Rådet for Digital Sikkerhed

03. december 2020

Rådet for Digital Sikkerheds vejledning om samspillet mellem DPO og informationssikkerhedsafdelingen

Der er overlap mellem organisationers klassiske sikkerhedsforanstaltninger, der etableres af sikkerhedsafdelingen, og de foranstaltninger, der skal sikre beskyttelse af de registreredes personoplysninger og efterlevelse af databeskyttelsesforordningen. Det er derfor vigtigt at sikre et godt samarbejde mellem DPO og sikkerhedsafdelingen. I denne vejledning adresserer vi, hvordan samspillet kan organiseres – herunder hvilke forhold der skal lægges vægt på for at sikre DPO'en ufhængighed – særligt i mindre organisationer med høj grad af sammenfald mellem funktioner.

Baggrund

Der er på en række områder et betydeligt overlap mellem de sikkerhedsforanstaltninger, som organisationer implementerer for at beskytte organisationens interesser (f.eks. efter ISO27001/2), og de sikkerhedsforanstaltninger, som skal beskytte de registreredes rettigheder efter databeskyttelsesforordningen. Det er derfor centralt, at der etableres et godt samarbejde mellem de personer, der har ansvaret for organisationens arbejde med informationssikkerhed og de personer, der har ansvaret for organisationens beskyttelse af personoplysninger. I nogle organisationer er der endvidere forskellige former for krav om audits af sikkerhedsforanstaltninger, og/eller der kan være krav om at udpege en DPO efter databeskyttelsesforordningen. Denne vejledning adresserer samspillet mellem disse personalegrupper.

Kravet om behandlingssikkerhed

I databeskyttelsesforordningens artikel 32 er der formuleret krav om, at der er etableret et passende teknisk og organisatorisk sikkerhedsniveau på baggrund af en risikovurdering, hvilket traditionelt er et område, som varetages af en organisations informationssikkerhedsafdeling. Det er derfor vigtigt, at en organisations databeskyttelsesrådgiver (DPOen) eller persondataansvarlige (f.eks. CPO) har etableret et tæt samarbejde med informationssikkerhedsafdelingen, således at de tekniske og organisatoriske sikkerhedskontroller etableret af informationssikkerhedsafdelingen også omfatter de krav til beskyttelse af persondata som angivet i databeskyttelsesforordningen, databeskyttelsesloven, de vejledninger, som Datatilsynet har udgivet og organisationens interne politikker og procedurer. Det er ideelt, hvis man kan dokumentere overholdelse af både sine persondataretlige forpligtelser (f.eks. som udtrykt ved ISO27701), og sine øvrige informationssikkerhedsmæssige forpligtelser (f.eks. som udtrykt ved ISO27001/2) i samme dokumentationssystem. På den måde sikrer man, at konkrete tiltag spiller sammen og får virkning i forhold til begge hensyn, at sproget er ens (teknisk og juridisk), og at der er en fælles samarbejdsplatform.

Har man f.eks. etableret data loss prevention som en teknisk foranstaltning efter ISO27002 med det formål at sikre, at fortrolige forretningsoplysninger ikke forlader organisationen, kan det være naturligt at udvide denne tekniske foranstaltning til at omfatte følsomme og fortrolige personoplysninger efter f.eks. databeskyttelsesforordningens artikel 9 og 10 og databeskyttelseslovens § 11, og dokumentere den risikominimerende effekt i samme dokumentationssystem.

Har man etableret organisatoriske foranstaltninger i form af krav til sine leverandører efter ISO27002, kapitel 15, er det naturligt at forlænge disse krav for de leverandører, der har en rolle som databehandler, med kravene fra databeskyttelsesforordningens artikel 28.

Rådet for Digital Sikkerhed
Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 53 36 02 23 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Databeskyttelsesrådgiverens opgaver

I databeskyttelsesforordningen artikel 39 er databeskyttelsesrådgiverens opgaver beskrevet. Opgaverne omfatter bl.a. at underrette og rådgive om forpligtelserne efter de persondataretlige regler, at overvåge overholdelsen af de persondataretlige regler og politikker udstedt i medfør heraf og at være kontaktpunkt for tilsynsmyndigheden. DPO'en skal særligt tage hensyn til den risiko, som behandlingen udgør for den registrerede.

