13.–14. pantā norādītā informācija.

Ja teritorijā tiek veikta videonovērošana, redzamā vietā jāizvieto informācija, kas, kādiem nolūkiem, uz kāda pamata veic datu apstrādi. Tomēr jāņem vērā, ka visu minēto informāciju sniegt informējošā uzlīmē ne tikai nav iespējams, bet tādējādi netiktu izpildīta Regulas prasība – sniegt informāciju pārskatāmi, vienkārši, saprotami. Tāpēc, tāpat kā līdz šim, ar informatīvās uzlīmes palīdzību var sniegt tikai būtiskāko informāciju (ziņas par pārzini, kontaktinformāciju, datu subjekta tiesības un datu apstrādes mērķi), norādot vietu, kur persona nepieciešamības gadījumā var atrast papildu informāciju (piem., uzņēmuma mājaslapā, sekretariātā). Viens no vienkāršākajiem veidiem, kā nodrošināt papildu informācijas sniegšanu, ir QR kods (Quick Response Code).

Izplatīts veids, kā sniegt datu subjektam Regulas 13.–14. pantā noteikto informāciju, ir privātuma politika.

Pārliecinies, ka Tava uzņēmuma privātuma politika ir aktuāla un satur informāciju, cik ilgi dati tiek glabāti, kāds ir to vākšanas iemesls, kam ir pieeja datiem, datu pārsūtīšanas politiku, pārskatu par tiesībām pieprasīt datus, atsaukt piekrišanu, iesniegt sūdzību, un vai ir norādīta aktuāla datu aizsardzības speciālista vai pārziņa kontaktinformācija.

Regulāri pārliecinies, vai politika ir redzamā vietā, brīvi pieejama Jūsu uzņēmumā – piemēram, pie ziņojuma dēļa klientiem vai uzņēmuma tīmekļa vietnē, lai Tu varētu viegli uz to atsaukties.

Nodrošini, ka esi noteicis datu apstrādes tiesisko pamatu, neatkarīgi no tā, vai tā ir piekrišana vai cits tiesiskais pamats, un vai Tev ir dokumentācija, kas pierāda tiesiskā pamata esamību.

Nodrošini, ka ir noteikta kārtība kā dzēst personas datus un visi sadarbības partneri – gan pārziņi, gan apstrādātāji – apliecina gatavību to ievērot.

Nodrošini, ka sadarbībā ar partneriem arī tiek ievērotas Regulas prasības. Izglīto darbiniekus par to, kas ir Regula un kā tā ietekmē personas datu apstrādi, un kas tiek uzskatīts par personas datu aizsardzības pārkāpumu.

Nodrošini, ka Tavā uzņēmumā ir skaidra politika, noteikumi un instrukcijas par personas datu aizsardzības jautājumiem.

Izstrādā kārtību kā dokumentēt, ziņot un pārvaldīt personas datu aizsardzības pārkāpumus.

Regulāri seko procesiem uzņēmumā, un izmaiņu gadījumā pārbaudi, vai privātuma politikā ir ietverta visa nepieciešamā informācija.

Regulāri pārskati arī privātuma politikas un līdzīgu informāciju, ko sniedz datu subjektiem.

Regulāri pārliecinies un dokumentē, vai ir tiesisks pamats personas datu apstrādei.

Regulāri pārbaudi, vai esošās IT sistēmas nodrošina Tev iespēju ievērot Regulas prasības.

IT sistēmas jāprojektē tā, lai tās varētu **nodrošināt personas datu aizsardzību, ko nosaka Regula.**

Drošības aspekti, kuriem IT sistēmai būtu jāatbilst, ir:

- Drošu paroļu un šifrēšanas izmantošana, tostarp, regularitāte paroļu un pieejas tiesību aktualizēšanā.
- Piekļuves atļauja personas datiem tikai tiem darbiniekiem, kam tas nepieciešams sava darba veikšanai.
- Atbilstoša autentifikācija, autorizējoties sistēmā pirms personas datu apstrādes uzsākšanas.
- Auditācijas pierakstu uzturēšana par lietotāju sistēmā veiktajām darbībām.
- Personas datu aizsardzība, tos nosūtot vai saglabājot (piemēram, šifrēšana).
- Pazaudētas vai nozagtas ierīces attālināta bloķēšana.

