Personas datu pārkāpumi un ziņošana. Mācības no citu kļūdām

Anna Bogdanova
anna.bogdanova@sorainen.com
+371 22441566

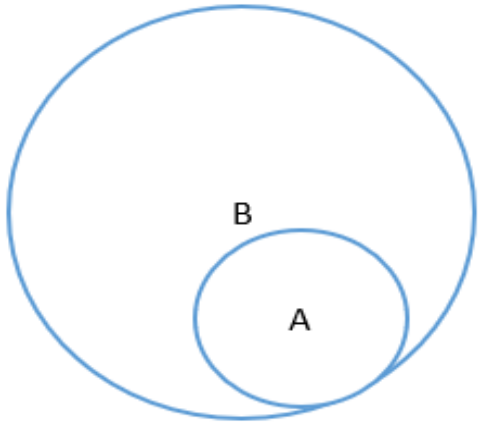
No Vispārīgās datu aizsardzības regulas līdz Mākslīgā intelekta regulai

2021.gada 13.maijs

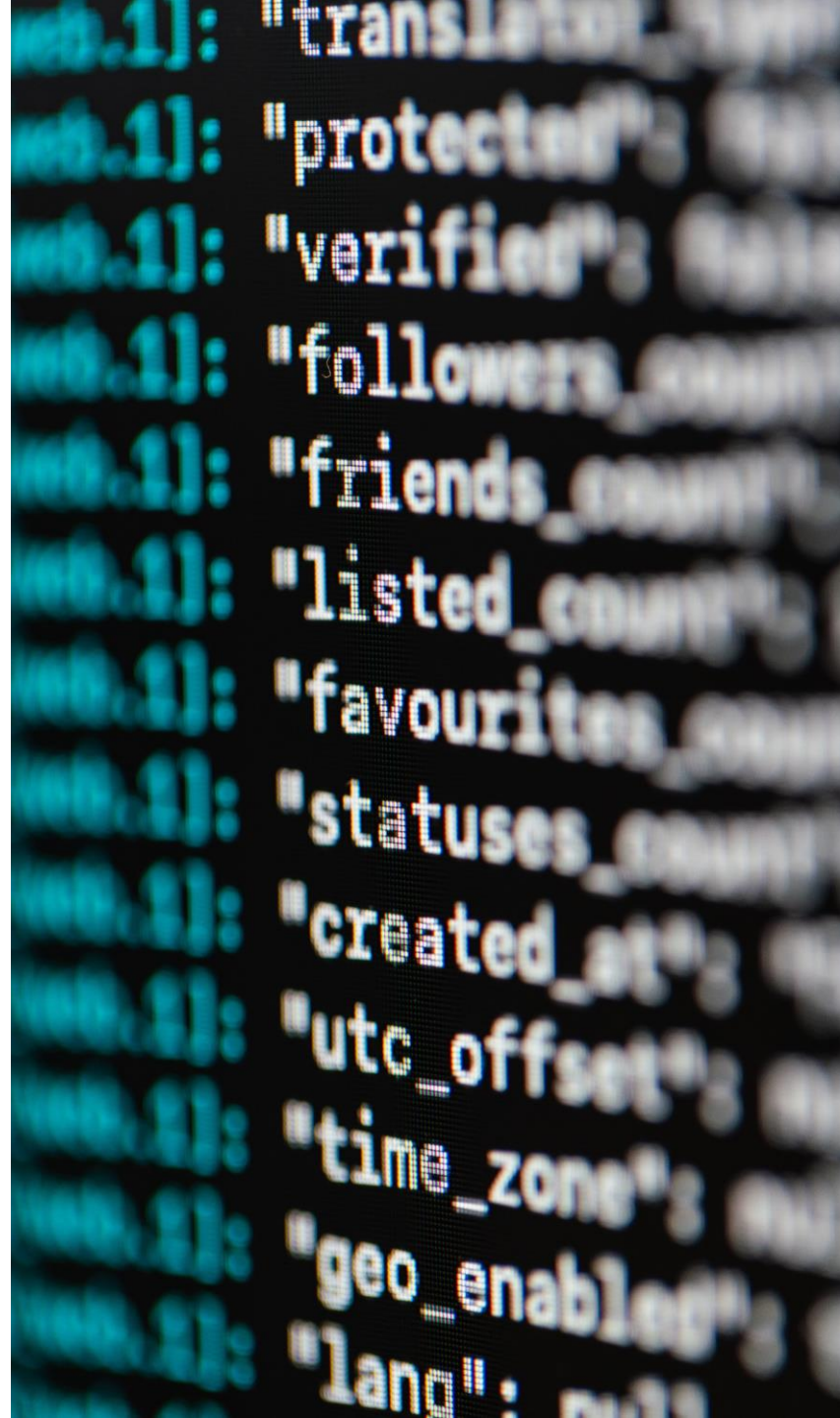
SORAINEN

Kas ir personas datu aizsardzības pārkāpums?

Drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem (GDPR 4.pants 12.punkts).



Vai visi drošības incidenti ir arī personas datu aizsardzības pārkāpumi?

