Rexel makulering

Hvorfor er gode rutiner for behandling av papirdokumenter en del av GDPR forordningen (General Data Protection Regulation)

Ansvarsbeskrivelse

Ikke noe i dette dokumentet er å anse som som juridisk rådgivning. Bedrifter bør søke juridisk rådgivning i forhold til overholdelse av personvernloven og annen gjeldende lovgivning og forordninger.

Om dette dokumentet

Denne rapporten gir deg **en oversikt over hva formålet med GDPR er**, og hvilke utfordringer det kan innebære for bedrifter og organisasjoner.

Formålet med dette dokumentet er å gi deg en innføring i den nye generelle forordning om datasikkerhet (GDPR). Hvordan kan denne påvirke ulike virksomheter så bedriften kan utvikle et rammeverk for rutiner for dokumentsikkerhet før bestemmelsen trer i kraft i mai 2018.

Hva er GDPR? Forordningen krever at virksomheten har en pålitelig sikkerhetspraksis rundt elektroniske og papirbaserte data, og at de i tilfelle av brudd på personsikkerheten underretter berørte eller potensielt berørte personer.
GDPR har en global rekkevidde til alle organisasjoner som kontrollerer eller bearbeider identifiserbare personopplysninger, uansett organisasjonens geografiske plassering.
Kravene i GDPR gjelder både elektroniske og papirbaserte personlige opplysninger. Det betyr at alle organisasjoner skal forholde seg til kravene i GDPR hvis de håndterer personlig, identifiserbare opplysninger.

For mange organisasjoner er sikring av elektroniske data med rette førsteprioritet, men det er mange som ikke i tilstrekkelig grad forholder seg til sikring av papirbaserte data. Faktisk erkjenner nesten to av tre virksomheter at de ikke makulerer fortrolige opplysninger[1]. Det gir en risiko for at virksomheten ikke overholder kravene i GDPR, og dermed at opplysninger kan utnyttes til bedrageri og identitetstyveri. Med utgangspunkt i dette, vil Rexel som et ledende varemerke innen makulering oppfordre virksomheter til å gjennomgå deres rutiner og praksis for både papirbaserte og elektroniske data.

DEN GENERELLE FORORDNINGEN OM DATABESKYTTELSE (GDPR)

En oversikt

GDPR sørger for å beskytte enkeltpersoners personsikkerhet. Disse rettighetene til beskyttelse av personlige opplysninger inkluderer, men er ikke begrenset til:

Informasjon
Retten til å få klare opplysninger om og hvordan virksomheten behandler personlige opplysninger.

Samtykke
Retten til å kontrollere hvordan virksomheten anvender personlige opplysninger.

Sikkerhet
Retten til å få opplysninger om og hvordan virksomheten beskytter og behandler personlige opplysninger.

Begrensning av innsamling og formål
Retten til å forvente at virksomheter minimerer innsamling og bruken av opplysninger.

Varsling om brudd på sikkerheten
Retten til å bli varslet i tilfelle av et brudd på datasikkerheten.

GDPR inngår i den europeiske kommisjonens plan for å modernisere og harmonisere personvernreglene.

Selv om den viktigste målsetningen for GDPR er å styrke retten til beskyttelse av personlige opplysninger elektronisk, omfatter den også papirbasert datasikkerhet.

Den fokuserer på håndteringen av de stadig større utfordringer i forbindelse med beskyttelse av privatlivets fred og personlige opplysninger, risikoen for sikkerhetsbrudd, hacking og andre former for ulovlig handling.

DEN GENERELLE FORORDNINGEN OM DATABESKYTTELSE (GDPR)

Hva er endret?

Følgende punkter **belyser de konkrete områdene i GDPR hvor nye** rettigheter for enkeltpersoner eller eksisterende rettigheter i henhold til Data Protection Act (DPA, databeskyttelsesloven), som har blitt styrket som en del av GDPR:

Dataoverføring og retten til å bli glemt

- En person har nå rett til å flytte sine personlige opplysninger fra en organisasjon til en annen.
- Personlige opplysninger skal oppgis i et format som er strukturert og maskinlesbart.
- En person kan anmode om sletting eller fjerning av personlige opplysninger.

