Vispārīgās datu aizsardzības regulas prasības: kam jāgatavojas?

Mg.iur. Māris Ruķers,
SIA E-sabiedrības risinājumi
valde, personas datu aizsardzības speciālists

2018.gada 6.aprīlis, Rīga

Lektora pieredze

- Datu aizsardzības tiesības – studiju kursa pasniedzējs Latvijas Universitātes Juridiskajā fakultātē: no 2001.gada
- Datu valsts inspekcijas direktora padomnieks 2001-2004.
- Dažādu apmācību vadītājs no 2001.gada
- Konsultācijas par personas datu aizsardzības jautājumiem – SIA E-sabiedrības risinājumi - no 2005.gada.
- Sertificēts personas datu aizsardzības speciālists: no 2012.gada
- Datu aizsardzības prasību ieviešanas Eiropas Savienības projekta īstermiņa eksperts Moldovā - 2018.gads.
- Regulas ieviešanas konsultants vairāk, kā 40 organizācijās – 2018.gads

Personas datu aizsardzības normatīvā sistēma pēc 25.05.2018.

- Eiropas Savienības tiesas prakse
- 27.04.2016. Eiropas Parlamenta un Padomes Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK. Eiropas Savienības oficiālais vēstnesis: 04.05.2016. nr.L119
- Personas datu apstrādes likums
- Latvijas tiesu prakse
- Fizisko personu datu aizsardzības likums zaudēs spēku

Jau izdotās vadlīnijas....

Direktīvas 95/46/EK 29.panta darba grupa:

- 2016.gada 13.decembra vadlīnijas par datu subjekta tiesību pārnesamību (dokuments WP 242)
- 2016.gada 13.decembra vadlīnijas par personas datu aizsardzības speciālistu (dokuments WP 243)
- 2016.gada 13.decembra vadlīnijas par pārziņa vadošās uzraudzības iestādes identificēšanu (dokuments WP 244)
- 2017.gada 8.jūnija vadlīnijas par personas datu apstrādi darba vietā (dokuments WP 249)

Jau izdotās izdotās vadlīnijas

- 2017.gada 3.oktobra vadlīnijas par personas datu aizsardzības pārkāpumu paziņošanu (dokuments Nr. WP 250)
- 2017.gada 3.oktobra vadlīnijas par administratīvo sodu piemērošanu (dokuments Nr. WP 253)
- 2017.gada 3.oktobra vadlīnijas par automātisko lēmumu pieņemšanu un profilēšanu Regulas Nr.2016/679 izpratnē (dokuments Nr. WP 251)
- 2017.gada 28.novembra vadlīnijas par *piekrišanu* Regulas izpratnē (WP 259)

Jaunākās vadlīnijas

- 2017.gada 28.novembra vadlīnijas par *pārskatāmību* Regulas izpratnē (WP 260)
- 2018.gada 6.februāra vadlīniju projekts par sertifikācijas institūciju akreditācijas kārtību (dokuments WP 261)
- 2018.gada 6.februāra vadlīniju projekts par Regulas 49.panta piemērošanu (dokuments WP 262)

Terminu izpratne: 4.pants

- **Personas dati**

Esošā definīcija + paskaidrojošā daļa

dati ir arī identifikators, pēc kura var identificēt: vārds, uzvārds, ID numurs, atrašanās vietas dati, tiešsaistes ID, vai viens, vairāki fiziskai personai raksturīgi fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem

Terminu izpratne: 4.pants

Īpašu kategoriju personas datu apstrāde

Termins bija Direktīvā 95/46/EK, bet tagad definēts plašāk

Esošais uzskaitījums (tautība, rase, arodbiedrības, reliģiskā, filozofiskā, politiskā pārliecība, veselība, seksuālā dzīve + ģenētiskie, biometriskie, seksuālā orientācija

