Data & More | Data Minimization Manager™

Remove privacy data from mail, OneDrive, SharePoint, and FileShares to protect digital privacy and minimize the risk, cost, and liability of processing unstructured data.

01 Executive Summary

In the end, all successful data privacy initiatives end with data minimization. That is, deleting data that is illegal to keep under data privacy laws such as GDPR, CCPA, and PIPEDA. Now, deleting data might sound easy—and it is. However, only deleting the correct data is a whole different story. To delete illegal data, you must first classify the data and identify the data subject, then verify your automated findings with the data owners, and only then can you delete the illegal data.

Luckily, we have been working on just that for the last seven years, both to implement and operate data minimization at scale, from organizations with fewer than 40 employees to those with over 40,000. Using the same simple approach of classify | verify | minimize. Building on this straightforward concept, our platform offers a comprehensive solution for data minimization.

If you want a demo of Data & More, you can try demo.dataandmore.com, and we will sponsor up to 25 test users for up to 2 months.

w: dataandmore.com // m: support@dataandmore.com

Table of Contents

02 About Data & More

Data & More was founded in 2016 by a European team of Data Scientists and Data Privacy advocates. When the EU rolled out GDPR in 2017, the Data & More|Privacy Platform quickly became the de facto standard for Document Classification, Data Breach Mitigation, and Data Minimization. Over the last few years, the Data & More | Privacy Platform has evolved to a full GRC suite for unstructured data. In 2024, the platform is used by more than 150,000 users in over 28 countries, including the US and Canada.

We provide our services to private, public, and non-governmental organizations, including law enforcement and defense. On a daily basis, we monitor over 3.000.000.000 documents in an effort to protect hundreds of thousands of data subjects.

Data & More is ISA 3000 and ISAE 3402 certified and 100% owned by the people working in Data & More.

INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS ISAE 3000

INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS ISAE 3402

THE EUGDPR INSTITUTE GDPR Practitioner (CEP) CERTIFIED ★★★

THE EUGDPR INSTITUTE GDPR DPO/Data Controller (DPO) CERTIFIED ★★

THE EUGDPR INSTITUTE GDPR Foundation (FAS) CERTIFIED ★

03 What is the Data & More| Privacy Platform

The Data & More | Privacy Platform is a comprehensive tool that enables organizations to identify, verify, and minimize privacy data in large unstructured data sources such as mail, file share, OneDrive, and SharePoint. It has severely award-winning features that have made it the platform of choice for CIOs, CISOS, and DPOs.

- Comprehensive International Privacy Data Classification (29 languages)
- Multiple Data Privacy Framework such as GDPR, CCPAM IAAP, and PIPEDA
- Data Subject Identification and Data Subject Acess Request
- Enduser Verification that moves the minimization responsibility from IT to the data owner
- Build-In Data Minimization
- High Speed and Scalability
- Privacy by design
- add-in for Microsoft Copilot Protection
- add-in for Microsoft Purvew
- add-on for Data Breach Mitigation

04 Why do we need Data Minimization

The simple answer is that 137 out of 194 countries require it by law, according to the UN Trade and Development Program (UNCTAD). In the EU, that is implemented as GDPR; in the US and Canada, different states have different implementations—all requiring data minimization.

From an organizational perspective, it is, first of all, a matter of maintaining trust from the consumers, employees, and shareholders. Suppose an organization loses or misuses personal data. In that case, it can be very costly and, in some cases, lead to bankruptcy, induced by consumer boycotts or by blackmail and extortion from bad actors.

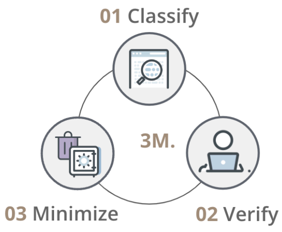
Most organizations can survive a data breach if they only have the data that they are legally entitled to. Still, if they have old privacy data such as old passports, customer records, CVs, health information, and travel books lying around - the cost of a data breach can be insurmountable.

The average cost of a data breach is 4,4 million euros in 2023, and the average price of a fine for non-compliance to GDPR is 1,7 million € in the EU.

