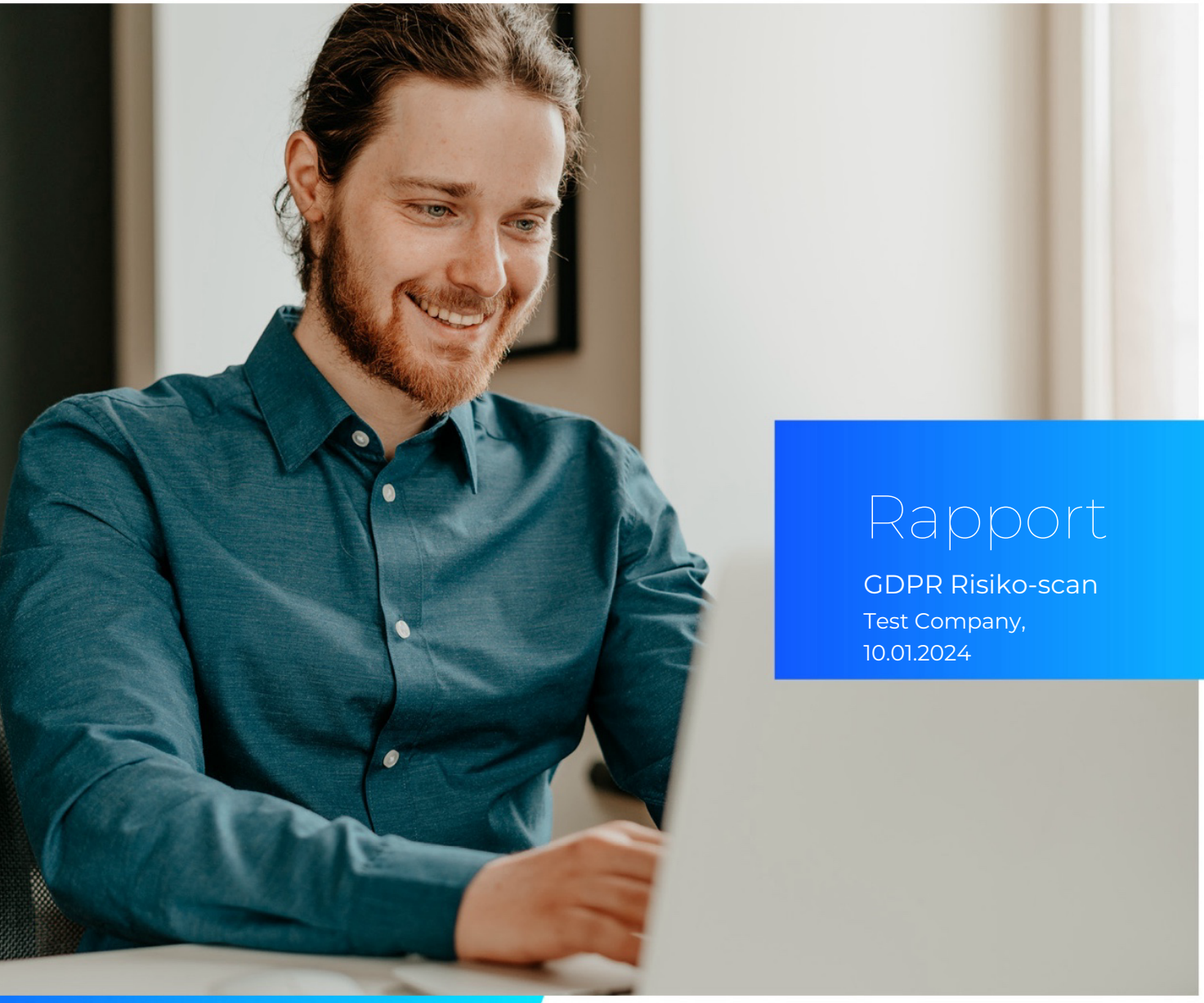
safeonline



Rapport

GDPR Risiko-scan

Test Company,
10.01.2024

SAMPLE TEST REPORT

Indholdsfortegnelse

Introduktion

Persondataforordningen GDPR fastsætter strenge standarder og regler for virksomhedens håndtering af persondata. Overholder man ikke disse regler, kan det resultere i alvorlige juridiske sanktioner, og i nogle tilfælde bøder på op til 4% af den årlige omsætning. Hertil kommer mistilliden hos kunder og interessenter, hvilket kan vise sig at have endnu mere vidtrækkende konsekvenser for en virksomhed.