Terminu izpratne: 4.pants

- **Profilēšana**

Jebkura veida automatizēta personas datu apstrāde, izpaužas, kā izmantošana ar mērķi izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, it īpaši: analizēt vai prognozēt aspektus saistībā ar personas sniegumu darbā, ekonomisko situāciju, veselību, personiskām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos

Terminu izpratne: 4.pants

- **Veselības dati**

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

Regula (EK) Nr.1338/2008

Terminu izpratne: 4.pants

- **Pseidonimizācija**

Personas datu apstrāde, ko veic, lai personas datus vairs nav iespējams sasaistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas ar noteikumu, ka šāda informācija tiek turēta atsevišķi un tiek veikti aizsardzības pasākumi

Uz kādu personas datu apstrādi regula attiecas (apstrādes forma)?

- A) Apstrāde pilnībā vai daļēji notiek elektroniskā formā (neatkarīgi no tā, vai apstrāde tiek organizēta kartotēkā, t.i. strukturizētā formā)
- B) Apstrāde nenotiek elektroniskā formā, bet veido daļu no kartotēkas
- Atsevišķas Regulas normas var piemērot tikai, ja dati ir apstrādāti elektroniskā formā

Eiropas Savienības tiesas 20.12.2017. spriedums lietā Nr.C-434/16 Peter Novak pret Data Protection Commissioner (Īrija)

Pārskatāmības princips

- Nemainās regulēšanas fokuss: pārziņa darbības ar personas datiem
- Pārzinim ir jāpamato personas datu apstrādes nepieciešamība, tiesiskums, jāspēj demonstrēt, ka prasības ir ieviestas. **Jāvērtē riski!**
- Datu aizsardzības regulējums kopumā (it īpaši saistībā ar Regulu) nozīmē vairāk procesuālus, nekā saturiskus pienākumus organizācijai. **Problēmas var radīt metodoloģijas trūkums vai atšķirīga izpratne par to.**
- Regula nosaka veicamo procesuālo darbību veidu, bet tā izpildes apjoms dažkārt balstās uz risku vērtēšanas principa
- Regulas ieviešana nav vienreizējs pasākums: **datu apstrādes atbilstība prasībām ir jāuztur pastāvīgi!**

Kas jādara atbilstības nodrošināšanai?

Koordinācija: atbildīgā persona, projekta vadītājs, atbildīgais departaments vai darba grupa Regulas prasību ieviešanai

Veicamie pasākumi:

1) izstrādāt rīcības plānu turpmāko pasākumu veikšanai ar noteiktiem termiņiem

2) personas datu apstrādē iesaistītos resursus, kanālus, informācijas sistēmas un tajā esošo personas datu veidus

3) izvērtēt apstrādājamo (arī glabājamo) personas datu veidus un konstatēt tiesiskā pamata esamību (vai neesamību), kā arī citus obligātos aspektus (piemēram, vai personas dati ir pieejami arī apstrādātājiem)

Kas jādara atbilstības nodrošināšanai?

Veicamie pasākumi:

4) auditēt vai pārskatīt informācijas sistēmu un procesu drošības situāciju

5) izvērtēt tiesisko pamatu esamību katram personas datu apstrādes posmam, nepieciešamības gadījumā to pamatot

6) izvērtēt līgumus ar personas datu apstrādātājiem un tajos iekļautās garantijas

7) kuras datu subjekta tiesības ir jānodrošina un vai tas notiek?

8) vai notiek pārrobežu personas datu apstrāde un, kuras valsts uzraudzības iestāde būs Jūsu vadošā uzraudzības iestāde?

Kas jādara atbilstības nodrošināšanai?