Finally, we need to minimize data because it is the right thing to do. Victims of Data breaches are subject to blackmail, having their financial lives destroyed. If we look at the new appetite for AI the risk of having old privacy data lying around in MS 365 or fileshares is increasing vertically. Data Breaches caused by tools like CoPilot are reported daily, sometimes due to bad luck and others due to evil intentions. (For more information, Data Breachdes caused by AI Data & More CoPilot Privacy Protections)

05 The Data Minimization Process

To effectively implement a data minimization process, it needs to be straightforward… exceptionally straightforward. If not, it becomes ineffective, leading to errors and vulnerabilities. One of the critical insights to design the D&M minimization process is the probability that a document that is older than three months AND, contains Personal Data AND is located in MS 365 AND will ever be opened again is less than 1 in 100.000. Therefore, we establish a rule called three by 3, which covers the data's 9-month lifespan from creation to deletion.



Classify | Verify |Minimize

In the first three months of a document's lifetime, the data owner can work with the data doing what ever the data is intended for. At the same time D&M Privacy Platform is classifying the data so it knows if the document that needs to be minimized sooner or later. We call the period the "Grace" period, and it is used to read and classify documents. (refer to section 04 of Insights into Classification)

Classify | Verify |Minimize

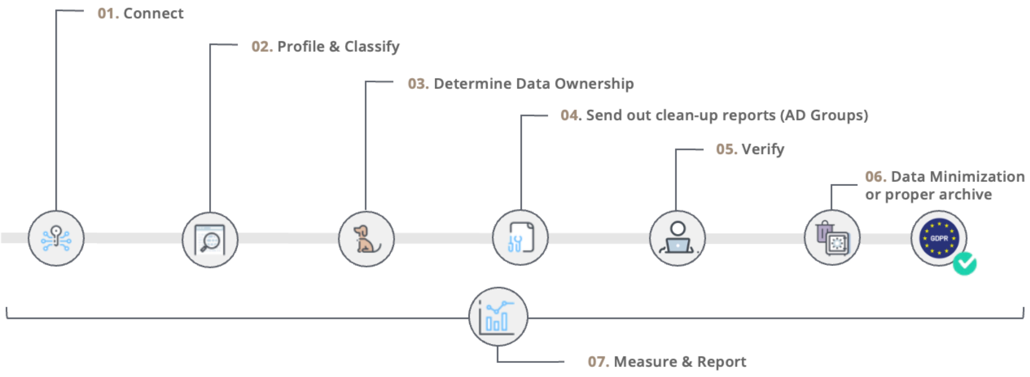
After three months, the document is added to the End-user Verification Report (see section 05) - and an email is sent to each of the data owners with a link to their reports. In this report, the user can mark any documents as private or for dispensation if they would like to keep them for a longer time. The user has three months to verify the classification and mark data that should not be deleted.

Classify | Verify |Minimize

Now, between six and nine months after the Privacy data has been created (or received), the data will be deleted by the DMCS. If the data resides in Microsoft 365, it can be retrieved within 30 days, after which point only organizations with custom MS 365 backup can recreate the data.

Data residing in file shares will be deleted immediately and can only be restored via backup. Note that if data is restored, it will be deleted again within 6-9 months if no data owner intervenes and marks it for dispensation.

Where to start


01. Connect
02. Profile & Classify
03. Determine Data Ownership
04. Send out clean-up reports (AD Groups)
05. Verify
06. Data Minimization or proper archive
GDPR
07. Measure & Report

Step 1. Data is connected to the DMCS using one of the many intelligent connectors in the DMCS.

Step 2. D&M Privacy Classification is applied to the data, and the standard 3X3 minimization policy is adapted

Step 3. Privacy Data with no apparent owners are identified, and custodians are assigned using the custodian mapping process.

Step 4. The Validation Report is sent out the the data owners and custodians

Step 5 The result of the first classification is verified, and the classification is updated.

Step 6. Data is minimized, aka deleted/moved/encrypted

Step 7. Online Reporting is available for PM, DPO, and Compliance Documentation

05 Data Classification

Data & More's data classification team has spent over six years developing a comprehensive privacy compliance classification system that is used, tested, and quality assured on billions of data each day. This system can identify privacy data as required by law for each country. It is maintained and optimized daily by a multilingual team.

