GDPR efterlevnadsområden

Contents

1 Policy och vägledning

Organisationen behöver fastslå integritetsrelaterad styrande dokumentation.

Integritetsmeddelande ligger ofta på extern webb, detta är efterlevnad på kravet om öppenhet mot omvärlden om behandlingarna av personuppgifter. Ibland kallas denna information för integritetspolicy. Öppenhet om behandling av personuppgifter bör innehålla ett antal saker som är inskrivna i lagen.

Integritetspolicy, till skillnad från integritetsmeddelande är framför allt ett fastställande mot den egna organisationen. Integritetspolicy bör följa standarden för policys som är:

Vad, varför, mål, medel och ansvaret inom organisationen.

Beroende på vilka behandlingar som görs, och vilka personuppgifter kan andra instruktioner eller vägledningar behövas. Särskilt om ansvar ligger spritt hos många personer inom organisationen.

2 Ansvar och roller

Det är inte alla organisationer som behöver ha en DPO, men det kan ändå vara fördelaktigt att ha en dedikerad roll för dataskyddsarbetet ändå. Exempelvis vid komplexitet för personuppgifter som behandlas eller för behandlingarna kan en formellt utsedd DPO bistå organisationen att implementera och upprätthålla rätt nivå på dataskyddsarbetet.

Det är manga gånger fler roller i organisationen som bör ha ett visst mått av ansvar inom dataskyddsområdet, och där medvetenheten om sådant ansvar i rollen behöver säkerställas. Exempel på sådana roller är chefer, HR personal, projektledare och tjänsteägare.

3 Kartläggning och dokumentation av personuppgifterna

Insamling och dokumentering av personuppgifter och behandlingar är en central del för att uppnå kontroll och dataskydd för företaget. I detta arbete ingår att samla och dokumentera ett antal uppgifter som kravställs av GDPR. Det råder dessutom ett beroende från andra lagkrav till den information som skall sammanställas, och informationen bör därför ha lämplig organisation och struktur.

4 Öppenhet och utbildning

Från GDPR stalls krav på organisationer att man skall vara transparent för de behandlingar av personuppgifter som organisationen utför. Det innebär skyldighet att tillhandahålla lätt åtkomlig information om behandlingarna, men även ytterligare information som exempelvis vilka personuppgifter som behandlas, motiv till behandlingarna, vilka rättigheter man har och hur man kan komma i kontakt för frågor.

Det är även viktigt att informera hela organisationen om vad som gäller, så att varje medlem i organisationen vet vilket ansvar som åligger henne eller honom.

5 Data minimering och avsikt-avgränsning

Dessa element återkommer I olika sammanhang över tid. Beskrivning på hur organisationen etablerat detta är kravställt att finnas med i registerförteckningens information för behandlade personuppgifter. Det måste finnas mekanismer som säkerställer dessa krav vid införande av nya behandlingar, och vid förändringar av behandlingar.

6 Processer och rutiner för verksamheten

För att uppnå tillräcklig kvalitet på processerna som stöder dataskyddsarbetet så behöver processer och rutiner vara väl beskrivna och delade med organisationen. Alla i organisationen behöver känna till när det kan vara frågan om ett dataskyddsärende, och hur man då skall agera.

Organisationen behöver beskriva processen som skall följas vid en personuppgiftsincident, då denna kan behöva rapporteras till IMY och då inom 72 timmar. Organisationen behöver ha definierat vilka roller som gör vad, och alla behöver känna till hur man rapporterar en misstänkt personuppgiftsincident. Det är en fördel om processbeskrivningen finns lättillgängligt i lättillgänglig form, där alla vet var den finns.

Utöver det behöver man ha definierat hanteringen av begäran av rättigheter, såsom registerutdrag och radering eller ändring av de egna personuppgifterna.