Vai esi domājis par to, kā varēsi apliecināt uzraudzības iestādei (DVI), ka ievēro Regulu?

Pārskatatbildība

Regula noteic, ka uzņēmumam ir jāspēj uzskatāmi parādīt un pierādīt kā uzņēmumā tiek apstrādāti personas dati. Regula to sauc par pārskatatbildību (Regulas 5. panta 2. punkts).

DVI uzrauga datu aizsardzības procesu ieviešanu un īstenošanu, lai visi datu aizsardzības, uzraudzības procesi tiktu īstenoti atbilstoši Latvijas un ES regulējumam.

Kādiem dokumentiem ir jābūt uzņēmuma rīcībā?

Normatīvie akti nenoteic konkrētus dokumentu veidus, kuriem jābūt uzņēmumā, taču te ir sniegti daži ieteikumi, kas var noderēt informācijas sistematizēšanai un procesu pārskatāmības nodrošināšanai. Kādus dokumentus un vai vispār tos izstrādāt uzņēmumā, ir atkarīgs gan no uzņēmuma specifikas, gan lietderības.

Tomēr, ņemot vērā Regulā noteikto pienākumu atsevišķos gadījumos veikt NIDA, uzturēt apstrādes darbību reģistru, kā arī dokumentēt personas datu aizsardzības pārkāpumus, uzņēmumā ir jābūt dokumentiem, kas apliecina, ka ir izpildīts minētais pienākums. Citos gadījumos, kā jau minēts iepriekš, NIDA un apstrādes darbību reģistrs izmantojams kā paškontroles rīks. Pārskatatbildības nodrošināšanai ieteicams saglabāt arī dokumentus, kas apliecinātu, ka atsevišķu pienākumu izpildi apsvēri, bet to vai citu apsvērumu dēļ izlēmi nepildīt (piemēram, attiecībā uz NIDA veikšanu), šādas dokumentācijas saglabāšana ļaus Tev labāk atcerēties kāpēc pieņēmi tieši šādu lēmumu un demonstrēs, ka jautājumu tomēr apsvēri.

Dokumentu veidi, kas var būt obligāti:

1. NIDA.
2. Apstrādes darbību reģistrs.
3. Personas datu aizsardzības pārkāpumu uzskaites reģistrs.
4. Privātuma politika.

Dokumenti, kas var palīdzēt nodrošināt pārskatatbildību:

- Datu plūsmas diagramma, kurā Jūs paši priekš sevis pārskatāmi esat uzzīmējuši, aprakstījuši kādi dati, kādā veidā tiek apstrādāti uzņēmumā un ārpus tā.
- IT sistēmu un to drošības apraksts – kādas sistēmas tiek izmantotas, kādas tām ir aizsardzības.

- Atbildīgo par personas datu aizsardzību uzņēmumā noteikšana (rīkojums, pienākumi amata aprakstā, darba līgumā u.tml.).
- Personas datu vākšanas, glabāšanas, aprites un dzēšanas kārtības apraksts.
- Dokumenti, kas apliecina darbinieku instruktāžu, apmācības par datu apstrādi, konfidencialitāti.
- Rīcības plāns personas datu aizsardzības pārkāpuma gadījumā, lai nav jādomā kā rīkoties, ja ir noticis pārkāpums u.c.

Raugies, lai būtu ieviesti organizatoriskie pasākumi, kas ļauj pārraudzīt personas datu aizsardzības sistēmas esamību un piemērošanu ikdienas saimnieciskajā darbībā, pārzini dokumentāciju, kas pierāda, ka tiek ievērota Regula vai vismaz to, ka Tavs uzņēmums ir ceļā uz Regulas prasību ieviešanu un Regulas ievērošanu.

Kā Tavā uzņēmumā tiek informēti un apmācīti darbinieki ievērot Regulas prasības? Vai darbinieki zina savus pienākumus?

Informē un izglīto savus darbiniekus!

