UDARBEJDET TIL

Acme A/S

GDPR-risikovurdering

Genereret **8. juni 2026**

Indhold

RISIKOSCORE

63 /100

C — Moderat — reel eksponering, der bør håndteres

RISIKOSCORE-BENCHMARK ILLUSTRATIVT DATASÆT

64 er typisk for **Finance** · **DK** · **50-250** medarbejdere ↘ 1 point under sammenligningsgruppen

VOLUMEN (35%)	ALVORLIGHED (35%)	KONCENTRATION (20%)	SEKTOR (10%)
99%	49%	16%	85%

NØGLETAL

Overordnede tal

Lav eksponering — opretholde nuværende kontroller.

1,922,295	7,371	19,032	26,403
SCANNEDE FILER	HØJRISIKO-FILER	RISIKO-FILER	I ALT MED RISIKO
			1.4% of scan

Med 26.403 eksponerede filer ud af 1.922.295 scannede er den samlede flagging-andel på 1%, hvilket er en håndterbar oprydningsopgave for en finansiel virksomhed på 125 ansatte, forudsat at indsatsen prioriteres mod de tre mest eksponerede brugere.

FORDELING

Filer efter risikoniveau

Høj risiko	7,371 (28%)
Risiko	19,032 (72%)

Risikofordelingen blandt eksponerede filer domineres af de 19.032 risikofiler, mens 7.371 højrisikofiler udgør det skarpe spor, der bør remedieres først — antallet er stort nok til at hæve sandsynligheden for en anmeldelsespligtig hændelse efter Artikel 33. Til kontekst er yderligere 1.895.892 rene filer scannet, men disse er ikke en del af eksponeringsbilledet.

RESUMÉ

Acme A/S opnår en samlet risikoscore på 63/100 (karakter C), hvilket placerer organisationen i et moderat-til-forhøjet risikoleje. Ud af 1.922.295 scannede filer er 7.371 klassificeret som højrisiko og yderligere 19.032 som risikofiler, mens 1.895.892 filer er rene. Samlet er 26.403 filer (1%) markeret som eksponerede, og denne koncentration af følsomme oplysninger i en finansiel virksomhed med 125 ansatte tilsiger et målrettet oprydningsspor frem for bredtfavnende kontroller.

De mest materielle fund er den massive koncentration af risiko i Outlook (6.904 højrisiko og 18.220 risikofiler) sammenholdt med beskedne mængder i OneDrive (467/795) og SharePoint (0/17). Eksponeringen drives af tre brugere — user01@acme.com (2.322 højrisikofiler), user02@acme.com (1.251) og user03@acme.com (996) — som tilsammen står for over halvdelen af alle højrisikofiler. Dominansen af e-mail som risikokanal og fund af 5.711 DK CPR-numre, 1.247 betalingskortnumre og 818 DK Pasnumre i højrisikofiler indikerer en svaghed i styringen af e-mailopbevaring og udveksling, hvilket berører principperne om dataminimering og opbevaringsbegrænsning i Artikel 5(1)(c) og 5(1)(e) samt sikkerhedskravet i Artikel 32.

Eksponeringen af særlige kategorier af personoplysninger efter Artikel 9 er betydelig: 20.172 hits på helbredsoplysninger, 4.031 på etnisk oprindelse og 790 på seksuel orientering. For en finansiel virksomhed er denne tæthed af helbredsdata atypisk og peger på sagsbehandling vedrørende sygemeldinger, forsikringskorrespondance eller AML/KYC-materiale, som ligger i ustrukturerede postkasser uden tilstrækkelig adgangsbegrænsning. Datatilsynet har gentagne gange håndhævet Artikel 9 strengt, og overtrædelser kan udløse administrative bøder op til 20 mio. EUR eller 4% af den globale årsomsætning, jf. Artikel 83(5).

