



PREPARED FOR

Acme A/S

GDPR Risk Assessment

Generated 26 May 2026

Contents

Score	3
Summary	3
Headline	4
Activity	4
Distribution	5
Age	5
Locations	6
Identifiers	6
Keywords	7
Article 9	8
Top users	8
Categories	9
Conclusion	10
Recommendations	10
Incident response	12

RISK SCORE

63 /100

C Moderate — meaningful exposure that should be addressed

RISK SCORE BENCHMARK ILLUSTRATIVE DATASET

64 is typical for Finance · DK · 50-250 employees ↗ 1 point below peers

HOW THIS WAS COMPUTED

VOLUME (35%)	SEVERITY (35%)	CONCENTRATION (20%)	SECTOR (10%)
99%	49%	17%	85%

Volume — share of files without any risk flag. Higher = better.

Severity — inverse of high-risk density + Article 9 (special-category) keyword hits. High-risk files weighted 3x.

Concentration — Gini coefficient on per-user risk. Diffuse = better (not concentrated in a few people).

Sector — regulatory-load multiplier. Healthcare / finance / legal are weighted 0.85x (stricter bar).

Composite = $\sum(\text{weight} \times \text{component}) \times 100$. Formula version v1.

EXECUTIVE SUMMARY

Acme A/S currently sits at a composite risk score of 63/100 (grade C). Out of 1,890,269 files scanned, 7,305 are classified as high-risk and a further 19,034 fall into the medium risk-tier, leaving 1,863,930 clean. The flagged share is approximately 1% of total volume — modest in proportion but material in absolute terms for a 125-employee finance firm and squarely within the scope of Article 5(1)(c) data minimisation and Article 32 security-of-processing obligations.

The most material findings are concentrated in mailboxes: Outlook holds 6,826 of the 7,305 high-risk files and 18,190 of the 19,034 medium-risk files, while OneDrive holds 479 high-risk and SharePoint effectively none. Exposure is heavily concentrated in a small number of accounts — user17@acme.com (2,319 high-risk), user24@acme.com (1,251) and user33@acme.com (996) together account for roughly 63% of the high-risk inventory. Identifier hits are dominated by 5,650 Danish CPR numbers, 1,248 bank-card numbers and 811 DK Passport numbers, all of which Datatilsynet singles out as high-risk under the Danish Databeskyttelseslov.

Article 9 special-category exposure is substantial: 20,133 Health information hits, 4,083 Ethnic origin hits and 796 Political opinion hits, supported by keywords such as "CPR" (x5,172), "covid" (x3,295) and "misbrug" (x1,430). Finance does not typically rely on Article 9, but health data can appear in insurance underwriting, pension files and medical-leave HR records — these workflows must be audited rather than assumed absent. Datatilsynet can recommend administrative fines to the public prosecutor, and Danish courts have issued GDPR fines exceeding 1m DKK; the maximum tiers mirror Article 83(5) GDPR (the higher of €20m or 4% of global turnover).

Organisational context reinforces the urgency. With 35 active and 5 non-active users in a 125-employee Danish finance entity, the dominant risk driver is long-tail inbox retention — 840,702 files (the >5y bucket) sit above any plausible business-purpose threshold under Article 5(1)(e), and Datatilsynet has previously criticised controllers for inbox archives held beyond stated purpose. Finance regulators (Finanstilsynet alongside Datatilsynet) typically see overlap between GDPR, AML and sector retention rules, so any cleanup plan must reconcile conflicting retention periods before deletion.

Headline numbers

Low exposure — maintain current controls.



1,890,269

Files scanned
From your DataMapper export



26,339

Files with risk
Across 3 locations



1.4%

Of scan with risk
7,305 high-risk · 19,034 medium




1,863,930


Clean files
No personal-data signals

✦ Of 1,890,269 files scanned, only ~1% are flagged — a modest share for a 125-employee finance firm but 7,305 high-risk items still represent material Article 32 exposure.

USER ACTIVITY

Who's actually using the system?


