CHECKLISTA - FÖRBEREDELSER INFÖR DATASKYDDSFÖRORDNINGEN (GDPR)

Denna checklista innehåller åtta punkter som SKL rekommenderar att alla kommuner, landsting och regioner går igenom inför att Dataskyddsförordningen (GDPR) börjar gälla den 25 maj 2018.

Det nya regelverket börjar gälla fullt ut det datumet och det förutsätts då att alla personuppgiftsansvariga organisationer kan visa att man följer reglerna.

Det finns flera nyheter i den nya förordningen som kräver att alla kommuner, landsting och regioner måste se över och vidta förändringar av verksamheten. De personuppgiftsansvariga organisationernas ansvar och skyldigheter förtydligas och utökas och de registrerades rättigheter förstärks.

Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariga organisationens skyldighet att kunna visa att förordningen följs och ställer ökade krav på dokumentation som kan påvisa detta.

1. Förbered verksamheten

Är er organisation medveten om EU:s nya dataskyddsförordning?

- ✓ Ni bör försäkra er om att beslutsfattare, medarbetare och nyckelpersoner inom er organisation är medvetna om att dataskyddsförordningen kommer att ersätta personuppgiftslagen (PUL).
- ✓ Ni bör också undersöka hur er organisation kommer att påverkas av förordningen och identifiera de områden som ni måste arbeta särskilt med.

Ni kan behöva avsätta betydande resurser för att hinna anpassa er organisation till de nya kraven innan dataskyddsförordningen ska börja tillämpas i maj 2018. Inledningsvis bör ni särskilt fokusera på att öka medvetenheten om de kommande förändringarna. Det kan bli både kostsamt och svårt att uppfylla reglerna i förordningen om ni väntar med förberedelserna till sista stund.

Det finns flera filmer och kortfattat material på SKL:s webbplats som kan användas för att informera chefer och medarbetare.

2. Organisera GDPR-arbetet

Se till att det finns en organisation på plats som kan arbeta med dataskydd.

En nyhet med det nya regelverket är att den personuppgiftsansvariga organisationens ansvar för att driva dataskyddsarbetet tydliggörs. Det finns även flera nya krav på att organisationen måste kunna visa upp att man följer regelverket och hur man följer det.

- ✓ SKL rekommenderar att kommuner och landsting/regioner nu ser över sin interna styrning och sina riktlinjer för hur personuppgifter hanteras i verksamheterna.
- ✓ Se till att det finns en organisation med utpekat ansvar och roller som inte enbart är en projektorganisation utan ger förutsättningar för att kontinuerligt arbeta med området.
- ✓ Utse någon ansvarig för organisationens dataskyddsarbete som kan rapportera till ledningen.

SKL har ett Samarbetsrum – en digital plattform för samverkan - som är öppen för de medarbetare i kommuner, landsting och regioner som ansvarar för GDPR-arbetet i organisationen. Där finns flera exempel på hur man kan organisera sitt arbete och möjlighet till diskussion med kollegor.

- ✓ **Utse Dataskyddsombud.**

Alla personuppgiftsansvariga myndigheter och offentliga organ måste utse ett dataskyddsombud. Varje nämnd med självständigt verksamhetsansvar räknas som en egen personuppgiftsansvarig och nämnd med samordningsansvar, som kommunstyrelse och landstingsstyrelse, är personuppgiftsansvarig för gemensamma behandlingar. Det finns inget som hindrar att man utser gemensamt dataskyddsombud för flera nämnder i samma kommun, landsting eller region, eller i samarbete regionalt, så länge ombudet har tillräckligt med tid och resurser för att utföra uppdraget. Det går även att anlita externt dataskyddsombud.

När det gäller kommunala/landstingskommunala företag så ska de enligt Datainspektionens bedömning inte räknas som ”myndighet eller offentligt organ”. Men i vissa fall kan de ändå vara skyldiga att förordna dataskyddsombud om deras kärnverksamhet omfattar behandling av personuppgifter som kräver regelbunden

och systematisk övervakning av de registrerade i stor omfattning eller behandling i stor omfattning av känsliga personuppgifter eller uppgifter om begångna brott.

SKL har tagit fram en vägledning om dataskyddsombud.

3. Kartlägg

Ta reda på vilka personuppgiftsbehandlingar som finns i verksamheten och upprätta en registerförteckning.

- ✓ Ni bör inventera och dokumentera vilka personuppgifter ni hanterar, hur de samlas in och till vem uppgifterna lämnas ut.
- ✓ Ni kan behöva göra en bred översyn för att ta reda på vilka uppgifter som hanteras inom de olika delarna av er organisation.
- ✓ Upprätta en registerförteckning över alla personuppgiftsbehandlingar. Om det finns en registerförteckning enligt personuppgiftslagen behöver den kompletteras och uppdateras.
- ✓ Se över rutiner och instruktioner så att det inte blir ett engångsarbete utan att registerförteckningen kan hållas kontinuerligt uppdaterad.

SKL kommer att ta fram en enkel mall för registerförteckning med en instruktion. Det finns även flera verktyg på marknaden för detta ändamål som kan upphandlas.

För att kunna säkerställa att personuppgifter i verksamheten hanteras på rätt sätt och kan skyddas, är det grundläggande att ha uppdaterad kunskap om vilka behandlingar som finns och som tillkommer och förändras löpande. Reisterförteckningen ska fungera som ett nav för arbetet med dataskydd.

