safeonline

Rapport

GDPR Risk Analysis

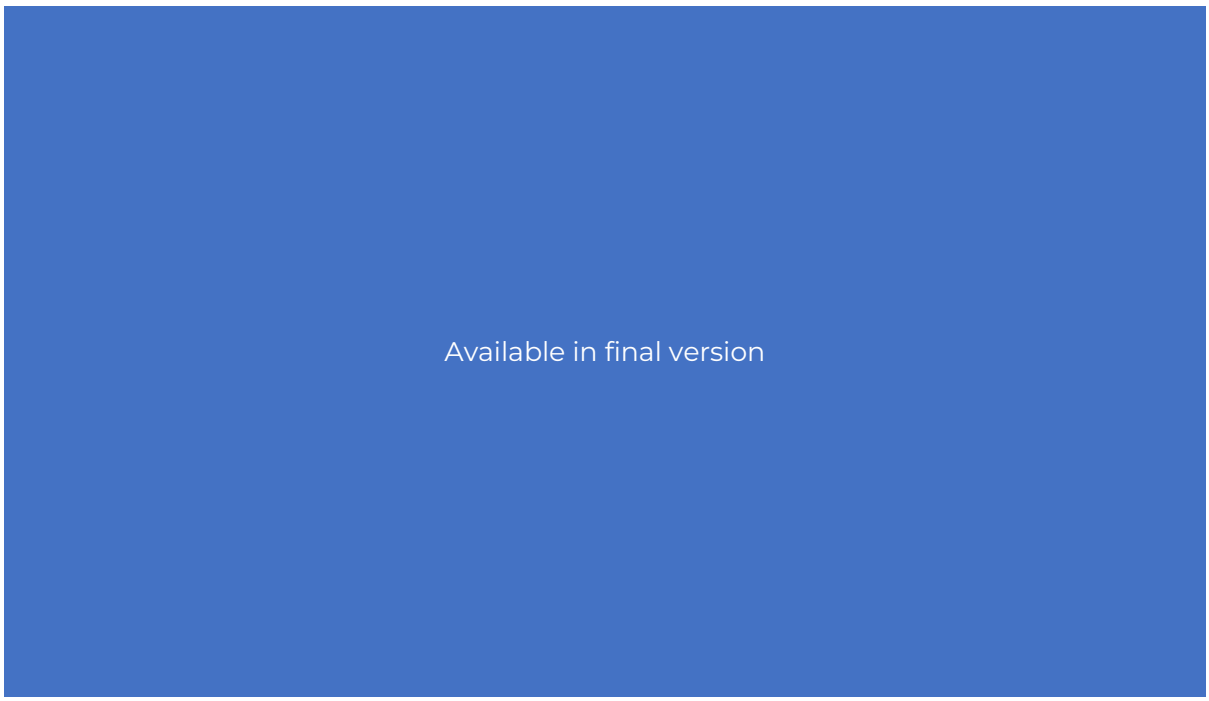
Table of Content

1. Summary

The report presents the results of a GDPR Risk Scan conducted across your Outlook accounts using DataMapper. The scan has identified the most critical areas where your company is vulnerable to GDPR violations.

The high concentration of sensitive information in specific email accounts and older documents underscores the need for a structured and continuous cleanup to ensure compliance and reduce risks.

Key Figures from The Analysis:



2. Introduction

The General Data Protection Regulation (GDPR) sets strict standards and rules for companies' handling of personal data. Non-compliance with these rules can result in severe legal sanctions and, in some cases, fines of up to 4% of the annual turnover. Additionally, distrust from customers and stakeholders can have even more far-reaching consequences for a company.

Ensuring compliance with GDPR is crucial for several reasons. It significantly reduces risk, promotes trust, improves customer relationships, and builds loyalty. Companies that actively take responsibility for personal data and data security gain a clear advantage by demonstrating they comply with the law and protect their customers' information, resulting in trust from both customers and employees.

To handle data both securely and responsibly, and to comply with GDPR, it is essential to apply a risk-based approach to information security. This approach involves conducting thorough risk assessments and GAP analyses to identify vulnerabilities, threats, and potential consequences of a data breach. By proactively addressing these gaps, companies can improve compliance with regulations like NIS 2 and strengthen their commitment to protecting sensitive information.