9) izveidot iekšējo personas datu apstrādes darbību reģistru

10) izlemt par personas datu aizsardzības speciālista nepieciešamību

11) veikt personas datu aizsardzības ietekmes novērtējumu, kā atsevišķu novērtējumu

12) iespējams, būs nepieciešams pārveidot informācijas sistēmu un citus procesus, novērst nepilnības

Tiesiskie pamati un principi

Regulas normas:

- Personas datu apstrādes principi: 5.pants
- Tiesiskie pamati: 6.pants
- Tiesiskie pamati īpašas kategorijas datiem: 9.pants
- Sodāmības dati: 10.pants

Personas datu apstrādes principi – 5.pants

- Likumīgums, godprātība, pārredzamība
- Mērķa ierobežojums
- Datu minimizēšana
- Datu pareizība un precizitāte
- Glabāšanas ierobežojums
- Integritāte un konfidencialitāte

Iekšējā izvērtēšanas piemērs: tiesiskie pamati

Darbības ar personas datiem un personas dati	Piekrišana	Līgums	Likums	Leģitīmā interese	Datu subjektam sniedzamā informācija
Dokumenta glabāšana	NĒ	NĒ	JĀ	JĀ/NĒ	Pirms personas datu ievākšanas jāsniedz informācijas saskaņā ar Regulas 13.pantu
Pieņemšana darbā	NĒ	JĀ	JĀ	NĒ	Informācija nav jāsniedz, ja tā jau ir datu subjekta rīcībā

Datu subjekta piekrišana un identitāte

- Pārzinim jāspēj uzskatāmi pierādīt, ka datu subjekts ir piekritis apstrādei (7.pants)
- Regula nepieprasa obligāti identificēt fizisku personu, lai uzskatītu, ka tiešām ir sniegta piekrišana. Jāsaglabā piekrišanas pierādījumi.
- Jāizvērtē, kuros gadījumos personas identitātes fiksēšana ir būtiska

Iestājoties 25.05.2018., piekrišanu nav vajadzīgs saņemt no jauna, ja vien tā ir dota atbilstoši piekrišana definīcijai, kas bija Direktīvā 95/46/EK (*Regulas preambulas 171.punkts*) un tā atbilst regulai (preambulas 43.punkts)

Pārziņa leģitīmā interese

29.Darba grupas viedoklis 06/2014 par leģitīmas intereses jēdzienu (WP217)

Leģitīmās intereses izvērtējuma bloki:

- vispārīga informācija par uzņēmumu (iestādi)
- leģitīmās intereses definēšana un identificēšana (kas ir šī tiesiskā interese, kuru pārzinis vēlas aizsargāt)?
- apstrādes nepieciešamības tests
- datu subjekta tiesību izvērtējums
- papildu pasākumi līdzsvara nostiprināšanai
- Uz šo tiesisko pamatu nevar atsaukties valsts pārvalde, veicot publisko tiesību funkcijas

Darbinieku privātums

- Jebkāda darbinieku uzraudzība veido papildu personas datu apstrādi.

Eiropas Cilvēka tiesas Lielās palātas spriedums lietā: *Barbulescu v Romania* (pieteikuma nr.61496/08):

- tikai aizliegums izmantot e-pastu un citas sistēmas privātām vajadzībām vēl nav pietiekams pamats veikt pašu novērošanu:
- aizlieguma klauzula neatbrīvo no pienākuma izvērtēt reālas legitīmās intereses esamību un uzraudzības samērīgumu
- otrkārt, šāds informatīvais apjoms darbiniekam nav pietiekams, jo nesniedz viņam informāciju par uzraudzības apjomu un ietekmi

Darbinieku privātums

- Datu subjekta informēšanai ir jānotiek pirms uzraudzības un jāinformē par tās apjomu: tikai trafiks vai arī saturs
- Darbiniekam ir jābūt informētam par uzraudzības veidiem un apjomu.
- Vadoties no pēdējās Eiropas Padomes tiesas lietas, nepietiktu pat ar frāzi "var tikt uzraudzīts", jo ir jāinformē tieši – tiek vai netiek uzraudzīts.
- *Nevar izmantot arī tikai šādu formulējumu: iestāde ir tiesīga kontrolēt bez iepriekšējas brīdināšanas (interneta, e-pasta, datortehnikas lietošana)*