DMCS provides an entire Data Privacy Classification in 28 languages, including local health information, unions, religious and sexual orientation, and all the sensitivity categories required in, e.g., the EU, North America, and Canada. Examples below:

Confidential Personal Data Document Classes (examples)

- European & international ID
- ID card, number, or information
- European & International Social Security info
- Social security card, number, or information
- European & international health cards
- Health card, number, or information
- European & international drivers' licenses
- The card, number, or information
- European & international passports
- The passport, number, or information
- Credit cards
- The credit card, number, or information
- Tax information
- Tax returns, etc.
- Residence permit
- Permits and or information in them
- Salary information
- Pay slips, etc.
- Employment documents
- Contracts etc.
- Recruitment (Application/job offer/CV)
- A wide range of information related to the recruitment process, job applications, CVs, job interviews, etc.
- Bonus agreements
- Dismissal or resignation
- Terminations or resignations
- Written warnings
- Expulsions

Criminal offenses document classes (examples)

- Criminal record
- Criminal records and information about them
- Offenses, fines, and convictions
- Convictions, fines, etc.

Sensitive personal data document classes (examples)

- Health info
- Diagnose

- Illnesses
- Medication
- Sick leave
- Health evaluation
- Prescriptions

Trade union membership (examples)

- Membership of a trade union

Orientations Belief & Origin (examples)

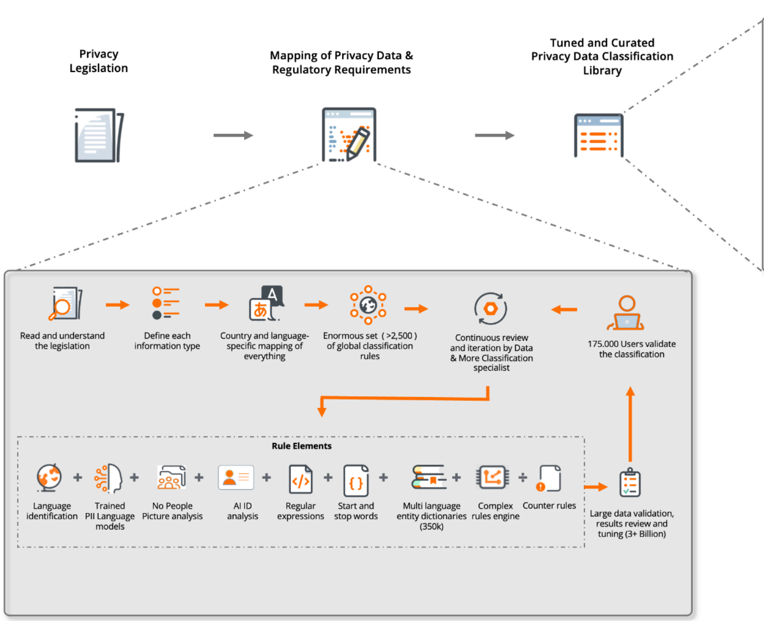
- Which country do you come from
- Ethnicity
- Membership in a political party
- Religious orientation
- Member of a religious church
- Religious congregation
- Gender types
- Information about sexual orientation

Non-sensitive personal data document classes (examples)

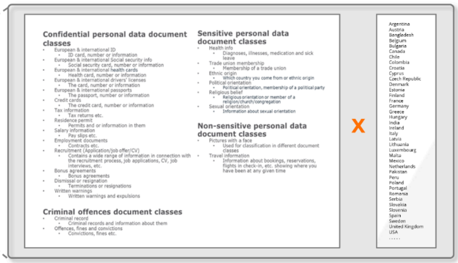
- Pictures with a face
- Used for classification in different document classes
- Travel information
- Travel bookings
- Reservations
- Check-ins, a.g.., showing where you have been at any given time

The above list is an example of some of the Privacy classifications. For each class, there are hundreds of thousands of classification elements that are used to identify positives and remove false positives.

Now the implementation of our classification is our "Secret Source" and requires a lot of technology and a lot of language expertise. See the illustration below.