Lai veiksmīgi izprastu Regulas mērķi un nozīmi, vispirms pats, kā MVU vadītājs, vai par personas datu apstrādi atbildīgais darbinieks Tavā uzņēmumā, iegūsti pamatzināšanas par Regulu, izstudējot Regulu, apmeklējot kursus vai DVI organizētos seminārus.

Apmāci savus darbiniekus rīkoties uzmanīgi, apstrādājot personas datus. Par datu apstrādes drošības kultūru uzņēmumā ir jāzina pilnīgi visiem (tajā skaitā vadītājam). Tieši klientu apkalpošanas speciālistiem būtu jābūt zinošākajiem ko drīkst un ko

nedrīkst izpaust, kādus datus drīkst pieprasīt un kā tos glabāt.

Noteikti nosaki, kurš uzņēmumā ir atbildīgs par personas datu drošību. Atceries, ka pārzinis ir atbildīgs par Regulai atbilstošu personas datu apstrādi, tāpēc viņam ir tiesības noteikt, vai par personas datu apstrādi atbildīgs būs viens vai vairāki darbinieki, vai varbūt tiks sadalītas atbildības sfēras, piemēram, atbildīgais par personas datu aizsardzību grāmatvedībā un personālvadībā.

Tomēr pats galvenais – atceries, ka nevajag ar citu datiem darīt ko tādu, ko negribētu, lai dara ar Taviem datiem.

Vai Tavā uzņēmumā ir datu aizsardzības speciālists, vai plāno tādu piesaistīt, vai plāno sakārtot savu uzņēmumu atbilstoši Regulas prasībām pašu spēkiem?

Personas datu aizsardzības speciālists palīdzēs nodrošināt un uzraudzīs, vai tiek ievēroti Regulas nosacījumi personas datu apstrādē un aizsardzībā.

Datu aizsardzības speciālista piesaiste ir obligāta šādos gadījumos:

- apstrādi veic publiska iestāde vai struktūra, izņemot tiesas, tām pildot savus uzdevumus;
- pārziņa vai apstrādātāja pamatdarbība sastāv no apstrādes darbībām, kurām to būtības, apmēra un/vai nolūku dēļ nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā;
- pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datus saskaņā ar Regulas 9. pantu un 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā.

Ja neesi pārliecināts, vai rīkojies pareizi, ieviešot Regulas prasības, piesaisti datu aizsardzības speciālistu kā konsultantu vismaz uz datu sakārtošanas laiku. Datu aizsardzības speciālists palīdzēs izvērtēt uzņēmuma risku pakāpi un ieteiks uzņēmumam obligāti nepieciešamos pasākumus.

Privāts drošības pakalpojumu uzņēmums veic vairāku privātu iepirkumu centru un sabiedrisku vietu novērošanu. Novērošana ir uzņēmuma pamatdarbība, kas, savukārt, ir nesaraujami saistīta ar personas datu apstrādi, tāpēc šim uzņēmumam arī ir jāieceļ datu aizsardzības speciālists.

No otras puses, visas organizācijas veic noteiktas darbības, piemēram, maksā saviem darbiniekiem vai veic standarta IT atbalsta darbības. Šie ir organizācijas pamatdarbības vai pamata uzņēmējdarbības veikšanai nepieciešamo atbalsta funkciju piemēri. Lai arī šīs darbības ir nepieciešamas un būtiskas, tās parasti uzskata par papildfunkcijām, nevis par pamatdarbību.[5] Šādos gadījumos datu aizsardzības speciālista norīkošana, balstoties uz pamatdarbības kritēriju, nebūs obligāta.

5 "Pamatnostādnes par datu aizsardzības speciālistiem ("DAS")" *https://www.dvi.gov.lv/lv/wp-content/uploads/datu-aizsardz%C4%ABbas-speci%C4%81listiem_LV.pdf*

SAKĀRTO

Vai zini kādos gadījumos nepieciešams datu apstrādes reģistrs?

Personas datu apstrādes reģistru jāveido:

- ja datu apstrāde ir regulāra;
- ja apstrāde varētu radīt risku datu subjektu tiesībām un brīvībām;
- ja tiek apstrādāti īpašās kategorijas dati (Regulas 30. panta 5. punkts).

