Frågor och svar om GDPR och digitala möten

Dessa frågor och svar bygger på ett REMM-webbinarium den 24 maj 2018, då Jesper Wokander från Malmö Universitet berättade om hur användningen av digitala möten påverkas av GDPR.

Vad är GDPR?

GDPR betyder General Data Protection Regulation och är en EU-förordning som ersätter PUL. Syftet är att bättre skydda vår personliga integritet genom att hårdare reglera hanteringen av personuppgifter. På svenska heter lagstiftningen Dataskyddsförordningen men den engelska förkortningen används allmänt för samma text.

Vad är personuppgifter?

Personuppgifter är all information som direkt eller indirekt kan kopplas till en enskild levande person, till exempel:

- Namn
- Personnummer
- Adress
- E-postadress
- Ljud
- Bilder
- Rörliga bilder
- Ip-adress
- DNA
- Fingeravtryck

När får personuppgifter behandlas?

Grundregeln för GDPR är att personuppgifter inte ska samlas in och sparas om det inte är nödvändigt. All behandling av personuppgifter måste uppfylla följande principer:

- Behandlingen ska vara laglig, korrekt och öppen
- Uppgifterna ska vara korrekta och uppdaterade
- Behandlingen ska vara säker
- Endast för uttryckligt angivna och berättigade ändamål
- Inte mer uppgifter än nödvändigt
- Inte under längre tid än nödvändigt

Vilka grunder finns för behandling av personuppgifter?

- Samtycke
- Myndighetsutövning eller allmänt intresse
- Tredje parts berättigade intresse
- Nödvändigt för att fullgöra ett avtal med den registreradeavtal
- Rättslig förpliktelse (landets lagar)
- Skydda den registrerades intressen

Ett samtycke kan alltid återkallas, när som helst och utan förklaring. Personens uppgifter ska då raderas. För att kunna hitta personuppgifter i inspelat material är det därför viktigt att metadata sköts noggrant.

Personuppgifter som samlas in baserat på samtycke kan övergå till att behandlas baserat på en annan grund, till exempel myndighetsutövning eller allmänt intresse. Då kan uppgifterna sparas trots att ett samtycke dras tillbaka.

Vilken information ska jag ge inför en inspelning?

GDPR syftar till öppenhet gentemot den vars personuppgifter samlas in och behandlas. Informationsplikten innebär att du ska berätta (inför mötet eller i början av mötet):

- att samtalet spelas in
- vilka personuppgifter som samlas in
- vad inspelningen ska användas till
- identitet och kontaktuppgifter till personuppgiftsansvarig
- vilken grund som finns för att personuppgifterna samlas in
- hur länge personuppgifterna ska behandlas
- om personuppgifterna ska delas vidare
- att den inspelade har rätt att ta del av uppgifterna
- hur man kommer i kontakt med aktuellt dataskyddsombud
- att den inspelade har rätt att klaga till Dataskyddsmyndigheten
- be om samtycke om det är den lagliga grunden

Undantag från informationsplikten ges i de fall då den som registreras redan är informerad. Detta innebär att man inte inför varje inspelning behöver lämna all information utan kan nöja sig med att begära samtycke under förutsättning att alla inblandade har kunskap om behandlingen sedan tidigare.

Hur dokumenterar jag ett samtycke?

Samtycke till behandling av personuppgifter ska alltid dokumenteras på ett sätt som gör att de kan sparas och visas fram vid behov. Dokumentationen kan vara skriftlig (även digitalt) eller, vid video eller telefonmöten, inspelad.

Om grunden för behandlingen är samtycke kan en enskild deltagare välja att inte delta men inte förhindra att mötet genomförs.

Vad ska jag tänka på innan jag spelar in?

Säkerställ att det finns ett giltig grund för inspelningen och att hanteringen är säker.

Allt som inte är nödvändigt att spara ska inte heller sparas. Till exempel kanske inte chattkonversationer behövs.

Hur identifierar man sig vid digitala möten?

Det är inte alltid nödvändigt att identifiera sig, men i de flesta fall gör alla det (även vid möten i det verkliga livet). I vissa fall kan det vara önskvärt att ställa anonyma frågor eller att få anonyma svar. Om det är viktigt att säkerställa en persons identitet kan man i dagsläget använda BankID, Swamid som för U&H, eller Siths som är vanligt för e-hälsa.

Får jag använda molntjänster?

Ja, om säkerheten kan garanteras enligt GDPR. Myndigheten bör ha en lista på vilka tjänster som får användas och i vilka syften. Det ska också finnas personuppgiftsbiträdesavtal med leverantören. Observera att det kan förekomma restriktioner för uppgifter som kan antas omfattas av sekretess eller känsliga personuppgifter.

Är skärmdelning, filöverföring och presence (dvs man kan se om någon är inloggad) tillåtet?

Det finns inget generellt hinder. En bra princip är att alla mötesdeltagare ska vara införstådda med vilka regler som gäller för varje enskilt möte.

Är inspelade möten offentliga handlingar?

En inspelning är med största sannolikhet en allmän handling redan när man tryckt på stopp efter inspelningen. Allmänna handlingar kan lämnas ut efter sekretessprövning. Alla myndigheter kan hävda sekretess, men innehållet avgör och det kan vara förvaltningsdomstolen som i slutändan bestämmer.

Inspelningar som sker för att underlätta anteckningar eller upprättandet av andra handlingar i ett senare skede bör raderas därefter.

Ibland sker inspelningen med syftet att spridas. Då görs handlingen offentlig och det går bra att till exempel lägga ut en länk till inspelningen.

Vad gäller för känslig och hemlig information?

Det finns ingen generell regel som säger att känslig personlig information och konfidentiella uppgifter och liknande inte får behandlas i digitala möten, men säkerhetskraven är naturligtvis högre. Det ska finnas riktlinjer för informationssäkerhet vid myndigheten, där det framgår vilken typ av information som får utbytas i olika kanaler. Riktigt hemlig information kanske hellre ska utbytas vid ett fysiskt möte i en kontrollerad lokal. Klassning ska göras av all information (MSBFS 2016:1 §9).

/REMM 180629