35
Active users

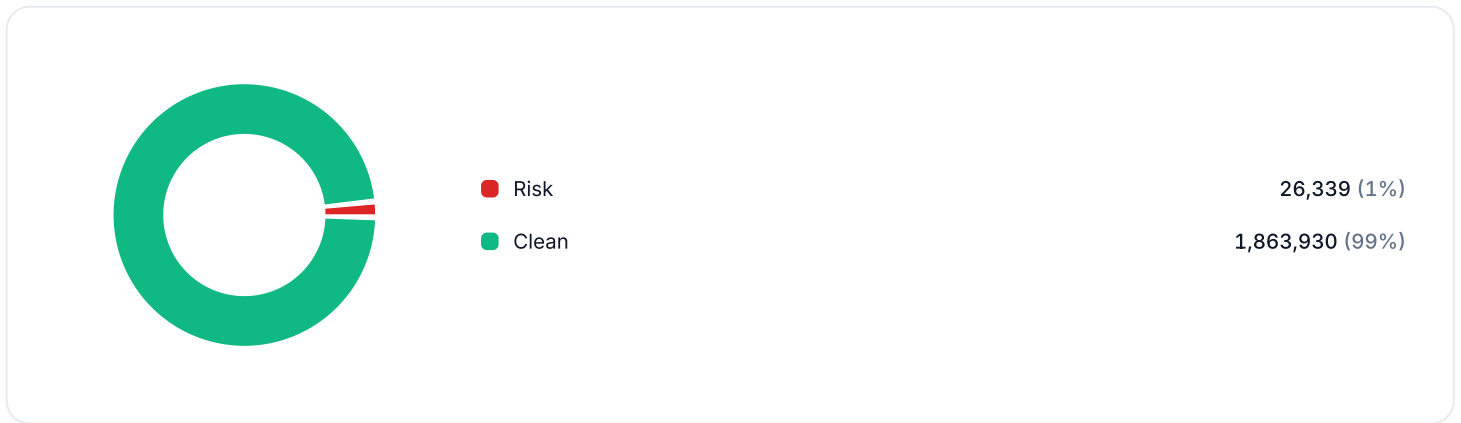

5
Non-active users

Non-active users still retain risk files. Consider deprovisioning or review.

✦ 35 active and 5 non-active users; the non-active accounts must be reviewed for offboarding completeness under Article 32 access-control obligations.

DISTRIBUTION

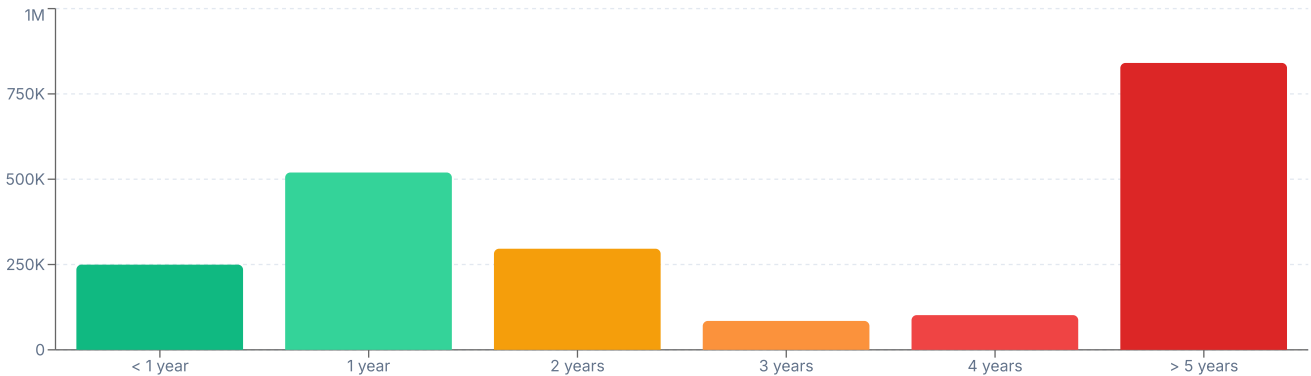
Clean vs Risk files



✦ With 1,863,930 clean files against 7,305 high-risk and 19,034 medium-risk, the split favours focused remediation on the ~1% flagged rather than a broad cleanup programme.