Varsling om brudd på datasikkerheten

- Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles.
- Personer som er berørt av sikkerhetsbruddet skal informeres.

Fortegnelse

- Virksomheter må opprettholde et register over bearbeidingsaktiviteter under deres ansvar.

Konsekvensanalyser vedrørende databeskyttelse og sikkerhet

- Formålet med konsekvensanalyser vedrørende databeskyttelse er å identifisere høy risiko i forhold til enkeltpersoners rett til beskyttelse av personlige opplysninger.
- Sikkerhetskrav og -anbefalinger skal baseres på en risikovurdering.

Dataforvaltning og ansvarlighet

- Virksomheter må kunne bevise at GDPR etterleves.

Manglende overholdelse av GDPR kan medføre **bøter på opptil 20 millioner Euro, eller 4% av foretakets globale inntekter**, alt etter hvilket beløp som er størst. Videre har en registrert person rett til å saksøke virksomheten.

DEN GENERELLE FORORDNINGEN OM DATABESKYTTELSE (GDPR)

Hvem gjelder den for?

Innføringen av GDPR i mai 2018 kommer til å påvirke følgende roller:

Dataansvarlige – de bestemmer hvordan og hvorfor personlige opplysninger behandles
Databehandlere – personer som handler på vegne av dataansvarlig

Disse to rollene har ansvaret for å sikre at deres kunder til fulle overholder alle aspekter av GDPR for å unngå bøter.

Databehandleren og den dataansvarlige kan ha behov for å **oppnevne et personvernombud** og ha rutiner for innsamling og bruk av personopplysninger.

GDPR omfatter personopplysninger og sensitive personlige opplysninger i elektroniske og fysiske formater

Det er viktig å overveie hvilke typer opplysninger GDPR gjelder for, før du etablerer retningslinjer og rutiner for din virksomhet.

Data som omfattes av GDPR gjelder informasjon om en identifiserbar person. Blant eksemplene som faller under GDPR finnes fullstendig navn, epostadresse og telefonnummer.

GDPR tilfører også ytterligere beskyttelse til en **underkategori av personlige opplysninger som kalles sensitive personlige opplysninger.**

GDPR omhandler personlige opplysninger som håndteres av virksomheten i både **elektroniske og fysiske formater**, som f. eks. papirdokumenter.

Et foretaksregelverk for overholdelse av GDPR

Virksomheter har tre overordnede områder som skal gjennomgås med henblikk på overholdelse av GDPR. Gjennom disse tre områdene kan virksomheten skape et tydelig rammeverk for en datasikkerhetsrutine som gjelder alle aspekter og som vil underlette overholdelse på alle områder av GDPR.

De tre områdene er:

Personer

Det er essensielt at medarbeiderne påtar seg eierskap og ansvar i forbindelse med alle data som behandles av dem i virksomheten. Virksomheten skal fastlegge klare rutiner for hver enkelt medarbeider for korrekt behandling av alle elektroniske og papirbaserte data. Disse bestemmelsene iverksetter kravene i GDPR-håndteringen av alle opplysninger. Du kan for eksempel med fordel innføre regler for bruk av papirdokumenter som inneholder sensitive opplysninger og prosessen for korrekt makulering av et dokument når det ikke lenger skal brukes, basert for sensitivitetsnivået for opplysninger i dokumentet.

Prosesser

Dette vedrører prosessene i virksomheten. For eksempel administrasjon av bruken av data, som behandling eller lagring av opplysninger om kunder. Det er meget viktig at virksomheten gjennomgår alle deres nåværende dataprosesser. Når det identifiseres hull og svakheter i de eksisterende prosedyrer, skal virksomheten utvikle en ramme som sikrer at disse områdene styrkes og endres der hvor det er nødvendig, med henblikk på overholdelse av GDPR.