About the Report

This report is a risk assessment based on a GDPR Risk Scan performed on your Outlook accounts by the data discovery tool DataMapper. The report presents your GDPR risk based on the data you store in Outlook. This gives you data-driven real-time insight into the company's overall GDPR risk. The report is used in connection with internal or external audits.

It is important to remember that this report is merely an analysis aimed at assessing your GDPR risk. In its conclusion, the report will provide recommendations for measures to clean up your personal data.

What is a GDPR Risk Scan?

To reduce GDPR risks associated with handling personal data, it is necessary for a company to have an overview of the personal data it possesses. The more sensitive data you have stored, the greater your risk. Being subjected to a hacker attack can be compared to a home burglary; if you've ensured that all valuables are removed from the house, the thief will have nothing to steal. A GDPR Risk Scan lays the foundation for removing all personal information, so unwanted guests have nothing to steal.

The GDPR Risk Scan is performed by DataMapper. DataMapper is a data discovery tool that uses AI and machine learning algorithms to find numbers and words categorized as sensitive across the company's employees, cloud storage, emails, systems, and apps. DataMapper scans data systems to find documents, emails, and images that contain words and terms related to GDPR. A GDPR Risk Scan is a DataMapper scan limited to the company's Outlook accounts. The scan can include all active Outlook accounts, as well as inactive accounts—for example, of former employees.

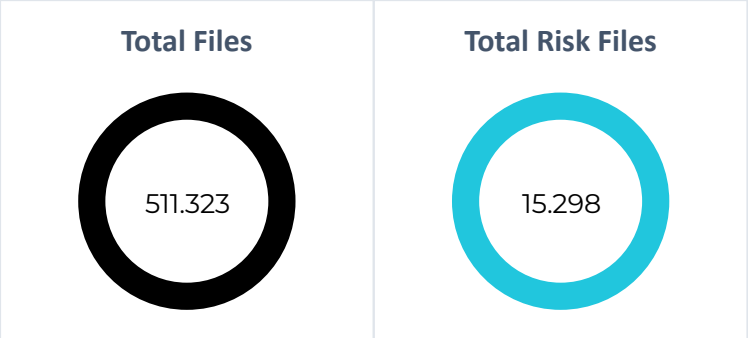
3. Analysis

An in-depth analysis of your risk data based on the DataMapper scan is presented here. The analysis section provides a clear picture of where your company stands in relation to GDPR compliance and where the risks are primarily concentrated.

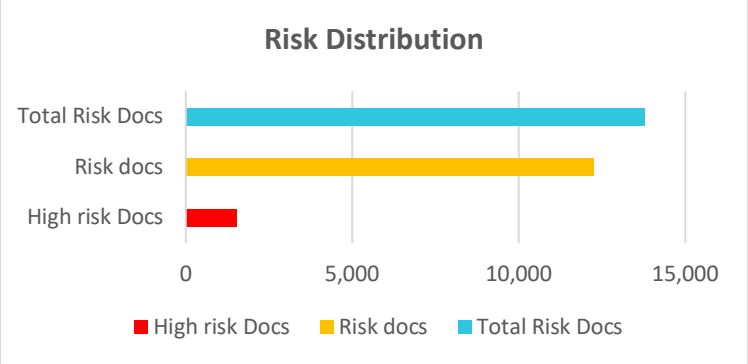
General Risk Assessment

To provide a general risk assessment, a general overview of your data is presented here.

