GDPR-granskning Valnämnden

2021-09-17

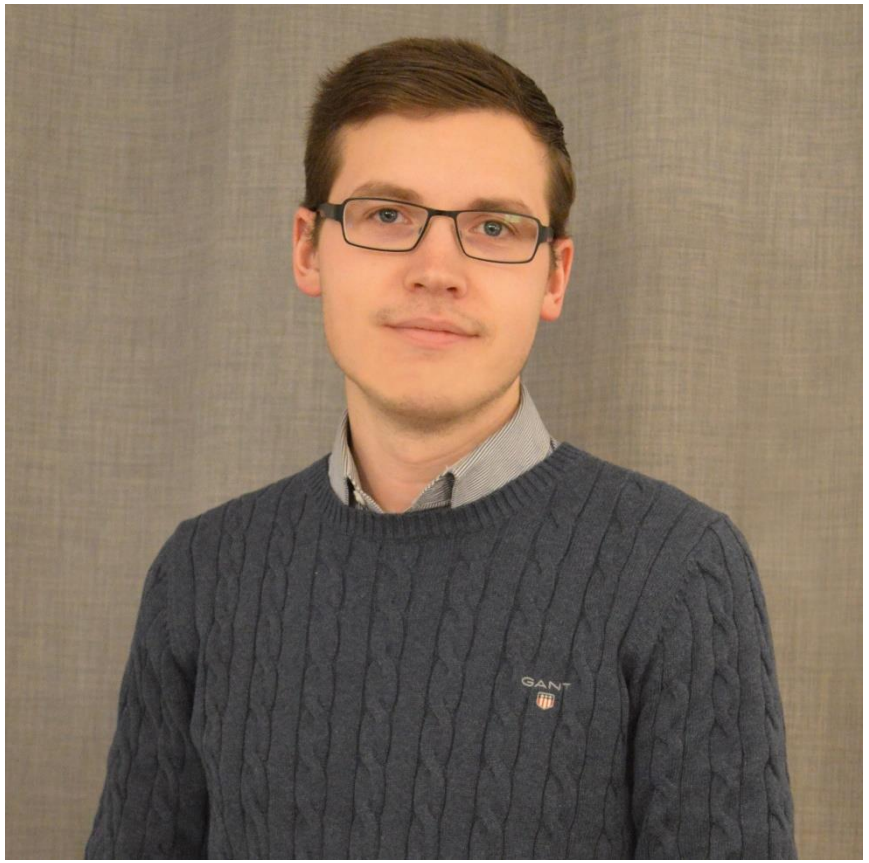
Patrik Jonasson

Patrik Jonasson
Externt dataskyddsombud

Grundare och delägare IT-Säkerhetsbolaget
ISO 27001 och 27701
Certifierad informationssäkerhetsarkitekt
Externt Dataskyddsombud för flera organisationer
Informationssäkerhetsspecialist
Tekniska säkerhetsgranskningar
Bor i Sundsvall

LinkedIn https://www.linkedin.com/in/patrikjonasson/
Mail: Patrik.jonasson@gavle.se
Telefon 0709-249 250
Lägg gärna till mig på LinkedIn!

Gustav Öst
Dataskyddsombud



Agenda

- Vad är GDPR?
- Goda effekter av ett systematiskt GDPR-arbete
- Vilka negativa konsekvenser har andra drabbats av?
- Styrelsens ansvar
- Granskning av Valnämndens dataskyddsarbete
- Summering

Förutsättningar

Tid: 45 minuter

Ni får presentationen efteråt

Det finns tid i slutet för frågor

Granskningsområden

GDPR-organisation

Register över personuppgiftsbehandlingar

Konsekvensbedömningar

Registrerades rättigheter

Kunskap om GDPR

Personuppgiftsincidenter

Inbyggt dataskydd och dataskydd som standard

3:e-landsöverföringar (Schrems II)

Personuppgiftsbiträdesavtal

Hantera ostrukturerad information

Intervjuade personer

- Linda Löfvenius

Vad är GDPR?

