Persondata forordningen Print/Scan/Kopi

Persondataforordningen i forhold til TA's Print/Scan/kopiering maskiner

Sammenfatning som vi forstår den hos OSP - Triumph-Adler DK.

Mange af de love og regler der er på området har været gældende i en del år (Lov om behandling af personoplysninger LOV nr. 429 af 31/05/2000), det der sker den 25. maj 2018 er at det er blevet til en forordning fra EU som skal opfyldes og der indføres bøder af betragteligt beløb hvis man ikke lever op til forordningen/ overtræder reglerne.
Selvom man opfylder kravene i dag er det ikke ensbetydende med at man gør det i fremtiden, da lovgivningen kan blive lavet om, og fra et teknisk synspunkt kan det være at der findes sikkerheds brister i den krypterings teknologi der benyttes på nuværende tidspunkt. (Mange krypteringer vil kunne brydes bare man har nok regnekraft altså en meget hurtig computer som på et tidspunkt i fremtiden vil være tilgængelig. Regnekraften på en ny computer bliver ca. fordoblet for hver 18 måned)

Hvis man skal være sikker på at man opfylder forordningen på nuværende tidspunkt, skal man have juridisk bistand for at få set alle forholdene igennem.

Det er vigtigt at have en arbejdsgang defineret i forhold til print og scanning kopiering og opbevaring og destruktion af personfølsomme data, samt håndtering hvis der skulle opstå brud på sikkerheden.

Her er synspunkter set fra Kopimaskinen/MFP/Printeren.
Der må gerne scannes personfølsomme oplysninger hvis maskinen står på et lukket netværk.
Det vil sige et netværk hvor kun godkendte personer har adgang, der er adgangskoder på PC'er, mailsystem, af tilstrækkelig grad. Hvis man har WiFi skal det være tilstrækkeligt krypteret, og adgangen må ikke deles til gæster. Man har sikret sit netværks udstyr router, firewall både på netværket

Hvis der scannes eller printes over et åbent netværk/ delt netværk eller netværk hvor der er BYOD enheder, skal data krypteres med en tilstrækkelig teknologi/protokol (TLS1.2).
Man skal opfylde betingelserne for at må scanne og opbevare disse data, det gælder både åbne og lukkede netværk.

Printning og kopiering skal man være sikker på, at uvedkommende ikke kan få adgang til printdata og udskrevet dokumenter. Det kan evt. gøres ved at bruge privat print, så man først får sine job udskrevet når man står ved maskinen. Se evt. guide her https://www.tadriver.dk "Privat print fra KX driver"

Data må ikke opbevares på maskinens harddisk, længere end man har hjemmel til (standard 6 mdr. eller til kundeforhold ophører hvis det indtræder først.)

For delvist at opfylde overstående punkt med hensyn til dataopbevaring på MFP'ens harddisk kan man tilkøbe et DataSecurity kit som kan aktiveres på MFP maskiner hvor der er harddisk, den vil slette midlertidige data i forbindelse med scanning print og kopiering.

Men hvis man bruger maskinens funktion "Elektronisk brugerdefineret boks print" skal man sætte maskinen til at slette data så de ikke opbevares længere end man har tilladelse til.

Man må ikke scanne personfølsomme oplysninger via delte postserver konti.

G-Mail må f.eks. ikke bruges til scanning af personfølsomme oplysninger, da datacenter ikke med sikkerhed ligger i EU land.

Hvis den postserver man benytter gemmer de scannede dokumenter i "Sendt post mappen" må de ikke opbevares længere der end det man har hjemmel til.

Persondata forordningen Print/Scan/Kopi

Hvis man f.eks. har benyttet G-Mail til scan vil alle sendte dokumenter fra maskinen ligge i sendt post, og disse gamle data skal man også have styr på, så de ikke opbevares for længe og uden hjemmel.

Ved nedtagelse/destruktion/videresalg af maskiner med Harddisk skal data slettes tilstrækkeligt, så det ikke er muligt at genskabe data.

Det er kundens ansvar (Dataansvarlige) at opfylde loven, og sikre sit netværk tilstrækkeligt, til den sikkerheds standard som datatilsynet mener er påkrævet.