7 Inbyggd integritet och integritet som förstahandsval.

Det behöver finnas fastställda krav och avgränsningar för hur välja integritet i första hand och hur integritet byggs in i behandlingarna av personuppgifter inom organisationen. Vilket inkluderar nya behandlingar, förändrade behandlingar samt existerande behandlingar som behöver förbättrad integritet

8 Överlämning från projekt till förvaltning

I arbetsprocessen för projekt behöver det finnas definierade krav som säkerställer att skydd av personuppgifter är hanterat i projektet och checkpunkter som finns med vid överlämning när projektet avslutas.

9 Fortlöpande efterlevnad och kontroller

En struktur och plan för kontrollaktiviteter möjliggör upprätthållandet av efterlevnad av den uppnådda nivån på skydd av personuppgifter. En genomtänkt strategi kan även minimera en eventuell belastning på organisationen för skyddsarbetet.

Aktiviteterna är en kombination av avstämningar och kontroller. Från detta bör utkomsten bli synliggjorda brister samt förbättringsåtgärder att planera.

10 Ändringsaktiviteter

Allt som kan förändra eller påverka dataskydds arbetet eller behandlingarna på personuppgifter kan inkluderas i ändringshanteringsarbetet. Även identifierade brister och förbättringsåtgärder från kontrollaktiviteterna och från personuppgiftsincidenter bör inkluderas i ändringsaktiviteterna

11 Leverantörskontroll samt leverantörsuppföljning

När personuppgiftsansvarig anlitar en leverantör där personuppgiftsbehandling ingår så benämns leverantören personuppgiftsbiträde, och det som leverantören utför åt

personuppgiftsansvarig måste regleras i ett juridiskt dokument benämnt personuppgiftsbiträdesavtal.

Personuppgiftsansvarig har skyldighet att kontrollera att leverantören håller lämplig nivå i sitt dataskyddsarbete.

Alla ändringar av behandlingarna måste kunna kontrolleras, accepteras och dokumenteras. Leverantörskontroller på regelbunden basis bör också ingå i det fortlöpande efterlevnadsarbetet.

12 Anställdas personuppgifter

Ofta behandlas de anställdas personuppgifter I helt andra system och processer än organisationens affärs- och verksamhetsdata. Och det kan vara lätt att glömma att dessa behandlingar också lyder under dataskyddsförordningen.

Visserligen finns lagliga krav för arbetsgivare att samla och behandlas de anställdas personuppgifter. Men det undantar inte dessa personuppgifter från kraven att behandlingarna skall kartläggas, dokumenteras, avgränsas och skyddas.

Skyddet av anställdas personuppgifter är viktigt eftersom arbetsgivares behandling av de anställdas personuppgifter som regel inbegriper särskilda kategorier, s.k. känsliga personuppgifter. Och därför måste tillräckligt skydd vara infört.

13 Schrems II domslutets påverkan

Domslutet från Schrems II ändrade i egentlig mening inte lagtexten, utan snarare fastställde krav i lagen. Som att varje enskild behandling skall konsekvensbedömmas. Och om behandlingen inte uppfyller lagkraven så skall behandlingen inte inledas alternativt omedelbart upphöra.

Det som domslutet ändrade var att Privacy Shield inte längre är möjligt att använda som säkerhetsmekanism för överföring av personuppgifter utanför EU.

Combitech har verktyg för att underlätta bedömning och framtagning av beslutsunderlag. Därmed kan Combitech stötta för att skapa förståelse för risknivåer och kunna besluta lämpliga åtgärder. Samt framtagning av anpassad strategisk rapport för de mekanismer som har eller kan ha påverkan utifrån Schrems II domslutet är även det en tjänst som Combitech kan tillhandahålla.

14 Förordningsförslag om articifiell intelligens

Detta förslag kommer visserligen inte att träda i kraft på ett tag. Kanske man redan idag använder, planerar eller funderar på AI lösningar och funderar både på hur förslaget kan komma att påverka redan gjorda investeringar och möjligheten att göra strategiska val redan nu. Här kan Combitech hjälpa till att göra en utvärdering utifrån vad vi idag om den riskbaserade modell som förslaget beskriver.