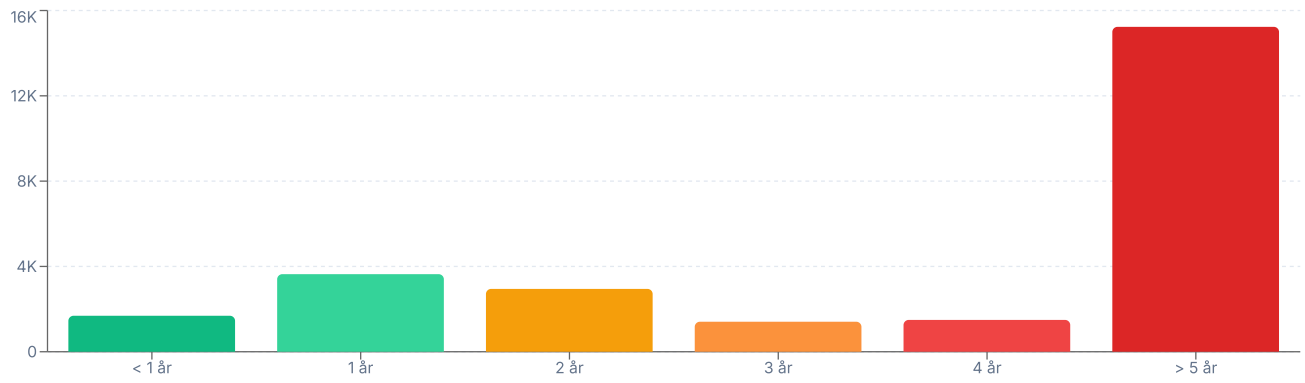
Acme A/S' profil som dansk finansiel virksomhed i størrelsesbåndet 50–250 medarbejdere indebærer skærpede forventninger til AML-dokumentation, kundekendskab og medarbejdersagsbehandling. De primære risikodrivere er e-mailopbevaring uden retention-politik, koncentration af eksponering hos få medarbejdere samt en stor bagkant af gamle dokumenter (15.234 risikofiler er over 5 år gamle), hvilket samlet kræver et programmatisk oprydningsspor frem for ad hoc-indsatser.

DOKUMENTALDER

Hvor gamle er risikofilerne?

Høj-risiko og risiko-filer samlet, fordelt på aldersgrupper.

21.079 risikofiler er 2 år eller ældre — overvej en gennemgang af opbevaringspolitikken.



Den aldersgruppe der fylder mest, er filer på over 5 år med 15.234 risikofiler, hvilket udgør størstedelen af den samlede eksponering og udgør en direkte overtrædelse af opbevaringsbegrænsningen i Artikel 5(1)(e).

LOKATIONER

Hvor risikoen befinder sig

Outlook — 25,124 filer

Høj: **6,904** · Risiko: **18,220** · Aktive brugere: **33**

OneDrive — 1,262 filer

Høj: **467** · Risiko: **795** · Aktive brugere: **26**

SharePoint — 17 filer

Høj: **0** · Risiko: **17** · Aktive brugere: **1**

Outlook bærer reelt hele risikoen med 6.904 højrisiko og 18.220 risikofiler fordelt på 33 aktive brugere, mens OneDrive (467/795) og SharePoint (0/17) er marginale — e-mail er den centrale risikokanal og bør være primært mål for DLP-politikker.

IDENTIFIKATORER

Højrisiko-identifikatorkategorier

DK CPR dominerer med 5.711 højrisikofiler, fulgt af betalingskortnumre (1.247) og DK Pasnumre (818) — en kombination der i en finansiel kontekst peger på AML/KYC-dokumenter opbevaret uden segmentering, hvilket forstærker bødeeksponeringen efter Artikel 83(5).

LANDESPECIFIKKE IDENTIFIKATORER

Danske CPR-numre (personnummer) fremhæves af Datatilsynet som højrisiko-identifikatorer. Ukrypterede CPR-numre i postkasser eller på delte drev er en hyppig årsag til anmeldte brud.

NØGLEORD

Risiko-nøgleordssignaler

Ord og identifikatorværdier, der matchede GDPR-nøgleordsbiblioteket på tværs af de scannede filer. Brug dette til at se hvilke kategorier der driver eksponeringen og hvilke sprog dine data findes på.

44,780
Antal nøgleordsfund
Det samlede antal gange et flagget nøgleord blev fundet på tværs af alle scannede filer.