How old are the risk files?

1,323,288 files are 2 years or older — consider a retention review.



✦ The >5y bucket dominates at 840,702 files — far above the next-largest 1y bucket (519,597) — a direct Article 5(1)(e) storage-limitation concern.

LOCATIONS

Where the risk lives

Location	High	Risk	Clean	Active users	Total / Percentage
Outlook	6,826	18,190	1,741,113	34	25,016 / 1,766,129 (1.4%)
OneDrive	479	827	120,262	25	1,306 / 121,568 (1.1%)
SharePoint	0	17	2,555	1	17 / 2,572 (0.7%)

✦ Outlook holds 6,826 of 7,305 high-risk files (93%); OneDrive holds 479 and SharePoint effectively none — the remediation target is mailbox hygiene, not collaboration platforms.

High-risk identifier categories



✦ DK CPR overwhelmingly dominates with 5,650 high-risk hits — exactly the category Datatilsynet singles out as high-risk — followed by 1,248 bank cards and 811 DK Passports.



COUNTRY IDENTIFIERS

Danish CPR numbers (personnummer) are singled out by Datatilsynet as high-risk identifiers. Unencrypted CPR in mailboxes or shared drives is a common cause of reported breaches.

Risk keyword signals

44,684

Total keyword hits

382

Unique keywords

2

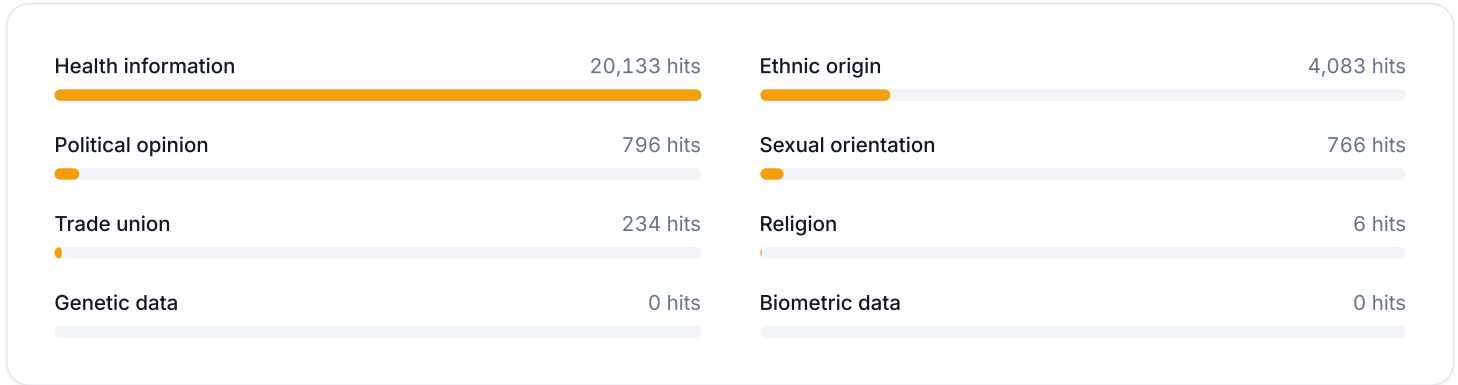
Locales found

Top 20 keywords

KEYWORD	HITS
CPR da_DK	5,172
covid da_DK	3,295
Covid-19 da_DK	2,883
french en_GB	1,561
health en_GB	1,469
hearing en_GB	1,436
misbrug da_DK	1,430
discharge en_GB	1,036
CPR-nummer da_DK	1,036
corona da_DK	941
Operation da_DK	938
overtrædelse da_DK	890
stævning da_DK	846
covid en_GB	835
oplysningspligt da_DK	774
German en_GB	732
fraud en_GB	729
COVID-19 en_GB	723
IBAN en_GB	611
fødselsdato da_DK	569

🌟 Danish-locale hits dominate ("CPR" ×5,172, "covid" ×3,295, "misbrug" ×1,430) alongside English health terms, confirming mixed-language exposure across health and identifier categories.