Hvis man er i tvivl om man opfylder specifikke ting kan man udfylde en forespørgsel hos datatilsynet for at få deres syn på sagen, svaret vil være et vejledende svar og ikke et juridisk bindende svar, det skal man selv have en jurist til at gennemgå.

Selvom man ikke behandler personfølsomme data kan det være fornuftigt at tage et kig på sikkerheden i forhold til sit netværk og print-scan-kopierings arbejdsgange. Det kan være at man har forretnings hemmeligheder som andre ikke skal have indsigt i, det kunne være licitations tilbud, kontrakter osv.

På websiden https://www.tadriver.dk under ” Data Sikkerhed” kan man hente sikkerheds beskrivelse (White Paper) for TA Triumph-Adler maskiner samt vores Fleet management system. Her er beskrivelse på hvordan man kan sikre sin maskine, samt en beskrivelse af hvordan vores system til opdatering og servicering kommuniker mellem maskiner og cloud server.

På følgende sider er samlet forskellige artikler fra datatilsynet med deres syn på specifikke emner.
Check selv op på deres side for at undersøge om artiklen er blevet opdateret.

Hvad er følsomme oplysninger?
E-mail med følsomme eller fortrolige personoplysninger.
Transmission af personoplysninger over internettet.
Sletning af data.
Trådløse netværk.
Ny skabelon skal hjælpe virksomheder og myndigheder med at blive klar til databeskyttelsesforordningen.

Vejledning hvis der sker et sikkerhedsbrug og hvad et sikkerheds brud er.
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf

Gratis skabelon til at kigge på de interne arbejdsgange vedr. Persondata forordningen.
https://dk.linkedin.com/pulse/nyt-gratis-v%C3%A6rkt%C3%B8j-kan-lette-arbejdet-med-henning-mortensen
https://ao.dk/gdpr-skabelon

Persondata forordningen Print/Scan/Kopi

Hvad er følsomme oplysninger?

https://www.advodan.dk/erhverv/persondata/hvad-er-foelsomme-oplysninger/

Hvordan en virksomhed skal behandle medarbejderes og kunders personoplysninger, afhænger af oplysningstypen. Jo mere følsom en oplysning, der er tale om, jo strengere er kravene til virksomhedens håndtering.

Hvad er almindelige oplysninger?

Håndtering af almindelige ikke-følsomme oplysninger kræver ikke et udtrykkeligt samtykke men kan ske f.eks. som led i opfyldelsen af et ansættelsesforhold. Det kan være:

- Identifikationsoplysninger (navn, adresse, tlf.nr, fødselsdato)
- Familieforhold
- Ansøgning og cv (uddannelse, eksamensoplysninger, tidligere beskæftigelse)
- Løn, arbejdstider, fravær, sygedage (men ikke årsagen til sygefraværet)
- Kontonummer
- Skat og gæld

Hvad er følsomme oplysninger?
Følsomme oplysninger går også under betegnelsen "særlige kategorier af oplysninger''. Det kan være:

- Oplysninger om helbredsforhold
- Fagforening
- Racemæssig eller etnisk baggrund
- Politisk, religiøs eller filosofisk overbevisning
- Seksuelle forhold
- Genetiske data

Behandling af følsomme oplysninger
Behandling af følsomme oplysninger er som udgangspunkt forbudt. Der er dog undtagelser – herunder hvis den registrerede har givet udtrykkeligt samtykke, hvis det eksempelvis kan beskytte den registreredes eller andres vitale interesser, eller hvis det er nødvendigt for at overholde arbejdsretlige forpligtelser.

Behandling af CPR-nummer
CPR-numre behandles som udgangspunkt fremover som følsomme oplysninger og må behandles, når det følger af lovgivningen, eller der er givet samtykke.

Strafbare forhold
Oplysninger om strafbare forhold kan behandles, hvis der foreligger samtykke, eller det er nødvendigt for at varetage en berettiget interesse.