Pārzinim apstrādes darbību reģistrā ietveramā informācija norādīta Regulas 30. panta 1. punktā:

1) pārziņa un attiecīgā gadījumā visu kopīgo pārziņu, pārziņa pārstāvja un datu aizsardzības speciālista, vārds un uzvārds vai nosaukums un kontaktinformācija;
2) apstrādes nolūki;
3) datu subjektu kategoriju un personas datu kategoriju apraksts;
4) to saņēmēju kategorijas, kuriem personas dati ir izpausti vai kuriem tos izpaudīs, tostarp saņēmēji trešajās valstīs vai starptautiskās organizācijas;
5) attiecīgā gadījumā informācija par personas datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju;
6) ja iespējams, paredzētie termiņi dažādu kategoriju datu dzēšanai;
7) ja iespējams, tehnisko un organizatorisko drošības pasākumu vispārējs apraksts.

Pildot apstrādātāja uzdevumus, Tev var būt jāuztur datu apstrādes reģistrs, atbilstoši Regulas 30. panta 2. punkta nosacījumiem.

Ko darīt?

- Paskaidro personas datu izpaušanas kārtību un nodošanu ārpus ES vai Eiropas Ekonomikas zonas.
- Nosaki un pamato personas datu glabāšanas termiņu un dzēšanu.
- Izveido personas datu aizsardzības sistēmu uzņēmumā.
- Datu apstrādes reģistrs var būt gan papīra formā, gan digitāli.

Personas datu apstrādes darbību reģistrs (žurnāls) saskaņā ar Vispārīgo datu aizsardzības regulu (2016./679., 13., 30. pants):

Pārzinis	SIA "XX"		
	Adrese Xxx iela 1, Latvija	Tālrunis +371 xxxxxx	Fakss +371 xxxxx
	E-pasta adrese Xxx@Xxx.lv	Vietne www.Xxx.lv	Datu aizsardzības atbildīgā e-pasta adrese aizsardziba@Xxx.lv
Personas datu apstrādes mērķis	Darba algas aprēķins un izmaksa		
Datu subjektu apraksts	▸ Darbinieki		
Personas datu kategorijas	▸ Vārds ▸ Uzvārds ▸ Norēķinu konta Nr.		
Personas datu saņēmēju kategorijas	Darbinieki, valsts iestādes likumā noteiktos gadījumos		
Personas datu nodošana ārpus ES vai Eiropas Ekonomikas zonas	Personas dati netiek nodoti ārpus ES vai Eiropas Ekonomikas zonas.		
Datu glabāšanas termiņi	10 gadi		
Tehnisko un organizatorisko drošības pasākumu vispārējs apraksts	1. Datu apstrādes tiesības tiek aizsargātas, izmantojot informācijas sistēmu piekļuves tiesību uzraudzības funkcijas. 2. Serveru datori, kas tiek izmantoti datu apstrādē, atrodas datoru centrā, kas ir aizsargāts ar piekļuves kontroles un drošības sistēmām. Reģistri, kuri satur personas datus, ir nošķirti no publiskās informācijas tīkliem, izmantojot tehniskos drošības pasākumus. 3. Papīra dokumentus uzglabā aizslēgtos skapjos, kas atrodas telpās ar piekļuves kontroli. 4. Personas, kas apstrādā personas datus, ir pakļautas konfidencialitātes pienākumam, kas izriet no likuma, pārziņa iekšējiem noteikumiem un vai ir parakstījuši konfidencialitātes līgumu. 5. Tiek veikta sistemātiska failu dublēšana.		
Apstrādes juridiskais pamatojums	Saskaņā ar Darba likuma ..p., Iedzīvotāju ienākuma nodokļu likuma ..p.		