393
Unikke nøgleord
Antal forskellige nøgleordsværdier der blev fundet. En identifikatorværdi (fx et bestemt CPR-nummer) tæller som ét nøgleord.

2
Fundne sprog
Antallet af sprog de matchede nøgleord spænder over (fx dansk og engelsk).

Top 20 nøgleord

NØGLEORD	KATEGORI	FUND
CPR da_DK	Other	5,247
covid da_DK	Health information	3,370
Covid-19 da_DK	Health information	2,933
french en_GB	Ethnic origin	1,539
misbrug da_DK	Health information	1,533
hearing en_GB	Health information	1,430
health en_GB	Health information	1,360
CPR-nummer da_DK	Other	1,090
discharge en_GB	Criminal offences	1,043
Operation da_DK	Health information	942
corona da_DK	Health information	939
overtrædelse da_DK	Criminal offences	888
stævning da_DK	Criminal offences	846
oplysningspligt da_DK	Criminal offences	779
covid en_GB	Health information	758
fraud en_GB	Criminal offences	757
German en_GB	Ethnic origin	680
COVID-19 en_GB	Health information	643
fødselsdato da_DK	Other	576
sygdom da_DK	Health information	574

Nøgleord domineres af danske helbreds- og identifikationstermer (CPR ×5.247, covid ×3.370, Covid-19 ×2.933, misbrug ×1.533) suppleret af engelske termer (health, hearing, discharge), hvilket bekræfter at både dansk og engelsk kundekorrespondance bærer Artikel 9-data.

ARTIKEL 9

Følsomme personoplysninger fundet

Helbredsoplysninger	20,172 forekomster	Etnisk oprindelse	4,031 forekomster
Seksuel orientering	790 forekomster	Politisk overbevisning	713 forekomster
Fagforeningsmedlemskab	268 forekomster	Religion	6 forekomster
Genetiske oplysninger	0 forekomster	Biometriske oplysninger	0 forekomster

Helbredsoplysninger udgør 20.172 hits, etnisk oprindelse 4.031 og seksuel orientering 790 — et omfang af særlige kategorier som kræver eksplicit retsgrundlag efter Artikel 9(2) og som Datatilsynet historisk har vægtet tungt i bødeudmålinger.

TILSYNSMYNDIGHEDENS VEJLEDNING

Finanssektoren anvender typisk ikke artikel 9 — men helbredsoplysninger kan optræde i forsikringsvurderinger, pensionssager og HR-sager om sygefravær. Gennemgå disse arbejdsgange frem for at antage, at de ikke findes.

KONTI

Hvem har den største eksponering

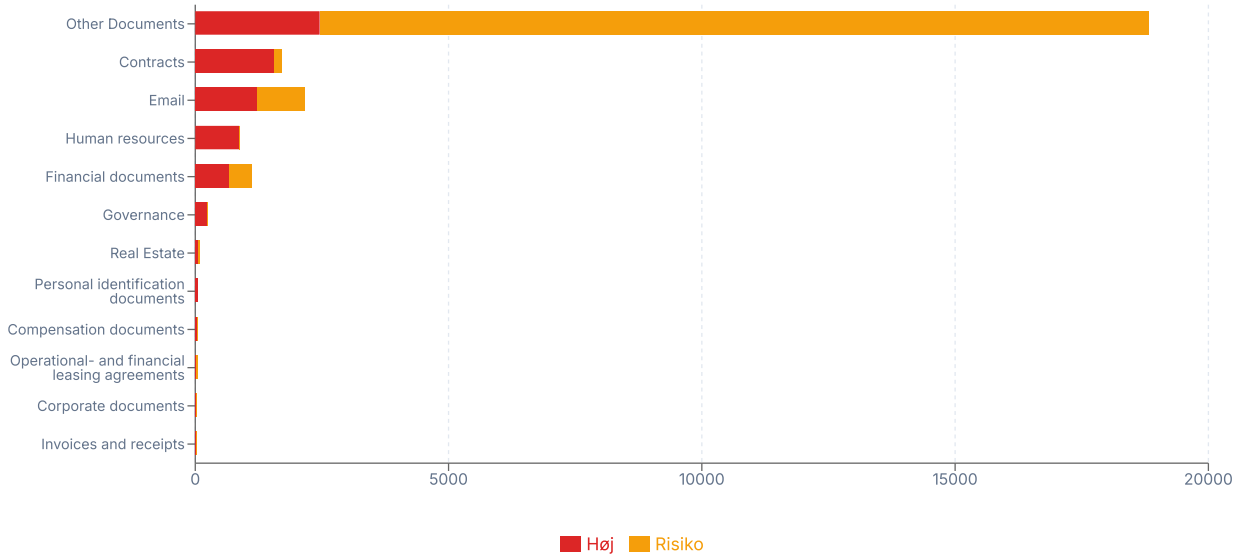
KONTO	HØJ RISIKO	RISIKO	INGEN RISIKO
user01@acme.com	2,322	3,829	212,885
user02@acme.com	1,251	1,308	185,226
user03@acme.com	996	3,013	214,308
user04@acme.com	133	307	28,184
user05@acme.com	109	499	24,671
user06@acme.com	94	619	55,933
user07@acme.com	92	473	64,139
user08@acme.com	88	479	34,200
user09@acme.com	82	324	35,284
user10@acme.com	42	135	29,733