Total Risk Distribution

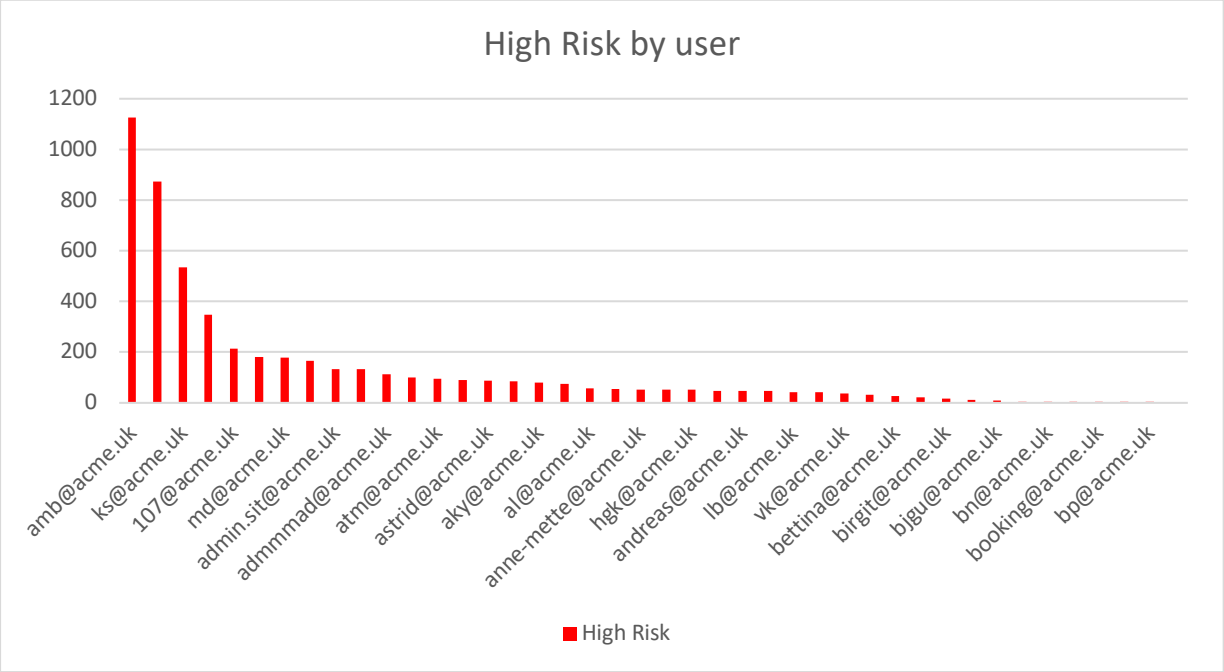


Distribution of Risk



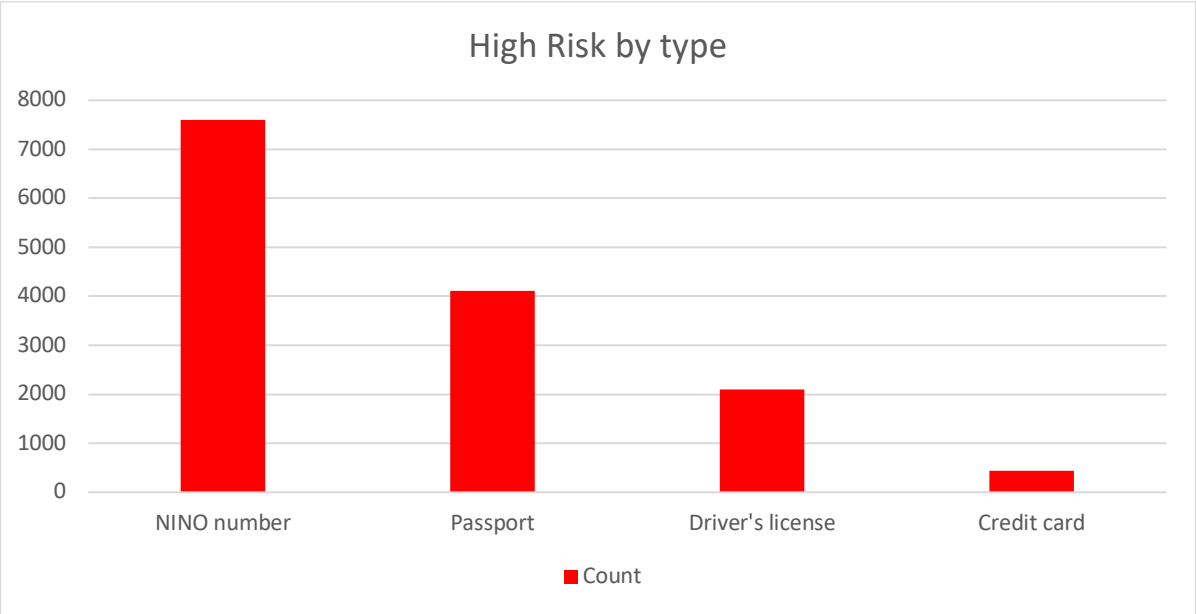
4. Users with Documents that Contain High Risk

