Safe Online ApS
CVR: 38589962
Nørrebrogade 47
2200 København N, Danmark
Tlf: (+45) 31 66 34 00

GDPR Risiko-rapport

Udarbejdet på vegne af Acme

Indholdsfortegnelse

1. Opsummering 3
2. Introduktion 4
3. Definitioner 5
4. Analyse 6
Risikofordeling 6
Risikonumre 7
Risikoord 9
5. Oprydningsmetode 13
6. Konklusion 14
7. Anbefalinger 16

1. Opsummering

Statistikken nedenfor viser resultaterne af et **GDPR-risikoscan**, der er udført på jeres data med IT-løsningen DataMapper. Scanningen identificerer de områder, hvor jeres virksomhed har størst risiko for at overtræde GDPR.

Et signifikant antal af risikofiler er blevet fundet i jeres data, hvilket understreger behovet for en struktureret og kontinuerlig oprydningsproces.

Nøglestatistik

Risikofordeling

- **5.113.230** filer er scannet i alt
- **166.314** (3.3% af alle) filer er fundet med risiko

Datakilder

- **Outlook:** 36.419 risikofiler ud af 941.124 scannede filer (3,87%)
- **OneDrive:** 22.641 risikofiler ud af 799.767 scannede filer (2,83%)
- **SharePoint:** 107.254 risikofiler ud af 3.372.339 scannede filer (3,18%)

Hyppigste dokumenttyper med risiko

1. **E-mails**: 85.603 dokumenter
2. **Øvrige dokumenter**: 16.636 dokumenter
3. **Finansielle dokumenter**: 15.601 dokumenter

Hyppigste risikonumre

1. **CPR-numre**: 9.598 dokumenter
2. **Pasnumre**: 5.113 dokumenter
3. **Kørekortnumre**: 3.101 dokumenter

2. Introduktion

Databeskyttelsesforordningen (GDPR) stiller skrappe krav og regler for virksomheders håndtering af personoplysninger. Overtrædelse af disse regler kan medføre alvorlige juridiske sanktioner og i nogle tilfælde bøder på op til **4% af den årlige omsætning**. Derudover kan mistillid fra kunder og interessenter få endnu mere vidtrækkende konsekvenser for en virksomhed.

At sikre overholdelse af GDPR er afgørende af flere grunde. Det reducerer risikoen markant, fremmer tillid, forbedrer kundeforhold og styrker loyaliteten. Virksomheder, der aktivt tager ansvar for persondata og datasikkerhed, opnår en klar fordel ved at vise, at de overholder lovgivningen og beskytter deres kunders oplysninger, hvilket skaber tillid hos både kunder og medarbejdere.

For at håndtere data både sikkert og ansvarligt – og for at overholde GDPR – er det essentielt at anvende en risikobaseret tilgang til informationssikkerhed. Denne tilgang indebærer at gennemføre grundige risikovurderinger og GAP-analyser for at identificere sårbarheder, trusler og potentielle konsekvenser ved et databrud. Ved proaktivt at lukke disse huller kan virksomheder styrke deres overholdelse af regler som NIS2 og samtidig vise deres engagement i at beskytte følsomme oplysninger.

Om denne rapport

Denne rapport er en risikovurdering baseret på en GDPR-risikoscan, der er udført på jeres data ved hjælp af IT-løsningen **DataMapper**. Rapporten præsenterer jeres GDPR-risiko baseret på de data, I opbevarer. Det giver jer datadrevne og opdaterede indsigter i virksomhedens samlede GDPR-risiko. Rapporten anvendes i forbindelse med interne eller eksterne audits.

Det er vigtigt at huske, at denne rapport udelukkende er en analyse med det formål at vurdere jeres GDPR-risiko. I konklusionen vil rapporten komme med anbefalinger til tiltag, der kan hjælpe med at rydde op i jeres personoplysninger.

Hvad er et GDPR-risikoscan?

For at reducere GDPR-risici forbundet med håndtering af personoplysninger er det nødvendigt, at en virksomhed har overblik over de persondata, den ligger inde med. Jo mere følsom data I har gemt, desto større er risikoen. At blive udsat for et hackerangreb kan sammenlignes med et indbrud i hjemmet – hvis I har fjernet alle værdigenstande, er der intet for tyven at stjæle. En GDPR-risikoscan lægger **grundlaget for at fjerne alle personoplysninger**, så uønskede gæster ikke har noget at stjæle.

GDPR-risikoscan foretages af DataMapper. DataMapper er et data discovery-værktøj, der anvender AI og maskinlæringsalgoritmer til at finde tal og ord, der kategoriseres som følsomme, på tværs af virksomhedens medarbejdere, cloud-lagring, e-mails, systemer og apps. DataMapper scanner datasystemer for at finde dokumenter, e-mails og billeder, der indeholder ord og udtryk relateret til GDPR. Scanningen dækker både aktive og tidligere brugerkonti i de valgte datakilder.

3. Definitioner

Risikoniveauer

For at skabe en bedre forståelse af risikoniveauerne i denne rapport er niveauerne opdelt i to kategorier baseret på indhold og potentielle GDPR-konsekvenser.

Risikonumre

Filer med risikonumre indeholder følsomme personnumre, der i sig selv kan bruges til at identificere en person direkte. Disse filer indeholder ofte:

- Personnummer (CPR)
- Pasnumre
- Kørekortnumre
- Kreditkortnumre

Risikoord

Filer med risikoord indeholder følsomme, personhenførbare ord, der nævnes i sammenhæng med en person.

DataMapper bruger en GDPR-taksonomi til at klassificere ord, der potentielt er følsomme. Men de betragtes kun som følsomme, hvis de nævnes i relation til en person. For eksempel i en sætning som “Peter Jackson var medlem af LGBT-klubben”, er “Peter Jackson” et navn, vi leder efter, og “LGBT” er et følsomt ord fra vores taksonomi. Hvis “Peter Jackson” ikke blev nævnt, ville udtrykket “LGBT” ikke blive betragtet som følsomt. Forud for denne rapport har du indtastet personnavne i DataMapper, som er relateret til din virksomhed.