Sensitive personal data found



✦ Health information leads at 20,133 hits, with Ethnic origin (4,083) and Political opinion (796) trailing — Article 9 processing requires an explicit Article 9(2) legal basis which finance entities rarely document.

ACCOUNTS

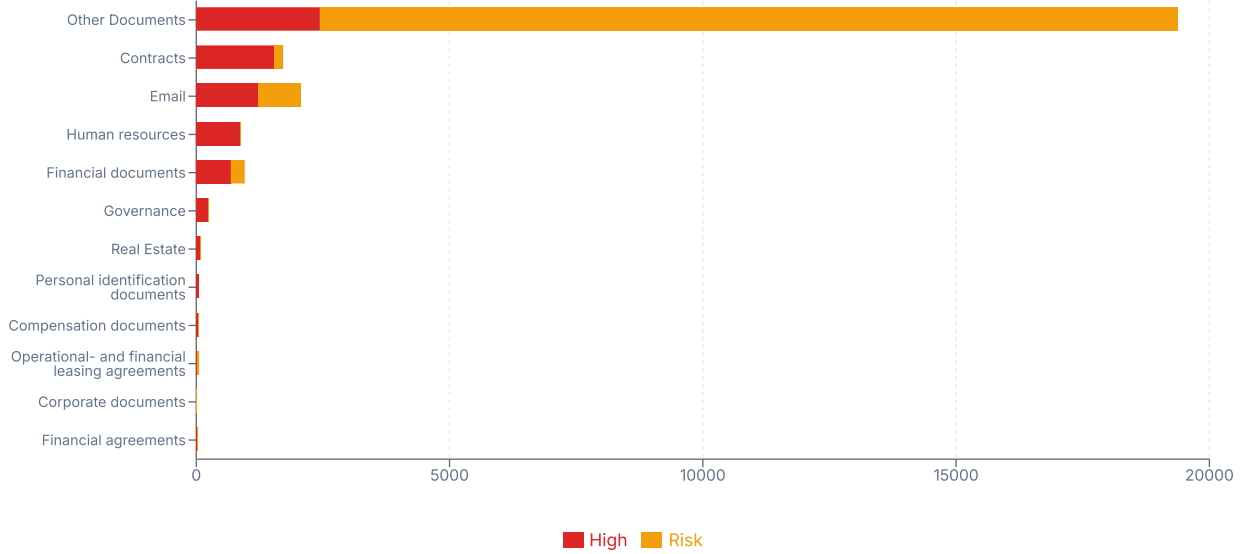
Who carries the most exposure

ACCOUNT	HIGH RISK	RISK	NO RISK
user17@acme.com	2,319	3,738	212,325
user24@acme.com	1,251	1,365	185,954
user33@acme.com	996	3,022	218,012
user03@acme.com	126	326	30,238
user31@acme.com	108	533	24,792
user08@acme.com	93	692	57,482
user23@acme.com	92	580	67,270
user36@acme.com	90	533	34,072
user41@acme.com	82	338	34,216
user16@acme.com	39	216	38,982

Showing the top 10 accounts by exposure. 25 additional accounts not displayed — the full list still informs the AI analysis below.

✦ Exposure is heavily concentrated: user17, user24 and user33 together hold ~63% of all high-risk files, indicating a small remediation cohort rather than a firm-wide hygiene problem.

Risk by document category



✦ Other Documents (2,440 high-risk) and Contracts (1,535 high-risk) lead the high-risk volume, with Email (1,225) and HR (866) close behind — typical for a finance entity with AML and onboarding workflows.

CONCLUSION

What this means for you



Acme A/S should prioritise **Recommendation 4** (DLP policies on mailboxes and shared drives) and **Recommendation 6** (review and minimise long-term inbox retention) as the highest-leverage controls — together they address the 6,826 high-risk Outlook files and the 840,702 files in the >5y age bucket, which are the two largest drivers of the grade C composite score and the clearest Article 5(1) (e) and Article 32 GDPR gaps. **Recommendation 1** (onboard the three concentrated users — user17, user24, user33 — into the cleanup workflow) is the fastest route to retiring the ~63% of high-risk inventory those accounts hold.

