Datu valsts inspekcija

Tehniskie un organizatoriskie pasākumi datu aizsardzības nodrošināšanā

Arnis Puksts, sertificēts fizisko personu datu aizsardzības speciāists, Latvijas Sertificēto personas datu aizsardzības speciālistu asociācijas valdes līdzpriekšsēdētājs

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

Saturs

- Tehnisko un organizatorisko pasākumu būtība – VDAR 32.pants;
- Konkrētās vai nekonkrētās prasības;
- Rīcība…

Tehnisko un organizatorisko pasākumu būtība

VDAR 32.pants - par visu: «Ņemot vērā **tehnikas līmeni**, **īstenošanas izmaksas** un **apstrādes raksturu, apmēru, kontekstu un nolūkus**, kā arī dažādas **iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām**, pārzinis un apstrādātājs īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam, tostarp attiecīgā gadījumā cita starpā[..]»

Tehnikas līmeni…

- Pēdējos 20 gados tehnikas līmenis ir eksponenciāli pieaudzis...
- Šobrīd liels izaicinājums ir «mākslīgā intelekta» risinājumi, piemēram, neironu tīkli...
- Arī kvantu datori vairs nav zinātniskā fantastika…
- Vai vispār parasts lietotājs apzinās, ko viņš izmanto?

Īstenošanas izmaksas..

- Vārds «izmaksas» sevī ietver ne tikai finanses; arī laiks un nepieciešamie cilvēkresursi ir izmaksas;
- Pārzinim, pirms vispār sākt vai turpināt konkrētu datu apstrādi, vajadzētu saprast, vai adekvātas datu aizsardzības nodrošināšana vispār ir iespējama, jo – fakts, ka «tas ir dārgi» NAV ATTAISNOJUMS sliktai datu aizsardzībai!
- Tomēr, ne vienmēr labs risinājums ir arī dārgs risinājums!

...apstrādes raksturu, apmēru, kontekstu un nolūku...

- Datu apstrādes nolūks ir būtiskākais kritērijs – no tā ir atkarīgas apstrādāto datu kategorijas un attiecīgi, arī risks konkrētas fiziskas personas tiesībām un interesēm;
- Apstrādes raksturs, apmērs un konteksts, savukārt izriet no izvēlētā datu apstrādes tehniskā risinājuma (kas var būt no papīra kartotēkas, līdz «pilnīgam mākonim»)…
- Jo labāks un izsmeļošāks ir datu apstrāžu (nolūku) reģistrs, jo tuvāk tam, ka pārzinis saprot, ko, kā un kādēļ viņš dara...
- Minimizācijas princips kā bāze – TIKAI TIK, CIK NEPIECIEŠAMS!

…iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām

- Kompleksa riska analīze - Nepieciešams jauns līmenis – katra riska iespējamā ietekme uz konkrētu datu subjektu tiesību un brīvību iespējamo aizskārumu:
  - «Parastā» riska analīze – resursi un resursiem iespējamie riski (tipiski vērtēti konfidencialitātei, integritātei un pieejamībai) un
  - Konkrēts nolūks, konkrēti dati (kategorijas), ar konkrētu ietekmi datu subjekta tiesībām un brīvībām…

VDAR (ne)konkrētums

- VDAR 32.pants: «[..]
  - personas datu pseidonimizāciju un šifrēšanu;
  - spēju nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību;
  - spēju laicīgi atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums;
  - procesu regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību.»

Pseidonimizācija un šifrēšana

- Tiešo identifikatoru aizstāšana vai visas informācijas pārveidošana veidā, kurā informācija zaudē saturu un jēgu;
- Pati par sevi nenodrošina neko!
- Būtiskie elementi ir:
  - Process – kā tiek veikta pseidonimizācija vai šifrēšana un
  - Arhitektūra – kāds ir algoritms (kur un kā tiek apstrādāti pseidonimizēto datu «atšifrējumi»; kāds šifrēšanas algoritms tiek izmantots; kāda ir šifrēšanas atslēgu pārvaldība…)…

… spēja nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību…

- Konfidencialitāte – informācija ir pieejama tikai konkrētai personai, konkrētā apmērā un konkrētā laikā;
- Integritāte – datu pilnīguma saglabāšanās visā datu apstrādes laikā jeb «ko ielikām, to izņemam»;
- Pieejamība – datu apstrādes nolūku sasniegt nav iespējams, ja nav pieejamības…
- Noturība – pilnīga izpratne par izmantoto tehnoloģiju kopumu un reāls «darbības turpinātības plāns» - stāsts par to, kā «piecelties», nevis «nenokrist»...

…spēju laicīgi atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums;

- Rezerves kopijas – datiem, loģikai, infrastruktūrai, jo - fizisko personu datus drīkst apstrādāt tikai tad, ja pastāv reāls datu apstrādes nolūks un tiesiskais pamatojums;
- Pārzinim ir jānosaka konkrēti saprātīgi kritēriji – «cik daudz» nepieejamības ir pieņemami un kad vairs nav noteiktā laika periodā (iekšēja pakalpojumu līmeņa vienošanās, SLA)
- Protams, tas jāattiecina arī uz apstrādātāju…

…procesu regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību

- Lai citiem (piem., datu subjektam, sadarbības partnerim, uzraudzības iestādei) pierādītu, ka tehniskās un organizatoriskās prasības tiek ievērotas, pārzinim pirmkārt tas ir jāpierāda sev!
- Formālā «ķeksīša» pieeja nekādā veidā šo nerisina – datu aizsardzība nav par dokumentu paketi plauktā, bet par reālu procesu kopumu.
- Katra konkrētā situācija ir īpaša un konkrēta – nav iespējams «sagatavju» risinājums, jo Velns slēpjas niansēs!
- Daļēji palīdzētu/-s sertifikācijas mehānismi un labās prakses kodeksi – līdz zināmai robežai tie iedos bāzes algoritmu, taču – šobrīd šo vēl īsti nav ☺

Apstrādātājs…

- Drošības prasības ir saistošas ne tikai pārzinim, bet – tā izvēlētajiem apstrādātājiem!
- Praksē šī ir pilnīga «bēdu ieleja»!

Ko tagad darīt?

- Nolūku reģistrs – izņemiet to «no plaukta» un kritiski pārvērtējiet. Vai tiešām tur ir viss?
- Ja tiešām ir viss – pārvērtējiet risku analīzes procesu, vai tiešām vērtējiet arī «ietekmi datu subjekta tiesībām un interesēm»;
- Ja vērtējiet – tad, vai Jums ir pilnīga pārliecība, ka esat efektīgi visās datu apstrāžu aizsardzībās?
- Ja, jā – apsveicu, domāju, ka Jūs var virzīt vismaz «Latvijas lepnumam»!
- PS. Ak, jā - paņemiet jebkuru līgumu ar apstrādātāju. Un godīgi sev atbildiet – vai tur tiešām ir tas, kas ir VDAR 32.panta «garā»…

Paldies!

PS. Ja Jums ir detalizēti jautājumi, droši uzdodiet tos:

- Zvanot 29235250;
- Rakstot arnis.puksts@topdpo.com

Veiksmi darbos!