Risikiord er i henhold til GDPR artikel 9(1) opdelt i følgende kategorier:

1. Race eller etnisk oprindelse
2. Politiske holdninger
3. Religiøs eller filosofisk overbevisning
4. Fagforeningsmedlemskab
5. Genetiske data
6. Biometriske data
7. Helbredsoplysninger
8. Seksuel orientering

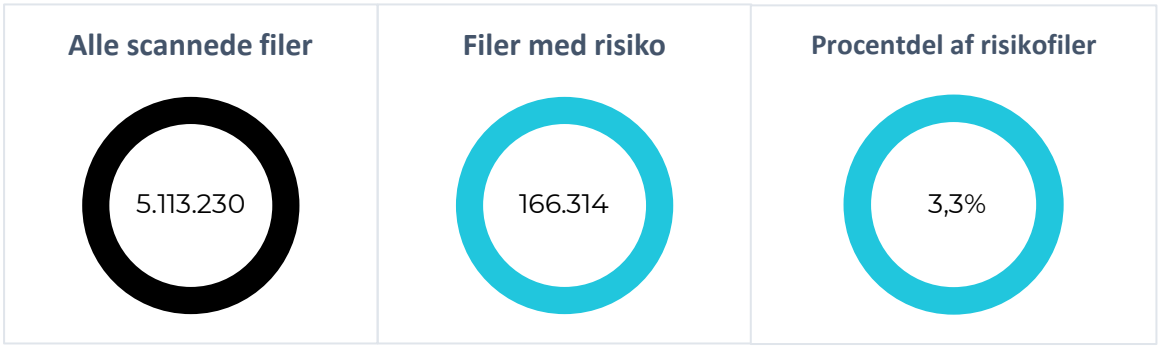
4. Analyse

Risikofordeling

For at give et klart overblik over jeres data er det vigtigt at forstå risikofordelingen. Dette overblik danner grundlaget for at vurdere, hvor I står i forhold til at overholde GDPR og for at kunne afbøde potentielle sikkerhedstrusler.

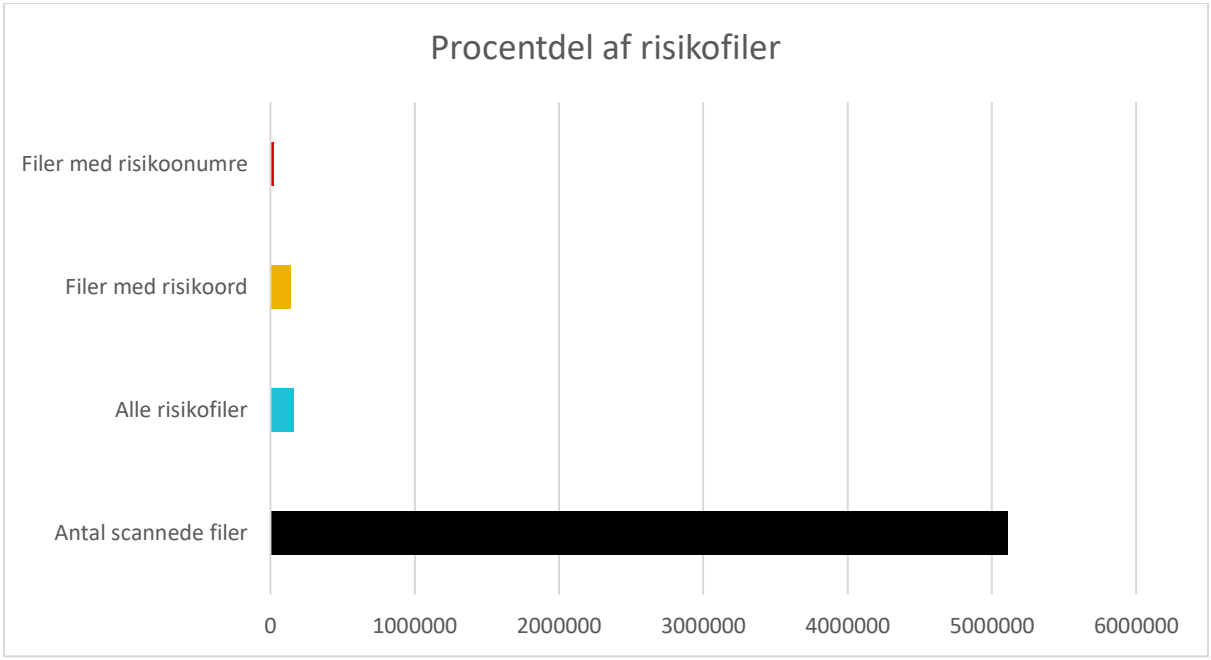
Samlet risikofordeling

Følgende statistik skal give jer et overblik over de scannede filer. Først angives det samlede antal scannede filer, dernæst antallet af filer, hvori der er risiko og endelig hvor stor en procentdel af jeres filer, der indeholder risiko.



Risikofordeling

Følgende diagram illustrerer fordelingen af risikofiler blandt det samlede antal scannede filer. Det opdeler risikoen i filer med risikonumre og filer med risikoord.

