

WEBINARIUM

Mäta GDPR-efterlevnad

Varmt välkomna!



Julianne



Daniel

WEBINARIUM

Mäta efterlevnad

Innehållet i dagens webinarium är generellt utformad information och utgör inte juridisk rådgivning. Kontakta gärna oss om ni önskar stöd.

Hur utvärderar ni ert GDPR-arbete?

- A) Utfall jämfört med uppsatt målbild för året (egna mål)
- B) Utifrån mängd eller avsaknad av klagomål (berördas upplevelse)
- C) Extern återkommande granskning (objektiv)
- D) Annat... (tipsa gärna i chatten)

Dagens fråga!



Julianne



Daniel

01

GDPR:s krav på att mäta efterlevnad

- Riskbaserat arbete
- Ansvarsskyldighet (art. 5.2)
- M.m...

Ställ gärna frågor i chatten så fångar vi upp dem längs vägen!

02

'Are we there yet?'

- Mognadsmodeller
- Proaktivt vs reaktivt
- Successivt framflyttad målbild och objektiv översyn

03

Gör det lätt för er!



Vilka är vi



- Fullservice-byrå inom dataskydd och integritetsfrågor
- Digitalt GDPR-verktyg
- Utbildning, konsultrådgivning och projektledning

E-learning



Klassrumsutbildning



GDPR-verktyg



Del 1 - GDPR:s krav på att mäta efterlevnad

"Vad kräver GDPR – och varför räcker det inte med policies?"

Artikel 5.2 – ansvarsskyldighet (accountability)

”Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs [principerna]”.

- Planera en laglig behandling [laglig grund, ändamål, uppgiftsminimering, lagringsminimering]
- Berätta om den [öppenhet]
- Reagera [korrekthet, relevans]
- Hålla uppgifterna säkra (se nedan) [integritet och konfidentialitet]

Riskbaserat angreppssätt (Artikel 24 och skäl 76)

”Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

[...]

Lämpliga strategier för dataskydd.”

 Del 2 – 'Are we there yet?'

"Vad kräver GDPR – och varför räcker det inte med policies?"

Artikel 5.2 – ansvarsskyldighet (accountability)

"Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs [principerna]".

- Planera och styra en laglig behandling [laglig grund, ändamål, uppgiftsminimering, lagringsminimering]
- Berätta om den [öppenhet]
- Reagera [korrekthet, relevans]
- Hålla uppgifterna säkra (se nedan) [integritet och konfidentialitet]

Riskbaserat angreppssätt (Artikel 24 och skäl 76)

"Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

[...]

Lämpliga strategier för dataskydd."

Intern policy, utbildning, SOP, styrdokument artikel 30-register, ansvarsfördelning leverantörer/partners (DPA, ...).

Personuppgiftspolicy, cookie-policy, sidfot, email-signatur, ...

Löpande utvärdera behov, föra statistik kring svar på förfrågan, mäta hur många som läser policy, fokusgrupper. Interna och externa incidentrapporter.

DPIA, årshjul, mötesprotokoll, audits,

"Att värdera sin dataskyddsnivå – hur ser man om man är på rätt väg?"

Mognadsmodeller (maturity models):

- 1. Nonexistent – inget är gjort.**
- 2. Initial – ad hoc-insatser.**
- 3. Repeatable – viss struktur, men beroende av enskilda.**
- 4. Defined – processer är formaliserade centralt.**
- 5. Managed – styrning och mätning finns.**
- 6. Best in class + följer samtliga rekommendationer (EDPB)**

Reflektionsfrågor att ställa till sig själv eller sin organisation:

- Är vårt arbete reaktivt eller proaktivt?
- Vem vet vad som gäller – alla eller bara dataskyddsombudet?
- Kan vi visa bevis på våra påståenden?

Problematisera idén om "compliant eller inte compliant". GDPR är inte en bocka-av-lista, det är ett systematiskt arbete.

Vad tycker ni är svårast
att mäta?

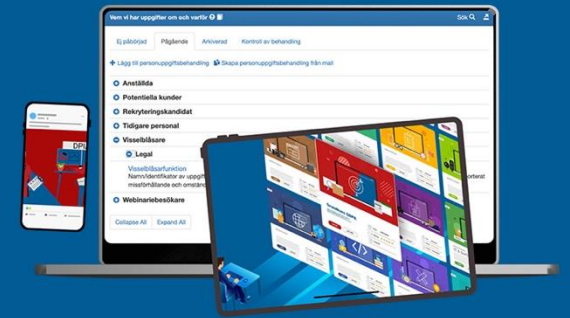
Fråga!

Del 3 – Så hjälper GDPR Hero Register till

Vad skulle underlätta
mest i ert GDPR-arbete
framöver?

Fråga!

Vill du ha mer information om vårt GDPR-verktyg?



Kontakta oss: info@gdprhero.se