**Blogg om tankelederskap**

19. Juni 2018

**Fra blindsone til samsvar: grunner til at organisasjoner bør revidere utskriftsprosessene sine med tanke på GDPR**

Mengden data som genereres verden over, vil øke eksponentielt, fra 16 zettabyte (ZB) i 2016 til anslagsvis 163 ZB – eller 163 billioner gigabyte – innen 2025.1

Denne "dataeksplosjonen", kombinert med nye måter å jobbe på, understreker behovet for ny lovgivning. Derfor forbereder selskaper over hele Europa nå sine IT- og datarevisjonsprosesser på den nye personvernforordningen (GDPR).

Dette er ingen liten oppgave, og det finnes en enorm blindsone som mange organisasjoner glemmer å ta med i planene sine: utskrift.

Til tross for at saken har vært mye omtalt, var situasjonen tidlig i 2017 som følger: 40 % av kjøperne av trykksaker visste ikke hva GDPR var. Ytterligere 19 % visste hva det var, men ikke at 25. mai 2018 var en viktig frist.2

Kanskje enda mer overraskende: 51 % av kjøperne av trykksaker som hadde kunnskap om GDPR, visste ikke at det hadde betydelige konsekvenser for utskrifter.2

Nå som fristen for gjennomføring er passer, er enkelte selskaper fortsatt lykkelig uvitende om sårbarhetene som er knyttet til utskrift, og som omtales i rapporten *"Ensuring Data Privacy: The Print and Document Management Challenge"* [Les her](https://www.brother.no/business-solutions/security-gdpr#security)

**GDPR – de nye reglene kort forklart**

Å forstå GDPR er første steg på veien mot å følge reglene. Og det er spesielt to ting selskaper må forstå.

For det første: Selskaper eier ikke folks opplysninger. I GDPR står det tydelig at selskaper må behandle personopplysninger korrekt og informere folk hvis opplysningene blir stjålet eller behandlet feil eller ved brudd på personvernet.

For det andre: Selskaper må svare på henvendelser fra enkeltpersoner som utøver sine lovfestede rettigheter ifølge GDPR, blant annet retten til å få vite hvordan personopplysningene behandles, til å be om sletting av personopplysninger og til å be om begrensning av behandlingen.

**Sårbarhet knyttet til utskrift**

Når GDPR trer i kraft, kan alle utskriftsenheter som ikke inngår i samsvarsplanene, medføre sårbarhet i systemet.

En usikret skriver kan brukes for å få tilgang til et nettverk, dvs. at den kan være en bakdør til systemdata. Denne risikoen kan bare reduseres ved at man finner ut om data lagres på den og hvor ofte minnet tømmes, og deretter sikrer enheten.

I tillegg må utskrift og skanning av sensitive opplysninger kunne spores. Selskaper må ha fullt innsyn i revisjonssporet for raskt å kunne identifisere hvilke opplysninger som behandles, hvor det skjer, hvem som gjør det, og om formålet er legitimt.

**Lykkelig uvitenhet ingen unnskyldning**

Bøter for manglende samsvar er med overlegg høye og kan utgjøre 20 millioner euro eller 4 % av årsomsetningen på verdensbasis, avhengig av hvilket beløp som er høyest. Faktisk bruker GDPR-loven selv – [www.eugdpr.org](http://www.eugdpr.org) – følgende ord: "effektive, forholdsmessige og avskrekkende sanksjoner".

Å unngå saftige bøter er selvsagt en god grunn, men manglende samsvar kan også skade selskapets omdømme.

Godt dokumenterte prosesser vil bidra til å redusere sikkerhetsbrudd, forebygge bøter og verne om organisasjonens omdømme. Hvis det oppstår et brudd på personvernet, fungerer de også som bevis på at tilstrekkelige personvernprosedyrer var på plass.

**Tre trinn fra blindsone til samsvar**

Å ta utskrifter med i planene er en god start, men GDPR-samsvar kan bare sikres gjennom aktiv ledelse med fokus på følgende områder:

Prosessrevisjon: Organisasjoner bør finne dyktige ansatte til å revidere retningslinjene for sikkerhet og personvern samt oppdatere dem i henhold til de nye kravene. Deretter bør man utarbeide en plan for kontinuerlig overvåking, opptrapping, oppdatering og håndheving av retningslinjene.

Sikre utskriftsenheter: Intern lagring bør sikres, og det bør foretas kontroller for å identifisere og rette opp sårbarheter for skadelig programvare og andre nettangrep.

Dokumentgjenfinning: Teknologi for brukerautentisering, for eksempel pull-utskrift og autorisering av enheter brukes for å sikre fortrolighet og garantere dokumentgjenfinning.

Selv om GDPR medfører store endringer for alle organisasjoner, bør man se på det som en mulighet. Rene, forskriftsmessige data vil gi selskapene informasjon som kan brukes til å forbedre kundeopplevelsen og skape vekstmuligheter.

1. *Data Age 2025: The Evolution of Data to Life-Critical, Don’t Focus on Big Data; Focus on the Data That's Big*, IDC White Paper, april 2017.
2. *Low Investment in Print Security and Increasing Compliance Challenges Leave European Companies at Risk*, IDC #EMEA42819617, juni 2017.