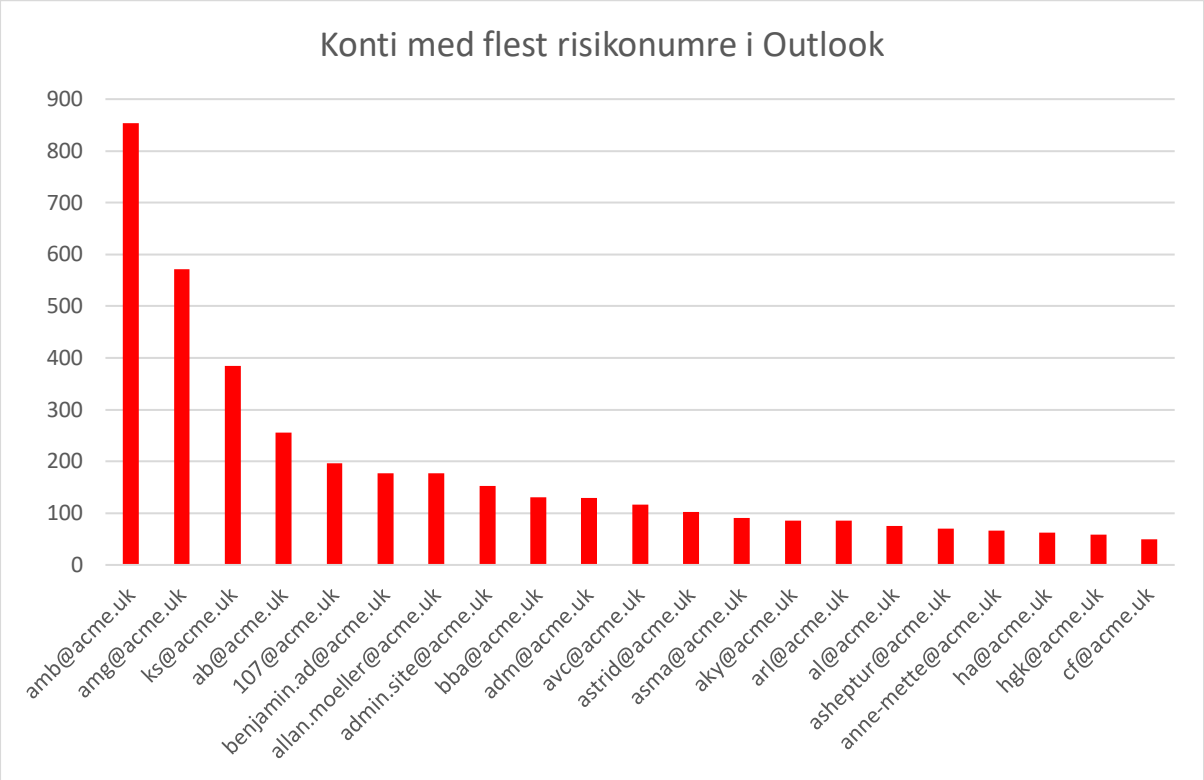


Ud af i alt **5.113.230 scannede filer** har GDPR risikoscannet identificeret **166.314 risikofiler** på tværs af jeres data, hvilket svarer til **3,3%**.

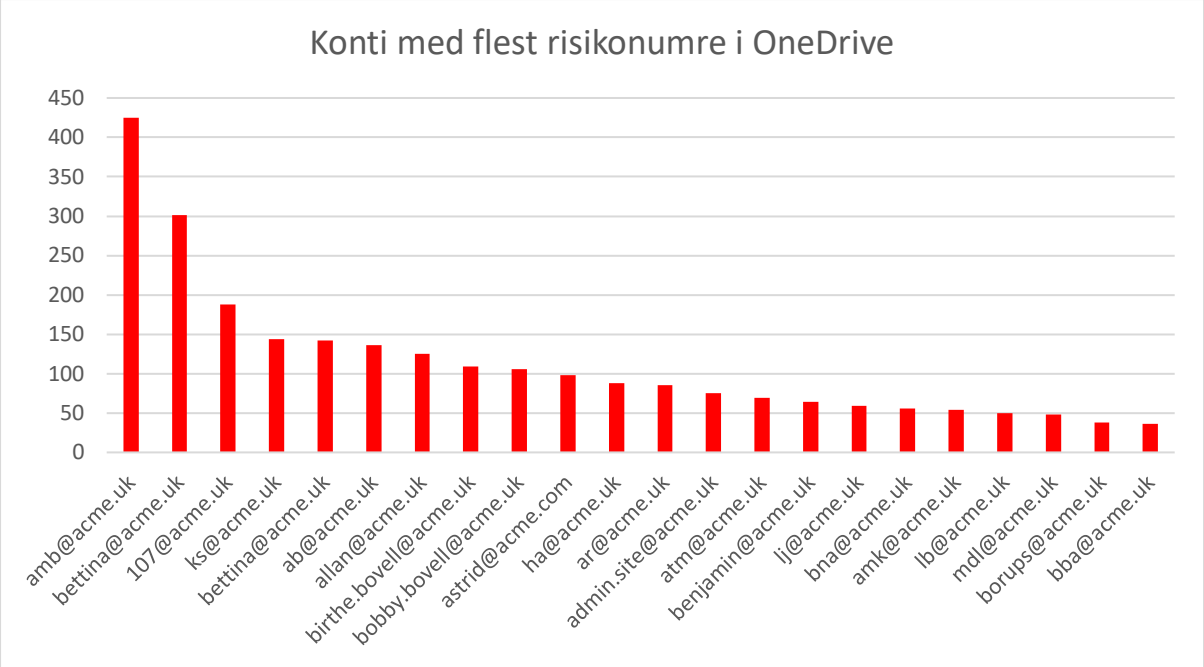
Risikonumre

Denne sektion fokuserer på filer med **risikonumre**. Som tidligere nævnt er filer med risikonumre filer, der indeholder følsomme numre, som i sig selv kan bruges til at identificere en person direkte.

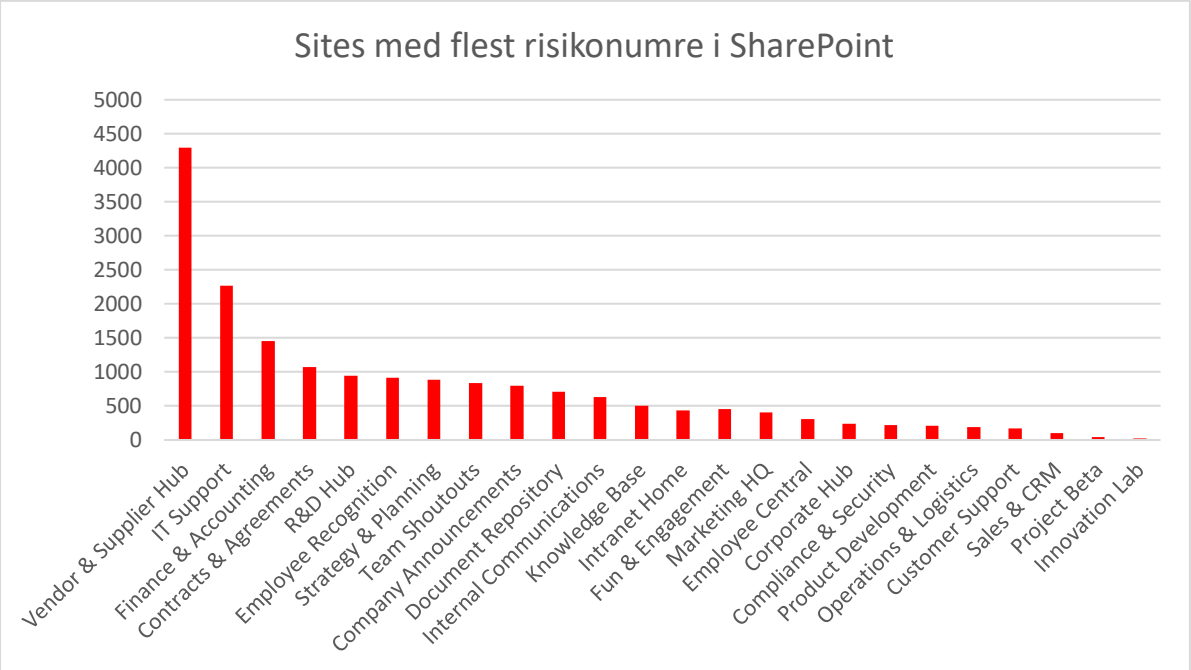
Sektionen indeholder et diagram for hver af jeres scannede datakilder, der hver især viser de konti, der har flest filer med risikonumre i den pågældende datakilde.