Pārziņa nosaukums	Datu aizsardzības speciālists	Apstrādes nolūki	Datu kategorijas	Datu subjektu kategorijas	Datu saņēmēju kategorijas	Informācija par datu nosūtīšanu uz trešo valsti	Glabāšanas termiņš	Tehnisko un organizatorisko drošības pasākumu vispārējs apraksts
SIA "XX" janis@xx.eu T. xxxxxxxx	Jānis XX info@xx.eu T. xxxxxxxx	Darbinieku nodarbināšana	Vārds, uzvārds, norēķinu konts u.c.	Darbinieki	Darbinieki, valsts iestādes	Netiek nosūtīti dati	10 gadi – .. 5 gadi – ..	ORGANIZATORISKIE: 1) procedūras; 2) apmācības; 3) auditi; 4) paroles; 5) [..] TEHNISKIE: 1) Aizslēgti skapji; 2) Serveri slēgtās telpās; 3) Ugunsmūri; 4) Šifrēšana u.c.
		Sava īpašuma aizsardzība	Personas atrašanās konkrētā vietā un laikā, vizuālais izskats u.c.	Personas, kuras iekļūst video novērošanas zonā	Datu apstrādātājs, valsts iestādes	Netiek nosūtīti dati	2 nedēļas	

Šajā vietnē ir publicēts Datu aizsardzības speciālistu reģistrs, ko var izmantot kā alternatīvu piemēru personas datu apstrādes reģistram: https://ec.europa.eu/dpo-register/detail/DPO-1346

SAKĀRTO

Kādi ir darba kārtības noteikumi Tavā uzņēmumā?

Normatīvajos aktos, tostarp Darba likumā, paredzēti tikai vispārīgi noteikumi, kas piemērojami darba tiesiskajās attiecībās. Darba līgumā vai darba koplīgumā visbiežāk nav iespējams ietvert visus darba kārtību regulējošos jautājumus, tādēļ darba kārtības noteikumi ir viens no galvenajiem dokumentiem, kas nosaka darba kārtību uzņēmumā.

Viens no darba kārtības galvenajiem uzdevumiem ir nopietna un īpaša attieksme pret datu subjektu datiem. Darba kārtības noteikumos jāparedz darbinieku pienākumi un rīcība personas datu apstrādē:

- Kā iegūtos personu datus apstrādāt?
- Kā risināt problēmas, rīkoties nestandarta situācijās?
- Kā rīkoties, ja noticis datu pārkāpums?
- Pie kā vērsties, ja ir jāziņo DVI par personas datu pārkāpumu?

Darba kārtības noteikumu ievērošana darbiniekiem ir obligāta. Uzņēmējs var papildināt darba kārtības noteikumus un brīdināt darbiniekus par to, kādas sekas var iestāties darbiniekam, ja tiks pārkāpti personas datu apstrādes noteikumi.

Kāda ir pārziņa darbinieka atbildība?

Kamēr pārziņa darbinieks ievēro visus uzņēmuma dokumentu aprites noteikumus, sava darba līguma noteikumus un darbojas pēc pārziņa noteiktās kārtības, viņš Regulas izpratnē uzskatāms par personu, kura pārziņa tiešā pakļautībā ir pilnvarota apstrādāt personas datus, bet līdz ko Tavs darbinieks (bez Tavas ziņas) pats pieņēmis lēmumu veikt datu apstrādi, dzēšanu, arhivēšanu, noteicis mērķus un līdzekļus, tad viņš kļūst par datu pārzini un uzņemas pilnu atbildību attiecībā uz Regulas ievērošanu.

Darbinieks ir dzirdējis, ka viens no uzņēmuma klientiem, par kuru ir ziņas uzņēmuma klientu datu bāzē, ir labs automehāniķis. Darbinieka uzņēmuma rīcībā esošā klienta informācija ir iegūta saistībā ar piegādes pakalpojuma sniegšanu un uzņēmumam nav zināma cita informācija par klienta nodarbošanos. Darbinieks pēc savas iniciatīvas atrod klienta kontaktinformāciju un sazinās ar viņu, lai sarunātu sava auto remontu. Šādā gadījumā darbinieks ir pārkāpis Regulas prasības, un darba devējam, konstatējot šādu rīcību, ir jāveic pasākumi, kas nodrošinātu, ka šādi gadījumi neatkārtosies.