Teknologi

Selv nåværende IT-kapasitet og -krav skal granskes og justeres innen mai 2018. Det er opp til den enkelte virksomhet å sikre at eventuelle eksisterende systemer som ikke fullt ut understøtter kravene, enten forbedres eller byttes ut for å unngå potensielle bøter når GDPR trer i kraft.

Hvorfor er papirsikkerhet viktig?

Etter å ha diskutert kravene til virksomheten som følge av GDPR, er det nå relevant å adressere problemet med papirsikkerheten og se på hvorfor det har stor betydning når man forbereder seg på å kunne leve opp til kravene i GDPR.

En PwC-rapport fra 2014 som var utarbeidet i samarbeid med sikkerhetsarkiverings-firmaet Iron Mountain[2] undersøkte hvordan europeiske bedrifter i mellomsegmentet oppfattet og administrerte sin informasjonsrisiko. Den viste at to tredjedeler av de spurte sa at risikohåndtering forbundet med papirdokumenter var et høyt prioritert problem.

Selv om digitale trusler står høyt på en virksomhets dagsorden, vil det være feil å anta at ***papirbasert sikkerhetsrisiko*** *ikke lenger finnes.*

Papirdokumenter utsettes fortsatt for mange vanlige sikkerhetsbrudd

Av 598 brudd på datasikkerhet som ble registrert mellom juli og september 2016 av de britiske tilsynsmyndighetene ICO (Information Commissioner's Office):

14% skyldes papirarbeid som ble mistet eller stjålet. **19%** ble sendt via post eller telefaks til feil mottaker. **4%** skyldes at opplysninger hadde blitt oppbevart på et ikke sikret sted. **Ytterlige 3%** skyldes ikke sikret kassering av papirdokumenter. Så til tross for vesentlig økning innenfor digitale teknologier-, kunne **40% av hendelsene** tilskrives papir [3].

40% av datasikkerhetshendelser i Storbritannia kunne tilskrives papir

Brukersamarbeid er avgjørende for overholdelse av GDPR

Hvis vi kan konkludere med at papirsikkerhet fortsatt er avgjørende for informasjonssikkerheten, er spørsmålet: Hva kan bedrifter gjøre med dette?

Rexel har spesialisert seg på å tilby bedrifter makuleringsmaskiner. Muligheten til å samarbeide direkte med virksomheter som Kensington - verdens ledende innenfor fysisk sikkerhet av it-hardware har gitt oss verdifull innsikt i de behov, ønsker og utfordringer som bedrifter stilles ovenfor når de vil beskytte seg selv og etterleve kravene i GDPR.

Med denne innsikten ser vi to hovedårsaker til at man ikke får til en effektiv makulering av dokumenter i bedriftene:

Manglende bevissthet

Virksomheter overser viktigheten av papir i en verden hvor stadig mer digitaliseres. Derfor tar de seg ikke tid til å løse sikkerhetsproblemene med papirdokumenter. Selv når det er etablert, vil det ofte være en manglende bevissthet om problemet hvis ikke bestemmelsene kommuniseres ut på en effektiv måte til alle nivåer i bedriften.

Brukervennlighet

Hvis en effektiv rutine for makulering av dokumenter skal bli vellykket, er tilgjengeligheten til riktig makuleringsmaskin en avgjørende suksessfaktor. Organisasjoner og bedrifter setter ofte sin lit til ineffektive, manuelle makuleringsmaskiner som ikke oppfyller kravene til en effektiv og produktiv makulering.

Når man har kartlagt de bakenforliggende årsakene for å implementere en effektiv makuleringsrutine, er neste steg å finne en passende løsning som takler disse hindringene.

Årsak 1
til at GDPR ikke overholdes

Manglende bevissthet

Medarbeidere utfører som regel oppgaver som deres overordnede har fremhevet som prioritet.

Med tanke på dette kan en klar og konkret rutine for dokumenthåndtering løse ineffektivitet ved makulering.

I PwC og Iron Mountains undersøkelse fra 2014 av det europeiske mellomsegmentet[2] fremgår det at kun 40% har tydelige retningslinjer for de ansatte for intern lagring og avhending av fysiske dokumenter. Kun 27% har en rutine for sikkerhet, sikker oppbevaring og makulering av konfidensiell informasjon.