Viser de 10 konti med størst eksponering. 25 yderligere konti vises ikke — den fulde liste indgår fortsat i AI-analysen nedenfor.

Eksponeringen er stærkt koncentreret: user01@acme.com (2.322 højrisiko), user02@acme.com (1.251) og user03@acme.com (996) står for ca. 62% af alle højrisikofiler, hvilket gør målrettet træning og oprydning hos disse tre brugere til den mest effektive indsats.

DOKUMENTKATEGORIER

Risiko pr. dokumentkategori



Højrisikoen er koncentreret i Øvrige dokumenter (2.455), Kontrakter (1.558), E-mail (1.228), HR-dokumenter (870) og Økonomidokumenter (678) — et mønster der er typisk for en finansiel virksomhed med kundesager og medarbejderdokumentation i ustrukturerede mapper.

KONKLUSION

Hvad betyder dette for dig

Acme A/S' risikobillede er entydigt: 7.371 højrisikofiler og 19.032 risikofiler er overvejende koncentreret i Outlook hos tre brugere, og 15.234 af risikofilerne er over 5 år gamle — en direkte konflikt med Artikel 5(1)(e) og Artikel 32. Den primære indsats bør derfor være Anbefaling 6 (gennemgang og minimering af langtidsopbevaring i postkasser) kombineret med Anbefaling 4 (DLP-politikker på postkasser og delte drev), således at både den historiske bagkant og fremadrettede flow adresseres samtidigt. Som tredje spor bør Anbefaling 3 (målrettet træning af de medarbejdere der håndterer følsomme data) prioriteres, idet user01, user02 og user03 alene bærer hovedparten af eksponeringen og dermed udgør det mest effektive interventionspunkt for en virksomhed af denne størrelse.

ANBEFALINGER

Næste handlinger, i prioriteret rækkefølge

FRA SAFE ONLINE

Værktøjer der kan hjælpe med det, I har fundet

DataMapper

Scanner løbende Microsoft 365, Google Workspace og netværksdrev for filer med persondata. Hver medarbejder får sin egen liste over flaggede filer og kan selv slette, flytte eller godkende.

RELEVANT FOR JERES SCANNING
7.371 høj-risiko · 19.032 risikofiler at håndtere.

Læs mere ↗

ShareSimple

Et Outlook-tilføjelsesprogram, der erstatter almindelige vedhæftninger med krypterede, log-førte links. Modtagere åbner filerne via et verificeret engangslink — uden installation.

RELEVANT FOR JERES SCANNING
DK CPR (5.711) + Bank card (1.247) driver identifikatorrisikoen.

Læs mere ↗

Træning

Tildel GDPR-træning til de medarbejdere, der bærer risikoen i denne rapport. 50+ indbyggede kurser plus en AI-bygger, der genererer skræddersyede kurser ud fra et emne eller et dokument.