Uzraudzība darba vietā: nepieciešamās rīcības

- Veikt procesu izvērtēšanas dokumentēšanu
- Atbilstoši izvērtēšanai īstenot attiecīgas iespējamās darbības : a) samazināt noteikta veida monitoringu vai tā pakāpi b) uzsākt jaunu monitoringu c) palielināt esošā monitoringa apjomu u.c.
- Paredzēt e-pastu vai citas komunikācijas uzraudzībai atsevišķu sadaļu kādā procedūrā vai, izstrādāt, kā atsevišķu procedūru
- Atbilstoši lēmumam par monitoringa veidiem un apjomu izstrādāt informatīvos dokumentus vai atrunas darbiniekiem, sniedzot visu nepieciešamo informāciju.
- Noteikt atbildīgos esošās kārtības uzraudzībai un periodus situācijas pārskatīšanai.

Datu subjekta informēšana par video (audio) novērošanu

- Latvijā nav speciāla zīmes standarta
- Zīmei jānodrošina Regulas 13.panta prasības
- Zīmes paraugs apstiprināts ar MK noteikumiem ir: robežsardzei un policijai
- Datu subjekts jābrīdina arī audio ieraksta gadījumā

Datu subjekta tiesības

- Tiesības piekļūt saviem personas datiem (15.pants)
- Pārzinis veicina datu subjekta tiesību īstenošanu
- Ne vēlāk, kā mēneša laikā informē un izsniedz pirmo bezmaksas kopiju
- Pārmērīgi pieprasījumi jāpierāda pārzinim (ja neizpilda datu subjekta lūgumu)
- *Eiropas Komisija vajadzētu izdot noteikumus par to, kā jālieto ikonas, kas sniedz informāciju par pārziņa veikto apstrādi (ikonām jābūt mašīnlasāmām)*

Datu subjekta tiesības

- Tiesības labot personas datus (16. un 19.pants)
- Tiesības tikt izdzēstam (17. un 19.pants)
- Tiesības uz personas datu apstrādes ierobežošanu (18.pants un 19.pants)
- Tiesības iebilst pret apstrādi (21.pants)

Datu glabāšana un dzēšana

Regula nosaka vispārīgu principu: personas datu tiek glabāti veidā, kas pieļauj datu subjekta identifikāciju, ne ilgāk, kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā. Regula nenosaka konkrētus personas datu apstrādes termiņus.

- *Princips attiecas:*

a) uz visiem personas datiem, kuri tiek apstrādāti informācijas sistēmās elektroniski, neatkarīgi no tā, vai dati tiek vai netiek aktīvi izmantoti (arī uz vēsturiskajiem datiem)

b) uz informācijas sistēmu rezerves kopijām

c) uz papīra informāciju, kura tiek glabāta tā, ka veido kartotēkas jēdzienu Regulas izpratnē (*dokumenta vai papīra mapīti par konkrētu fizisku personu var atrast, izmantojot īpašus kritērijus vai kopsakarā ar IS sistēmas ierakstiem*)

Personas datu izpaušana amatpersonām

- Regulas preambulas 31.punkts: *publisko iestāžu nosūtītiem informācijas pieprasījumiem vienmēr vajadzētu būt rakstiskiem, motivētiem un neregulāriem, un tiem nebūtu jāattiecas uz visu kartotēku kopumā vai jārada kartotēku savstarpēji savienojumi.*
- Identisks noteikums iekļauts Eiropas Savienības Direktīvas Nr.2016/680 preambulas 22.punktā
- Administratīvā lieta A420409113 un Eiropas Savienības tiesas spriedums lietā Nr.C-13/16

