EU:s dataskyddsförordning (GDPR) – vad betyder den för er förening?

Dataskyddet – ett nytt sätt att tänka på.
Verktyg för ett bättre dataskydd.

Datainspektionen

Adress: Elverksgatan 10 (Kv. iTiden)
Telefon: 25 550, 0457 343 2081
Hemsida: www.di.ax
E-post: inspektion@di.ax

• EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (GDPR) om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om *upphävande av direktiv* 95/46/EC (allmän dataskyddsförordning)

• Träder ikraft den 25 maj 2018

Varför en EU-förordning? Stärkta rättigheter

- Förbättra enskildas kontroll över sina personuppgifter (förenhetliga)

1. Ta med sina uppgifter (byta onlinetjänster, sociala nätverk)
2. Mera insyn (lättare utöva sina rättigheter mot myndigheter o bolag)
3. Säkrare för barn (åldersgräns 16 år, annars föräldrars samtycke)
4. Lättare att klaga (nationell tillsynsmyndighet - Datainspektionen)
5. Större sanktionsrättigheter (max 20 000 000 euro)

Varför en EU-förordning? Stärkta rättigheter

6. Rätten att bli glömd (begära att sökmotorer tar bort sökträffar som negativt påverkar skyddet av ens personliga integritet eller att webbplats raderar info om en)

- Modernisering- öka förtroendet för EU:s digitala inre marknad o elektroniska tjänster

Hur berörs vi av reglerna?

- Gäller direkt som lag o ersätter nationella regler såsom personuppgiftslagen
- Förordningen ger utrymme för mer preciserade bestämmelser i nationell lagstiftning (tillsynsmyndighet, personuppgiftsbehandling hos myndigheter, sanktionsavgiften gällande offentlig sektor o speciallagstiftning)
- Mycket är oförändrat (rättsligt stöd för behandling, samtycke, information, tillräckliga säkerhetsåtgärder, särskilda krav gällande behandling av känsliga personuppgifter)

Personuppgiftsansvarigs ansvar

1. **Dataskyddsombud**

Ska *under alla omständigheter* utnämnas av pu-ansvarig o Personregisterbiträde om

- Behandlingen genomförs av myndighet eller offentligt organ
- Kärnverksamheten består av behandling, som pga sin karaktär, omfattning o/eller sina ändamål, kräver regelbunden o systematisk övervakning eller består av känsliga pu eller som rör fällande domar i brottmål o överträdelser

Personuppgiftsansvarigs ansvar, forts.

2. Tekniska och organisatoriska åtgärder för dataskydd - ju känsligare personuppgifter alternativt stora ekonomiska konsekvenser för enskilda kräver hög säkerhetsnivå.

3. Information till registrerade – se dagens registerbeskrivningar!

4. Särskilda krav vid behandling som medför stora integritets-risker (konsekvensbedömning) – innan ny pu-behandling planeras som innebär särskilda risker ska en bedömning av vilka konsekvenser (konsekvensanalyser/privacy impact assessments) behandlingen kan få och vilka åtgärder (inbyggda dataskyddsgarantier/privacy by design) som behövs för att minska risken.

Personuppgiftsansvarigs ansvar, forts.

5. Behandling av personuppgifter i anställningsförhållanden

- Möjlighet att i kollektivavtal fastställa mera specifika regler.

6. Anmälan om personuppgiftsincident

- Om det inträffar en säkerhetsincident (t.ex. dataintrång eller oavsiktlig förlust av uppgifter) krävs en anmälan till tillsynsmyndigheten inom 72 timmar. Ev. information till de registrerade om det handlar om särskild integritetskänslig information.

Några viktiga definitioner

- **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 onelineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska kulturella eller sociala identitet

Några viktiga definitioner, forts.

- **Behandling**

- En åtgärd eller en 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.

Några viktiga definitioner, forts.

- **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.

Några viktiga definitioner, forts.

- **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 personuppgiftsansvariga eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller medlemsstaternas nationella rätt.

Några viktiga definitioner, forts.

- **Personuppgiftsbiträde** - en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
- **Samtycke av den registrerade** - Varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne (dokumentation).
- **Personuppgiftsincident** - En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Vad är känsliga personuppgifter?

- Ras och etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Behandling av genetiska uppgifter, biometriska uppgifter
- Uppgifter om hälsa
- Uppgifter om sexualliv eller sexuell läggning

Huvudregel: Förbud

Undantag vid samtycke eller om nödvändigt vid skyldigheter/rättigheter, arbetsrätt, social trygghet och skydd.

Personbeteckning är extra skyddsvärd (nationell lagstiftning)

Principer för behandling av personuppgifter

- Berättigade ändamål och begränsning av mängden uppgifter som är nödvändiga för ändamålen
- Ansvarsskyldighet för pu-ansvarig
- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet

Artikel 5/skäl 39,50, 58, 60

Laglig behandling av personuppgifter

- Samtycke
- För att fullfölja ett avtal med registrerad som part
- Fullgöra en rättslig förpliktelse
- Intresseavvägning- behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter eller friheter väger tyngre och kräver skydd av pu, särskilt när den registrerade är ett barn (möjlighet till invändningar)

Artikel 6.1, 21/skäl 47, 48, 49 och 69

Tredjelandsöverföring

- EU-regler gällande överföring av personuppgifter från EU till organisationer i USA (Facebook, Google; Apple, Microsoft) i USA som anslutit sig till reglerna
- EU-kommissionens beslut 12.6.2016 Privacy Shield (tid. Safe Harbour)
- Krävs adekvat skyddsnivå i mottagarlandet, eller samtycke, eller standardavtalsklausuler som EU-kommissionen godkänt, eller bindande företagsinterna regler (Binding Corporate Rules) t.ex. Isle of Man, Jersey, Schweiz.

Checklista gällande förberedelser

- Hur kommer er organisation att påverkas? Var ska ansvaret ligga? Utnämn dataskyddsombud
- Kartlägg vilka personuppgifter som används
- Vilken information lämnar ni till registrerade
- Se över era rutiner för att tillmötesgå de registrerades rättigheter
- Undersök vilka personuppgifter ni behandlar och med vilket rättsligt stöd (dokumentera)
- Hur inhämtar ni samtycke, vilken information lämnar ni och hur dokumenteras samtycket?

Checklista gällande förberedelser, forts.

- Tillräckliga rutiner för att upptäcka, rapportera och utreda personuppgiftsincidenter (ansvaret)
- Vilka särskilda integritetsrisker finns med er behandling? Gör en riskbedömning- kartlägg även avtal
- Har ni byggt in skydd för personuppgifter i era IT-system?(inte mer, inte längre än nödvändig, inte för annat ändamål - skydda uppgifterna under hela deras livslängd)
- Agera förebyggande – det blir billigare så
- Agera transparent och öppet!