PRIVĀTUMA PĀRVALDĪBAS DZĪVES CIKLS

Arnis Puksts

Sertificēts personas datu aizsardzības speciālists,

2018.Gada 25.maijs

Saturs

- **Privātums;**
- **Iejaukšanās privātumā;**
- **Atbildība;**
- **Četri «soļi» privātuma pārvaldībā;**
- **Dokumentēšana un apmācība;**
- **Atbildība.**

Privātums

- Ir viens no personas neaizskaramības pīlāriem, tāpat kā tiesības uz dzīvību un tiesības uz personisko brīvību!
- Fizisko personu dati ir privātuma būtiska sastāvdaļa.
- Jebkura iejaukšanās privātumā ir cilvēka tiesību aizskārums, kas drīkst notikt tikai izņēmuma gadījumos, ievērojot konkrētus nosacījums!
- Izņēmuma gadījumi ir definēti normatīvajos aktos un tos var reducēt līdz:
  - *Obligāti pastāv datu apstrādes mērķis (kādēļ privātums tiek aizskarts);*
  - *Obligāti pastāv datu apstrādes tiesiskais pamatojums.*

Privātuma pārvaldības dzīves cikls

- Privātuma pārvaldība sākas ar ideju par datu apstrādi (un nevis ar brīdi, kad datus jau faktiski apstrādā!) un turpinās līdz pilnīgai datu iznīcināšanai;
- Privātuma pārvaldība ir uz konkrētiem, aprakstītiem un pierādāmiem aspektiem (piemēram, dokumentācijas) balstīta pieeja, ar ko:
  - *Ir pilnīgi skaidrs, kurā datu apstrādes dzīves cikla stadijā ir konkrētā datu apstrādes situācija;*
  - *Kādi ir ar konkrēto datu apstrādi saistītie riski privātumam (ņemot vērā datu apstrādes kontekstu, nolūku un izmantototās tehnoloģijas);*
  - *Nodrošina dinamiskumu, nevis statiku (vide ir mainīga ikdienā!)...*

Atslēgas elements - atbildība

- Pārzinis – attiecīgs subjekts, kas iejaucas privātumā – ir pilnībā atbildīgs par jebkurām sekām, kuras iestājas ar iejaukšanos (t.sk. par pašu iejaukšanās faktu)!
- Atbildība nav tikai atbilstība normatīvo aktu prasībām! Atbildība ir:
  - *Skaidra izpratne par to, kādēļ kaut kas tie darīts;*
  - *Pilnīga apstrādāto datu pārvaldība (tātad, pārzinis precīzi zin, kur un kas tiek darīts, kā tiek darīts, kurš datu apstrādes dzīves cikla posms ir, u.tml.)*
  - *Tiek veikta risku pārvaldība un brīdis starp riska konstatēšanu un rīcības ar risku (riska akceptēšana, pretpasākumu ieviešana, riska pārnese) ir pēc iespējas mazāks;*
  - *No jebkuriem incidentiem (kļūdām, vainojamām vai nejaušām, iekšēju vai ārēju cēloņu) tiek izdarīti secinājumi, kuri tiek ieviesti privātuma pārvaldībā;*
  - *Cikls PDCA: (Plan)plānot→(Do)darīt→(Check)pārbaudīt→(Act)rīkoties*

Privātuma pārvaldības četri «soļi»

1. Ideja par iejaukšanos privātumā – jeb datu apstrādes mērķa definēšana: Kādēļ?
2. Uz konkrēto jomu attiecināmo speciālo un vispārīgo tiesību normu izvērtējums: Kas ir jāņem vērā? Kādi vēl datu apstrādes mērķi veidojas? Veicamās datu apstrādes tiesiskie pamatojumi?
3. Riska izvērtējums: kā mērķa(-u) sasniegšanai veiktā datu apstrāde var ietekmēt datu subjekta privātumu, ko darīt, lai ietekmi minimizētu?
4. Attiecīgu tehnoloģisko līdzekļu izvēle – atceroties Vispārīgās datu aizsardzības regulas pīlāru: privātums pēc noklusējuma un pēc konstrukcijas (privacy by default and by design)!

Dokumentēšana

Iejaukšanās privātumā ir jādokumentē:

1. Iekšējā dokumentācija ir primāra tā ir jāveido pirms reālas iejaukšanās privātumā jeb datu apstrādes uzsākšanas; iekšējā dokumentēšana izpaužas kā – datu apstrāžu nolūku (mērķu) apraksts, riska analīzes (t.sk., privātuma ietekmes novērtējuma) veikšana, privātuma politikas izstrāde/esamība, līgumu ar apstrādātājiem, u.tml. (pēc sava rakstura – iekšējā dokumentācija ir vairāk formāla, tās mērķis ir definēt robežas un pareizo rīcību, kā arī informēt par nepareizu rīcību un tās sekām).

2. Ārējā dokumentācija ir iekšējās dokumentācijas «esence», kuras galvenais mērķis ir – informēt datu subjektu par plānoto (vai jau esošo) iejaukšanos privātumā, mērķiem, tiesībām, riskiem, un citiem būtiskiem aspektiem, kas izpaužas kā privātuma paziņojums (ārējā dokumentācija – mazāk formāla, tās mērķis ir precīzi, viennozīmīgi, uztverami informēt esošo vai potenciālo datu subjektu).

Apmācības

- Ikviens, kurš piekļūst vai var piekļūt, pie informācijas, tajā skaitā, fizisko personu datiem, ir potenciāls drauds.
- Iespēja, ka potenciālais apdraudējums kļūs reāls, pieaug ar katru brīdi, kurā piekļuve pie informācijas ir Neapmācītām vai pienācīgi neapmācītām personām.
- Apmācības ir privātuma pārvaldības atslēgas elements ar mērķi radīt izpratni!
- Izpratnes uzturēšanai svarīgākais ir – atkārtošana!
- Apmācībām ir jābūt plānotam un regulāram pasākumu kopumam, nevis atsevišķām, epizodiskām akcijām.
- Arī slikta apmācība ir labāka par nekādu apmācību!

Atbildīga rīcība

- «Ja kaut kas slikts var notikt, tas notiks un, iespējams, vissliktākajā veidā» (nedaudz modificēts «Mērfija likums»);
- Nav tādas rīcības, kas pilnībā pasargātu no incidentiem! Līdz ar to – atbildīga rīcība nozīmē jau sākotnēji definēt rīcību drošības incidentu gadījumā;
- Ne katrs drošības incidents ir arī «datu pārkāpums» (data breach) un atšķiršana ir atslēgas elements:
  - *Drošības incidents ir jebkāds notikums, kas negatīvi ietekmē konfidencialitāti, integritāti vai pieejamību;*
  - *Datu pārkāpums ir ar lielu varbūtības pakāpi konstatējams fakts, ka dati ir vai varētu būt kļuvuši zināmi nesankcionētai pusei;*
  - *Visi datu pārkāpumi ir incidenti, bet ne visi incidenti ir datu pārkāpumi!*

MĒS ESAM CEĻA SĀKUMĀ...