Privacy Legislation
Mapping of Privacy Data & Regulatory Requirements
Tuned and Curated Privacy Data Classification Library
Read and understand the legislation
Define each information type
Country and language-specific mapping of everything
Enormous set (>2,500) of global classification rules
Continuous review and iteration by Data & More Classification specialist
175.000 Users validate the classification
Rule Elements
Language identification
Trained PII Language models
No People Picture analysis
AI ID analysis
Regular expressions
Start and stop words
Multi language entity dictionaries (350k)
Complex rules engine
Counter rules
Large data validation, results review and tuning (3+ Billion)

https://support.dataandmore.com/en/knowledge/what-is-gdpr-data-classification



Confidential personal data document classes

- European & international ID
  - ID card, number or information
- European & international Social security info
  - Social security card, number or information
- European & international health cards
  - Health card, number or information
- European & international drivers' licenses
  - The card, number or information
- European & international passports
  - The passport, number or information
- Credit cards
  - The credit card, number or information
- Tax information
  - Tax returns etc.
- Residence permit
  - Permits and or information in them
- Salary information
  - Pay slips etc.
- Employment documents
  - Contracts etc.
- Recruitment (Application/job offer/CV)
  - Contains a wide range of information in connection with the recruitment process, job applications, CV, job interviews, etc.
- Bonus agreements
  - Bonus agreements
- Dismissal or resignation
  - Terminations or resignations
- Written warnings
  - Written warnings and expulsions

Criminal offences document classes

- Criminal record
  - Criminal records and information about them
- Offences, fines and convictions
  - Convictions, fines etc.

Sensitive personal data document classes

- Health info
  - Diagnoses, illnesses, medication and sick leave
- Trade union membership
  - Membership of a trade union
- Ethnic origin
  - Which country you come from or ethnic origin
- Political orientation
  - Political orientation, membership of a political party
- Religious belief
  - Religious orientation or member of a religion/church/congregation
- Sexual orientation
  - Information about sexual orientation

Non-sensitive personal data document classes

- Pictures with a face
  - Used for classification in different document classes
- Travel information
  - Information about bookings, reservations, flights in check-in, etc. showing where you have been at any given time

X

Argentina
Austria
Bangladesh
Belgium
Bulgaria
Canada
Chile
Colombia
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
India
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Mexico
Netherlands
Pakistan
Peru
Poland
Portugal
Romania
Serbia
Slovakia
Slovenia
Spain
Sweden
United Kingdom
USA
.....

For example, here's *one part* of the country and language-specific classification rule for detecting civil status:

In **Germany** these documents need to be detected and mapped:

Lebenspartnerschaftsurkunde
(Registered partnership)
Personenstandsurkunde
Familienstandsurkunde
Familienbuch
(Marital status)
Lebenspartnerschaftsurkunde
(Dissolution of a registered partnership)
Scheidungsurkunde
(Invalidity of the marriage/divorce)

In **Poland** these documents need to be detected and mapped:

odpis skrócony aktu małżeństwa
(Short-form marriage certificate)
odpis zupełny aktu małżeństwa
(Long-form marriage certificate)
zaświadczenie o stanie cywilnym
(Certificate of civil status)
orzeczenie sądu o rozwodzie
(Court ruling on divorce)
orzeczenie sądu o separacji
(Court ruling on legal separation)
orzeczenie sądu o zniesieniu separacji
(Court ruling on termination of legal separation)
orzeczenie sądu o unieważnieniu małżeństwa
(Court ruling on the annulment of a marriage)

In **Czechia** these documents need to be detected and mapped:

potvrzení o uzavření manželství (vydané zastupitelským úřadem ČR v zahraničí)
(Confirmation of marriage issued by a Czech embassy or consulate)
doklad o registrovaném partnerství (Registered-partnership certificate)
vysvědčení o právní způsobilosti ke vstupu do registrovaného partnerství
(Certificate of legal capacity to enter into a registered partnership)
potvrzení o údajích zapsaných v matriční knize
(Confirmation of data entered in the family register)

(Data & Mores Serect Souce in the form of technology and language integration)