Årsak 2
til at GDPR ikke overholdes

Brukervennlighet

En annen vanlig grunn til at medarbeidere ikke overholder kravene for dokument-makulering, er at oppgaven er vanskelig og tidkrevende.

Selv om medarbeiderne har tilgang til en makuleringsmaskin, er det ikke alle som nødvendigvis makulerer dokumentene som skal makuleres, hvis prosessen er for tidkrevende eller for vanskelig å administrere.

Det er ikke overraskende at ingen bedrifter vil investere i en makuleringsmaskin som deres ansatte trolig ikke bruker på grunn av dårlig produktivitet eller brukervennlighet. Disse problemene bør løses for å sikre maksimal bruk.

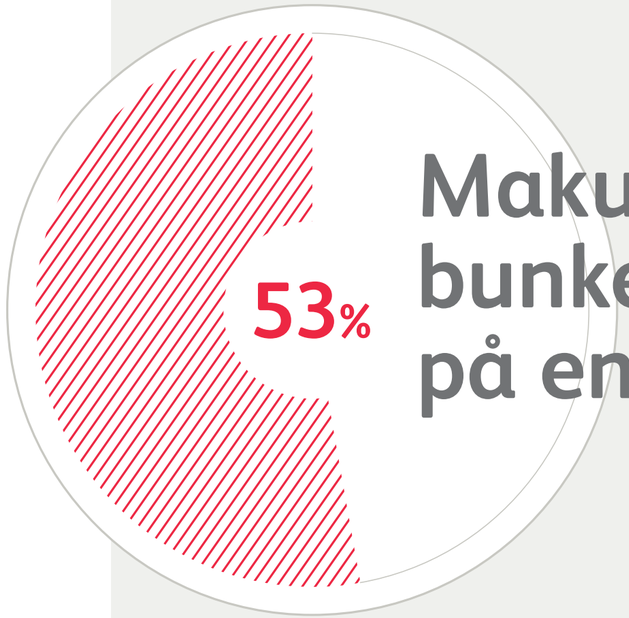
Få økt produktivitet med en makuleringsmaskin med automatisk dokumentmating

Konklusjon:

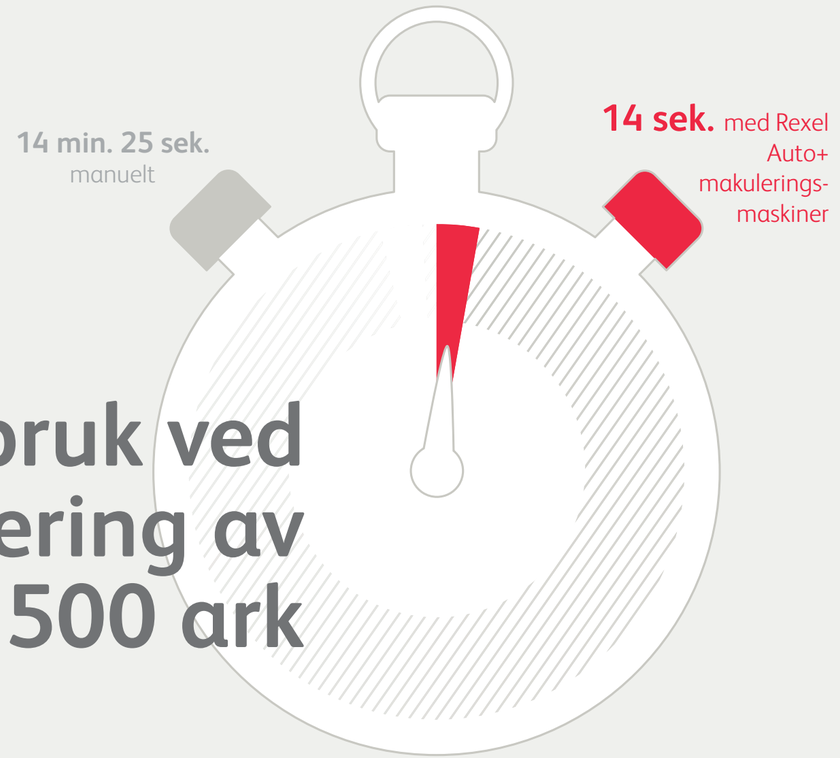
Makuleringsmaskiner med automatisk dokumentmater er et direkte svar på bedriftenes behov for å sikre at de ansatte etterlever kravet til papirsikkerhet.