Der er i alt fundet **760 Outlook-konti** i jeres virksomhed. Ud af disse indeholder **320** konti filer med risikonumre. Det samlede antal filer med risikonumre er **3.891**.



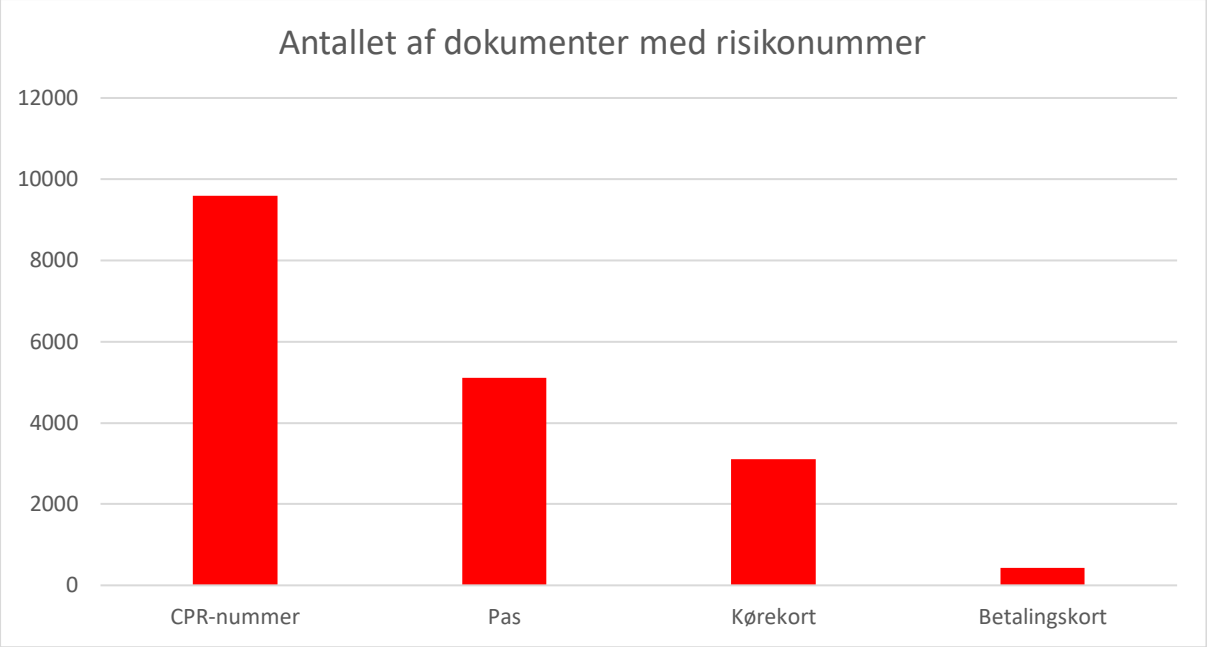
Der er i alt fundet **760 OneDrive-konti** i jeres virksomhed. Ud af disse indeholder **174** konti filer med risikonumre. Det samlede antal filer med risikonumre er **2.496**.



Der er i alt fundet **164 SharePoint-sites** i jeres virksomhed. Ud af disse indeholder **128** sites filer med risikonumre. Det samlede antal filer med risikonumre er **18.103**.

Type af risikonumre

Nedenstående diagram viser antallet af dokumenter med specifik type af risikonumre.