DataMapper identifies documents, emails, and images with high risk. These involve numbers that may be extra sensitive. This can include British NINO numbers, driver's license numbers, passport numbers, and credit card numbers. These numbers are particularly sensitive and will therefore be marked as high risk.



A total of 76 email accounts have been found at your company. Out of these, 32 accounts contain high-risk information (e.g. NINO numbers, passport numbers, driver's license numbers, or credit card numbers).

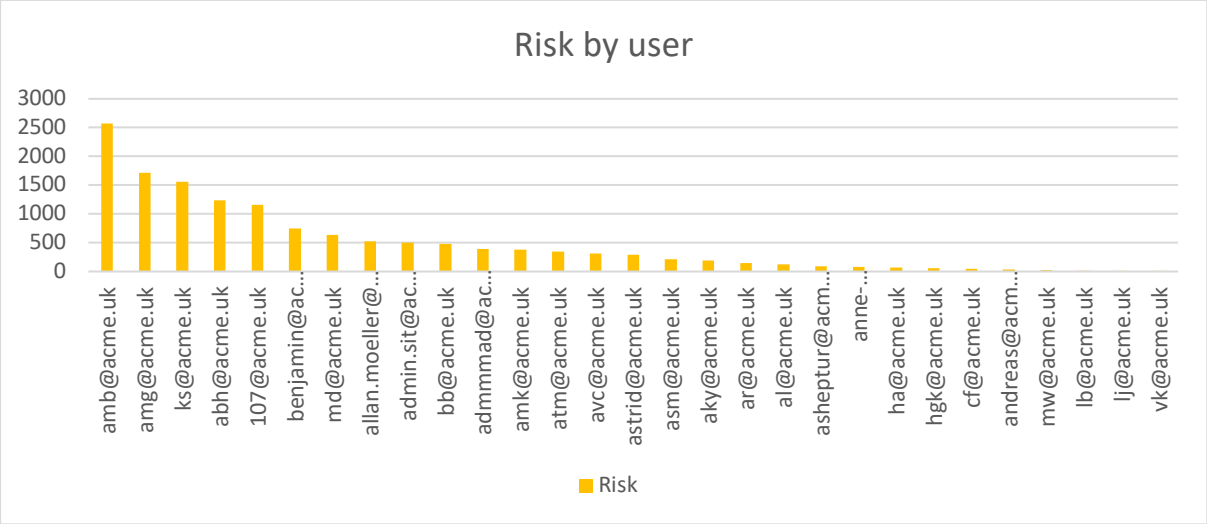
High-Risk Information by Type



A total of 7,598 NINO numbers, 4,113 passport numbers, 2,101 driver's license numbers, and 434 credit card numbers have been found in emails.

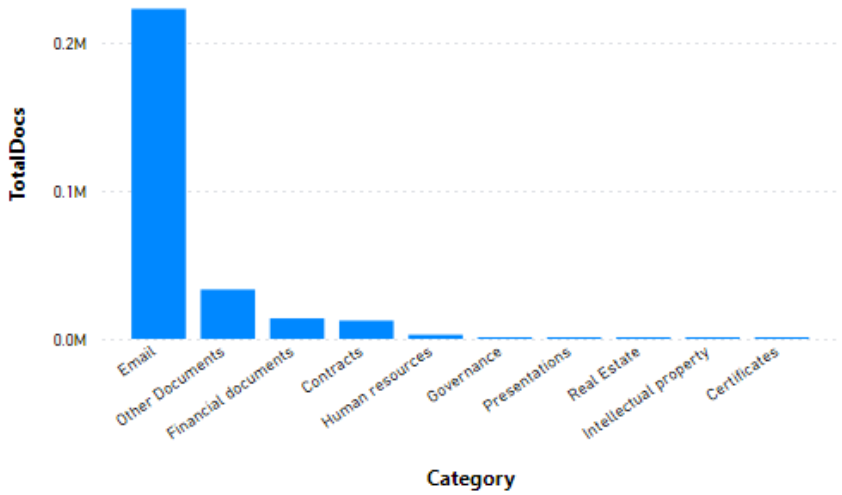
5. Users with Documents that Contain Risk

