DATATILSYNET

It-sikkerhedstekst ST3

Sletning af personoplysninger

Dokumentnavn: ST3
Version 1
September 2014

Sletning af personoplysninger

Når en dataansvarlig behandler personoplysninger, omfattes behandlingen af regler i persondataloven, herunder:

Persondatalovens § 5, *Stk. 5,*:

> *"Indsamlede oplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. "*

I praksis betyder det, at personoplysninger må behandles, hvis der er en legal grund, og at personoplysninger enten skal anonymiseres eller slettes, når der ikke længere er grundlag for at behandle dem.

I det følgende beskrives nogle overvejelser, som den dataansvarlige kan gøre sig omkring sletning. Der tages udgangspunkt i den situation, at der ikke længere er grundlag for at behandle og opbevare personoplysninger, og de derfor skal slettes.

Hvad er en sletning

Når personoplysninger behandles, sker der typisk en lagring af personoplysninger i forbindelse med behandlingen. Lagring sker på lagringsmedier, fx en harddisk, der er placeret i en server. Det er ikke ualmindeligt, som en naturlig del af normal it-drift, at data over tid vil være lagret på flere lagringsmedier, fx flere harddiske og flere generationer af backupbånd.

Sletning af personoplysninger betyder i praksis, at personoplysninger uigenkaldeligt fjernes fra alle de lagringsmedier, hvorpå de har været lagret, og at personoplysninger på ingen måde kan genskabes. Dette gælder for samtlige lagringsmedier, der har været i anvendelse i forbindelse med den pågældende databehandling.

Ultimativt kan sletning af personoplysninger gennemføres ved destruktion af anvendte lagringsmedier.

Ikke-sletninger

Som dataansvarlig skal man være opmærksom på, at der findes mange løsninger, som tilsyneladende sletter data, men hvor data med rette midler kan genskabes.

Eksempler kan være:

- Løsninger, hvor data bliver gjort ikke-læsbare eller ikke tilgængelige ved at fjerne rettigheder til at tilgå data.
- Løsninger, hvor der ved "sletning" blot er tale om, at referencer til filer fjernes. Når referencer til filer fjernes, er der ikke længere umiddelbart adgang til data, men data er hverken overskrevet eller slettet. Data kan med den rigtige viden og/eller værktøjer genskabes.
- Løsninger, hvor data, efter at være blevet gjort utilgængelige, over tid måske bliver overskrevet med andre data.

Medietyper

Forskellige medietyper har forskellige egenskaber i forhold til lagringskapacitet, læse- og skrivehastigheder, holdbarhed, pris og hvilken type af løsninger, de kan benyttes til. Der kan anvendes mange forskellige typer af lagringsmedier, afhængig af den konkrete løsning, hvori personoplysninger skal behandles.

Ofte anvendte medietyper er:

- magnetiske lagringsmedier, fx traditionelle harddiske og magnetbånd,
- optiske lagringsmedier, fx CD, DVD og Blue-ray,
- memory chip baserede lagringsmedier (solid-state medier) fx memory kort, flash hukommelse, USB-disk og SSD-disk.

I nogle situationer benyttes flere forskellige typer af lagringsmedier i forbindelse med en konkret løsning, fx harddiske eller SSD-diske til data i et produktionsmiljø, magnetbånd til backup eller sikkerhedskopier af data.

For nogle enheder er der tale om kombinationer af forskellige typer af lagringsmedier i samme enhed, fx en hybridenhed bestående af en SSD-disk og en magnetisk harddisk.

Slettemetoder

De forskellige typer af lagringsmedier lagrer data på forskellige måder, og data skal derfor også slettes efter forskellige metoder.[1]

Magnetiske lagringsmedier kan typisk slettes ved overskrivning af alle dataområder med random data. Der eksisterer flere metoder og værktøjer, som benytter overskrivning af enten hele eller dele af lagringsmediet. En anerkendt metode[2] foreskriver bl.a., at dataområder overskrives flere gange for at sikre mod, at data kan genskabes ud fra rester af magnetisk spor på mediet.

Magnetiske lagringsmedier kan også afmagnetiseres ved anvendelse af særligt afmagnetiseringsudstyr for at slette data. Her vil alle magnetisk lagrede data på lagringsmediet blive slettet[3].

I mange løsninger lagres data fordelt på flere harddiske, der styres af en RAID controller. I en sådan opsætning er det ikke ualmindeligt, at alle fysiske læse- og skriveoprationer styres af controlleren og således ikke giver en bruger mulighed for at vælge, hvilke fysiske områder på en harddisk der evt. skal overskrives. Med sådanne diskteknologier kan der opstå fejl, som medfører, at områder på diske markeres som ikke brugbare og efterfølgende ikke længere kan tilgås på normal vis. I disse markerede områder, som ikke kan tilgås på normal vis, kan der ligge data, som ikke er blevet slettet.

Ligeledes vil en formatering af diske i en sådan opsætning, i nogle tilfælde, ikke medføre en overskrivning af data på diskområder. Disk controlleren vil markere diskområderne som ledige, og diskene vil umiddelbart fremstå som tomme, selvom data med visse værktøjer kan genskabes.