ESI GATAVS

Vai spēsi identificēt un izvērtēt personas datu aizsardzības pārkāpumu savā uzņēmumā? Vai Tu un Tavi darbinieki zināt kam un pie kādiem apstākļiem jāziņo par personas datu aizsardzības pārkāpumu?

Sekretārei zvana Tava uzņēmuma darbinieka sieva un jautā, vai vakar viņas vīrs bija darbā, cikos aizgāja, vai algas pārskaitījumu saņēma utt. Sekretāre sniedz darbinieka sievai informāciju. Šajā situācijā ir noticis personas datu aizsardzības pārkāpums, jo darbinieki netika informēti, ka šādu informāciju par uzņēmumā strādājošiem darbiniekiem nedrīkst sniegt.

Apdomā, vai personas apgalvojums pa tālruni, ka viņa ir darbinieka sieva, ir pietiekams, lai šo personu tiešām identificētu kā darbinieka sievu?

Tu palūdz sekretārei nosūtīt Tev sarakstu par darbiniekiem, kuriem nepieciešams arodārsta atzinums, ārstu privātpraksei. Sekretāre sajauc e-pastus un nosūta sarakstu citam sadarbības partnerim. Līdz ar to ir noticis personas datu aizsardzības pārkāpums.

Personas datu pārkāpums ir noticis, ja:

- personas dati ir nejauši vai nelikumīgi iznīcināti;
- pazaudēti vai izmainīti;
- tiem piekļuvis kāds no uzņēmuma darbiniekiem, kuram nav autorizētas piekļuves personas datiem;
- dati nozagti, noticis hakeru uzbrukums;
- dati nopludināti un publiski pieejami, u.c.

Ko darīt?

Ja noticis personas datu aizsardzības pārkāpums (pārkāpums ir maznozīmīgs, piemēram kļūdaini nosūtīts klientam sagatavotais piedāvājums uz trešās personas e-pasta adresi, nosūtīti dati minimālā apjomā – tikai vārds, uzvārds), uzņēmums ar datu pārkāpumu tiek galā pats, atbilstoši uzņēmuma darba kārtības noteikumos vai kādā citā procedūrā norādītajam. Šādā gadījumā ir jāsazinās ar personu, kurai kļūdaini nosūtīts e-pasts un jālūdz to dzēst. Par notikušo faktu ir jāizdara atzīme personas datu aizsardzības pārkāpumu žurnālā.

Ja datu pārkāpums ir nozīmīgs, piemēram, notikusi īpašas kategorijas datu noplūde, tad nekavējoties ir jāinformē datu aizsardzības speciālists vai uzņēmuma vadītājs, kurš attiecīgi rīkosies un par notikušo ziņos DVI – ne vēlāk kā 72 stundas pēc atklāšanas.

MVU ir jādokumentē visi personas datu aizsardzības pārkāpumi, to sekas un veiktie pasākumi.

Identificē pārkāpumu

Šajā posmā tiek noteikts, kāda veida personas datu pārkāpums noticis.

Izvērtē pārkāpuma nozīmīgumu

Šajā posmā jāanalizē personas datu pārkāpuma sekas un ietekme uz datu subjektu – cik lielā mērā datu aizsardzības pārkāpums var kaitēt datu subjekta mantiskajām un nemantiskajām interesēm.

Veic problēmas novērtējumu un prioritāšu noteikšanu, nosaki rīcības plānu un darbības tā īstenošanai.

- Kāda veida atgadījums ir noticis.
- Kādas cilvēku kategorijas atgadījums var ietekmēt.
- Cik daudz cilvēku atgadījums ietekmē.
- Kādas var būt pārkāpuma sekas.

➔ Kādus pasākumus varam nekavējoties veikt, lai neitralizētu negatīvās sekas.

Ziņo

Par datu pārkāpumu un pasākumiem jāpaziņo attiecīgajām personām, ja pārkāpums varētu radīt būtiskas negatīvas sekas datu subjektiem.

Datu aizsardzības pārkāpuma gadījumā, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām, jāpaziņo – DVI **72 stundu laikā no pārkāpuma konstatēšanas brīža.**

Izcelsmes problēmu identificēšana

https://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/

Mērķis šādam paziņojumam ir veikt cēloņa analīzi, lai novērstu līdzīgu problēmu atkārtošanos.