06 End-User Verification

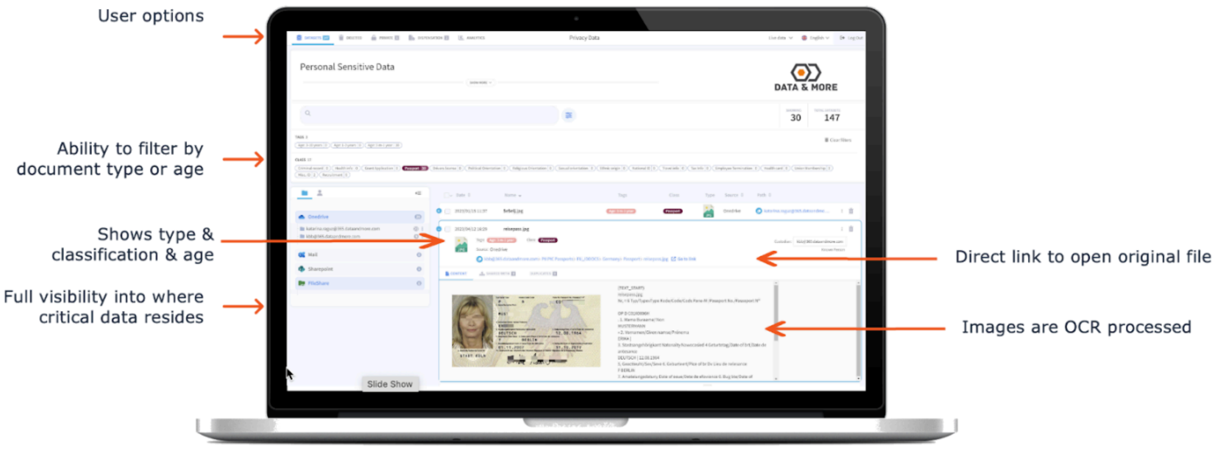
The Verification Report

Data & More End-user Verification gives the data owners a complete overview of the data that has been auto-classified as non-compliant. The data owner can then use the report to mark documents as misclassified, private, or dispensation, depending on the individual’s needs.

It gives the ensure quick preview of the and insight into:

- The total amount of data that must be cleaned up
- Document Age
- Document Class
- Document Location
- Document Type
- Document Owen
- Data Subjects

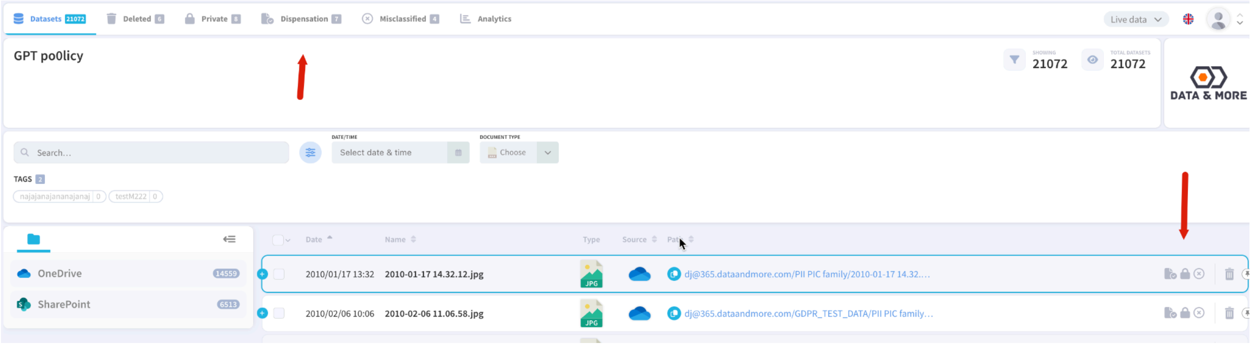
By combining the age filter with location and class, the end-user can very quickly identify, e.g., passports older than five years that are located in the inbox or health certificates older than ten years in an HR SharePoint site.


User options
Ability to filter by document type or age
Shows type & classification & age
Full visibility into where critical data resides
Direct link to open original file
Images are OCR processed
Privacy Data
Personal Sensitive Data
DATA & MORE
30
147
Slide Show

(The End-user Validation Report gives each end-user easy access to their own Privacy Data)

One of the many advantages of the D&M for Purview End User Verification Report is that the end user can quickly check the data and mark data that they need to keep with “Dispensation” or, in the case of Private data, as Private Data. This type of marking can be customized to specific organizational needs.