Våre undersøkelser[4] viser at 53 % av medarbeidere makulerer i omganger, det vil si de samler en stabel av dokumenter før de føler det er på tide med et besøk til makuleringsmaskinen.

Når de ansatte får mulighet til å makulere større bunker med papir, viser det seg i følge en uavhengig undersøkelse, at man **bruker 98% mindre tid på å makulere**[5] og man blir mer motivert til å makulere oftere.



Makuler mindre bunker eller alt på en gang



Tidsforbruk ved makulering av 500 ark

6 vesentlige punkter om GDPR som bør overveies

1. Overvei å utnevne et personvernombud

Ombudet må være fullstendig inneforstått med virksomhetens ansvar i forhold til GDPR og ha inngående kjennskap til hvilke opplysninger i virksomheten som er personlige, hvor de lagres, hvem som har tilgang til dem, hvordan brudd på sikkerheten oppdages, når det skjer og hvem det skal rapporteres til. **Ombudet kan være en ansatt eller en profesjonell tredjepart.**

2. Analyser dine systemer

Gjennomgå alle kontrakter, teknisk support, prosedyrer og verktøy som brukes i forbindelse med behandling, håndtering, oppbevaring og sletting av data så du blir i stand til å identifisere alle svakheter eller mangler som krever endringer.

3. Utarbeid en strategi

Etabler en ny strategi som sikrer full overholdelse av GDPR. Strategien kan omfatte investering i ny teknologi, revidering av medarbeider-prosedyrer, og ansvaret for databehandling samt opprettelse av nye roller i organisasjonen.

4. Implementer nye organisasjonsrutiner

Det neste skrittet mot overholdelse av GDPR er å iverksette din handlingsplan på alle nivåer i organisasjonen. Invester i og introduser ny teknologi og nye systemer som er nødvendige. Offentliggjør en informativ veiledning til datahåndtering- og behandling.

5. Engasjement hos de ansatte

Presenter de nye dataoverholdelses-rutinene for alle medarbeidere og sørg for at de får de nødvendige kvalifikasjoner, opplysninger og veiledninger for å være velinformerte og bevisste om de endringer som skjer og om deres eget ansvar for å sikre at virksomheten oppfyller kravene i GDPR.

6. Evaluering og forbedring

Når du har lansert din GDPR plan, er tiden inne til å evaluere og forbedre før forordningen trer i kraft. Identifiser alle nødvendige forbedringer i god tid før fristen i mai 2018, så din bedrift er tilpasset forandringene og overholder GDPR.

KILDER

1 envirowaste.co.uk/blog/articles/third-companies-shred-private-documents

2 Beyond good intentions: The need to move from intention to action to manage
information risk in the mid-market. PwC-rapport utarbeidet i samarbeid med Iron Mountain, juni 2014.

3 ico.org.uk/action-weve-taken/data-security-incident-trends

4 Evaluating Auto Feed Shredders. Utarbeidet for ACCO Brands v Deep Blue Insights

5 Uavhengig test fra Intertek Testing & Certification Ltd, juni 2012.
Størst besparelse ved bruk av Auto+ 500X i forhold til en tradisjonell makuleringsmaskin på tilsvarende prisnivå.
Undersøkelsen viser at det tar i gjennomsnitt 14 minutter og 25 sekunder å manuelt makulere en papirbunke på 500 ark
i en vanlig, manuell makuleringsmaskin. Til sammenligning tar det kun 14 sekunder å legge ned samme antall ark i en Rexel Auto+ makuleringsmaskin.