GDPR på tre minuter

- *Till skydd för mänskliga rättigheter*
- *Underlätta digitalisering*
- *Påverkar nästan hela planeten!*
  Ca 1 200 000 org. Bara i Sverige
- *Följa samt visa att man följer*
- *Ska tillämpas från 2018-05-25 och framåt*

- Inventera personuppgifter
- Tydligare informationssäkerhetskrav
- Rapportera personuppgiftsincidenter inom 72 timmar
- Sanktionsavgifter och skadestånd-även för myndigheter
- Allt är inte klart än- förtydliganden kommer 2021-2022
- Ger massor med positiva effekter!

Dataskyddsombud

- Dataskyddsenhetens arbetsområden
- Obligatoriskt för myndigheter att utse
- Självständig roll
- Inget verksamhetsansvar
- Övervakande och stödjande roll
- Kulturbärare
- Kan inte avsättas eller bli föremål för sanktionsavgift för utförd arbetsuppgift
- Rapporterar direkt till högsta förvaltningsnivå, dvs nämnd/bolagsstyrelse
- 27 personuppgiftsansvariga

Adrian Vinsa	Patrik Jonasson/Gustav Öst
Omvårdnadsnämnden	Kommunstyrelsen
Socialnämnden	Utbildningsnämnden
Arbetsmarknads- och funktionsrättsnämnden	Kultur- och fritidsnämnden
Gävle Hamn AB	Samhällsbyggnadsnämnden
Gavliakoncernen	Överförmyndarnämnden
AB Gavlegårdarna	Gästrike Vatten AB
SKFAB	Gävle Energi AB
Gävle Parkeringsservice AB	Ekogas AB
Ockelbo kommun	Valnämnden
Hofors kommun	
Hoforshus AB	
Ockelbogårdar AB	

Ordlista

Några bra ord, som du bör förstå om du ska kunna ta del av innehållet i granskningen

Personuppgifter

varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Dvs allt som direkt eller indirekt kan kopplas till en levande människa.

Extra skyddsvärda personuppgifter

- Personnummer
- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden.

Känsliga personuppifter

- ras eller etniskt ursprung,
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- personuppgifter som rör hälsa eller sexualliv.
- Uppgifter om hälsa kan vara till exempel sjukfrånvaro, graviditet och läkarbesök
- behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person
- uppgifter om en fysisk persons sexuella läggning

Personuppgiftsansvarig (data controller)

En personuppgiftsansvarig är den **organisation** som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Personuppgiftsansvarig är normalt den juridiska person (till exempel aktiebolag, stiftelse eller förening) eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till.

Personuppgiftsbiträde (data processor)

Personuppgiftsbiträde är den **organisation** som behandlar personuppgifter för den personuppgiftsansvariges räkning, exempelvis en tjänsteleverantör eller webbhotell. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen.

Goda effekter av ett systematiskt dataskyddsarbete

- Hållbar digitalisering
- Skyddar vårt varumärke
- Minskad risk för sanktionsavgifter
- Nöjdare medarbetare
- Ordning och reda

Exempel på negativa konsekvenser av ett undermåligt dataskyddsarbete

- Statens Servicecenter 250 000 SEK
- Skellefteå kommun 200 000 SEK
- 1177.se (14 miljoner)
- Vastaamo (Konkurs)
- 435 utdömda sanktionsavgifter sedan 25 maj 2018 på totalt € 1.2 miljarder i EU i totalt 765 fall
- IMY (Datainspektionen) beslutade om 150 milj. SEK 2020

Vad är styrelsens/nämndens ansvar för organisationens dataskydd?

- Tillse att det finns tillräckliga resurser utifrån beslutad ambitionsnivå med dataskyddet
  - Beslutad dataskyddsorganisation med den kompetens, tid och de IT-stöd som krävs utifrån aktuell risknivå
- Omvärldsbevaka
  - Kunder
  - Ägare
  - Andra organisationer i samma bransch
  - Sverige
  - EU

Vilken ambitionsnivå har ni med ert dataskyddsarbete?