At sikre overholdelse af GDPR er afgørende af flere årsager. Det reducerer markant risikoen fremmer også tillid, forbedrer kunderelationer og opbygger loyalitet. Virksomheder, der aktivt tager ansvar for persondata og datasikkerhed, opnår en klar fordel ved at kunne vise de overholder loven, samt beskytter deres kunders information, hvilket resulterer i tillid fra kunder såvel som ansatte.

For at kunne håndtere data både sikkert og ansvarligt, samt at overholde GDPR, er det afgørende at anvende en risikobaseret tilgang til informationssikkerhed. Denne tilgang involverer udførelse af grundige risikovurderinger og GAP-analyser for at identificere sårbarheder, trusler og potentielle konsekvenser ved et databrud. Ved at tackle disse huller proaktivt kan virksomheder forbedre overholdelsen af reguleringer som NIS 2 og styrke forpligtelse til at beskytte følsom information.

Om rapporten

Denne rapport er en risikovurdering baseret på et GDPR Risiko-scan udført på jeres Outlook-konti af Data Discovery-værktøjet DataMapper. Rapporten præsenterer jeres datastatistik, og klæde jer på til at navigere i kompleksiteten af at behandle data, som indeholder følsomme personoplysninger i overensstemmelse med GDPR. Endelig kan rapporten her anvendes i forbindelse med intern eller ekstern audits.

Det er vigtigt at huske, at denne rapport blot er en analyse med henblik på at give en vurdering af jeres GDPR-risiko. Rapporten vil i sin konklusion komme med anbefalinger af tiltag for at få ryddet op i jeres persondata.

Hvad er et GDPR Risiko-scan?

For at kunne mindske GDPR-risici i forbindelse med håndteringen af persondata, forudsætter det, at man som virksomhed har et overblik over hvilke persondata man råder over. Jo flere følsomme data man har liggende desto større er éns risiko. At bliver udsat for et hackerangreb kan sammenlignes med at blive udsat for et hjemmetyveri; hvis man har sørget for at fjerne alle værdier i huset, vil tyven ikke have noget at stjæle. Med et GDRP Risiko-scan lægges fundamentet for at rydde alle personoplysninger af vejen, så ubudne gæster ikke har noget at stjæle.

GDPR Risiko-scannet bliver foretaget af DataMapper. DataMapper er et Data Discovery-værktøj, der bruger AI og Machine Learning-algoritmer til at finde tal og ord, der kategoriseres som følsomme på tværs af virksomhedens medarbejdere, cloud storage, e-mails, systemer og apps. DataMapper scanner datasystemer for at finde de dokumenter, mails og billeder, som indeholder ord og termer relateret til GDPR. Et GDPR Risiko-scan er et DataMapper-scan afgrænset til virksomhedens Outlook-konti. Scannet kan omfatte alle aktive Outlook-konti, samt inaktive konti - på f.eks. forhenværende medarbejdere.

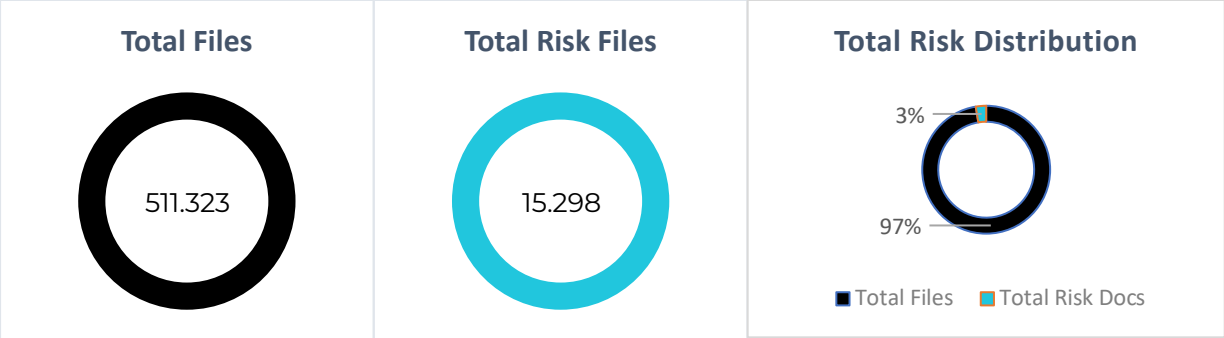
Analyse

Rapportens analyse vil bestå at tre afsnit. Først vil I få et billede af hvordan jeres risikovurdering er generelt. Dernæst vil I få statistik for data med højrisiko, og til sidst får I statistik for jeres data med middel risiko.