Personas datu apstrādes nepieciešamība termiņa griezumā

- Ņemot vērā Regulas uzstādījumu «*ne ilgāk, kā nepieciešams*», nozīmē to, ka personas datu pieejamība, izmantošana un pat glabāšana rezerves kopiju veidā ir cieši pakārtota definētajam personas datu apstrādes *mērķim un biznesa procesam*, kuram šie dati vispār ir paredzēti
- **Personas datu apstrādes mērķi vispirms tiek fiksēti, izvērtējot personas datu apstrādes procesus konkrētās informācijas sistēmās. Pārskatot, iespējams var identificēt šādas problēmas:**

a) **noteikti personas datu lauki kādreiz ir tikuši aizpildīti, bet pašreiz netiek izmantoti**

b) **noteiktu personas datu lauku izmantošanas nepieciešamība nav skaidra**

c) **glabāšanas termiņš personas datiem informācijas sistēmās pašreiz praktiski nekur nav definēts**

Personas datu glabāšanas termiņu izvērtēšana

Nepieciešamās rīcības:

1) jāpārskata personas datu apstrādes prakses reālā nepieciešamība konkrētam biznesa procesam vai mērķim
2) kad (kurā brīdī) izpildās sākotnējais personas datu apstrādes mērķis, kura dēļ personas dati bija nepieciešami?
3) ja sākotnējais mērķis tika izpildīts, vai kādi un vai visi personas dati turpmāk ir nepieciešami kāda cita vai vēsturiskā mērķa gadījumā?

Personas datu glabāšanas termiņu izvērtēšana

4) jāizvērtē arī vēsturisko datu (jautājums atrisināts, līgums izpildīts, darbs paveikts) uzkrāšanas un noteikta glabāšanas termiņa nepieciešamība

5) atbilstoši vēsturisko datu uzkrāšanas nepieciešamībai jāpārskata rezerves kopiju veidošanas principi.

Ja nav nepieciešami vēsturiskie dati, rezerves kopiju veidošanai jāparedz tikai aktuālās rezerves kopiju versijas glabāšana, nosakot periodus, pēc kuriem datu kopijas versijas tiek atjaunotas un pieejamas

Personas datu apstrādes pārtraukšana

Neapstrādāt personas datus nozīmē veikt darbības, lai informācijas kopumu vairs nevarētu uzskatīt par personas datiem (*procesa īstenošanai var būt nepieciešams sākotnējais IT atbalsts vai programmas funkcionalitātes vai piekļuves apjoma pārskatīšana*).

Apstrādes pārtraukšana praktiski var izpausties:

- personas datu kopuma dzēšana
- personas datu anonimizācija, nedzēšot visu informācijas apjomu, bet gan anonimizējot personas identitātes datus

(*Procesu īstenošanai var būt nepieciešams sākotnējais IT atbalsts vai programmas funkcionalitātes, kā arī piekļuves apjoma pārskatīšana*).

Automātiska personas datu apstrāde un profilēšana

- Līdz šim Direktīvā 95/46/EK tika regulēts tikai automatizētas datu apstrādes rezultātā pieņemto lēmumu statuss – Direktīvas 15.pants (daļēji iekļauts FPDAL 18.pantā)
- Automatizētas apstrādes rezultātā pieņemto lēmumu definīcijas Regulā nav, tikai kritēriji.
- Kas ir profilēšana un automatizētas datu apstrādes rezultātā pieņemtie lēmumi Regulas izpratnē? Regulas 4.panta 4.punkta un 22.panta korelācija.
- Galvenais kritērijs: minētās personas datu apstrādes darbības tiek veiktas **ar vai bez cilvēka līdzdalības**.
- Cilvēka līdzdalības nav: jāpiemēro Regulas 22.pants.

Apstrādes drošība

- Regulas 32.pants - attiecīgas tehniskās un organizatoriskās prasības
- 28.07.2015. Ministru kabineta noteikumi Nr.442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām*
- 12.05.2015. Ministru kabineta noteikumi Nr.216 Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu
- Grozījumu projekts Informācijas tehnoloģiju drošības likumā/ES Direktīva 2016/1148. *Izsludināts VSS 25.01.2018.*

Kas ir personas datu apstrādes darbību reģistrs?