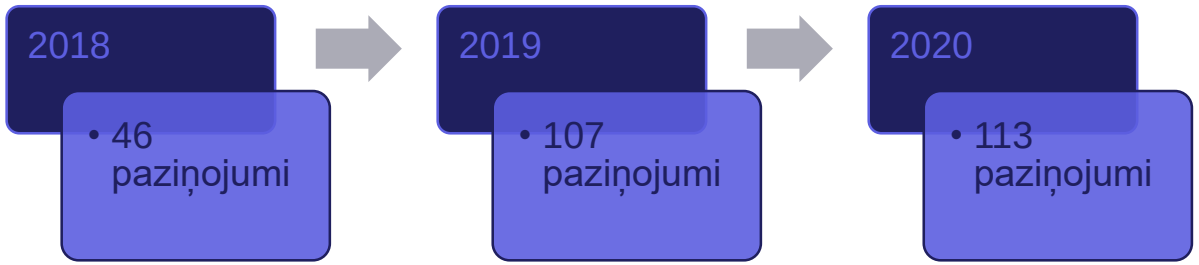


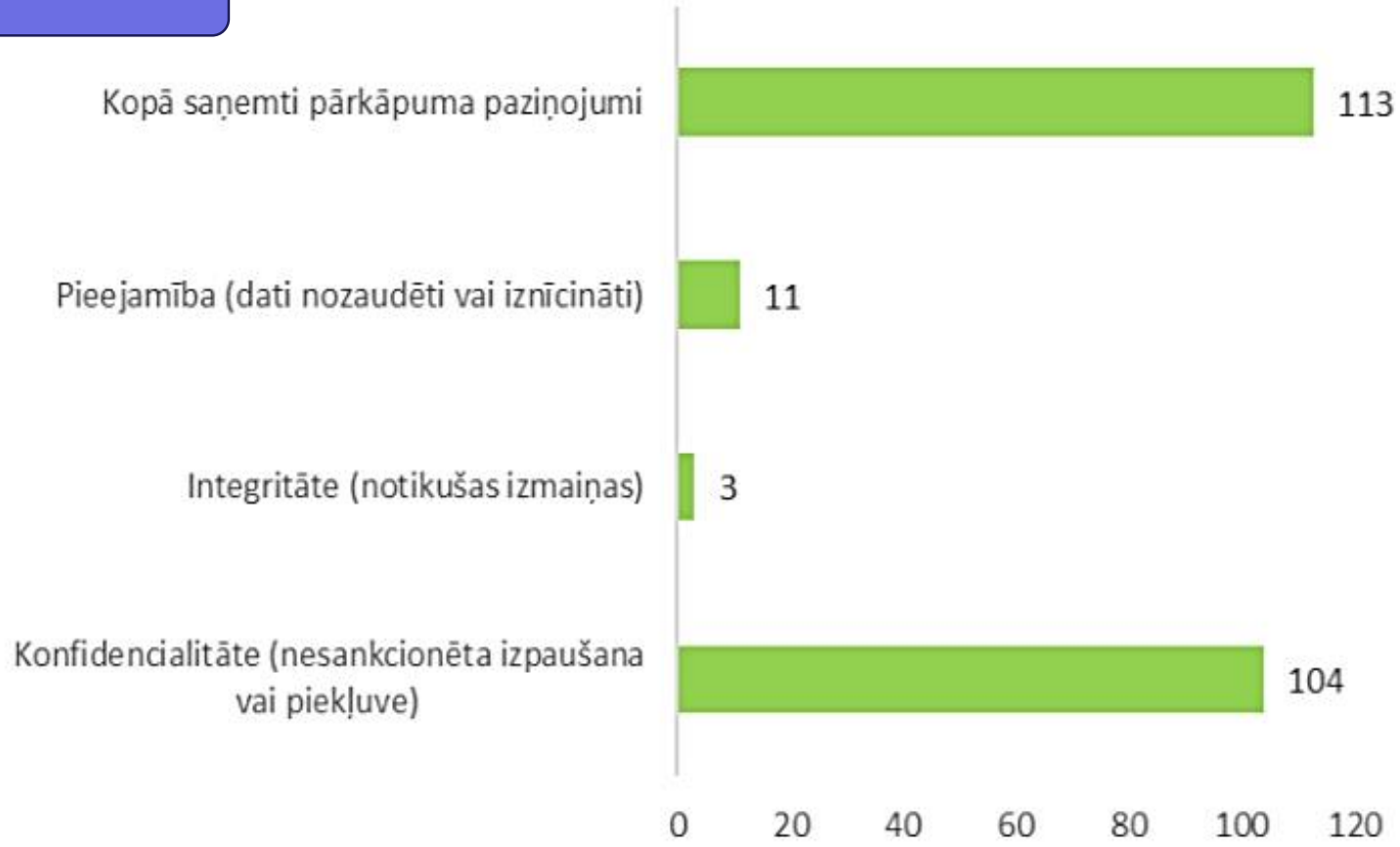
Kam ir jāziņo?

Saskaņā ar GDPR 33. pantu pārzinim ir pienākums ziņot par datu aizsardzības pārkāpumu **DVI** 72 h laikā no brīža, kad ir kļuvis zināms par pārkāpumu.

Subjektiem – bez nepamatotas kavēšanās, ja rada augstu risku personu tiesībām un brīvībām.

Cik bieži uzņēmumi LV ziņo par pārākumiem?





Ziņošana DVI

Kādos gadījumos var neziņot?

Gadījumos, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām.

Pienākums dokumentēt izvērtēšanas procesu pat tad, ja tiek secināts, ka nav jāziņo.

Cik ilgā laikā ir jāziņo?

Ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms.

Kad pārkāpums ir kļuvis zināms?

Pretējā gadījumā ir jāpievieno paskaidrojumi par kavēšanos.

Kādā valodā?

Saziņa ar iestādēm – valsts valodā.

Steidzamības gadījumā sākotnēji var ziņot angļu valodā, vēlāk – latviešu.

Kādā veidā?

Var izmantot DVI izstrādāto veidlapu.

Iesniedz pārzinis vai viņa pilnvarotais pārstāvis (tajā skaitā, apstrādātājs, ja ir pilnvarots).

Elektroniski parakstītu, nosūtot uz oficiālo e-pasta adresi, ierakstītā sūtījumā vai personīgi Datu valsts inspekcijā, kā arī veicot autorizāciju valsts pārvaldes pakalpojumu portālā www.latvija.lv.