In parallel, Acme should reconcile GDPR retention with AML and Finanstilsynet sector rules before any deletion sweep, and re-run this assessment quarterly (**Recommendation 8**) to confirm the high-risk count begins to move below the current flat 7,305 baseline.

Next actions, in priority order

FROM SAFE ONLINE

Tools that can help with what you found



DataMapper

Find, classify, and minimise sensitive data across mailboxes, OneDrive and SharePoint — without manual review.

[Learn more ↗](#)



ShareSimple

Send personal data and sensitive files through encrypted, audited channels instead of plain attachments.

[Learn more ↗](#)



Training

Targeted GDPR and data-handling training for the people who actually carry the risk.

[Open Training ↑](#)

1

Add your users so they can clean up identified risk files

DATAMAPPER

user17@acme.com (2,319 high-risk), user24@acme.com (1,251) and user33@acme.com (996) hold roughly 63% of Acme's high-risk inventory. Adding these three to DataMapper as priority assignees will retire the majority of exposure faster than any firm-wide initiative.

[Open DataMapper →](#)

2

Minimise sensitive data being shared externally

SHARESIMPLE

With 5,650 DK CPR and 1,248 bank-card identifiers in scope, route any external transmission through ShareSimple to ensure encryption and audit logging — Datatilsynet treats unencrypted CPR in mailboxes as a common reportable breach scenario.

3

People handling sensitive data should be properly trained

TRAINING

The three top users handling Article 9 health data and CPR identifiers should receive role-specific training on lawful basis under Article 6 and Article 9(2), plus secure-handling procedures for the 20,133 health-information hits surfaced in this scan.

[Open Training module →](#)

4

Apply DLP policies to mailboxes and shared drives

PROCESS

Outlook holds 6,826 of 7,305 high-risk files. A DLP policy blocking outbound CPR, bank-card and passport patterns — combined with quarantine rules for the 19,034 medium-risk items — directly addresses Acme's largest Article 32 gap.

5

Restrict external sharing of high-risk locations

PROCESS

Lock down external sharing on the Outlook and OneDrive locations carrying the 7,305 high-risk files. SharePoint shows 0 high-risk files — keep that posture by tightening guest-access defaults across all 17 Acme sites.

6

Review and minimise long-term inbox retention

PROCESS

840,702 files sit in the >5y bucket — Acme's single largest Article 5(1)(e) storage-limitation concern. Implement a documented mailbox retention schedule reconciled with AML and Finanstilsynet obligations, then apply a phased deletion sweep starting with the >5y inbox cohort.

7

Send sensitive data via secure channels only

PROCESS

Standardise on encrypted transmission for all communications touching the 5,650 DK CPR or 1,248 bank-card records. Block unencrypted attachments at the mail gateway to prevent the recurrence of high-risk Outlook items.

8

Re-run this assessment quarterly

ASSESSMENT

The three-day history shows medium-risk dropping from 22,270 to 19,034 but high-risk flat at 7,305. Quarterly re-scans will confirm whether DLP and retention controls are moving the high-risk core, and provide an audit trail for Datatilsynet should it ever be requested.

[Open Assessments](#) →

INCIDENT RESPONSE

Incident response readiness

Should a personal data breach occur, Article 33 GDPR requires notification to Datatilsynet within 72 hours of becoming aware. Realistic scenarios for Acme include misdirected Outlook mail exposing one or more of the 5,650 DK CPR records, account compromise of one of the top three concentrated users (collectively holding ~63% of high-risk files), or accidental external sharing of an Article 9 health record from the 20,133 health-information hits. A rehearsed playbook covering detection, severity triage, Datatilsynet notification templates and Article 34 data-subject communication enables Acme to meet the 72-hour window without improvisation.



DISCLAIMER

Processed under the EU GDPR and the Danish Databeskyttelseslov. Datatilsynet is the competent supervisory authority; this report is not an inspection filing.

Danish fines are issued through the criminal courts on Datatilsynet recommendation. Maximum tiers mirror the GDPR: the higher of €20m or 4% of global turnover (upper) / €10m or 2% (lower).