Dataskyddsförordningen innehåller dessutom flera rättigheter för individer som ska kunna garanteras i ett informationssamhälle. För att säkerställa att de registrerade kan ta tillvara sina rättigheter är det även en förutsättning att kunna hitta uppgifter om enskilda individer för att till exempel genomföra rättelser eller kunna redovisa till vilka andra uppgifter har lämnats ut.

4. Analysera

Ta reda på vilka rättsliga grunder ni har för att behandla personuppgifterna i organisationen. Vilka skyddsåtgärder behövs och vilka risker kan finnas?

- ✓ Ta reda på vilka rättsliga grunder som tillåter att personuppgifter får behandlas för varje behandling.
- ✓ Se till att detta dokumenteras i registerförteckningen.
- ✓ Om personuppgifter behandlas med stöd av samtycke, se till att det i efterhand kan visas att ett giltigt samtycke har lämnats.
- ✓ Genomför konsekvensanalys för behandlingar med särskilda integritetsrisker.

Konsekvensanalys måste göras vid behandlingar där personuppgifter om hälsa, etniskt ursprung, politisk uppfattning, medlemskap i fackförening eller andra särskilt känsliga kategorier av uppgifter behandlas i stor omfattning. Läs mer om detta.

Det nya regelverket medför flera förändringar och en sådan som kan få stor praktisk påverkan gäller just vilka grunder för behandling som finns. En viktig ändring när det gäller behandling av personuppgifter i löpande text är att ett undantag som fanns i PuL, den så kallade missbruksregeln nu försvinner. Det innebär bland annat att man nu måste dokumentera vilken rättslig grund som ger stöd för att behandla även personuppgifter som finns i löpande text och i annan ostrukturerad form. Läs mer om detta.

5. Dokumentera

Samla systematiskt och fortlöpande dokumentation som visar hur ni följer dataskyddsförordningen, utöver registerförteckningen.

- ✓ Besluta en övergripande policy för dataskydd som beskriver mål, styrning, organisation och ansvar för dataskyddsarbetet.
- ✓ Se till att dokumentation om dataskydd hålls på ett ordnat och systematiskt sätt och att rutiner finns för att hålla det uppdaterat.
- ✓ Samla bevis för hur reglerna följs.

Dataskyddsförordningen ställer krav på att den personuppgiftsansvariga organisationen ska kunna visa att man följer reglerna och även hur man följer reglerna. Detta kräver utöver registerförteckningen och konsekvensanalyser att flera analyser ska dokumenteras, till exempel riskanalyser om säkerhetsåtgärder.

6. Inför nya rutiner

Se till att förberedelsearbetet tar sikte på att arbetet med dataskydd ska fungera kontinuerligt i organisationen.

- ✓ Planera för att organisationen ska kunna upprätthålla ett långsiktigt arbete kring dataskydd.
- ✓ Se även över befintliga processer och styrdokument för nära liggande processer som t.ex. informationssäkerhet, dokument- och ärendehantering, upphandling, systemförvaltning och IT-drift så att de vid behov kompletteras med dataskyddsåtgärder.
- ✓ Påbörja arbetet med inbyggt dataskydd, ”Privacy by Design”, i verksamheten inför upphandlingar av system och tjänster och vid utveckling. Läs mer om detta.
- ✓ Förbered rutiner för att kunna upptäcka och anmäla personuppgiftsincidenter. Läs mer om detta.

7. Leverantörer och avtal

Se till att avtal med leverantörer och pågående upphandlingar har tillräckliga krav på åtgärder för dataskydd.

- ✓ Se över aktuella avtal och säkerställ att de är uppdaterade med personuppgiftsbiträdesavtal och instruktioner som är anpassade till dataskyddsförordningen.
- ✓ Kontrollera att pågående upphandlingar tar med aktuella krav och personuppgiftsbiträdesavtal.
- ✓ Ta kontakt med leverantörer för att säkerställa att kunskap om det nya regelverket finns och att det finns samstämmighet om roller och ansvarsfördelning.

8. Säkerställ individens rättigheter

Se till att det arbete med dataskydd som genomförs i organisationen genomsyras av att de registrerade individernas rättigheter är i fokus.

- ✓ Se till att ni har rutiner på plats för att säkerställa att ni kan uppfylla alla rättigheter som de registrerade har enligt dataskyddsförordningen.

- ✓ Se till att det finns information på webbplatsen eller på andra kontaktytor så att individer kan få information om de behandlingar som utförs, om de registrerades rättigheter och hur de kan utöva dem.

De viktigaste rättigheterna för de registrerade är att:

- Vid begäran få tillgång till sina personuppgifter.
- Få felaktiga personuppgifter rättade.
- Kunna få sina personuppgifter raderade (här finns omfattande undantag för myndigheter).
- Ha möjlighet att invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering.

Datainspektionen har mer information om detta.

Mer information och stöd:

SKL har mer information, mallar och vägledningar om Dataskyddsförordningen.

Läs mer även hos Datainspektionen, där finns det nya regelverket i fulltext, FAQ och definitioner av vanliga begrepp.

För alla som arbetar med GDPR och dataskyddsfrågor inom kommuner, landsting, regioner och deras bolag finns ett samarbetsrum för erfarenhetsutbyte, diskussion och delning av goda exempel.

Läs mer om samarbetsrummet och hur du kommer med i rummet.