RELEVANT FOR JERES SCANNING
3 brugere holder tilsammen ~62% af højrisiko-filerne.

Åbn træning ↑

Generate training from these findings

1 **Tilføj dine brugere, så de kan rydde op i risikofiler** — DATAMAPPER

Med 35 aktive brugere og koncentreret eksponering hos user01, user02 og user03 bør disse tre tildeles DataMapper-adgang først, så de selv kan gennemgå og afvikle deres 4.569 højrisikofiler.

Åbn DataMapper →

2 **Begræns deling af følsomme data eksternt** — SHARESIMPLE

Med 5.711 CPR-numre og 1.247 betalingskortnumre i højrisikofiler bør ShareSimple anvendes til at erstatte vedhæftninger i ekstern e-mail med sikre links, særligt for de tre mest eksponerede brugere.

3 **Medarbejdere, der håndterer følsomme data, skal have ordentlig uddannelse** — TRÆNING

Målret GDPR-træning mod user01, user02 og user03, som tilsammen bærer over 4.500 højrisikofiler — træningen bør fokusere på Artikel 9-håndtering og korrekt brug af CPR-numre i finansielle sagsforløb.

Åbn træningsmodul →

4 **Anvend DLP-politikker på postkasser og delte drev** — PROCES

Da 6.904 ud af 7.371 højrisikofiler ligger i Outlook, er DLP-politikker på Microsoft 365-tenanten den mest direkte tekniske foranstaltning efter Artikel 32 — politikker bør detektere CPR, betalingskort og pasnumre i både indgående og udgående mail.

5 **Begræns ekstern deling af højrisiko-lokationer** — PROCES

OneDrive-eksponeringen hos user04 (123 højrisikofiler) bør sikres med betingede adgangsregler og blokering af anonyme delelinks for de mapper, der indeholder kundedata.

6

Gennemgå og begræns langsigtet opbevaring i indbakken

PROCES

15.234 risikofiler er over 5 år gamle, hvilket overtræder Artikel 5(1)(e) — implementer en e-mailopbevaringspolitik med automatisk arkivering eller sletning efter 3-5 år, tilpasset finansielle opbevaringskrav efter hvidvaskloven.

7

Send kun følsomme data via sikre kanaler

PROCES

Med 1.228 højrisiko-emails identificeret bør al fremsendelse af CPR-numre, kontoudtog og helbredsoplysninger ske via krypteret kanal eller sikker portal frem for almindelig e-mail.

8

Kør denne vurdering hvert kvartal

VURDERING

Med 9.656 filer slettet i denne periode er momentum til stede, men en kvartalsvis genkørsel er nødvendig for at dokumentere effekten af de igangsatte indsatser over for Datatilsynet og over for bestyrelsen.

Åbn Vurderinger →

BEREDSKAB

Beredskab ved sikkerhedsbrud

Skulle der indtræffe et brud på persondatasikkerheden, skal Acme A/S anmelde forholdet til Datatilsynet inden for 72 timer efter konstatering, jf. Artikel 33. Realistiske scenarier i dette eksponeringsbillede omfatter en kompromitteret Outlook-konto hos user01, user02 eller user03 med adgang til tusindvis af CPR-numre og helbredsoplysninger, fejladresseret e-mail med kundedokumentation indeholdende betalingskortnumre, samt utilsigtet ekstern deling fra OneDrive af AML/KYC-materiale. En forberedt og afprøvet beredskabsplan med foruddefinerede roller, kommunikationsskabeloner og logging-adgang sikrer, at 72-timersfristen kan overholdes uden improvisation, og at vurderingen efter Artikel 34 af eventuel underretning af de registrerede kan foretages på et oplyst grundlag.

FORBEHOLD

Behandlet under EU's GDPR og den danske databeskyttelseslov. Datatilsynet er den kompetente tilsynsmyndighed; denne rapport er ikke en tilsynsindberetning.

Danske bøder udstedes gennem retssystemet på Datatilsynets indstilling. De maksimale niveauer afspejler GDPR: det højeste af 20 mio. EUR eller 4 % af den globale årsomsætning (øvre) / 10 mio. EUR eller 2 % (nedre).