GDPR

UTBILDNINGSDAG SKKF
2018-10-25

Vad ska vi prata om idag?

- Presentation Andreas
- Bakgrund till GDPR
- Personuppgifter och känsliga personuppgifter
- Rättslig grund för att behandla personuppgiftsbehandling
- Generella konsekvenser
- Att tänka på för anställda inom krematorieverksamhet
- Tips
- Frågor

Varför GDPR?

- GDPR - General Data Protection Regulation (Dataskyddsförordningen)
- Anpassad för att hantera ökad digitalisering i samhället (internet, sociala nätverk, big data)
- Harmonisering av lagstiftningen inom EU
- Stärka enskilda individers rättigheter
- Ökad kontroll vid personuppgiftsbehandling
- Ökade krav på tydligare roller och ansvar

Begrepp inom GDPR

- **Den registrerade** - Den som en personuppgift avser, ex anhörig, anställd, individ hos en leverantör
- **Personuppgiftsansvarig** - Den organisation (församling, pastorat) som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till.
- **Dataskyddsombud (DPO)** - utses på för att säkerställa att behandlingen av personuppgifter hanteras korrekt genom att utföra kontroller och utbildning. Svenska Kyrkans Arbetsgivarorganisation (SKAO) rekommenderar att varje församling har ett dataskyddsombud.
- **Personuppgiftsbiträde** - Den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation.

GDPR - vad händer i Sverige?

- GDPR gäller from 2018-05-25
- PUL upphävdes
- Datainspektionen tillsynsmyndighet i Sverige (föreskrifter, allmänna råd och sanktioner)
- Regel om undantag för ostrukturerade data, missbruksregeln (löpande text på internet, ordbehandlingsprogram, mail etc) tas bort
- Förslag på lag i Sverige – dataskyddslagen

Vad är en personuppgift?

- Datainspektionen - ”All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet”.
- Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns.
- Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer.

Vad är en känslig personuppgift?

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös övertygelse
- Medlemskap i fackförening
- Hälsa (sjukfrånvaro, graviditet, läkarbesök)
- Sexuell läggning

I princip förbjudet att behandla **känsliga personuppgifter.** Det finns dock en rad undantag (ex uttryckligt samtycke, sjukvård).

Måste skyddas mer än andra uppgifter.

Rättslig grund? När behandling är tillåtet!

- Behandlingen är nödvändig för att ett **avtal** med den registrerade ska kunna fullgöras
- Om den registrerade har lämnat sitt **samtycke**, det vill säga godkänt behandlingen
- **Rättslig förpliktelse**, behandlingen är nödvändig för att uppfylla lagar (ex begravningslagen, arkivlagen, bokföringslagen etc)
- **Intresseavvägning**, om organisationen kan visa att dess intresse av att hantera uppgifterna väger tyngre än den enskildes rätt till privatliv.

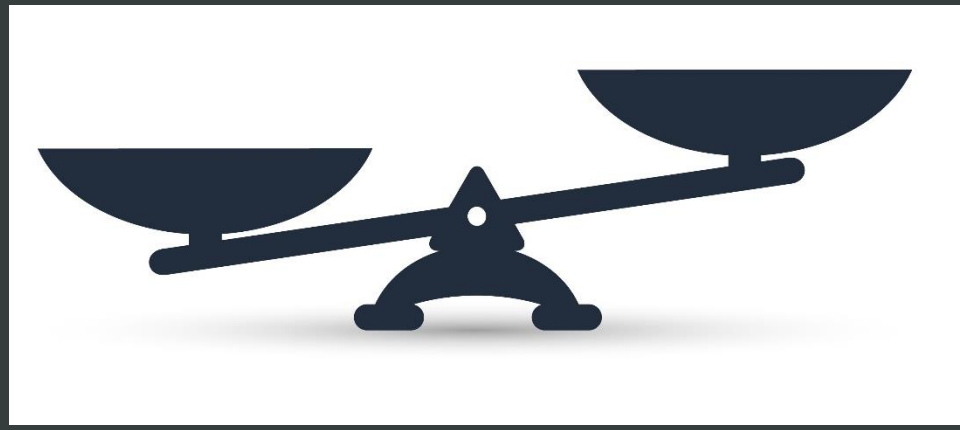
- **Undantag:** myndigheters register, till exempel inom polisen eller sjukvården

Exempel på rättsliga grunder

- Anställda som behandlas i ett lönesystem - Avtal
- Kunder registrerad i ett kundregister - Avtal
- Register med potentiella kunder - Intresseavvägning
- Webbplatsen - Samtycke eller intresseavvägning

Konsekvenser av GDPR – en översikt!