[1] NIST Special Publication 800-88 Guidelines for Media Sanitization.
[2] DoD 5220.22-M.
[3] Ved afmagnetisering af fx en hybridenhed vil det kun være data på den magnetiske harddisk, der bliver slettet. Data lagrede på SSD delen af hybridenheden skal slettes med en anden metode.

Enkelte typer af optiske lagringsmedier og memory chip baserede lagringsmedier kan have en indbygget slettefunktion, der tilbyder sletning ved overskrivning af hele memory området. Men de fleste lagringsmedier har ikke en sådan slettefunktion, hvorfor andre slettemetoder skal anvendes.

Fælles for alle lagringsmedier er, at det er nødvendigt at undersøge præcis, hvilke medieteknologier der benyttes og hvilke slettefunktionaliteter og -metoder, der er til rådighed – om nogen.

Mediedestruktion

I nogle tilfælde kan det vise sig, at det i praksis ikke er muligt at sikre, at data på lagringsmedier reelt kan slettes. I disse tilfælde kan destruktion af de anvendte lagringsmedier være en løsning.

En meget effektiv metode til destruktion af fx et magnetbånd brugt til backup er fuldstændig afbrænding ved høj temperatur. Det vil ikke efterlade rester, hvorfra data kan genskabes.

For mange typer af lagringsmedier, fx magnetiske lagringsmedier som harddiske og magnetbånd, optiske medier som CD og DVD eller nogle typer af memory chip baserede lagringsmedier som hukommelseskort eller USB-diske, kan en makulering[4] af det fysiske lagringsmedie være en effektiv metode til destruktion.

I den konkrete situation skal den dataansvarlige afgøre, hvilken slettemetode eller destruktionsmetode der passer bedst til de lagringsmedier, som har været anvendt.

Anvendes en tredjepart til destruktion af lagringsmedier, bør den dataansvarlige sikre sig, at destruktionen af datamedier faktisk sker, og at lagringsmedier ikke i en periode ligger opmagasineret hos tredjeparten. Ved anvendelsen af en tredjepart til destruktion af lagringsmedier øger det sikkerheden, at destruktionen foretages af tredjeparten under opsyn af den dataansvarlige og efter dennes instruks.

Sammenblandede data

En særlig problemstilling opstår, hvis personoplysninger, der skal slettes, ligger på ét lagringsmedie sammen med andre data, der ikke skal slettes. Det kan bl.a. være resultatet af manglende adskillelse af data eller virkemåden af den lagringsteknologi, der anvendes.

Dette kan give den dataansvarlige udfordringer i forhold til, hvordan sletninger foretages i praksis. Det kan være en fordel, at den dataansvarlige fra starten tænker sletterutiner og data-adskillelse ind i databehandlingen og sikrer sig, at personoplysninger kan slettes.

En metode kan være at kopiere de data, som skal bevares, over på et andet datemedie, hvorefter det oprindelige lagringsmedie slettes uigenkaldeligt.

[4] Der eksisterer standarder for sikker makulering, som fx DS/EN 15713:2009.

Alle kopier af personoplysninger skal slettes

Hvis lagrede personoplysninger skal slettes, er det vigtigt, at den dataansvarlige forinden har dannet sig et overblik over, hvor og i hvor mange kopier personoplysningerne findes.

Ofte vil der findes flere kopier af de personoplysninger, som skal slettes. Ved normal drift af it-løsninger kan der fx være tale om flere lagringsmedier som harddiske og flere generationer af backup-medier, der skal slettes. En anden situation kunne være legal overførsel af personoplysninger fra en anden part. I en sådan situation skal eventuelle lagringsmedier, der er modtaget eller anvendt, ligeledes slettes.

I nogle tilfælde kan personoplysninger behandles på flere fysiske lokationer, og personoplysninger kan dermed være lagret flere forskellige steder. Dette kan der være gode grunde til, fx for at opnå redundans i databehandlingen for at sikre tilgængelighed ved driftssvigt. Også her skal den dataansvarlige sikre sig, at alle personoplysninger bliver slettet fra samtlige lagringsmedier, der har været anvendt.

Den dataansvarlige skal sikre sig, at alle kopier af personoplysningerne kan og bliver identificeret og slutteligt slettet.

Databehandler

Anvendes en eller flere databehandlere, gælder også krav om sletning.

Ved anvendelse af databehandlere, kan den dataansvarlige være i den situation, at databehandleren ikke fysisk holder behandlede personoplysninger adskilt fra andre data, fx fra andre kunders data, som databehandleren også behandler. Hvis databehandleren fx lagrer flere kunders data på samme medie, så kan det vise sig vanskeligt for den dataansvarlige at sikre sig, at personoplysningerne reelt bliver slettet uigenkaldeligt hos databehandleren.

Når personoplysninger hos en databehandler skal slettes, skal den dataansvarlige derfor sikre sig at:

- samtlige lagringsmedier, der indeholder personoplysninger, kan slettes eller destrueres - dette gælder også hvis databehandleren anvender underleverandører,
- have kendskab til, hvor personoplysninger befinder sig hos databehandlere og disses eventuelle underleverandører,
- samtlige kopier af personoplysninger reelt bliver slettet hos databehandleren og dennes eventuelle underleverandører, når der er behov for dette,
- det kan kontrolleres, at samtlige kopier af personoplysninger er blevet slettet hos databehandleren og dennes eventuelle underleverandører.