Datu valsts inspekcija

Paziņojums par personas datu aizsardzības pārkāpumu

3. Informācija par pārkāpumu * (obligāts vismaz viens no sekojošajiem variantiem)

- ☐ Konfidencialitāte (nesankcionēta izpaušana vai nesankcionēta piekļuve)
- ☐ Integritāte (notikušas izmaiņas)
- ☐ Pieejamība (dati ir zaudēti vai iznīcināti)

Pārkāpuma raksturs * (obligāts vismaz viens no sekojošajiem variantiem)

- ☐ ierīce ir nozaudēta vai nozagta
- ☐ dokuments ir nozaudēts vai atstāts brīvi pieejamā vietā;
- ☐ pasts (papīra formātā) ir nozaudēts vai piegādāts atvērts;
- ☐ urķēšana;
- ☐ ļaunprogrammatūra (piem. ransomwares);
- ☐ pikšķerēšana ;
- ☐ nepareiza personas datu iznīcināšana papīra formātā;
- ☐ E-atkritumi (personas dati atrodas novecojušā ierīcē);
- ☐ nepārdomāta publikācija;
- ☐ izpausti personas dati citam/nepareizam datu subjektam;
- ☐ personas dati nosūtīti nepareizam adresātam;
- ☐ verbāla nesankcionēta personas datu izpaušana
- ☐ cits

[Cits pārkāpuma raksturs] (nav jānorāda)

Pārkāpuma cēlonis * (obligāts vismaz viens no sekojošajiem variantiem)

- ☐ Iekšēja neapzināta ļaunprātīga rīcība (iekšējās politikas pārkāpums)

Ziņošana subjektam

Kādos gadījumos var neziņot?

Ja tiek izpildīts jebkurš no šādiem nosacījumiem:

a) ir īstenoti atbilstīgi tehniski un organizatoriski aizsardzības pasākumi (piemēram, šifrēšana);

b) ir veikti turpmāki pasākumi, ar ko nodrošina, lai, visticamāk, vairs nevarētu materializēties augstais risks

c) tas prasītu nesamērīgi lielas pūles. Šādā gadījumā tā vietā izmanto publisku saziņu vai līdzīgu pasākumu, ar ko datu subjekti tiek informēti vienlīdz efektīvā veidā.

Cik ilgā laikā ir jāziņo?

Bez nepamatotas kavēšanās.

Kādā valodā?

Atbilstošā valodā.

Kādā veidā?

Uzskatāmi un viegli saprotami. Tos nevajadzētu iekļaut regulārajos paziņojumos par jaunumiem, īpašajiem piedāvājumiem u.tml.

Pārredzami saziņas veidi ietver: sms, e-pastus, pamanāmus paziņojumus mājaslapā, pasta sūtījumus, lieli un uzskatāmi paziņojumi drukātajos preses izdevumos.

Preses relīze vai korporatīvā bloga ieraksts netiek uzskatīts par uzskatāmu paziņošanas veidu.

Kas ir jāņem vērā?

- **Personas datu kategorijas** (īpašo kategoriju dati (sensitīvie dati), dati par sodāmību, dati par datu subjekta uzvedību, dati par datu subjekta finansiālo stāvokli u.tml., piemēram, ir daudz lielāka iespēja, ka tiks būtiski aizskartas datu subjekta intereses, ja pārkāpums skars īpašo kategoriju personas datus);
- **aizskarto personas datu apjoms** (piemēram, jo lielāks datu subjektu skaits, jo lielāks ir kopējais kaitējums);
- **identifikācijas spēja** (cik viegli datu subjektu ir identificēt, balstoties uz šiem datiem; vai ir iespējama tieša identifikācija, vai arī ir nepieciešama papildu informācija?);
- **radītais kaitējums** (piemēram, kaitējums reputācijai, fiziskas neērtības, iespējama identitātes zādzība, patērēts laiks, lai atkārtoti ievadītu informāciju, aizkaitinājums);
- **īpašās datu subjektu raksturojošās pazīmes** (piemēram, piederība pie neaizsargātas personu grupas – nepilngadīgas personas, pensionāri u.c.);
- **īpašās datu pārzini raksturojošās pazīmes** (piemēram, darbības specifikas dēļ ir viegli radīt kaitējumu lielai personu grupai, kas kļūs plaši zināms lielai sabiedrības daļai).