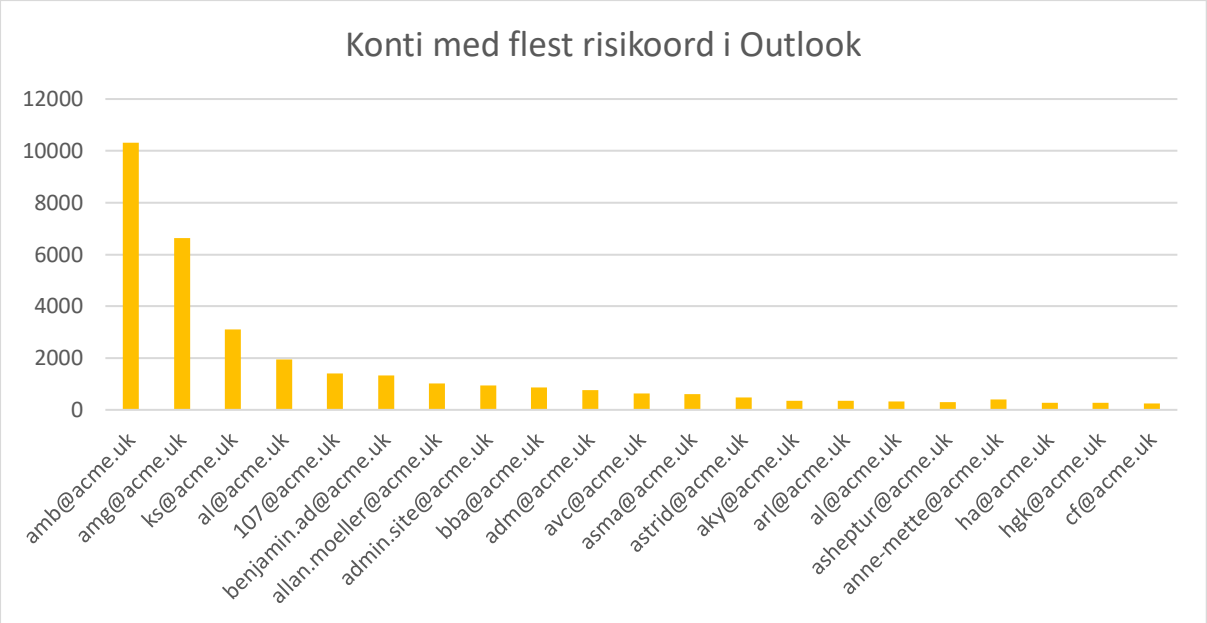


Der er i alt fundet **9.598** dokumenter med CPR-numre, **5.113** dokumenter med pasnumre, **3.101** dokumenter med kørekortnumre og **434** dokumenter med kreditkortnumre.

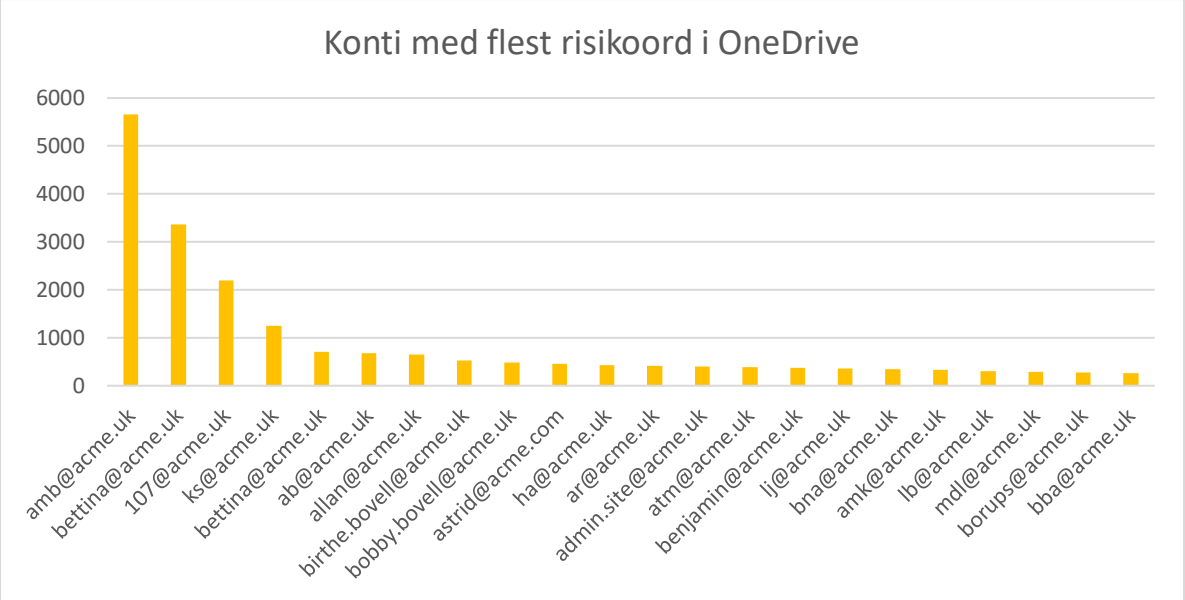
Risikoord

Denne sektion fremhæver filer med risikoord. Som tidligere nævnt er dette filer, der indeholder følsomme personrelaterede ord, som nævnes i relation til en person.

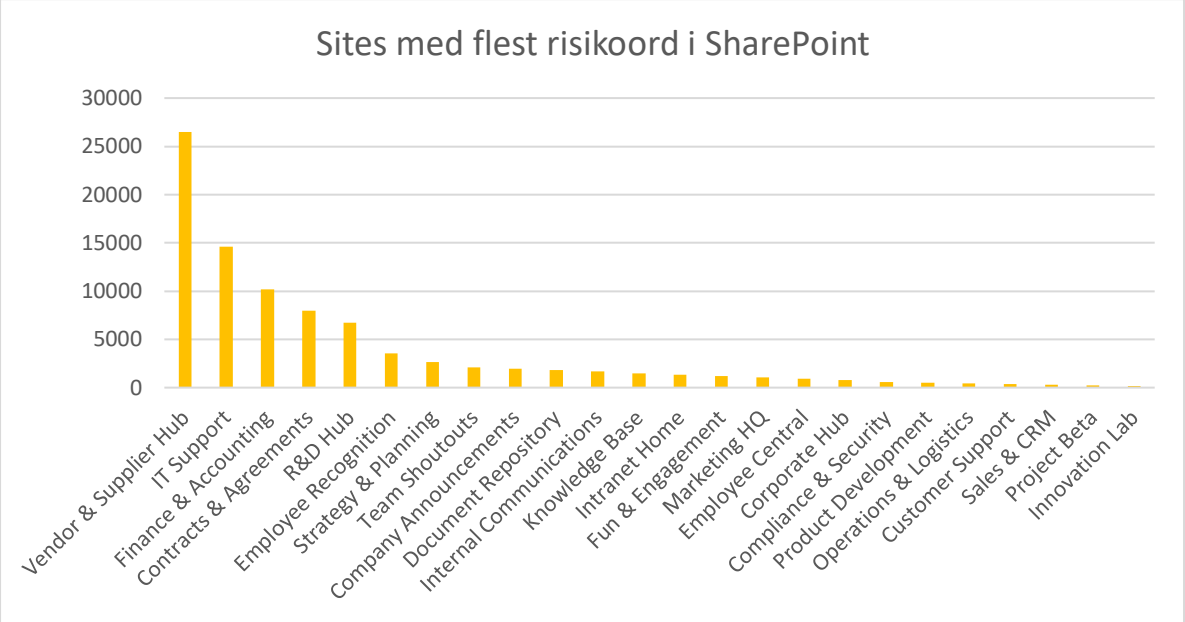
Sektionen indeholder et diagram for hver af jeres scannede datakilde, som viser de konti med det flest antal filer med risikoord i den pågældende placering.



470 ud af **760** konti blev identificeret som indeholdende risikoord. Det samlede antal filer med risikoord, der er fundet i jeres konti, er **32.528**.