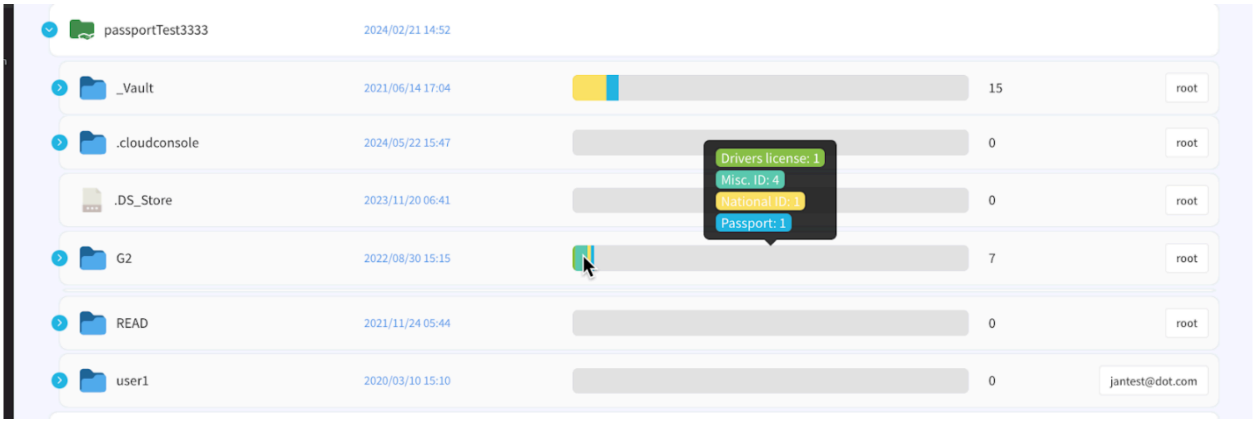
If the end-user thinks that a document has been falsely classified, the end-user can mark it as misclassified as input to the Data & More's classification team.



Date	Name	Type	Source	Path
2010/01/17 13:32	2010-01-17 14.32.12.jpg	JPG		dj@365.dataandmore.com/PII PIC family/2010-01-17 14.32....
2010/02/06 10:06	2010-02-06 11.06.58.jpg	JPG		dj@365.dataandmore.com/GDPR_TEST_DATA/PII PIC family...

Custodian Mapping

Proper data management requires that one (or more) person be responsible for a specific data repository. This is easy for Mail and OneDrive, as it is the owner's responsibility. However, with SharePoint and FileShare, this is often much more blurry due to the rotation and churn of employees. Data & More offers a great tool to identify, manage, and maintain "Custodians." The best thing about custodian mapping is that it works by a risk-first approach, so you can start mapping the data that is a risk and leave the rest for later.



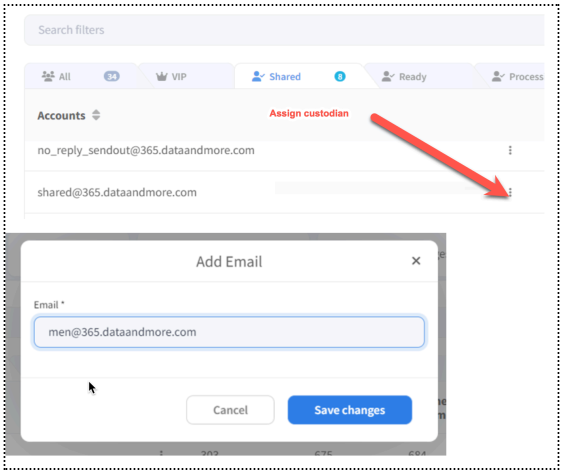
passportTest3333	2024/02/21 14:52		
_Vault	2021/06/14 17:04	15	root
.cloudconsole	2024/05/22 15:47	0	root
.DS_Store	2023/11/20 06:41	0	root
G2	2022/08/30 15:15	7	root
READ	2021/11/24 05:44	0	root
user1	2020/03/10 15:10	0	jantest@dot.com

When the custodian mapping is done, all data can be verified appropriately - using the Validation Report.

Shared Mailboxes

Establishing ownership of shared mailboxes is another critical requirement for efficient data minimization. This can be done in multiple ways.

1. If a shared mailbox has an assigned manager (like a normal user), the manager will automatically get custody of the shared mailbox.
2. If a normal user is assigned via the Azure portal as “another email,” that user will get custody of the shared mailbox.
3. Finally, if neither a manager nor another user has been assigned, the DMCS supports manual assignment of the shared mailbox to specific users.



