# IEKŠĒJAIS AUDITS: KOPĪGI SASNIEDZOT ATBILSTĪBU GDPR

The Institute of Internal Auditors


Karlis Majevskis, President @ IIA Latvia
Internal audit manager @ Kesko
Digital Era 2018 Conference, Riga, 25.5.2018

# GDPR - DRAUDS VAI IESPĒJA?

?

# KAM JŪS UZTICĒTU SAVUS DATUS?

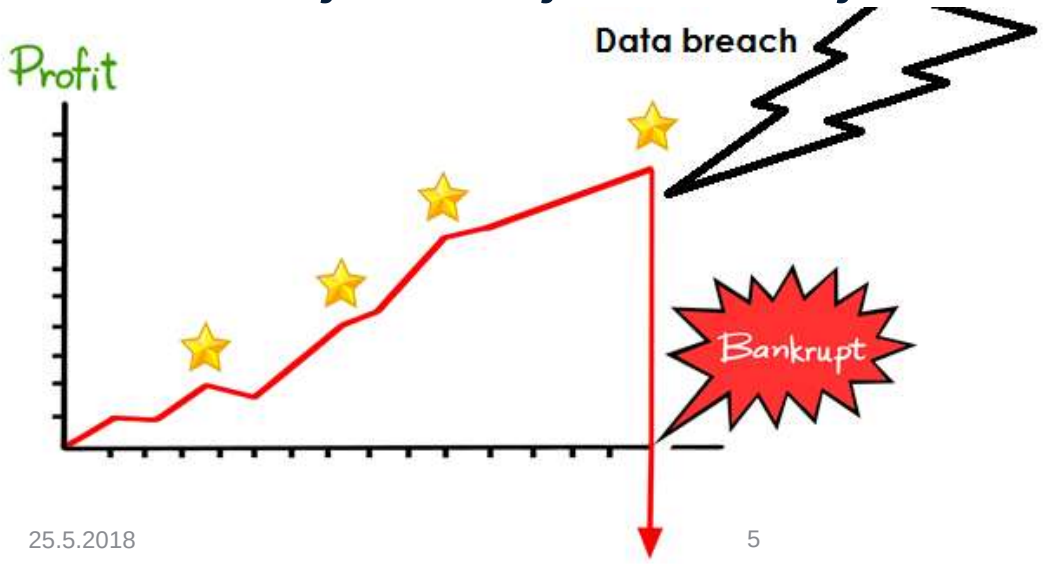
- Pārdevējs A
  - Vārds
  - Uzvārds
  - E-pasts
  - Tālrunis
  - Laulība
  - Ģimenes stāvoklis
  - Alga
  - Automašīna
  - Darba vieta
- Pārdevējs B
  - Vārds
  - Uzvārds
  - E-pasts

# VAI MĒS ZINĀM KAM IR MŪSU DATI?

- Pēdējās desmitgades laikā cilvēki ir nodevuši pārāk daudz savu privāto datu pakalpojumu sniedzējiem.
- Paceliet savu roku, ja jūs 100% zināt visas tīmekļa vietnes un organizācijas, kurām jūs kādreiz esat iesnieguši savus privātos datus


# IEMESLS KĀPĒC NEPIECIEŠAMA ATBILSTĪBA

- Vispopulārākais un dzirdamais iemesls, kādēļ organizācijām būtu jāpieņem GDPR, ir SODS.
- Bet patiesībā organizācijai vairāk jāuztraucās nevis par naudas sodiem, bet gan par uzticības zaudēšanu.
- IEDOMĀJATIES! ja ļaundariem ir jūsu klientu privātie dati, un tos var izmantot jebkas, jebkad un jebkādam nolūkam...



# KLIENTU ATTIEKSME PĒC DATU NOPLŪDES


- Data Breach impact study by Ponemon

# ATSLĒGAS VĀRDS - ATBILDĪBA

- Atbildība – ir īstā atslēga!
- GDPR jābūt daļai no organizācijas kultūras.
- Lai gan GDPR atbilstību var uzskatīt par risku, to vajadzētu uzskatīt par riska mazināšanas līdzekli.
- Organizācijām ir jāizmanto GDPR kā palīgs, lai mazinātu risku, kas saistīts ar datu pārkāpumu.

# UN KĀ IR AR AUDITORIEM….

# IZLASIET SARKANU GRĀMATU

# KAS IR IEKŠĒJIE AUDITORI?

- Iekšējais audits **palīdz organizācijai sasniegt tās mērķus, ieviešot sistemātisku, disciplinētu pieeju, lai novērtētu un pilnveidotu riska vadības, kontroles un pārvaldības procesu efektivitāti**.

# VAI IA IR ATBILSTOŠA LOMA ORGANIZĀCIJĀ?

***1100 – Neatkarība un objektivitāte***

- Iekšējā audita struktūrvienībai jābūt neatkarīgai, un iekšējiem auditoriem, veicot darbu, jābūt objektīviem.