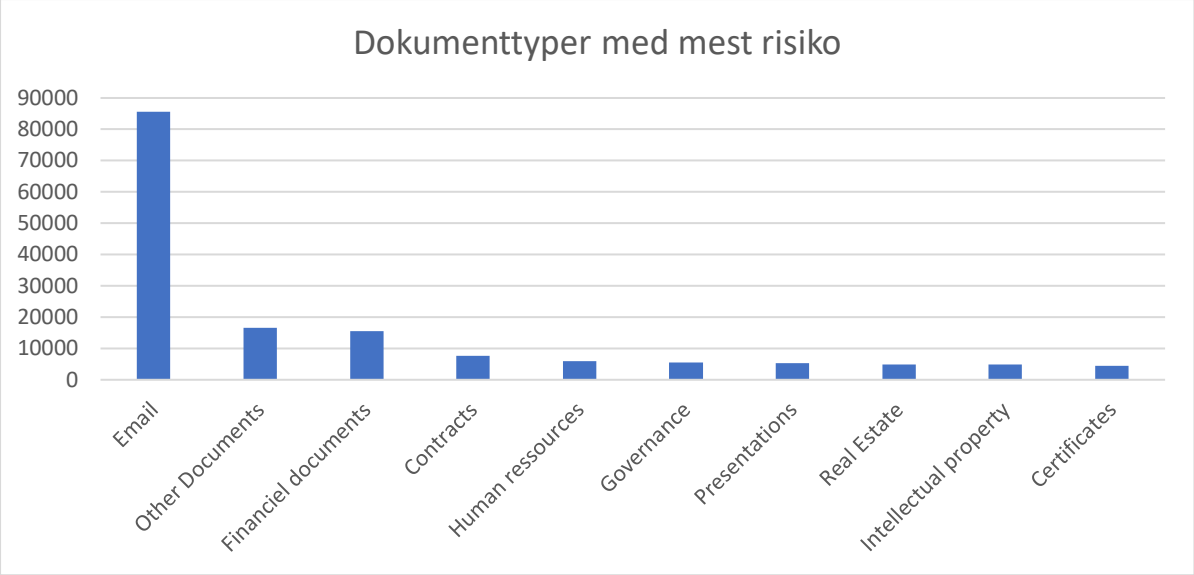
202 ud af **760** konti blev identificeret som indeholdende risikoord. Det samlede antal filer med risikoord, der er fundet i jeres konti, er **20.145**.



140 ud af **164** sites blev identificeret som indeholdende risikoord-indhold. Det samlede antal filer med risikoord, der er fundet i jeres konti, er **89.151**.

Dokumenttyper med mest risiko

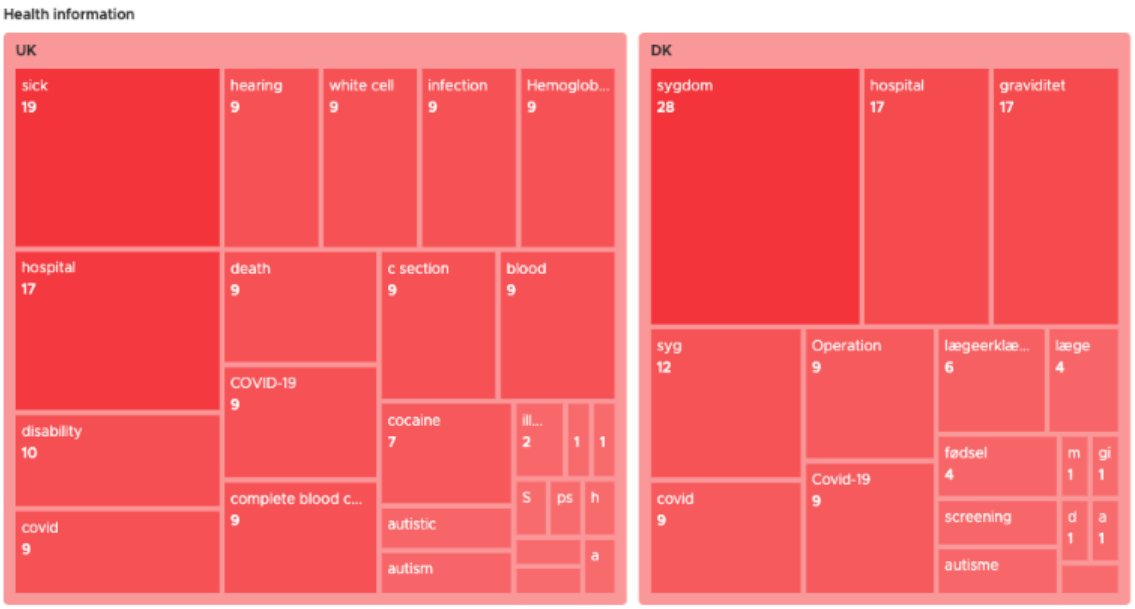
For at skabe et overblik opdeles alle scannede filer i dokumenttyper. Følgende diagram viser de dokumenttyper, der indeholder mest risiko.