Accounts

no_reply_sendout@365.dataandmore.com

shared@365.dataandmore.com

Email *: men@365.dataandmore.com

When the custodian has been assigned to the shared emails, all data can be verified appropriately - using the Validation Report.

07 Data Minimization

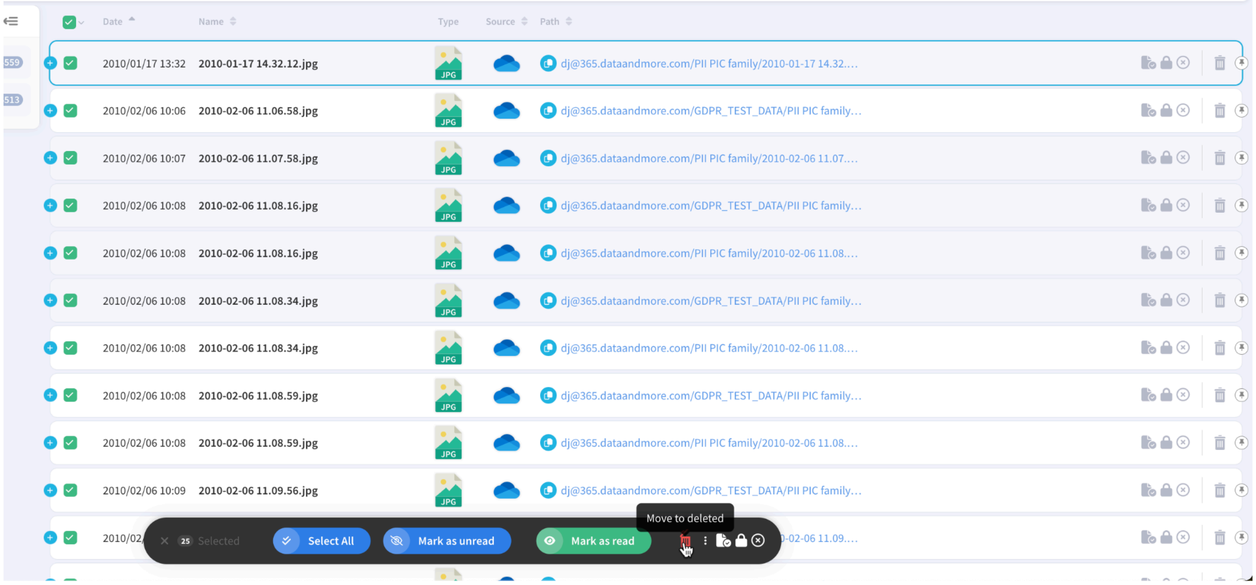
One of the significant advantages of using the Data & More Data Minimization tool is that the responsibility for deletion is moved from the IT department to the owner or custodian of the Privacy Data. The actual data can be configured either som opt-in or opt-out, also known as **Confirmed Delete** or **Automatic Delete**.

Automatic Delete

Automatic Delete, as the wording implies … deletes the data that has been sent to the data owners for verification after a predefined time period. We recommend deleting data that has been notified after three months if the organization's verification shields follow the recommendation UNLESS a dataset has been marked as private / Dispensation or Misclassifed.

Confirmed Delete (optional)

Some organizations prefer to let the data owner or custodian “press the button” for each data set that should be deleted. Now, this might sound more tedious than it is - because a user can select multiple data sets by classification, type, or age and delete them all at the same time.

