Datatilsynet indstiller møbelfirma til bøde på 1,5 mio. kr.

I efteråret 2018 udvalgte Datatilsynet en række virksomheder, som skulle være genstand for tilsyn efter Databeskyttelsesforordningen og -loven. Blandt disse virksomheder var IDdesign, som Datatilsynet foretog tilsyn hos den 8. oktober 2018.

Tilsynet havde særlig fokus på virksomhedens procedurer for sletning af personoplysninger, som det kræves efter Databeskyttelsesforordningens artikel 5, stk. 1, litra e.

Allerede forinden det planlagte tilsyn blev foretaget, havde IDdesign efter anmodning oplyst, at der i tre af virksomhedens butikker fortsat anvendes et ældre system, som i de øvrige butikker er erstattet af et nyere system. Under tilsynsbesøget blev det oplyst, at der i det ældre system blev behandlet oplysninger om ca. 385.000 kunder. De omtalte oplysninger vedrører kundernes navn, telefonnummer, adresse, e-mailadresse samt deres købshistorik. IDdesign oplyste endvidere under tilsynsbesøget, at der i det omtalte ældre system ikke er fastsat slettefrister, hvorfor personoplysninger, der opbevares i dette system, ikke slettes.

Mangel på stillingtagen til og fastsættelse af slettefrister er i strid med Databeskyttelsesforordningens artikel 5, stk. 1, litra e, som fastslår, at personoplysninger skal opbevares således, at det ikke er muligt at identificere de registrerede i et længere tidsrum, end det er nødvendigt til de formål, hvortil oplysningerne behandles.

Datatilsynets afgørelse

Efter tilsynet har Datatilsynet sammenfattende konkluderet følgende:

1. At IDdesign ikke har overholdt kravene i Databeskyttelsesforordningens artikel 5, stk. 1, litra e (opbevaringsbegrænsning), idet virksomheden i systemet AX 2.5 har behandlet personoplysninger om cirka 385.000 kunder i en længere periode end nødvendigt til de formål, hvortil de blev behandlet.
2. At IDdesign ikke i forhold til oplysningerne i systemet AX 2.5 har overholdt kravene i Databeskyttelsesforordningens artikel 5, stk. 2, jf. artikel 5, stk. 1, litra e, idet virksomheden ikke har fastlagt og dokumenteret frister for sletning af personoplysninger.
3. At IDdesign ikke har overholdt kravene i Databeskyttelsesforordningens artikel 5, stk. 1, litra e, idet virksomheden i systemet AX 2012 fortsat har behandlet personoplysninger om kunder, efter virksomhedens egen fastsatte slettefrist for oplysningerne er nået.
4. At IDdesign ikke i forhold til virksomhedens rekrutteringssystem og HR-system har overholdt kravene i Databeskyttelsesforordningens artikel 5, stk. 2, jf. artikel 5, stk. 1, litra e, idet virksomheden ikke i tilstrækkelig grad har dokumenteret sine procedurer for sletning af personoplysninger.

Punkt 1 ovenfor har medført, at Datatilsynet har indgivet en politianmeldelse til Østjyllands Politi indeholdende en indstilling til en bøde på 1,5 mio. kr.

Punkt 2-4 har derimod ikke resulteret i en politianmeldelse, men Datatilsynet har udtalt alvorlig kritik.

Det bemærkes, at IDdesigns manglende sletning ikke kan undskyldes med henvisning til udtalelsen vedrørende Databeskyttelsesforordningens artikel 25 i Justitsministeriets betænkning nr. 1565 om Databeskyttelsesforordningen, hvoraf det fremgår, at det ikke kræves, at et gammelt system skal re-designes, hvis der findes andre tilstrækkelige organisatoriske sikkerhedsløsninger. Dette henset til, at IDdesign allerede har re-designet systemet, men forsømt at installere den nye version i tre af sine butikker og til, at IDdesign ikke har foretaget sig nogen form for organisatoriske tiltag for at sikre, at de opbevarede personoplysninger slettes manuelt, når opbevaring af dem ikke længere er nødvendig.

Det er ikke længe siden, at Datatilsynet indstillede en anden virksomhed, Taxa 4x35, til en bøde for manglende overholdelse af Databeskyttelsesforordningens krav om sletning af persondata.