For at kunne varetage sine opgaver skal DPO'en inddrages i beslutninger vedr. behandlinger af personoplysninger rettidigt og i alle spørgsmål. DPO'en må ikke være under instruktion af ledelsen (mere herom nedenfor). DPO'en skal have adgang til passende ressourcer for at kunne udføre sit arbejde. DPO'en bør rapportere til øverste ledelse, hvilket i private virksomheder vil sige direktionen og i myndigheder, den øverste administrative ledelse. DPO'en må ikke kunne afskediges på baggrund af sine anbefalinger. DPO'en skal fungere som kontaktpunkt for tilsynet og de registrerede. DPO'en er underlagt tavshedspligt.

Organisationer, som ikke er pligtige til at udpege en DPO, kan i stedet udpege en Chief Privacy Officer, CPO, til at sikre efterlevelse af de persondataretlige regler. CPO'en vil ikke være underlagt de samme krav, som gør sig gældende for DPO'en, da CPO'en ikke er omfattet af de persondataretlige krav.

Man skal dog være opmærksom på, at hvis der udpeges en databeskyttelsesrådgiver i tilfælde, hvor der ikke er pligt til dette, jf. GDPR art. 37, stk. 4, vil denne databeskyttelsesrådgiver være omfattet af de samme krav, som en pligtmæssigt udpeget databeskyttelsesrådgiver.

Ansvarsfordeling i forhold til teknisk og organisatorisk sikkerhed

I artikel 38 i databeskyttelsesforordningen, står der endvidere, at DPO'en kan udføre andre opgaver end at være DPO, så længe dette ikke er i konflikt med de opgaver, der udføres som DPO. I betænkning 1565, p. 584, uddybes dette med, at DPO'en f.eks. ikke kan være den øverste ansvarlige for IT eller HR. DPO'en må altså gerne være tilknyttet IT- eller HR-afdelingen, men må ikke være øverste ansvarlige. Det vil sige, at der som sådan ikke er noget til hinder for, at databeskyttelsesrådgiveren organisatorisk kan være tilknyttet en organisations informationssikkerhedsafdeling, så længe det sikres, at funktionen ikke medfører en interessekonflikt. I praksis er det derfor, hvis man har muligheden, bedst at sikre, at der er funktionsadskillelse mellem DPO-rollen og CISO-rollen.

Hvis DPO-rollen og CISO-rollen er sammenfaldende, skal man være ekstra opmærksom på, om der kan opstå interessekonflikter, og om DPO'ens uafhængighed kan drages i tvivl. Man skal i sådanne situationer være opmærksom på, at når man anbefaler noget i sin egenskab af CISO, må anbefalingen ikke være i strid med det, man anbefaler i sin egenskab som DPO. Der er en risiko for konflikter, bl.a. fordi man som CISO er organisationens repræsentant, og som DPO er repræsentant for de registrerede. Det bør være beskrevet, at DPO'en ikke har nogen instruktionsbeføjelser i forhold til behandling af "forretningens" personoplysninger og således ikke må "eje" forretningens systemer eller behandlingsaktiviteter. DPO'en må altså ikke have indflydelse på, hvorvidt forretningen skal behandle personoplysninger til bestemte formål.

DPO'en skal kunne agere uden instruks og kunne rapportere direkte med den øverste ledelse i deres organisation. Dette er den centrale præmis i databeskyttelsesforordningens artikel 38, stk. 3 og også i Datatilsynets egen vejledning om databeskyttelsesrådgiver (side 25 og 26). Derfor skal DPO'en i fuld uafhængighed og uden at gå på kompromis med de persondataretlige regler kunne vurdere, om personoplysninger "i forretningen" behandles lovligt, sikkert og i øvrigt i overensstemmelse med de persondataretlige regler. Ligeledes er det vigtigt at sikre, at der ikke opstår en kultur om, at DPO'en ikke kan

få den nødvendige adgang og rapportering til organisationernes ledelse, eller at ledere i organisationer påtager sig at instruere deres databeskyttelsesrådgivere i, hvordan de skal udføre deres arbejde, hvornår de må udføre deres arbejde eller over for hvilke dele af organisationen, de ikke må udføre deres arbejde.

Hvis CISO'en og DPO'en er sammenfaldende, kan det overvejes, om en anden person kan gennemføre interne sikkerhedsmæssige og persondataretlige audits af de foranstaltninger, som der træffes beslutning om. Dette tiltag kan overvejes for at sikre, at der er funktionsadskillelse, så personen ikke auditerer sit eget arbejde. Audits kan passende gennemføres for både IT-sikkerhedsforanstaltninger iværksat til at mitigere organisationens risici såvel som de registreredes risici.