Persondata forordningen Print/Scan/Kopi

E-mail med følsomme eller fortrolige personoplysninger

Oprettet: 07.01.08 Opdateret: 06.05.15

https://www.datatilsynet.dk/offentlig/sikkerhed/e-mail-med-foelsomme-eller-fortrolige-personoplysninger/

Datatilsynet har taget stilling til sikkerhedsforanstaltningerne ved behandling af følsomme personoplysninger i et lokalt e-post system.
Datatilsynet udtalte i den forbindelse, at så længe der er tale om en transmission, der foregår i et lokalnet, og der således ikke er tale om ekstern kommunikation, stilles der ikke krav om kryptering.
Forudsætningen er, at lokalnettet ikke er et åbent net.
Datatilsynets udtalelse kan sammenfattes i følgende:
Et e-post system må kun indeholde følsomme eller fortrolige oplysninger, hvis adgang til sådanne oplysninger er begrænset til de brugere, som er autoriseret dertil.
Behandling af følsomme og fortrolige personoplysninger i e-post systemer falder ind under undtagelsesbestemmelsen i § 19, stk. 2, i sikkerhedsbekendtgørelsen. Der skal således ikke foretages logning, hvis oplysningerne slettes efter en vis kortere periode, der generelt bør være af en størrelsesorden på højst en måned.
I overensstemmelse med ovenstående er det et krav, at postsystemets adgangskontrolsystem skal være aktiveret, således at en bruger kun har adgang til sin postkasse efter afgivelse af password.
Ved sletning skal e-post slettes i såvel afsenders udbakke som i modtagers indbakke samt efterfølgende i papirkurven.
Endelig skal der være truffet sædvanlige sikkerhedsmæssige foranstaltninger, herunder bl.a. beskyttelse mod uvedkommendes adgang til lokalnet og postserver.
Det tilføjes, at myndigheder må gemme e-postmeddelelser i længere tid, hvis dette sker i et system, der opfylder logningskravet.

Transmission af personoplysninger over internettet

Oprettet: 07.01.08 Opdateret: 14.01.16

https://www.datatilsynet.dk/offentlig/sikkerhed/transmission-over-internettet/

Af persondatalovens § 41, stk. 3, fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.
Det fremgår af lovforslagets bemærkninger til denne bestemmelse, at iværksættelse af de fornødne sikkerhedsforanstaltninger særligt er påkrævet, hvis behandlingen omfatter fremsendelse af oplysninger i et net.
Efter Datatilsynets opfattelse bør der ved transmission af oplysninger om personnumre over det åbne Internet som minimum foretages kryptering. Der bør også foretages kryptering, hvis andre oplysninger, som må betragtes som fortrolige (f.eks. oplysninger om økonomiske forhold o.l.), transmitteres.
Hvis der er tale om følsomme oplysninger omfattet af persondatalovens § 7 og § 8 (f.eks. oplysninger om fagforeningsmæssige tilhørsforhold, helbredsforhold eller strafbare forhold), skal der som minimum anvendes en stærk kryptering, baseret på en anerkendt algoritme.
Det er således Datatilsynets opfattelse, at persondatalovens § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i private virksomheder m.v. som i den offentlige forvaltning.
Ifølge sikkerhedsbekendtgørelsen (Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning) må der kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.
I Datatilsynets sikkerhedsvejledning (vejledning nr. 37 af 2. april 2001) er det nærmere angivet, hvorledes sikkerhedsbekendtgørelsens krav vil kunne opfyldes. Det fremgår heraf, at

- Ved tilslutning til Internet eller andre åbne net skal der træffes foranstaltninger, som sikrer imod uvedkommende trafik og forhindrer adgang fra det åbne net til den dataansvarliges interne net.

Datatilsynet finder, at det normalt vil øge sikkerheden at etablere en firewall, som løbende kontrolleres og om nødvendigt ajourføres. Men ofte vil det være nødvendigt med yderligere sikring. Eksempelvis vil etablering af hjemmesider (web-applikationer) eller web-services normalt kræve, at også disse sikres og løbende kontrolleres for sårbarheder.