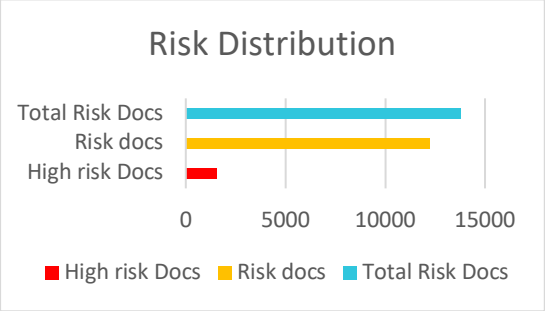
1. Generel risikovurdering

For at give en generel risikovurdering, præsenteres her et generelt overblik over jeres data.

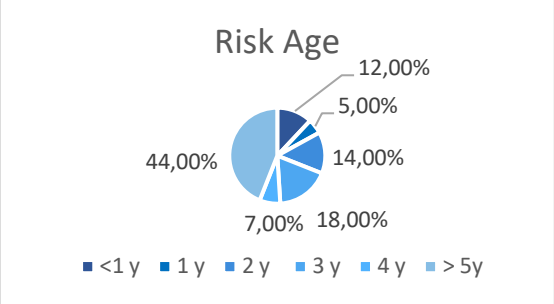
3.1 Total risiko-fordeling



1.2 Fordeling af risiko



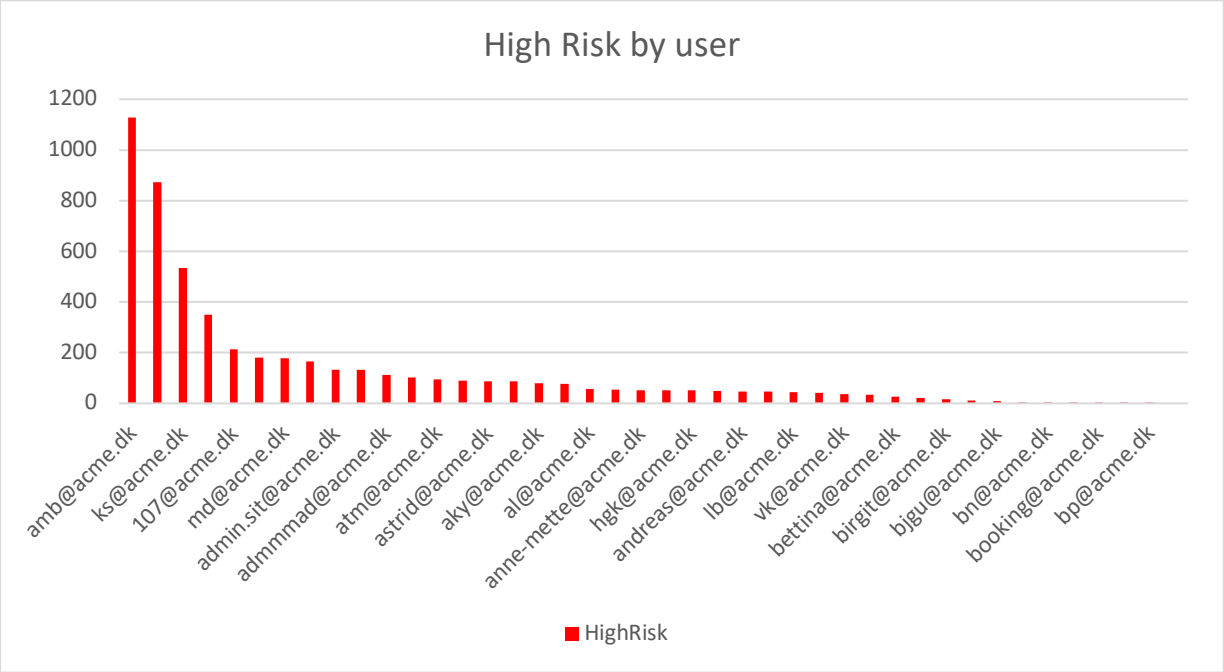
1.3 Fordeling af risiko efter alder



2. Dokumenter med højrisiko

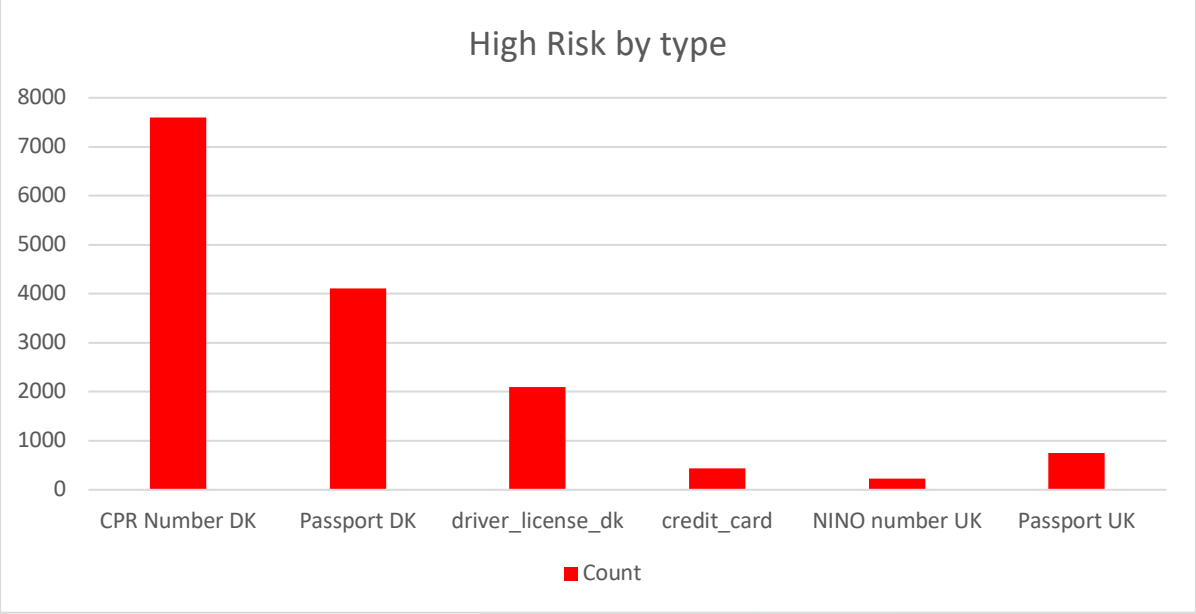
2.1 Brugere med højrisiko

DataMapper identificerer dokumenter, mails og billeder med højrisiko. Her er tale om numre, der muligvis er ekstra