DataMapper identifies documents, emails, and images that carry risk. These are documents containing sensitive information about individuals that can be considered personally identifiable information (PII). Our method involves the use of an extensive taxonomy, which is a list of specific keywords and phrases associated with race, ethnic origin, political beliefs, religion, trade union membership, health status, and sexual preferences. If any of these keywords are found near a person's identity within a document, email, or image, it is marked as a risk document.



Personally Identifiable Information (PII: Personally Identifiable Information) identified in your email accounts: 24

Risk Information by Document Category



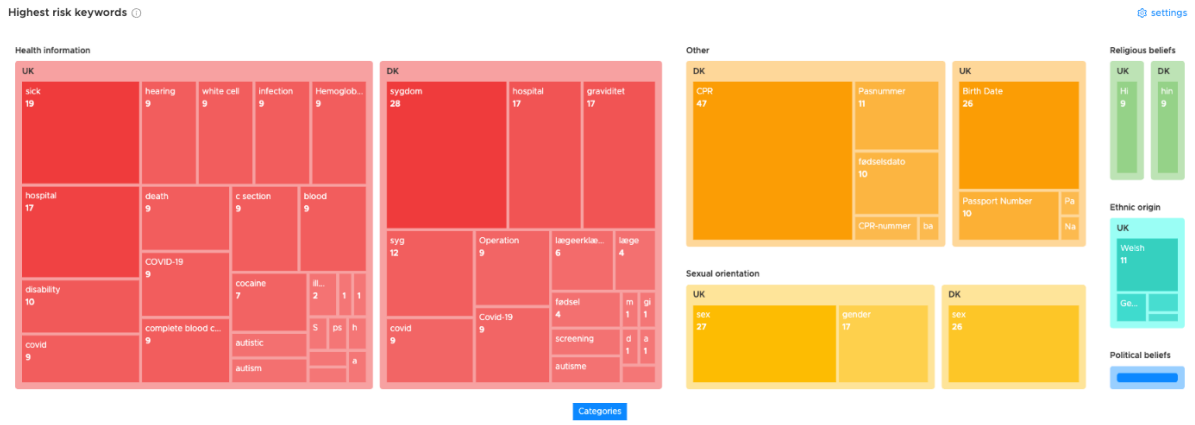
There are many different types of documents that can potentially be sensitive in employees' emails. For example: 642 HR documents, 211 employee evaluations, 631 personal identification documents, 54 board meeting documents, 471 documents marked as confidential, 821 contracts, 1,213 CVs, 71 IP-related documents.

GDPR Keywords Related to Named Individuals

Certain keywords only constitute a GDPR risk if they are mentioned in relation to a person. These are keywords that pertain to race, ethnic origin, political beliefs, religion, trade union membership, health information, and sexual preferences.

Prior to this report, you have input personal names into DataMapper related to your company. Below is a heatmap and a chart of the GDPR keywords that appear in emails alongside these individuals.

We use a GDPR taxonomy to classify words that are sensitive by nature. For example, in a sentence like "Peter Jackson was a member of the LGBT club," "Peter Jackson" is a name we search for, and "LGBT" is a sensitive word from our taxonomy.



This heat map visualizes the risk keywords found in correlation with personal names, categorized by different types of sensitive information. It provides a clear representation of which sensitive keywords appear most frequently and highlights potential GDPR risks. If you want to see more of the heat map, you can access it under **Dashboard → General**.