- For transmission af personoplysninger over åbne net (f.eks. Internet) gælder konkret nedenstående minimumskrav om sikkerhedsforanstaltninger:

Ved transmission af oplysninger over det åbne Internet er der generelt en risiko for, at oplysningerne undervejs læses og endog ændres af uvedkommende. Derudover er der en risiko for, at parterne i kommunikationen ikke er dem, de udgiver sig for.
Disse risici må vurderes af den dataansvarlige i den konkrete situation, således at der kan træffes de fornødne sikkerhedsforanstaltninger.
Hvad angår fortrolighed kan denne sikres ved forsvarlig kryptering af de transmitterede oplysninger. Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages en kryptering. Hvis de transmitterede oplysninger er af følsom karakter (omfattet af persondatalovens § 7, stk. 1 og § 8, stk. 1), skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.
Sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) må sikres i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger, f.eks. elektronisk signatur eller individuelle, fortrolige adgangskoder.
VPN-forbindelser kan bruges til at sikre både fortrolighed og autenticitet, idet forbindelsen kan være krypteret og samtidig kræve autentificering ved brug af f.eks. et certifikat. At en forbindelse betegnes som VPN er dog ikke i sig selv en garanti for tilstrækkelig kryptering eller autentificering.
I forbindelse med vurdering af planerne for elektronisk borgerservice i Københavns Kommune har Datatilsynet besvaret en række spørgsmål. Der er derved udstukket vejledende retningslinier for graden af sikkerhed i identifikationen af en borger i forbindelse med kommunikation af forskellige typer af personoplysninger.

Persondata forordningen Print/Scan/Kopi

Sletning af data

Oprettet: 07.01.08 Opdateret: 06.05.15

https://www.datatilsynet.dk/offentlig/sikkerhed/sletning-af-datamedier/

Ifølge sikkerhedsbekendtgørelsen (Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning) skal der ved salg og kassation af anvendte datamedier træffes de nødvendige foranstaltninger for at sikre, at personoplysninger ikke kommer til uvedkommendes kendskab.
Man skal være opmærksom på, hvor der anvendes datamedier. Store kopimaskiner kan f.eks. indeholde en harddisk, hvorpå der lagres kopier af dokumenter. Disse datamedier vil i så fald også være omfattet af reglerne. Det betyder, at der ved reparation af en kopimaskine, hvor en del af reparationen går ud på at udskifte eller at indsende harddisken til et værksted, også skal træffes foranstaltninger der forhindrer, at persondata kommer til uvedkommendes kendskab. Vær også opmærksom på brugen af USB-nøgler, Smartphones, hukommelseskort og PDA'er.
Data kan i almindelighed ikke slettes tilstrækkelig effektivt fra f.eks. en harddisk, USB-nøgle eller mobiltelefon (hukommelseskort) ved hjælp af de standardfunktioner, som er til rådighed i et operativsystem. Data vil således ikke blive slettet effektivt ved f.eks. at slette en fil i Windows og efterfølgende tømme papirkurven. Data slettes heller ikke effektivt ved en formatering.
I Datatilsynets sikkerhedsvejledning (vejledning nr. 37 af 2. april 2001) er det nærmere angivet, hvorledes sikkerhedsbekendtgørelsens krav vil kunne opfyldes. Det fremgår heraf, at

- Ved kassation af lagringsmedier og udstyr, som indeholder personoplysninger, bør lagringsmedierne destrueres eller afmagnetiseres, så der ikke er mulighed for at læse indholdet.
- Hvis den dataansvarlige frem for at destruere lagringsmedier afhænder disse med henblik på genbrug, skal lagrede oplysninger slettes effektivt ved overskrivning.
- Datatilsynet anbefaler, at der til overskrivning af datamedier anvendes et af de dertil beregnede specialprogrammer, som over skriver data flere gange i overensstemmelse med en anerkendt specifikation (f.eks. DOD 5220.22-M).