1. Jāveic, ja nodarbināto skaits pārsniedz 250. Vai veikt arī pie mazāka cilvēku skaita?

- Izņēmumi no atbrīvojuma:

a) Apstrāde var radīt risku datu subjekta tiesībām un brīvībām;

b) Apstrāde nav neregulāra

c) Apstrāde ietver īpašas kategorijas datus

d) Apstrāde ietver sodāmības datus

2. Ko nozīmē personas datu **apstrādes darbības**?

3. Vai reģistrā ir jāiekļauj personas datu veidi?

Kas ir mūsu apstrādātāji un kādi ir ar tiem noslēgtie līgumi?

Problemātiskie jautājumi un Regulas 28.pants:

- Vai Jūsu ārpakalpojums piekļūst personas datiem un tos apstrādā?
- Tehniskās un organizatoriskās prasības – cik detalizēti
- Konfidencialitātes prasības
- Kas ir apakšuzņēmēji un, kā tos var mainīt?
- Kas notiek, kad līgums tiek izpildīts?
- Personas datu kopijas
- Trešās valstis

Terminu izpratne: 4.pants

- **Personas datu aizsardzības pārkāpums**

Ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem

Personas datu incidentu ziņošana

- Ne visi drošības incidenti noved pie personas datu aizsardzības pārkāpuma Regulas izpratnē
- Neziņo, ja «maz ticams», ka pārkāpums varētu radīt risku fizisko personu tiesībām un brīvībām, ziņo, ja var radīt «risku». Ja rada «augstu risku», jāziņo arī datu subjektam (piemēram, identitātes zādzība, diskriminācija, finansiāli zaudējumi utt.
- Personas datu aizsardzības pārkāpums jāsaista ar drošības kritērijiem un var izdalīt pieejamības, integritātes un konfidencialitātes incidentu
- Pārzinim «kļuvis zināms» tad, kad apstrādātājam «kļuvis zināms»
- Ziņojums jāizdara vadošajai uzraudzības iestādei, bet ja ir šaubas arī lokālajai!
- Jāved pārkāpumu reģistrs. Kāds ir tā saturs?

Personas datu aizsardzības speciālists Regulas 37.pants

Regula nosaka 4 kritērijus speciālista obligātai piesaistei (gan pārzinim, gan apstrādātājam):

a) apstrādi veic publiska iestāde vai struktūra

b) pamatdarbība sastāv no apstrādes darbībām, kuras pēc būtības, apmēra vai mērķa dēļ nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā

c) pamatdarbība ietver īpašas kategorijas datu apstrādi plašā mērogā

d) pamatdarbība ietver sodāmības datu apstrādi plašā mērogā

Kā interpretēs pārziņa jēdzienu saskaņā ar Regulu attiecībā uz valsts un pašvaldību sektoru? Ko nozīmē «plašā mērogā»?

Personas datu apstrādes likums (projekts)

- Noteikt uzraudzības iestādes statusu, struktūru, pienākumus un tiesības, lēmumu pārsūdzēšanas jautājumus
- Noteikt personas datu aizsardzības speciālista statusu
- Noteikt izņēmumus no Regulas prasībām, ciktāl tas pieļaujams, piemēram, tiesiskie pamati, datu subjekta tiesības u.tml.
- Sodu uzlikšana pārziņiem, kuri ir valsts vai pašvaldību iestādes u.c. jautājumi

Par ko var uzlikt sodu?

- Līdz EUR 10milj vai līdz 2% no kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma
- Pārziņa un apstrādātāja pienākumi: 8., 11., 25.-39., 42. un 43.pants
- Sertifikācijas struktūras pienākumi
- Pārraudzības struktūras pienākumi
- Līdz 20milj vai līdz 4% no kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma
- Apstrādes pamatprincipi, nosacījumi par piekrišanu, ievērojot 5., 6., 7. un 9.pants
- Datu subjekta tiesības: 12.-22.pantu
- Personas datu nodošana uz trešo valsti
- Nacionālās valsts likumi