6. Choice of Cleanup Method: Manual or Automated?

The analysis shows that your organization has personal data that requires cleanup to ensure GDPR compliance and protect against potential risks. You are now faced with a choice: Should the cleanup be done manually or with the help of DataMapper?

Manual Cleanup

Manual cleanup is both time-consuming and often difficult to ensure that employees perform consistently. Many companies experience challenges in getting employees to prioritize cleanup among their other tasks. Additionally, it can be difficult to control whether the cleanup is happening at all and whether it is performed adequately. This increases the risk that sensitive data is overlooked, which can lead to fines and damage to the company's reputation.

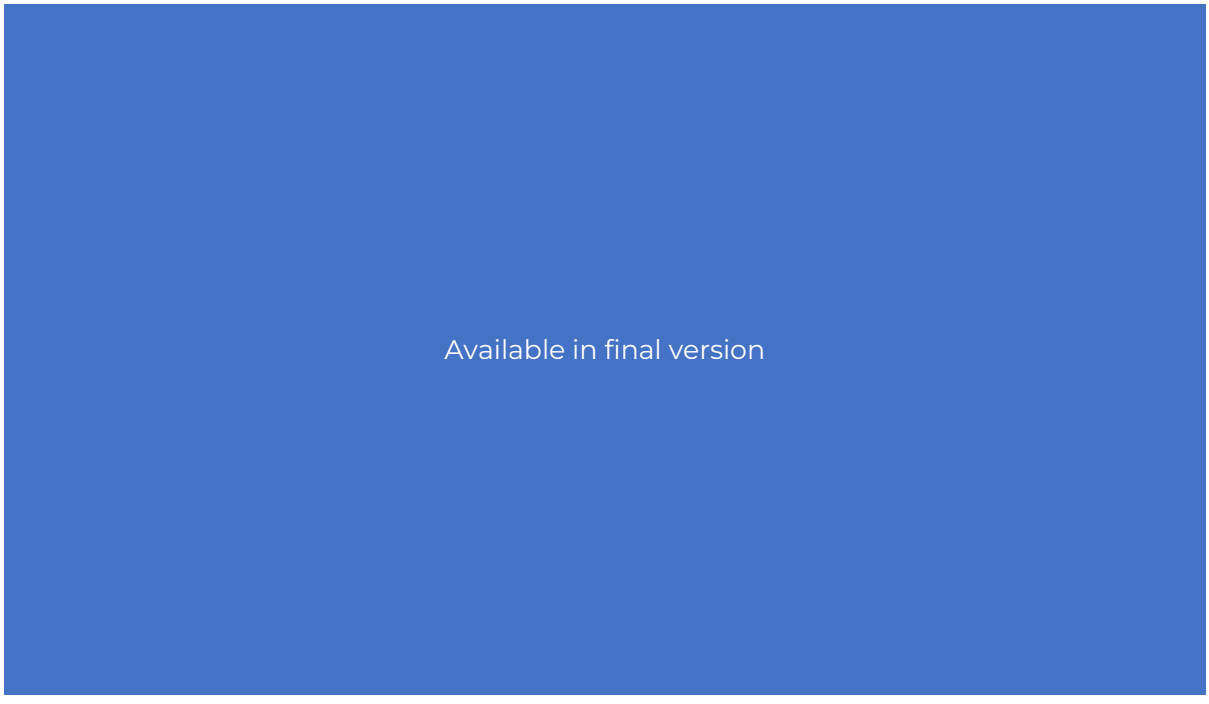
Automated Cleanup with DataMapper

DataMapper offers a much more effective solution, where large parts of the cleanup are automated. The tool continuously scans your data for sensitive information and identifies the risk-filled elements that require action. Employees still need to make decisions about deleting or moving data, but DataMapper significantly reduces the necessary time.

With DataMapper, you can:

- Significantly reduce the time spent on cleanup.
- Minimize the risk of human errors and lack of oversight.
- Gain a clear overview of where the biggest risks are and how they should be handled.
- Free up resources so your employees can focus on their core tasks.

Cost Comparison Between Manual and Automated Cleanup



7. Conclusion

Available in final version

8. What Should You Do Now

Available in final version