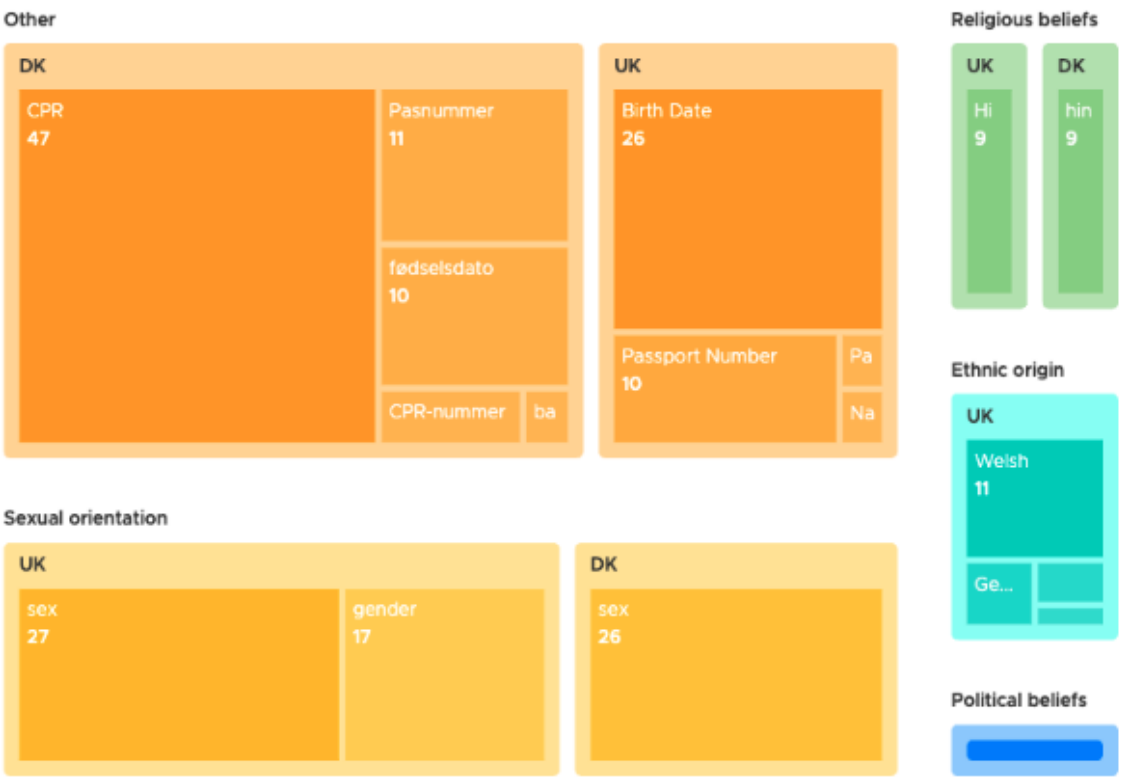


Dokumenttyperne med mest risiko er som følger: **85.603** e-mails, **16.636** øvrige dokumenter, **15.601** finansielle dokumenter, **7.594** kontrakter, **5.993** HR-dokumenter, **5.478** styringsdokumenter, **5.214** præsentationer, **4.869** ejendomsdokumenter, **4.782** dokumenter vedrørende immaterielle rettigheder og **4.544** certifikater.

Hyppigste risiko-termer

Heatmappet nedenfor visualiserer de risiko-termer, der er fundet i sammenhæng med personnavne. Disse termer er opdelt i 8 grupper i overensstemmelse med de følsomme kategorier, der er defineret i GDPR artikel 9, stk. 1. Dette giver et klart overblik over, hvilke kategorier af følsomme termer der forekommer hyppigst. Hvis I vil se mere af heatmappet, kan I få adgang til det via **Dashboard → Generelt**.




Other
DK
CPR
47
Pasnummer
11
fødselsdato
10
CPR-nummer
ba
UK
Birth Date
26
Passport Number
10
Pa
Na
Religious beliefs
UK
Hi
9
DK
hin
9
Ethnic origin
UK
Welsh
11
Ge...
Political beliefs
Sexual orientation
UK
sex
27
gender
17
DK
sex
26

5. Oprydningsmetode

Analysen viser, at jeres virksomhed har følsomme oplysninger, der kræver oprydning for at sikre overholdelse af GDPR, og beskyttelse mod potentielle risici. I står nu over for et valg: Skal oprydningen ske manuelt eller automatiseret?

Manuel oprydning

Manuel oprydning er både tidskrævende og er ofte svært at tjekke, om medarbejdere udfører den konsekvent. Mange virksomheder oplever udfordringer med at få medarbejderne til at prioritere oprydning blandt deres øvrige opgaver. Dette øger risikoen for, at følsomme data overses, hvilket kan føre til bøder og skade virksomhedens omdømme.

Automatiseret oprydning

DataMapper tilbyder en langt mere effektiv løsning, hvor store dele af oprydningsprocessen automatiseres. Værktøjet scanner løbende dine data for følsomme oplysninger og identificerer de risikofyldte elementer, der kræver handling. Medarbejderne skal stadig træffe beslutning om, hvorvidt data skal slettes eller flyttes, men DataMapper reducerer den nødvendige tid markant.

Med DataMapper kan du:

- Reducer tiden brugt på oprydning markant
- Minimer risikoen for menneskelige fejl og manglende tilsyn
- Få et klart overblik over, hvor de største risici er, og hvordan de skal håndteres
- Frigør ressourcer, så jeres medarbejdere kan fokusere på deres kerneopgaver

Sammenligning for jeres virksomhed

Tabellen nedenfor sammenligner omkostninger og effektivitet ved manuel oprydning med brugen af DataMapper for en virksomhed med **100 medarbejdere**.

Oprydningsform	Medarbejdertimer*	Omkostning**
Manuuel	1.600	DKK 44,000
DataMapper	150	DKK 41.250 (+ abonnement)

* Tid det tager en virksomhed at rydde op årligt. Ifølge vores data bruger en medarbejder i gennemsnit 16 timer om året på manuel oprydning, mens det tager 1,5 time med DataMapper. Tiden er ganget med antallet af medarbejdere.
** Antal mandetimer ganget med gennemsnitlig timeløn for en medarbejder, som vi antager er DKK 275.

Som man kan se, viser resultaterne en markant reduktion i mandetimer og omkostninger.

6. Konklusion

Ud af i alt **5.113.230 scannede filer** har GDPR risikoscannet identificeret **166.314 risikofiler** på tværs af jeres data, hvilket svarer til **3,3%**.

Outlook
Der er i alt fundet **760 Outlook-konti** i jeres virksomhed. Ud af disse indeholder **320** konti filer med risikonumre. Det samlede antal filer med risikonumre er **3.891**.
470 ud af **760** konti blev identificeret som indeholdende risikoord. Det samlede antal filer med risikoord, der er fundet i jeres konti, er **32.528**.

OneDrive
Der er i alt fundet **760 OneDrive-konti** i jeres virksomhed. Ud af disse indeholder **174** konti filer med risikonumre. Det samlede antal filer med risikonumre er **2.496**.
202 ud af **760** konti blev identificeret som indeholdende risikoord. Det samlede antal filer med risikoord, der er fundet i jeres konti, er **20.145**.