følsomme. Dette kan omfatte danske CPR-numre, britiske NINO-numre, kørekort-numre, pas-numre og kreditkort-numre. Disse numre er særligt følsomme, og vil derfor blive markeret som højrisiko.



Der er fundet i alt 76 email-konti hos jer. Ud af disse er der i 32 konti med højrisiko-information (f.eks. CPR-numre, pasnumre, kørekortnumre eller kreditkortnumre).

2.2 Højrisiko-information efter type

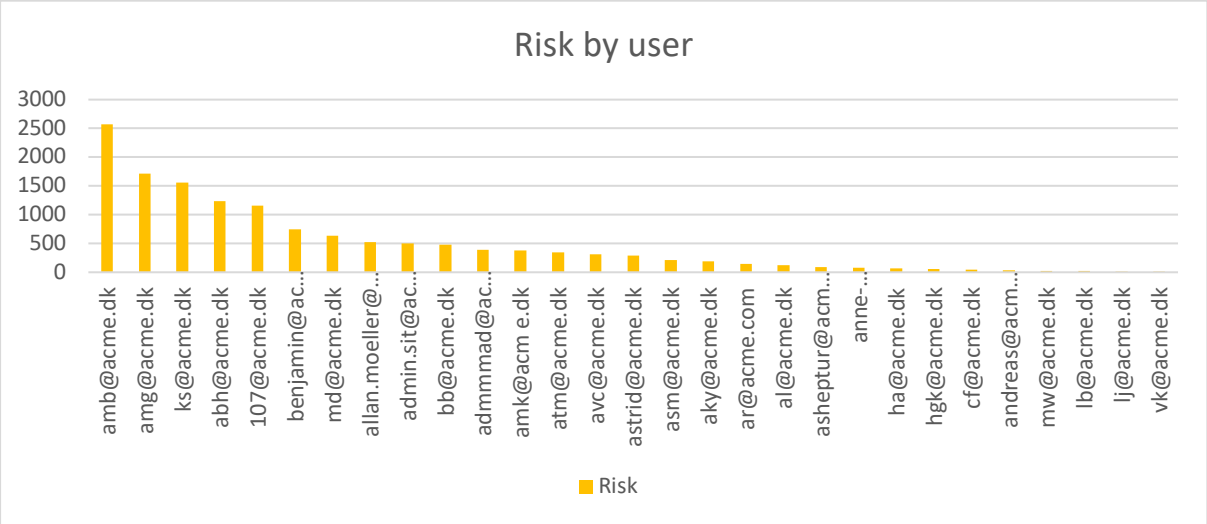


Der er fundet 7.598 CPR-numre, 4.113 pas-numre, 2.101 kørekort-numre og 434 kreditkort-numre i e-mails.