Uzņēmums	Valsts	Soda nauda, eiro	GDPR panti	Netika paziņots uzraudzības iestādei	Netika paziņots subjektam	Novēlots paziņojums
MisterTango UAB	Lietuva	61,500	5.,32.,33.			
Saunier-Tec Mantenimientos de Calor y Frio, SL.	Spānija	3,600	33.			
Tusla Child and Family Agency	Īrija	40,000	32.,33.			29 nedēļas
National Government Service Centre (NGSC)	Zviedrija	18,700	33.,34.			5 mēn. attiecībā uz datu subjektiem, 3 mēn. attiecībā uz uzraudzības iestādi
Booking.com	Nīderlande	475,000	33.			22 dienas vēlāk
Ungāru politiskā partija	Ungārija	34,375	32.,33.,34.			

Mācība Nr.1 : MisterTango UAB (Lietuva)

Pārkāpuma būtība

- Personas datu pārkāpums maksājumu pakalpojumu sistēmā, par kuru, cita starpā, nav ziņots uzraudzības iestādei. Proti, internetā 2 dienas bija pieejami dažādu banku klientu veiktie maksājumi, izmantojot MisterTango UAB maksājumu iniciēšanas pakalpojumu sistēmu, un šādu klientu personas dati.

Atziņas

- Lietuviešu uzraudzības iestādes ieskatā:
- tam būtu jābūt nozīmīgam signālam citiem uzņēmumiem, kuri tikai deklaratīvi ievēro GDPR prasības;
- gadījums, kad nepilnvarotām personām 2 dienas tika piešķirta piekļuve personas datiem internetā, jāuzskata par datu pārkāpumu, par kuru jāziņo uzraudzības iestādei;
- pārbaudes laikā tika atklāta virkne citu problēmu - tika secināts, ka uzņēmums apstrādāja lielāku personas datu apjomu nekā bija vajadzīgs, pārkāpjot datu minimizācijas principu; uzņēmums glabā personas datus ilgāk, nekā tas ir vajadzīgs un pati to ir noteikusi, pārkāpjot personas datu glabāšanas ierobežojuma principu; personas dati netika šifrēti u.tml.

Mācība Nr.2 : politiskā partija (Ungārija)

Pārkāpuma būtība

- Hakeris, izmantojot sistēmas ievainojamību, piekļuva datu bāzei ar personas datiem, kā rezultātā tā bija pieejama pat cilvēkiem ar minimālām IT zināšanām.

Atziņas

- Tika norādīts ne tikai uz apstākli, ka pārkāpums netika ziņots, bet uzsvērts arī tas, ka netika izpildīts dokumentēšanas pienākums.