Persondata forordningen Print/Scan/Kopi

Trådløse netværk

Oprettet: 07.01.08 Opdateret: 06.05.15

https://www.datatilsynet.dk/offentlig/sikkerhed/traadloese-netvaerk/

Af persondatalovens § 41, stk. 3, fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for data behandlere.
Ifølge sikkerhedsbekendtgørelsen (bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning) må der kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.
Datatilsynet anser i denne forbindelse et trådløst netværk for en ekstern kommunikationsforbindelse.
Trådløse netværk er forbundet med en række sikkerhedsrisici afhængig af den benyttede standard og den specifikke konfiguration. Der kan således være en vis risiko for, at uvedkommende kan få adgang til personoplysninger, som transmitteres på det trådløse netværk.
Ved anvendelse af trådløse netværk bør der derfor træffes særlige foranstaltninger med henblik på at sikre data på samme niveau som på et lukket kablet netværk. Eksempelvis vil en sådan beskyttelse kunne bestå i at sikre personoplysninger, som transmitteres over trådløse netværk, efter samme retningslinjer, som gælder ved transmission over det åbne internet. Det betyder blandt andet, at der ved transmission af fortrolige oplysninger herunder personnummer skal foretages kryptering, og at følsomme personoplysninger, jf. persondatalovens § 7 og § 8, skal krypteres ved anvendelse af stærk kryptering baseret på en anerkendt algoritme.
Det skal endvidere sikres, at eventuelle uvedkommende, som skulle få adgang til det trådløse netværk, ikke derved kan aflytte kommunikationen og opsnappe brugeridentifikationer og dertil hørende fortrolige adgangskoder, som anvendes i forbindelse med autoriserede brugeres adgang til personoplysninger.

Persondata forordningen Print/Scan/Kopi

Ny skabelon skal hjælpe virksomheder og myndigheder med at blive klar til databeskyttelsesforordningen

16.02.18

Myndigheder og virksomheder arbejder hårdt på at leve op til de nye krav, der kommer med den europæiske databeskyttelsesforordning om godt tre måneder. En af de ting, som mange kæmper med, er indgåelse af databehandleraftaler, og derfor offentliggør Datatilsynet nu en skabelon, som gør det lettere at få indgået aftaler, der lever op til kravene i forordningen.

Med databeskyttelsesforordningen kommer der 25. maj en række nye krav, som skal sikre borgernes rettigheder bedre. Et af de krav, som mange myndigheder og virksomheder lige nu bruger kræfter på, er udarbejdelsen af databehandleraftaler, der lever op til databeskyttelsesforordningens krav. Det er en aftale, der skal indgås, når en virksomhed eller myndighed vælger at benytte en anden myndighed eller virksomhed til at behandle personoplysninger på sine vegne.

Hvis en privat virksomhed fx bruger en ekstern leverandør til at holde styr på sine kundeinformationer, er det et krav, at de to virksomheder indgår en skriftlig aftale om, hvordan leverandøren må behandle virksomhedens oplysninger. Også med den nuværende lovgivning skal der indgås databehandleraftaler, men med databeskyttelsesforordningen stilles der yderligere krav til indholdet.

"For at hjælpe myndigheder og virksomheder med at leve op til reglerne har vi nu lavet en skabelon til en standard-databehandleraftale, som overholder minimumskravene i forordningen. Det er et værktøj, vi stiller til rådighed for de dataansvarlige, så de får et konkret bud på, hvordan en databehandleraftale kan se ud," siger Datatilsynets direktør Cristina Angela Gulisano og fortsætter:

"Når vi har gennemført tilsyn hos myndigheder og virksomheder i de seneste år, har vi set en del udfordringer med netop manglende eller mangelfulde databehandleraftaler. Det skal der rettes op på, og der kan skabelonen være en hjælp."

Ud over selve skabelonen (Standard-databehandleraftale) offentliggør Datatilsynet også en følgetekst, der forklarer, hvordan skabelonen kan anvendes (Databehandleraftale - følgetekst).

Fakta

- **Dataansvarlig:** Typisk en virksomhed eller offentlig myndighed, der afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.
- **Databehandler:** Typisk en virksomhed eller offentlig myndighed, der behandler personoplysninger på den dataansvarliges vegne og efter instruks fra den dataansvarlige.

Læs mere i vejledningen om datansvarlige og databehandlere.

Spørgsmål?

Har du spørgsmål om skabelonen, databehandleraftaler eller databeskyttelsesforordningen, kan du kontakte Datatilsynet på tlf. 33 19 32 00.