Læs vores artikel om Datatilsynets indstilling af bøde til taxavirksomheden Taxa 4x35

Slettepolitik og tidsfrister

For at sikre overholdelse af kravene om sletning af persondata bør den dataansvarlige sætte sletningen i system. I den sammenhæng bør den dataansvarlige udarbejde en slettepolitik, som tager stilling til, hvornår de forskellige typer af persondata, som den dataansvarlige behandler, skal slettes. Uanset om den dataansvarlige har en egentlig politik for sletning eller ej, skal den dataansvarlige kunne dokumentere, at der er taget stilling til sletningsspørgsmålet. Det er da også et krav, at slettefrister angives i den dataansvarliges fortegnelse over behandlinger.

Med undtagelse af de tilfælde, hvor slettefristen er beskrevet i lovgivningen, er det den dataansvarlige selv, der fastsætter, hvornår de behandlede persondata skal slettes. Der er dog ikke helt frie tøjler, idet den dataansvarlige som følge af principperne om dataminimering og opbevaringsbegrænsning i GDPR ikke må opbevare persondata længere, end det er nødvendigt af hensyn til formålet, hvortil persondatane behandles.

Den dataansvarlige skal altså i forhold til alle behandlede persondata konkret overveje, hvor længe de pågældende persondata er nødvendige at opbevare og dokumentere dette.

Det er dog ikke nok, at den dataansvarlige udarbejder en slettepolitik, der tager stilling til, hvornår de behandlede data skal slettes – sletningen skal også faktisk gennemføres i overensstemmelse med politikken, hvilket desværre ikke altid sker. Og den dataansvarlige bør kunne vise, at sletningen rent faktisk er gennemført – også selvom databehandlingen sker hos en databehandler, hvorfor dette skal haves in mente, når der indgås databehandleraftaler og gennemføres kontrol af databehandlere.

Backups – en konflikt mellem jura, teknik og praktik

Særligt i forhold til backups har kravet om sletning medført en konflikt mellem jura, teknik og praktik. Juridisk set omfatter kravet om sletning alle persondata, også selvom de måtte være lagret i en backup.

Fra en teknisk og praktisk vinkel er det imidlertid ikke altid muligt at gennemføre sletningen i overensstemmelse med slettefristerne. En sletning af persondata i backuppen vil nemlig i mange situationer medføre, at den dataansvarlige vil skulle indlæse backuppen, slette de sletningsmodne persondata og 'pakke backuppen ned' igen. Ikke alene medfører dette et meget omfattende arbejde og en praktisk udfordring, men det strider tillige mod princippet bag en backup, at denne ofte skal findes frem og redigeres – og en sådan gentagen håndtering af en backup vil samtidig ofte være sikkerhedsmæssigt uforsvarligt.

I backupsystemer, hvor det er teknisk muligt at slette enkelte dataposter uden risiko for at korrumpere den øvrige del af backuppen, skal sletning ske på denne måde. I forhold til andre – og mere gængse – backupsystemer, hvor dette ikke er teknisk muligt, har rådgivningen i en årrække været, at såfremt data skulle slettes i en backup, måtte den dataansvarlige i stedet notere sig, hvilke data det var, der skulle slettes, og så tage højde for dette, hvis backuppen skulle genindlæses, og ellers skulle backuppen ligge uberørt. Betragtningen bag dette var ganske enkelt, at manglende sletning af enkeltdata indtil det tidspunkt, hvor backuppen alligevel blev slettet, var en mindre risiko, end en gentagen håndtering af backuppen, som medførte en risiko for, at backuppen var korrupt, når og hvis den blev nødvendig til sit egentlige formål; nemlig at sikre muligheden for genetablering af data.

Datatilsynet har lykkeligvis bekræftet denne tilgang.

Læs mere om sletning af persondata

NIS PETER DALL
ADVOKAT (L), PARTNER

(+45) 77 40 10 18
NPD@NJORDLAW.COM

PERNILLE KIRK ØSTERGAARD
ADVOKAT, SENIORSPECIALIST

(+45) 77 40 11 74
POS@NJORDLAW.COM