Dataskyddsförordningen 2018

Adress till denna presentation:
bit.do/gdprant

Ant Simons
Webbhuset.

- Vi talar om *dataskyddsförordningen* och *GDPR General Data Protection Regulation*
- Trädde i kraft 24.5.2016, gäller i Finland fr.o.m. 25.5.2018
- Dataskyddslagen stiftas i Finland, ersätter nuvarande Personuppgiftslagen (PuL)
- Dataskyddsombudsmannen blir dataskyddsmyndigheten

Perspektivet ändras:
Tidigare: ansvar att från att följa lagen
Nu: ansvarsskyldighet att säkerställa att lagen följs

Lagen gäller alla som behandlar personuppgifter men ansvaret ligger hos organisationen

Kräver inbyggt dataskydd och dataskydd som standard
Privacy and Security by Design

Inför ett “konsumentskydd” för personuppgifter.

Personuppgifter bör behandlas lika som vi idag behandlar PENGAR i en organisation.

Vad händer?

- Styrelsen i organisationen blir personuppgiftsansvarig och därmed ansvarig för att förordningen följs
- Styrelsen får ansvaret att *säkerställa* att planering, rutiner, regelverk, avtal, samtycke, dokumentering och utbildning förverkligas
- Människor får nya rättigheter, t.ex. rätt att få sin data i maskinläsbar form och rätt att bli bortglömd
- Dataskyddsmyndigheten får rätt att bötfälla (med böter upp till 4% av omsättningen)
- Personuppgiftsincidenter måste anmälas inom 72 timmar.

Behandling av personuppgifter

Möjligheter för tredje sektorn

- Använda det goda ryktet och stärka förtroendet
- Intressebevakning och utbildning för medborgare
- Mera träffsäker marknadsföring och informationsspridning, kvalitet framom kvantitet

Definitioner

- En personuppgift
- Behandling av personuppgift
- Register
- Personuppgiftsansvarig
- Personuppgiftsbiträde

Art 4.1: personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person, 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

Art 4.2: behandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring

Art 4.6: register: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

Art 4.7: personuppgiftsansvarig: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt

Art 4.8: personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning

Personer har en omfattande rätt till alla uppgifter som de kan identifieras med hjälp av – men den kör inte automatiskt över andra rättigheter.

OBS: det är inte och blir inte förbjudet att behandla personuppgifter – behandlingen måste helt enkelt ske enligt vissa regler.

Dataskyddsprinciper för personuppgifter

1. behandlas lagligt, korrekt och öppet
2. användas endast för ändamålet
3. uppgiftsminimering
4. alltid vara korrekta
5. lagringsminimering
6. behandlas med integritet och konfidentialitet

Personregisteransvarige har ansvaret

Berättigade ändamål

6.1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a. Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
b. Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
c. Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
d. Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
f. Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.
Detta ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Samtycke

1. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.

2. Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

3. De registrerade ska ha rätt att när som helst återkalla sitt samtycke. Det ska vara lika lätt att återkalla som att ge sitt samtycke.

Förbjudna uppgifter

Art 9.1: 1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

Det finns flera undantag:

- den registrerade har uttryckligen lämnat sitt samtycke
- behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder

Vad göra nu?

1. Kartlägg vilka register ni har (databokslut)
2. Kartlägg alla kanaler där ni samlar in personuppgifter
3. Fastställ rättslig grund för behandling av personuppgifter
4. Gå igenom hur ni hanterar samtycke
5. Beakta dataskyddet i IT-system och -rutiner
6. Kartlägg om samarbetsparter och leverantören följer lagen (uppförandekoder, certifiering)
7. Dokumentera – allt som görs ska kunna påvisas

När du skapar en blankett
Frågor som behöver svar och skrivas ner

1. Samlar jag nu in personuppgifter?
2. Vem är jag som samlar in uppgifterna?
3. Har jag rätt att samla in uppgifterna?
4. För vilket ändamål samlar jag in uppgifterna?
5. Vilka uppgifter behöver jag? Samlar jag in onödiga uppgifter?

6. Ger jag uppgifterna vidare till någon?
7. Hur länge sparar jag uppgifterna och vilka uppgifter sparar jag?
8. Hur behandlar jag uppgifterna, gör jag kopior?
9. Är uppgifterna säkra och konfidentiella hos mig?
10. Hur raderar jag uppgifterna, på riktigt?

Framgår det i blanketten hur personen:

1. meddelar korrigeringar till de egna uppgifterna
2. meddelar att alla uppgifter bör raderas
3. får tillgång till alla uppgifter som har samlats in om hen

Uttrycker jag att detta tillräckligt tydligt, så personen förstår?

Tack!

Ant Simons
ant@webbhuset.fi, 050 3300819
www.webbhuset.fi

Adress till denna presentation:
bit.do/gdprant