***2110 - Pārvaldība***

- Iekšējā audita struktūrvienībai jānovērtē un jāsniedz atbilstoši pārvaldības procesu uzlabošanas ieteikumi:
  - stratēģisku un operatīvu lēmumu pieņemšanai;
  - risku vadības un kontroles pārraudzīšanai;
  - atbilstošas ētikas un vērtību veicināšanai organizācijā
  - <…..>

# VAI DARBS IR FOKUSĒTS UZ SVARĪGĀKIEM RISKIEM?

***2010 – Plānošana***

- Iekšējā audita vadītājam jāizveido **uz riskiem balstīts plāns**, kurā noteiktas iekšējā audita struktūrvienības prioritātes, kas saskan ar organizācijas mērķiem.

**2120.A1 – *Risku vadība***

- Iekšējā audita struktūrvienībai jāizvērtē ar organizācijas pārvaldību, darbībām un informācijas sistēmām saistītais risks attiecībā uz:
  - Organizācijas stratēģisko mērķu sasniegšanu;
  - finanšu un operatīvās informācijas ticamību un konsekvenci;
  - darbību un programmu efektivitāti un lietderību;
  - aktīvu aizsardzību
  - **atbilstību normatīvajiem aktiem**, politikām, procedūrām un līgumiem.

# VAI KOMANDA IR PIETIEKOŠI IZGLĪTOTA?

***1210 – Lietpratība***

- Iekšējiem auditoriem jābūt zināšanām, iemaņām un prasmēm, kas vajadzīgas viņu individuālo pienākumu vai struktūrvienības uzdevumu veikšanai, vai tās jāiegūst.

***1230 – Pastāvīga profesionālā izaugsme***

- Iekšējiem auditoriem jāpilnveido zināšanas, iemaņas un prasmes, pastāvīgi rūpējoties par savu profesionālo izaugsmi.

# SEŠI REGULAS PRINCIPI VIEGLI SAPROTAMĀ FORMĀ


1. Likumīgums, godīgums un pārredzamība
2. Precizitāte
3. Konfidencialitāte
4. Mērķa ierobežojums
5. Glabāšanas ierobežojums
6. Datu minimizēšana

# IEKŠĒJIEM AUDITORIEM VAJAG RĪKOTIES!

- Iekšējais audits var un tam vajadzētu uzņemties līderību pirms, 2018. gada 25. maija un pēc tam.
- Gada audita plāna pielāgošana - GDPR ir tieši tas ko iekļaut uz riskiem balstītajam gada plānam
- Iekšējam auditam jāpalīdz paaugstināt izpratni visos organizācijas līmeņos un nepārtraukti pielietot uz risku balstītu pieeju auditiem.

# DAŽI PRAKSTISKI PADOMI

**1. Izpratne**

Jums vajadzētu pārliecināties, ka lēmēji un galvenie jūsu organizācijas darbinieki apzinās, kas ir GDPR. Viņiem ir jāapzinās ietekme uz organizāciju.

**2. Jūsu rīcībā esošā informācija**

Jums vajadzētu dokumentēt, kādi jūsu rīcībā esošie personiskie dati, no kurienes tie tika saņemti un ar ko jūs tos kopīgojat. Jums var būt nepieciešams organizēt informācijas auditu.

# DAŽI PRAKSTISKI PADOMI

**3. Informācija par konfidencialitāti**

Jums ir jāpārskata jūsu pašreizējie paziņojumi par konfidencialitāti un jāievieš plāns, lai veiktu nepieciešamās izmaiņas GDPR ieviešanas ietvaros.

**4. Indivīdu tiesības**

Jums vajadzētu pārbaudīt savas procedūras, lai nodrošinātu, ka tās aptver visas personas tiesības, tostarp to, kā jūs izdzēsīsiet personas datus vai nodrošināsiet to pieeju datu subjektam.

# DAŽI PRAKSTISKI PADOMI

**5. Likumīgais datu apstrādes pamats**
Jums ir jāidentificē jūsu datu apstrādes likumīgais pamats, dokumentējiet to un izskaidrojiet to datu subjektiem

**6. Piekrišana**
Jums būtu jāpārskata, kā jūs saņemat, reģistrējat un pārvaldāt piekrišanu. Atjauniniet pašreizējās piekrišanas tagad, ja tie neatbilst GDPR standartam.

# DAŽI PRAKSTISKI PADOMI

**8. Bērni**

Jums vajadzētu sākt domāt par to, vai jums ir jāievieš sistēmas, lai pārbaudītu personu vecumu un saņemtu vecāku vai aizbildņa piekrišanu jebkurai datu apstrādes darbībai.

**9. Datu pārkāpumi**

Jums vajadzētu pārliecināties, ka jums ir piemērotas procedūras, lai atklātu, ziņotu un izmeklētu personas datu aizsardzības pārkāpumu.

# DAŽI PRAKSTISKI PADOMI

**10. Līgumi**

Pārbaudiet vai jums ir atbilstoši līgumi ar trešām pusēm kurām jūs nododat datus

**11. Atbildības un lomas**

Vai ir nodefinēts kas ir datu apstrādātājs, kontrolieris. Pie kā datu subjekts var vērsties.

# PROGRESS THROUGH SHARING!!!

Iekšējo Auditoru Institūts

*Progress caur sadarbību*

Visit us at http://iai.lv