Daži raksturīgākie pārkāpumu veidi:

- ➔ Datu sistēmas parole nonākusi pie personas, kurai nav pilnvaras un nav dota atļauja piekļūt datu sistēmai.
- ➔ Nepareizam adresātam tika nosūtīts e-pasts ar informāciju par citu personu, vai nosūtīta vesela datu kopa – datu bāze.
- ➔ Uz printera palikusi izdruka ar algu sarakstu vai pacientu slimībām.
- ➔ Datorā iekļuvis vīruss, kas var bojāt vai nopludināt personu datus.
- ➔ Nozaudēts vai nozagts personas datu nesējs, dators, telefons.

Regulas 34. pants noteic, ka gadījumā, ja personas datu aizsardzības pārkāpums varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis bez nepamatotas kavēšanās paziņo datu subjektam par personas datu aizsardzības pārkāpumu.[6]

[6] *https://www.dvi.gov.lv/lv/wp-content/uploads/Pamatnostādnes-par-personas-datu-aizsardzības-pārkāpumu-paziņošanu-saskaņā-ar-Regulu-2016_679-LV.pdf*

Bibliogrāfija

Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) 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) (Dokuments attiecas uz EEZ) (OJ L 119, 4.5.2016). Pieejams: ***http://data.europa.eu/eli/reg/2016/679/oj***

Datu valsts inspekcijas 2018. gada 18.decembra rīkojuma Nr. 1-2.1/125 pielikums "Apstrādes darbību veidi,attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. panta 4. punktu". Pieejams: ***https://www.dvi.gov.lv/lv/datu-aizsardziba/organizacijam/ieteikumi/***

29. panta darba grupas vadlīnijas 16/LV WP 243 vers. 01 "Pamatnostādnes par datu aizsardzības speciālistiem" ("DAS") (2017. gada 5. aprīlī). Pieejams: ***https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048***

29. panta darba grupas vadlīnijas 18/LV WP250rev.01 "Pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679 " (2017. gada 3. oktobrī). Pieejams: ***https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052***

29. panta darba grupas vadlīnijas DG248 "Par Novērtējumu par ietekmi uz datu aizsardzību (NIDA) un Regulas 2016/679 vadlīnijām" (2017. gada 4. oktobris). Pieejams: ***https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236***

Edīte Brikmane (2018) "Personas datu apstrādes principi. Vispārīgā datu aizsardzības regula III", Latvijas Vēstnesis. Pieejams: ***https://lvportals.lv/skaidrojumi/295244-personas-datu-apstrades-principi-vispariga-datu-aizsardzibas-regula-iii-2018***

Edīte Brikmane (2018) "Piekrišana datu apstrādei. Vispārīgā datu aizsardzības regula IV", Latvijas Vēstnesis. Pieejams: ***https://lvportals.lv/skaidrojumi/295548-piekrisana-datu-apstradei-vispariga-datu-aizsardzibas-regula-iv-2018***

Ivo Krievs (2018) "DATU AIZSARDZĪBAS REGULA –KAS JĀZIN UZŅĒMUMIEM?". Pieejams: ***https://www.dbhub.lv/sites/default/files/articles/2018-05/GDPR_seminars_22.05.2018.pdf***

Information Commissioner's Office "How well do you comply with data protection law: an assessment for small business owners and sole traders". Pieejams: ***https://ico.org.uk/for-organisations/data-protection-self-assessment/assessment-for-small-business-owners-and-sole-traders/***

Šīs publikācijas finansējumam ir saņemts Eiropas Komisijas atbalsts.
Šajā publikācijā ir atspoguļots vienīgi DVI viedoklis, un Komisija neuzņemas atbildību par publikācijā ietvertās informācijas iespējamo izmantošanu.

Datu valsts inspekcija
Tālr. 67223131
Blaumaņa iela 11/13-15,
Rīga, LV-1011
e-pasta adrese: info@dvi.gov.lv
www.dvi.gov.lv