Martina Marinović, DPO u MPG

Stanko Cerin, direktor Ostendo Consulting

Aleksandar Crnković, odvjetnik

Moderator: Biljana Cerin

# 2 GDPR MASTERCLASS

Kolačići, da ili ne?

Kako zaštititi svoja prava?

Kako se obraniti od upornog odvjetnika?

Kako Možemo biti sigurni da smo sve dobro napravili na webu?

Što s ostalim javnim objavama (nagradne igre, mediji, fotografije...?

Ostendo
THE ACHIEVING GROUP

# 2 GDPR MASTERCLASS

**Mjere smanjenja rizika sa najboljim omjerom utrošenog i postignuta**

Ostendo
THE ACHIEVING GROUP

# Ostendo Consulting

- Specijalizirani za upravljanje usklađenošću i rizicima informacijske sigurnosti.
- Osnovana je 2011. godine u Londonu i Zagrebu, od kada svoje savjetodavne usluge pruža uglavnom vodećim tvrtkama na engleskom i hrvatskom govornom području, klijentima u visoko-reguliranim industrijama poput:
  - Financijska industrija (zaštita informacija u bankama, osiguravateljima i poreznoj upravi)
  - Zdravstvo i biotehnologija (zaštita privatnosti podataka o pacijentima i zaštita poslovne tajne)
  - Telekomunikacije (globalni projekti dizajna sigurnosnih arhitektura i zaštite osobnih podataka)
  - Energetika (analize sigurnosti i dizajn sigurnosnih arhitektura i rješenja)
  - Državna uprava (analiza sigurnosti podataka i dizajn arhitektura i rješenja za njihovu zaštitu)

# Postupak GDPR usklađivanja?

- Imenovanje odgovorne osobe za savjetovanje o obradama osobnih podataka (DPO gdje treba)
- Dodjela resursa DPO-u – Kojih i zašto?
- Identifikacija obrada i dokumentiranje
- Identifikacija pravnih osnova obrada

# Kako se identificiraju obrade?

- Top – Down
- Bottom -  Up

# Top -Down

- Razgovori s odgovornim osobama
- Identifikacija
  - obrada
  - razloga iz koje se obrade provode
  - pravne osnove
  - i ostalih elemenata iz čl.13

# Zašto uopće trebamo evidenciju?

- ?
- NE MOŽEMO UPRAVLJATI RIZICIMA AKO NE ZNAMO ŠTO RADIMO
- …. i Nadzorno tijelo će je možda tražiti

# Evidencija i rizici

- Veza na poslovne procese I IT servise
  - Tko što radi u obradi?
  - Imamo li snimku kompletnog toka podataka kroz obradu?
  - Kako znamo da će osobe uključene u obradu štititi podatke?
    - Odgovorno se odnositi prema njima
    - Čuvati tajnost
    - Neće zloupotrebljavati
    - Uključiti se u identifikaciju rizika
  - Kako znamo da su IT servisi koji su uključeni u obradu sigurni?
    - Upravljanje informacijskom sigurnošću
    - IT revizije (end-to-end - od početka do kraja obrade)

# Top Down - minusevi

- Daje informaciju o tome:
  - kako management misli da poslovni procesi izgledaju (gotovo nikad nisu takvi)
  - Gdje management misli da su podaci
  - Mjerama za koja management misli da su uspostavljene

# Bottom - Up

- Data discovery
  - Gdje se podaci stvarno nalaze i koliko ih je?
  - Rezultati su impresivni!

# Glavni izazovi

- Prepoznavanje podataka (točno)
- Brzina
- Management rezultata (što s njima?)

# Izazovi

- Email
  - Skaniranje maila zahtijeva pristup mailbox i samo po sebi je rizik
  - Dio podataka je u arhivama do kojih mail server ne može doći
- Nestrukturirani podaci
  - Količine su u PB
  - Sporost
  - Velik broj pronađenih podataka
- Strukturirani podaci
  - Utjecaj na performance produkcijskih sustava

# Pravilo broj 1

- MINIMIZACIJA

  NE PRIKUPLJATI SUVIŠNO

# UKLONITI VIŠAK!

# Data discovery vs DLP

- Bolje se snalazi s raznim vrstama meta
- Omogućava provedbu akcija nad podacima (brisanje, anonimizacija…)

- U pravilu mora učiti prije primjene
- Izvorno zamišljen za skaniranje u realnom vremenu i prevenciju kršenja politika
- End point security – kompleksna instalacija

# Projekt minimizacije

- Identifikacija osobnih podataka
- Usporedba sa evidencijom aktivnosti obrada
- Identifikacija suvišnih podataka -> uklanjanje
- Identifikacija sivih zona -> kriptiranje, karantena

- Da ne pričamo o milijunima, ovo bi bilo jednostavno - ali pričamo!

# Hvala!

info@ostendogroup.com