3. Dokumenter med middel risiko

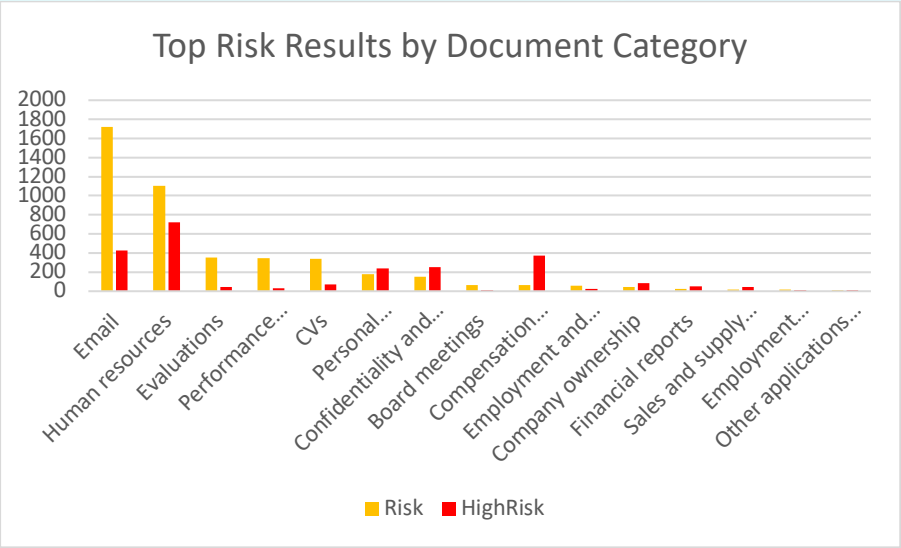
3.1 Brugere med middel risiko

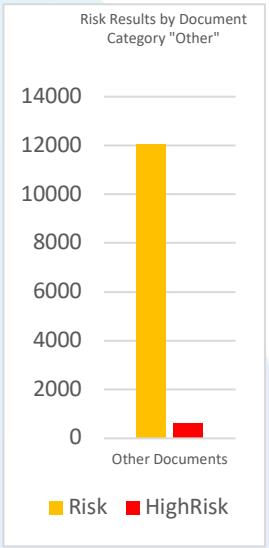
DataMapper identificerer dokumenter, mails og billeder med middel risiko. Her er tale om dokumenter, der indeholder følsomme oplysninger om personer, som kan betragtes som personhenførbar information (PII). Vores metode involverer brugen af en omfattende taksonomi, som er en liste over specifikke nøgleord og fraser, der er forbundet med race, etnisk oprindelse, politiske overbevisninger, religion, medlemskab af fagforeninger, helbredstilstand og seksuelle præferencer. Hvis nogen af disse nøgleord findes i nærheden af en persons identitet inden for et dokument, mail eller bilede, markeres det som et risiko-dokument.



Personhenførbar information (PII: Personal Identifiable Information) identificeret i email-konti for jer:

3.2 Højrisiko-information efter dokument-kategori



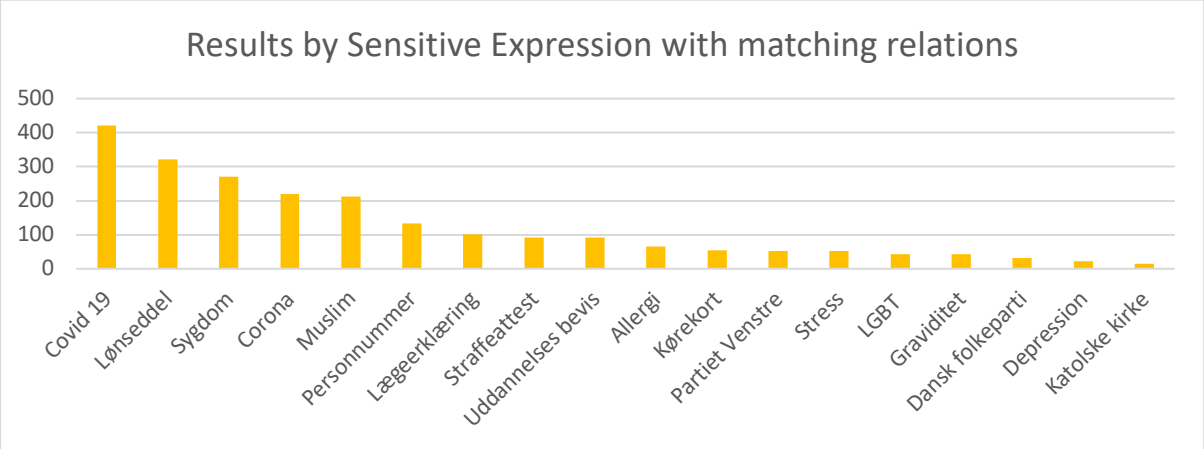


I har mange forskellige dokumenttyper, der potentielt kan være følsomme i medarbejderes e-mails. For eksempel: 642 HR-dokumenter, 211 medarbejdervurderinger, 631 personidentifikationsdokumenter, 54 bestyrelsesmødedokumenter, 471 dokumenter mærket som fortrolige, 821 kontrakter, 1.213 CV'er, 71 IP-relaterede dokumenter.

3.3 GDPR-term med relation til navngivne personer

Visse termer udgør kun en GDPR-risiko, hvis de nævnes i relation til en person. Dette er termer der vedkommer race, etnisk oprindelse, politiske overbevisninger, religion, medlemskab af fagforeninger, helbredstilstand og seksuelle præferencer.

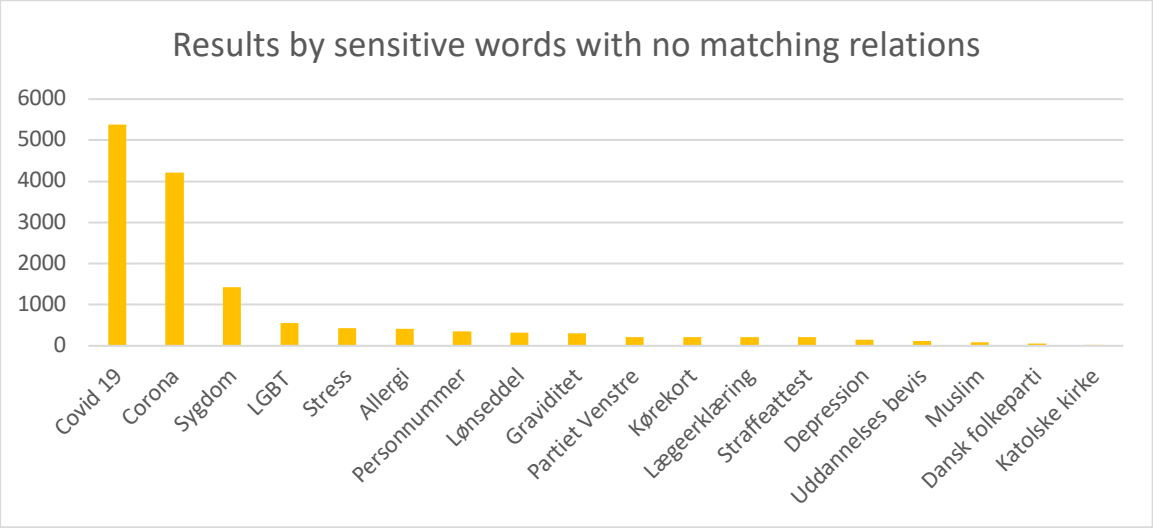
Forinden rapporten her har I indtastet personnavne i DataMapper med relationer til jeres virksomhed. Nedenstående vises en statistik over de GDPR-termer, der optræder i mails sammen med disse relationer.



32 navngivne personer blev fundet i relation til et GDPR-term.

3.4 GDPR-term uden relation til navngivne personer

DataMapper kan finde GDPR-termer, selv når de ikke er direkte knyttet til personer. Selvom disse termer ikke nødvendigvis udgør en GDPR-risiko, fungerer de som vigtige indikatorer for forebyggende risikovurdering og strategier for databehandling. Disse termer kan således give værdifuld indsigt i tilstedeværelsen af følsomme emner eller indhold, der potentielt kunne indikere områder, der kræver yderligere undersøgelse.



Konklusion

TILGÆNGELIG FOR DIN VIRKSOMHED

Hvad bør I gøre nu?

TILGÆNGELIG FOR DIN VIRKSOMHED