- Enskilda individers rättigheter stärks
- Högre krav för samtycke
- Kännbara sanktioner vid överträdelse
- Skärpta krav vid personuppgiftesincidenter
- Ökade krav på tydliga roller och ansvar
- Privacy by design (IT-system)
- Konsekvensbedömning/riskanalys (PIA)
- Hårdare krav vid gränsöverskridande behandling



Den enskildes rättigheter

Den enskilde individen har rätt att:

- Få personuppgifter raderade (rätten att bli glömd)
- Få personuppgifter förflyttade (dataportabilitet)
- Rätt till tydlig och omfattande information om vilka personuppgifter som behandlas

Detta innebär att:

- Rutiner och systemstöd för att kunna hantera gallring, radering och dataportabilitet
- Rutiner för förfrågningar och systemstöd för att säkerställa att den enskilde individen får tillräcklig och rätt information

Krav på samtycke

- Samtycke lämnas ***frivilligt, specifikt och otvetydigt***
- Samtycke ska vara ***urskiljbart***

Detta innebär:

- Nytt samtycke bör inhämtas om befintligt inte uppfyller ovan krav
- Rutiner för hur samtycke inhämtas och lagras bör ses över
- Kontrollera att samtycker är spårbart (loggas)

Sanktioner

Datainspektionen kan utdöma sanktioner upp till max 20 miljoner Euro eller 4 procent av global årsomsättning vid överträdelser

1. Reprimand/varning
2. Förbud att utföra viss behandling
3. Sanktionsavgift

Detta innebär att:

- Efterlevnad av GDPR prioriteras (styrelse, ledning)

- Organisationer måsta kunna visa upp ett bra skydd av personuppgifterna som behandlas

Utökande krav på roller och ansvar

- Personuppgiftsansvarig - bestämmer vilka uppgifter som ska behandlas och vad de ska användas till.
- Personuppgiftsbiträde - behandling av personuppgifter för annans räkning, ex outsourcing av IT-drift, administration, systemförvaltning etc. Eget ansvar att efterleva GDPR.
- Dataskyddsombud (DPO)

Detta innebär att:

- Etablera och kommunicera roller och dokumentera ansvar

- Upprätta avtal för personuppgiftsbiträden, kravställ efterlevnad med GDPR

Incidentrapportering

- Vid incident som kan äventyra skyddet av den enskildes personuppgifter
  - Anmälan till Datainspektionen inom 72 timmar
  - Information till den enskilde utan dröjsmål
  - Gäller även leverantörer som hanterar personuppgifter

Detta innebär att:

- Införa riskbaserade metoder och processer för att upptäcka, rapportera och utreda personuppgiftsincidenter
- Utse roller och ansvar för personuppgiftsincidenter
- Kravställ incidentrapporteringsprocess hos leverantör

Exempel på incidenter

Tidigare Facebook-anställd säger att hemlig datainsamling var rutin

PUBLICERAD 20.03.2018 - 17:33. UPPDATERAD 20.03.2018 - 19:03

DELA: 18

Banken skickade kända politikerns känsliga uppgifter fel

EKONOMI En IT-företagare ville testa personuppgiftslagen GDPR och begärde ut sina känsliga uppgifter från banken. Det gick så där – istället fick han det lokala kommunalrådets uppgifter om lån, konton och bankärenden.

Övriga konsekvenser

Privacy by design

- Inbyggd integritet
- Integritets- och skyddsaspekter ska tas om hand genom ett IT systems **hela** livscykel

PIA (Privacy Impact Assessment)

- Utökade krav på dokumentation samt risk- och konsekvensbedömning av personuppgifter. Syftet är att införa skydd av personuppgifter baserat på risk och dokumentera tagna beslut

Gränsöverskridande behandling

- Krav på adekvat skyddsnivå för överföring till tredje land
- Personuppgifter i molnet - kontrollera leverantören

Datainspektionens granskningar

- Hösten 2018

- Roller och ansvar (dataskyddsombud)
- Samtycken
- Gränsdragningen mellan personuppgiftsansvarig och personuppgiftsbiträden
- Granskningar baserade på tips från allmänhet

Vad bör krematoriepersonal ha koll på?

- **Stöd och riktlinjer** specifikt framtagna för er verksamhet - **Läs igenom detta!**

- **Svenska kyrkans arbetsgivarorganisations** information om GDPR

- I webbaserade **handboken Beda** finns uppdaterade blanketter, förslag på personuppgiftsregister och förslag till integritetspolicy

- Blanketter som används i **centrala IT-system** (bla Enjac) är uppdaterade

- Information till den registrerade, mallar för detta är framtagna

- Internwww.svenskakyrkan.se/dataskydd finns information om GDPR. Gå in och kika där med jämna mellanrum!

- **Hur sparas och skyddas fysiska dokument?**

- dödsbevis, beställningsdokument, kremeringsintyg, dagregister, kremeringsjournaler etc

- **Vem ska jag kontakta vid frågor?**

Tips och kom ihåg!

- Spara endast de personuppgifter ni verkligen behöver
- Lagra personuppgifter i centrala IT-system, undvik egna register (ex excel) och fysiska dokument om det går
- Använd GDPR-anpassade mallar som SKAO tagit fram
- Skydda personuppgifterna som ni hanterar - Om ni råkar ut för en ”personuppgiftsincident” måste ni informera församlingen/pastoriatet för vidare rapportering till Datainspektionen. Ett exempel kan vara ett usb-minne med personuppgifter som tappats bort.
- Använd sunt förnuft - Tänkt en extra gång när du behandlar personuppgifter, är detta känsligt? Går det att maila oskyddat?
- Bättre att fråga än att våga! Kontakta församlingens dataskyddsombud vid frågor.
- Lär dig mer på datainspektionens hemsida (www.datainspektionen.se)

Frågor?

TACK FÖR MIG!

Andreas Persson

andreas@awpconsulting.se

073-335 94 25