Uanset om DPO-rollen og CISO-rollen er sammenfaldende eller ej, bør det ligeledes være beskrevet, at det er ledelsen, som har det øverste ansvar for informationssikkerheden og behandlingen af personoplysninger. I praksis sker dette typisk ved, at CISO og DPO refererer til direktionen, som godkender CISOen's og DPO'ens indstillinger og anbefalinger – herunder politikker, procedurer og andre foranstaltninger. Skulle ledelsen finde på at tilsidesætte DPO'ens (eller CISO'ens) indstillinger og anbefalinger, så skal denne tilsidesættelse dokumenteres - f.eks. i form af mødereferater - så DPO'ens uafhængighed og faglighed ikke kan drages i tvivl. I større organisationer, hvor organisationen har lavet politikker, procedurer med videre, og justeret disse efter rådgivning fra DPO'en, skal det ligeledes dokumenteres, hvis DPO'ens rådgivning ikke følges.

Sikring af et passende teknisk og organisatorisk sikkerhedsniveau

I artikel 32 i databeskyttelsesforordningen er udgangspunktet for de passende tekniske og organisatoriske foranstaltninger, som iværksættes, at de skal passe til den risiko, som de registrerede udsættes for ved behandling af deres personoplysninger. Risikovurderingen er altså baggrund for de konkrete foranstaltninger.

Fra praksis kan vi konstatere, at risikovurderingerne ikke altid har været grundige nok til at imødese risici, der har materialiseret sig i hændelser til skade for de registrerede. Det er derfor centralt, at man kan dokumentere, at man har iværksat de foranstaltninger, som er passende henset til risici.

Adfærdskodekser efter artikel 40 eller certificeringsmekanismer efter artikel 42 i databeskyttelsesforordningen kan i henhold til artikel 32, stk. 3, i samme forordning bruges til at påvise overholdelse af kravene i artikel 32, stk. 1. Der findes imidlertid ikke for nuværende en af Datatilsynet godkendt adfærdskodeks eller certificeringsmekanisme. Derfor må man sikre, at man kan dokumentere en efterlevelse af de vejledninger, som Datatilsynet har udgivet vedrørende teknisk og organisatorisk sikkerhed, God it-skik udgivet af FSR - danske revisorer (dokumenteret i form af en ISAE 3402 type II erklæring), at man kan fremlægge en revisionserklæring efter ISAE3000 eller tilsvarende internationale erklæringer, eller at man er certificeret efter en international anerkendt sikkerhedsstandard som f.eks. ISO/IEC 27001:2013, hvis vil man vil være i stand til at dokumentere sin implementering af teknisk og organisatorisk sikkerhed jf. databeskyttelsesforordningens artikel 32, stk. 1.

Man bør dog være opmærksom på, at God it-skik og de international anerkendte sikkerhedsstandarder ikke altid er fuldt dækkende i forhold til at opfylde specifikke persondata krav til teknisk og organisatorisk sikkerhed. Dette betyder, at der kan være en opgave for databeskyttelsesrådgiveren i at gennemgå den valgte standard og rådgive den ansvarlige for en organisations informationssikkerhedspolitik om, hvilke yderligere sikkerhedskontroller der bør implementeres.

I forhold til de internationalt anerkendte sikkerhedsstandarder er der typisk en tilføjelse til standarden, som opremser de nødvendige tilføjelser, f.eks. i ISO/IEC 27701:2019 afsnit 4.3 og annex F

Dokumentation af et passende teknisk og organisatorisk sikkerhedsniveau.

Der er i databeskyttelsesforordningen ikke specifikke krav til hvorledes, man som organisation skal dokumentere et passende teknisk og organisatorisk sikkerhedsniveau, men en måde hertil kunne være at have en ekstern part til at lave en ISAE3402 eller ISAE 3000 revisionserklæring eller tilsvarende international erklæring. Her skal man huske at sikre, at der i vurderingen af implementerede sikkerhedskontroller også vurderes de persondatarelevante sikkerhedskontroller. Man kan også vælge at være certificeret efter en international sikkerhedsstandard som f.eks. ISO/IEC 27001:2013 og igen her sikre, at man har medinddraget de nødvendige tilføjelser i sit kontrolkatalog for at opfylde de specifikke persondatakrav til teknisk og organisatorisk sikkerhed.