SharePoint
Der er i alt fundet **164 SharePoint-sites** i jeres virksomhed. Ud af disse indeholder **128** sites filer med risikonumre. Det samlede antal filer med risikonumre er **18.103**.
140 ud af **164** sites blev identificeret som indeholdende risikoord-indhold. Det samlede antal filer med risikoord, der er fundet i jeres konti, er **89.151**.

Risiko-information
Der er i alt fundet **9.598** dokumenter med CPR-numre, **5.113** dokumenter med pasnumre, **3.101** dokumenter med kørekortnumre og **434** dokumenter med kreditkortnumre. Dokumenttyperne med mest risiko er som følger: **85.603** e-mails, **16.636** øvrige dokumenter, **15.601** finansielle dokumenter, **7.594** kontrakter, **5.993** HR-dokumenter, **5.478** styringsdokumenter, **5.214** præsentationer, **4.869** ejendomsdokumenter, **4.782** dokumenter vedrørende immaterielle rettigheder og **4.544** certifikater.

Disse nøgletal indikerer væsentlige compliance-risici og understreger behovet for en struktureret oprydning.

Der er flere grunde til, at I bør tage disse risici alvorligt:

- Dataforordninger såsom GDPR, UK-GDPR og CCPA kræver, at virksomheder beskytter personlige data. En eventuel straf kan være en bøde på op til 4% af virksomhedens årlige omsætning.
- Hvis I afslører personlige data eller får et omdømme som en dårlig databehandler, mister I folks tillid. Dette kan forårsage langsigtede skader, hvilket kan være meget mere skadeligt end en bøde.
- Hvis I afslører følsomme dokumenter, der indeholder virksomhedens forretningshemmeligheder såsom patenter, IP-dokumenter eller lignende, risikerer I at miste jeres konkurrenceevne.

Det kommende NIS2-direktiv opfordrer virksomheder til at implementere en risikobaseret tilgang til cyber- og informationssikkerhed. I praksis betyder det, at man som virksomhed skal beskrive en risikoproces, som man skal overholde. I overholder processen ved at udføre risikovurderinger og GAP-analyse på jeres data for at identificere sårbarheder, trusler og potentielle konsekvenser af et databrud. Denne rapport kan derfor bruges sammen med NIS2-direktivet.

Virksomheder, der proaktivt adresserer GDPR-risici, udfører grundige risikovurderinger og lukker sikkerhedshuller, opfylder ikke kun deres juridiske forpligtelser, men opnår også en konkurrencemæssig fordel, sikrer deres kunders og interessenters tillid og sikrer overholdelse af direktiver såsom NIS2. I betragtning af de GDPR-risici, der er identificeret I denne rapport, er det en strategisk nødvendighed for jer at styrke jeres datasikkerhed.

7. Anbefalinger

Her er vores anbefalinger til, hvordan I kan rydde op i filer med følsomme oplysninger og reducere jeres GDPR-risiko:

1. **Ryd op i fundne data:** Denne rapport giver jer et overblik over de følsomme data, I opbevarer. Næste skridt er at fjerne de følsomme data, I ikke længere har brug for i henhold til GDPR. Med en automatiseret løsning som DataMapper kan I effektivt slette følsomme filer – værktøjet giver jer mulighed for at slette filer direkte fra DataMapper, uanset hvor de er placeret.
2. **Find andre GDPR-relaterede data:** Rapporten viser et overblik over jeres GDPR-data i de scannede datakilder. Men hvad med andre steder, hvor I opbevarer følsomme data? DataMapper kan scanne en lang række systemer – læs mere om hvilke her. I kan også forsøge at finde GDPR-relaterede data manuelt, men det kan være problematisk – læs hvorfor her.
3. **Sørg for at data opbevares sikkert:** Rapporten har vist, at I har filer, der indeholder følsomme oplysninger. I bør sikre jer, at jeres IT-systemer er i stand til at opbevare personoplysninger sikkert. Læs hvordan du opnår dette her.
4. **Indhent samtykke:** Medmindre I allerede har indhentet samtykke fra de personer, hvis data I opbevarer, bør I kontakte dem og få deres samtykke hurtigst muligt. Fremover bør I automatisk indhente samtykke, hver gang I modtager følsomme personoplysninger.
5. **Skab awareness:** Det er jeres medarbejdere, der modtager, opbevarer, deler og håndterer de følsomme data, som I som virksomhed er ansvarlig for. I bør derfor uddanne og træne jeres medarbejdere i håndtering af følsomme data, så der skabes sikre interne arbejdsgange. Læs mere om awareness-træning her.
6. **Send sikre e-mails:** Outlook er den mest almindelige måde at dele følsomme data via e-mail. Men Outlook krypterer ikke e-mails som standard. Hvis du vil kommunikere sikkert via Outlook, kræver det enten et dyrt Office 365 E3-abonnement eller et tilføjelsesprogram til Outlook.
7. **Overvåg følsomme data:** I bør løbende overvåge jeres datakilder for nye filer, der indeholder følsomme oplysninger. Historisk set har følsomme data hobet sig op i jeres datakilder, og denne tendens vil sandsynligvis fortsætte. Med DataMapper modtager I regelmæssige notifikationer, når nye filer med følsomt indhold dukker op.
8. **Overvej en cyberforsikring:** Én ud af fire danske virksomheder (med 10+ medarbejdere) har oplevet et brud på IT-sikkerheden inden for de seneste 12 måneder (kilde: IT-Branchen). Det tyder på, at det er vanskeligt helt at undgå angreb. Derfor anbefales det – ud over at minimere mængden af følsomme data – at tegne en cyberforsikring, så skaderne i forbindelse med et cyberangreb kan begrænses. Læs mere her.

Kontact

Safe Online ApS
CVR: 38589962
Nørrebrogade 47
2200 København N, Danmark
Tlf: (+45) 31 66 34 00

Ansvarsfraskrivelse

Denne rapport udgør ikke en service til at sikre jeres virksomheds fulde GDPR-overholdelse. Rapporten er en vurdering af personlige oplysninger (PII) risici baseret på en analyse af jeres data i Outlook. Safe Online påtager sig intet ansvar for fejl, udeladelser eller konsekvenser baseret på denne rapport. Rapporten leveres "som den er" uden garantier for fuldstændighed, nøjagtighed eller aktualitet. Det anbefales altid at søge juridisk rådgivning for at sikre overholdelse af gældende lovgivning.