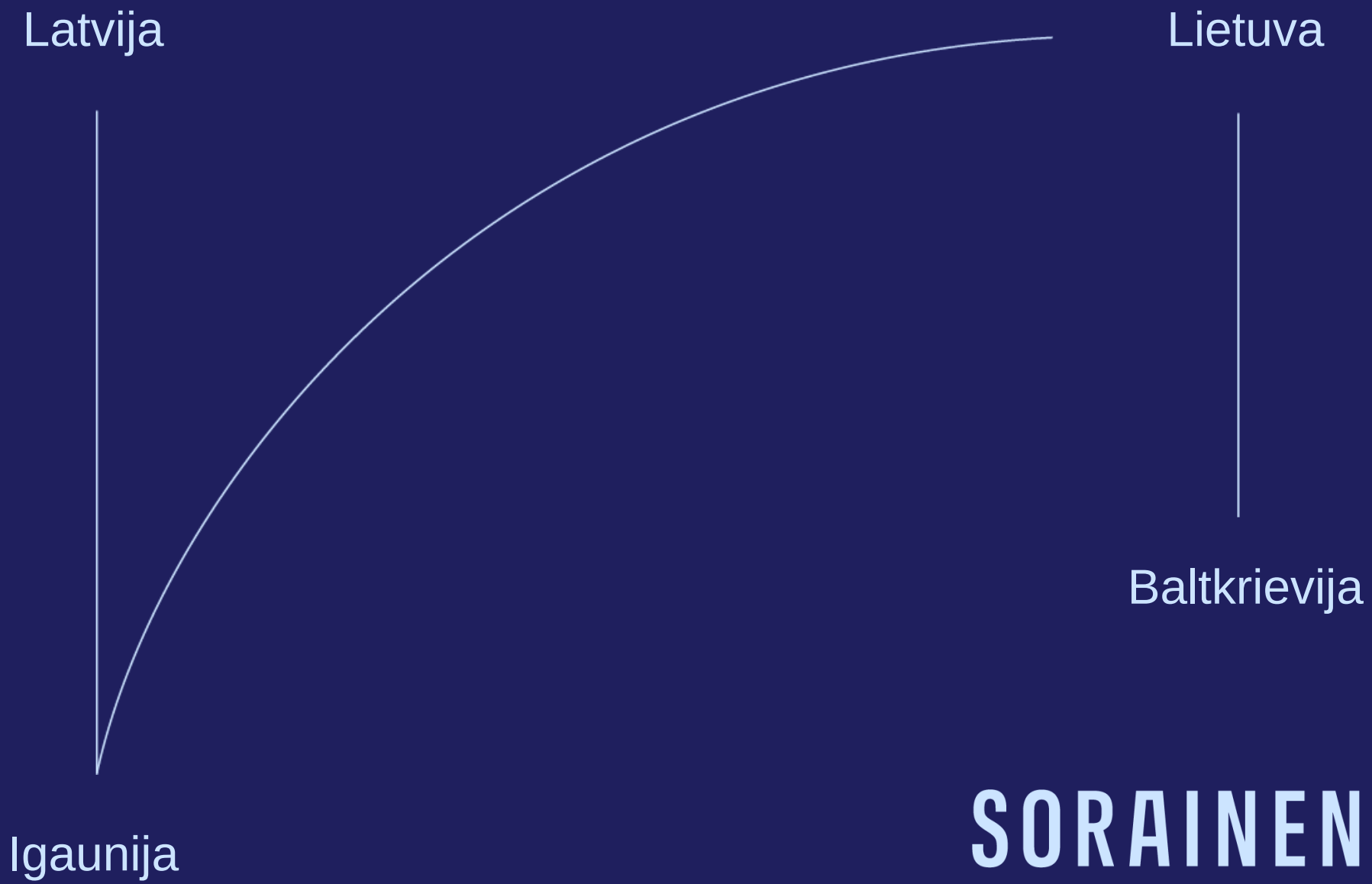
Mācība Nr.3 : National Government Service Centre (NGSC) (Zviedrija)

Pārkāpuma būtība

- Datu aizsardzības iestāde uzsāka izmeklēšanu pret NGSC, saņemot vairākus paziņojumus par personas datu pārkāpumiem saistībā ar kļūdu algu administrēšanas IT sistēmā. Kļūda radīja iespēju nesankcionēti piekļūt gan sistēmu izmantojošo iestāžu personāla, gan NGSC personāla datiem.

Atziņas

- Pārkāpuma izmeklēšana un koordinēšana nav notikusi pietiekoši ātri, jo iekšējo procedūru trūkuma dēļ, nebija skaidra rīcības plāna. Kā rezultātā par pārkāpumu netika ziņots savlaicīgi.



SORAINEN sorainen.com