VAGGERYDS KOMMUN

2018-10-26

Rapport från Informationssäkerhetssamordnare efter kontroll av personuppgiftsbehandling i Vaggeryds Kommun 22 okt. 2018.

Bakgrund

Den 25 maj började den nya dataskyddsförordningen (GDPR) att gälla. Tidigare lagstiftning Personuppgiftslagen (Pul) upphörde och ersattes av GDPR.

Några punkter att peka på gällande skillnaden i de båda lagstiftningarna är främst

- Hårdare sanktioner
- Ökad kontroll
- En ny roll tillsätts (Dataskyddsombud)
- Strängare regler för information och samtycke,
- Ökade rättigheter för den enskilde
- ”Missbruksregeln” försvann (gäller personuppgifter och e-post)

På ett mer konkret plan innebär GDPR att kommuner/företag/myndigheter måste kunna visa vad de vill göra med personuppgifter. Pul har mer varit inriktat på hur data hanteras när en kommuner/företag/myndigheter väl har skaffat dem. Det går inte att ha dolda syften med att samla in personuppgifter d.v.s. använda uppgifterna till annat än vad som avsågs från början. Vi får inte heller hantera uppgifter för att ”de kan vara bra att ha”, det kan inte vara det enda syftet. Kommuner/företag-/myndigheter ska ha klart för sig på vilken rättslig grund de hanterar uppgifterna.

Förutom de ovannämnda delarna ska kommuner/företag/myndigheter också anmäla personuppgiftsincidenter till datainspektionen, kontraktera de som hjälper till att behandla uppgifterna (personuppgiftsbiträden) samt föra registerförteckning.

Registerförteckningen beskriver bl.a. de ovannämnda punkterna, alltså hur kommuner/företag/myndigheter hanterar personuppgiftsbehandlingen, varför, på vilka rättsliga grunder, hur behandlingen går till samt hur vi kontrakterar andra som hjälper oss i behandlingen.

Registerförteckningen används för granskning av bl.a. dataskyddsombudet samt underlag till den enskilde som önskar information om specifik behandling.

Från Pul till GDPR Vaggeryds Kommun - sammanfattning

Kommunen och de bolag anslutna inom den kommunala verksamheten arbetar mot att anpassa personuppgiftsbehandling till GDPR lagstiftningen.

Arbetet med att anpassa kommunen och bolagen till GDPR är mycket resurskrävande. Stor analys och kartläggning av processer med personuppgiftsbehandling krävs för att kunna svara upp till GDPR´s intentioner och informationen i registerförteckningen samt skyldigheten med avtalsförfarande mot personuppgiftsbiträden.

Kommunen har införskaffat ett systemstöd för att föra registerförteckning (Draftit).

Mot bakgrund av oklarheterna kring lagstiftningen både nationellt och kunskapsnivån i vår egen organisation kring GDPR har arbetet och hanteringen varit varierande. Från början fanns mycket litet stöd nationellt så också inom organisationen. Vi hanterade uppgiften på bästa sätt utefter den kunskapsnivån som fanns.

Genom tillsättning av samordningsfunktion inom informationssäkerhet har arbetet organiserats och fått styrning. Förändringar har gjorts i systemstöd och utbildningar genomförs på bred kant inom hela organisationen för att uppnå medvetande nivå inom informationshantering och GDPR. Ett strukturerat arbete pågår nu inom informationshantering och vårt arbete att förändra samt registrera underlag i vår registerhantering.

Granskning/kontroll

Vaggeryds kommuns satta organisation kring dataskyddsarbetet GDPR ger förutsättningar för en interkontrollshantering. Utsedda roller ska stötta organisationen kring registerhanteringen. Utveckling av systematisering i arbetet pågår.

Extern part i kontroll och granskningsförfarande för kommunen är Dataskyddsombudet (innefattat ej bolagen). Dataskyddsombudet ger rådgivning och juridiskt stöd i hanteringen av personuppgiftsbehandling och granskar också vår registerförteckning. Dataskyddsombudet är också den som anmäl till datainspektionen (tillsynsmyndighet) om brott föreligger kring hanteringen av personuppgifter.

Kontroll 22 oktober 2018 i registerförteckning av dataskyddsombud

Kommentarer utifrån Dataskyddsombudets rapport:

Mot bakgrund av utlåtande från dataskyddsombud och sammanfattningen gällande Vaggeryds kommuns arbete i anpassning mot lagföljsamhet GDPR, går arbetet framåt i godtycklig takt utefter de förutsättningar organisationen har. Vi tar med oss bra synpunkter från dataskyddsombudet och anpassar vårt arbete. Process kring incidenthantering finns men den är dåligt förankrad inom organisationen, här krävs ett förbättringsarbete.

I jämförelse på regional och nationell nivå gällande kommunal anpassning till GDPR, befinns sig kommunen i en mitt sektion. Genom fortsatt planering i ett strukturerat tänk kring informationshanteringsområdet kommer också följsamhet inom GDPR som en naturlig del.

Det fortsatta arbetet innefattar:

- Nämnderna fortsätter inventering av personuppgiftsbehandling.
- Kartläggning och klassificering av processer för att identifiera risker och personuppgiftsbehandlingar.
- Klassificering av information och system utefter konfidentialitet, riktighet, tillgänglighet och spårbarhet.
- Incidenthantering
- Riskhantering

//Annika Lagerqvist, samordnare Informationssäkerhet