Vilken ambitionsnivå har ni med ert dataskyddsarbete?

1.Initial

Dataskyddet som helhet kännetecknas av att den **skapas varje gång för ett specifikt projekt,** och ibland till och med som kaotiskt. Endast ett fåtal processer identifieras och framgången beror på individers insatser.

2. Repeterbar

De viktigaste delarna i dataskyddsprocesserna har upprättats som gör att du kan spåra hur du ska arbeta. **Processen är etablerad,** vilket är nödvändigt för att upprepa de framgångar som uppnåtts tidigare. **Medveten om integritetsrisker.**

3. Definierad (den nivå jag har granskat mot)

Dataskyddsprocessen dokumenteras och standardiseras för både lednings- och designarbete. **Denna process är integrerad i organisationens övriga processer som informationssäkerhet och kvalitetsprocesser. Alla i organisationen följer anvisade processer.**

4. Strukturerad

Detaljerade kvantitativa indikatorer för dataskyddsprocessen och kvaliteten på den hur dataskyddet i organisationen **mäts**. Kvaliteten på dataskyddet **utvärderas och kontrolleras ur kvantitativ synvinkel**.

5. Optimerad

Kontinuerlig processförbättring uppnås genom kvantitativ feedback från processen och implementering av avancerade idéer och tekniker. **Ambassadör**-hjälper andra att höja sitt integritetsskydd

Granskning av Valnämndens dataskyddsarbete

Granskningsområden

GDPR-organisation

Register över personuppgiftsbehandlingar

Konsekvensbedömningar

Registrerades rättigheter

Kunskap om GDPR

Personuppgiftsincidenter

Inbyggt dataskydd och dataskydd som standard

3:e-landsöverföringar (Schrems II)

Personuppgiftsbiträdesavtal

Hantera ostrukturerad information

GDPR-organisation

Säkerställ att ni har en beslutad dataskyddsorganisation där rollen dataskyddssamordnare har en minimitid per vecka för dataskyddsfrågor så att identifierade risker och brister hanteras inom rimlig tid.

Register över personuppgiftsbehandlingar

Ert register är inte komplett. Det saknas information på flera ställen. Ni har sannolikt identifierat för få behandlingar. Registret uppdateras inte kontinuerligt.

Ni skulle också kunna använda registret för andra nyttor inom dataskyddsarbetet som är möjligt. Vill se ett uppdaterat register enligt GDPR:s krav.

Konsekvensbedömningar

Ni har inte genomfört några konsekvensbedömningar. Alla behandlingar som är särskilt riskfyllda måste ni göra en konsekvensbedömning för i enlighet med artikel 35.

Kunskap om GDPR

Genomför en kortare lärarledd utbildning för alla medarbetare.

Personuppgiftsincidenter

Totalt noll rapporterade incidenter på 3,5 år, vilket är onormalt lågt. Lägg mycket tid på vikten av personuppgiftsincidenter i framtida utbildningar.

Radera e-post som ej är allmänna handlingar (arbetsmaterial)

Enligt GDPR ska personuppgifter som inte längre behövs raderas. Vill därför se en plan för hur ni gallrar e-post.

Summering:

Summering: Identifierade risker och brister

Önskar beslut av Valnämnden i följande frågor inom en månad

- Er ambitionsnivå med organisationen dataskyddsarbete
- Vilka identifierade risker och brister som kommer åtgärdas med tidpunkt, handlingsplan och ansvarig person

Patrik Jonasson
Externt dataskyddsombud

Grundare och delägare IT-Säkerhetsbolaget
Certifierad informationssäkerhetsarkitekt
Externt dataskyddsombud
Tekniska säkerhetsgranskningar
Informationssäkerhetsexpert
Bor i Sundsvall

LinkedIn https://www.linkedin.com/in/patrikjonasson/
Mail: Patrik.jonasson@gavle.se
Telefon 0709-249 250

Lägg gärna till mig på LinkedIn!