Sletning af persondata

Persondatalovgivningen regulerer håndteringen af persondata fra det tidspunkt, hvor de opstår – altså hvor der etableres en forbindelse mellem en oplysning og en person – og frem til det tidspunkt, hvor denne forbindelse ikke længere er til stede, hvilket normalt er det tidspunkt, hvor persondata slettes. Men hvad sletning er, fremgår ikke af lovgivningen, og sletning er ikke bare sletning!

Kravet om sletning fremgår indirekte af Persondataforordningen (GDPR), som i artikel 5, stk. 1, litra e, anfører at persondata skal "opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles".

Det betyder, at når det formål, som persondata anvendes til, er udtømt, skal de pågældende persondata enten anonymiseres eller slettes. Anonymisering beskrives ikke i nærværende, men vil blive beskrevet ved en anden lejlighed.

Tilgang til slettet data

Sletning er imidlertid ikke altid det samme som, at brugeren af et it-system sletter data! Nogle it-systemer er opbygget således, at selvom brugeren sletter data, bevares disse i det bagvedliggende system. At dataene bevares, selvom brugeren sletter disse, er nogle gange helt tiltænkt, fordi data herved nemt kan genoprettes, hvis nu sletningen var en fejl, eller data senere bliver relevante igen. I andre situationer kan det også skyldes det bagvedliggende system. I flere styresystemer medfører en sletning nemlig reelt blot, at referencen til filen fjernes, og derved kan systemet (og brugerne) ikke umiddelbart finde filen, som derfor forekommer slettet. Imidlertid vil data ofte kunne tilgås ved direkte tilgang til den bagvedliggende database, eller endog ved at en it-kyndig med snilde og de rigtige værktøjer genfinder data direkte på disken.

Vurdering af rimelighed og genskabelse af data

Betyder det så, at den dataansvarlige altid skal sikre sig, at persondata, der slettes, nu også er helt væk ned til sidste bit på harddisken? Ikke altid - faktisk sjældent!

Også i forhold til sletning viser GDPR's risikobaserede tilgang sig nemlig. Persondata skal derfor slettes på en måde, så de rimeligvis ikke kan genskabes.

At data blot slettes fra brugergrænsefladen, men reelt bevares i backend-systemet vil ikke være fornøden sletning, idet data rimeligvis kan genskabes.

Sletning, hvor data slettes fra systemet på en sådan måde, at data reelt blot ligger på en disk uden direkte reference, indtil de på et eller andet tidspunkt bliver overskrevet med andre data, kan og vil meget ofte være en sletning – også i GDPR's forstand. Datatilsynet har da også udtalt, at sådanne overskrivnings-ventende data betragtes som slettet, da oplysningerne ikke længere med rimelige midler er tilgængelige.

Men risikobetragtningen må nødvendigvis indgå i vurderingen, idet sletning jo netop afhænger af, om data rimeligvis kan genskabes. I en sådan rimelighedsbetragtning vil blandt andet indgå værdien af de 'slettede' data. Jo større værdi dataene har, jo større indsats må der forventes rimeligvis at blive anvendt på en genskabelse. I denne forbindelse tænkes ikke alene den økonomiske værdi, men værdi i bred forstand. Behandles fx meget følsomme data, som i hænderne på de forkerte kan have betydelig værdi eller medføre betydelig skade for den registrerede, vil rimelighedsvurderingen sandsynligvis falde ud til fordel for en mere grundig sletning af persondata.

Bortskaffelse af medier

Dette kommer da også tydeligt til udtryk, hvor talen falder på bortskaffelse af medier. Risikoen for, at ikke-fuldt-ud-slettede data kommer til en uberettiget tredjemands kendskab, er væsentlig større i den situation, hvor mediet bortskaffes af den dataansvarlige, end hvor mediet forsat er i brug. Tredjemand, der får det bortskaffede medie i hænde, vil have væsentlig bedre tid og lejlighed til at genfinde eventuelle data, uden at den dataansvarlige vil opdage noget. I forbindelse med bortskaffelse af medier udtaler Datatilsynet da også, at persondata skal slettes forsvarligt, så oplysningerne ikke kan komme uvedkommende i hænde, og henviser i den forbindelse til den amerikanske standard NIST SP 800-88, rev. 1, som anbefaler ganske skrappe sletningsmetoder afhængigt af medietypen.

Læs guiden her

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 på Datatilsynets hjemmeside her

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