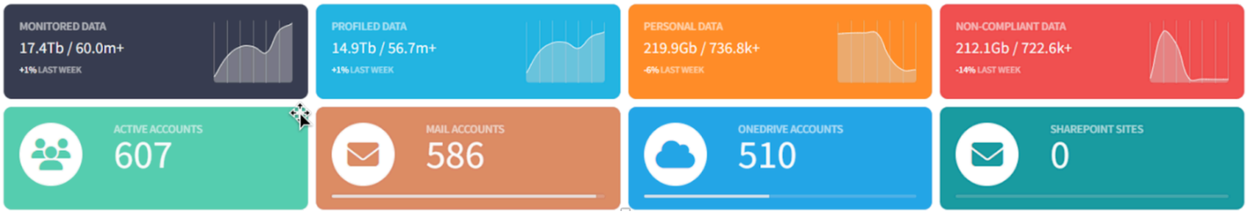


Date	Name	Type	Source	Path
2010/01/17 13:32	2010-01-17 14.32.12.jpg	JPG		dj@365.dataandmore.com/PII PIC family/2010-01-17 14.32.…
2010/02/06 10:06	2010-02-06 11.06.58.jpg	JPG		dj@365.dataandmore.com/GDPR_TEST_DATA/PII PIC family…
2010/02/06 10:07	2010-02-06 11.07.58.jpg	JPG		dj@365.dataandmore.com/PII PIC family/2010-02-06 11.07.…
2010/02/06 10:08	2010-02-06 11.08.16.jpg	JPG		dj@365.dataandmore.com/GDPR_TEST_DATA/PII PIC family…
2010/02/06 10:08	2010-02-06 11.08.16.jpg	JPG		dj@365.dataandmore.com/PII PIC family/2010-02-06 11.08.…
2010/02/06 10:08	2010-02-06 11.08.34.jpg	JPG		dj@365.dataandmore.com/GDPR_TEST_DATA/PII PIC family…
2010/02/06 10:08	2010-02-06 11.08.34.jpg	JPG		dj@365.dataandmore.com/PII PIC family/2010-02-06 11.08.…
2010/02/06 10:08	2010-02-06 11.08.59.jpg	JPG		dj@365.dataandmore.com/GDPR_TEST_DATA/PII PIC family…
2010/02/06 10:08	2010-02-06 11.08.59.jpg	JPG		dj@365.dataandmore.com/PII PIC family/2010-02-06 11.08.…
2010/02/06 10:09	2010-02-06 11.09.56.jpg	JPG		dj@365.dataandmore.com/GDPR_TEST_DATA/PII PIC family…
2010/02/				-02-06 11.09.…

However, experiences with more than 150.000 users show that now all are getting around to clean deleting illegal privacy data - and that is why all our organizations sooner or later turn to automatic delete.

08 Compliance Analytics

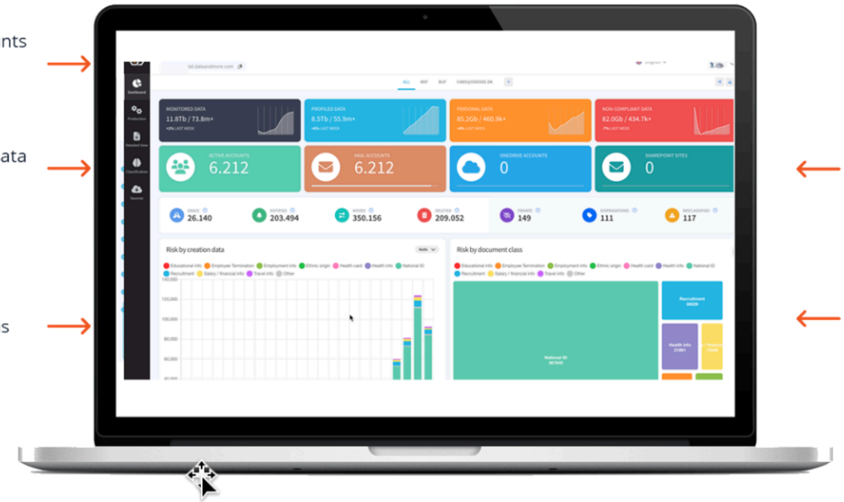
Compliance analytics serves a dual purpose. First, it helps C-level executives, DPOs, and middle managers ensure that data minimization is proceeding as planned and allows them to follow up on any irregularities in the Data Privacy landscape. This could include data sources with a large amount of unmanaged Privacy Data or individual users who have marked large data sets with Dispensation or as Private. The second purpose of Compliance Analytics is to provide comprehensive and trustworthy documentation to auditors—both internal and external Data Privacy Authorities.



(Dashboard header in Compliance Analytics)

Key metrics in the Compliance analysis include:

- Total number of Data Subjects
- Total number of datasets with Privacy Data
- Document age
- Data location
- Owner or custodian
- Document classes
- Data for data minimization (Owner, Type, Location)



High risk accounts

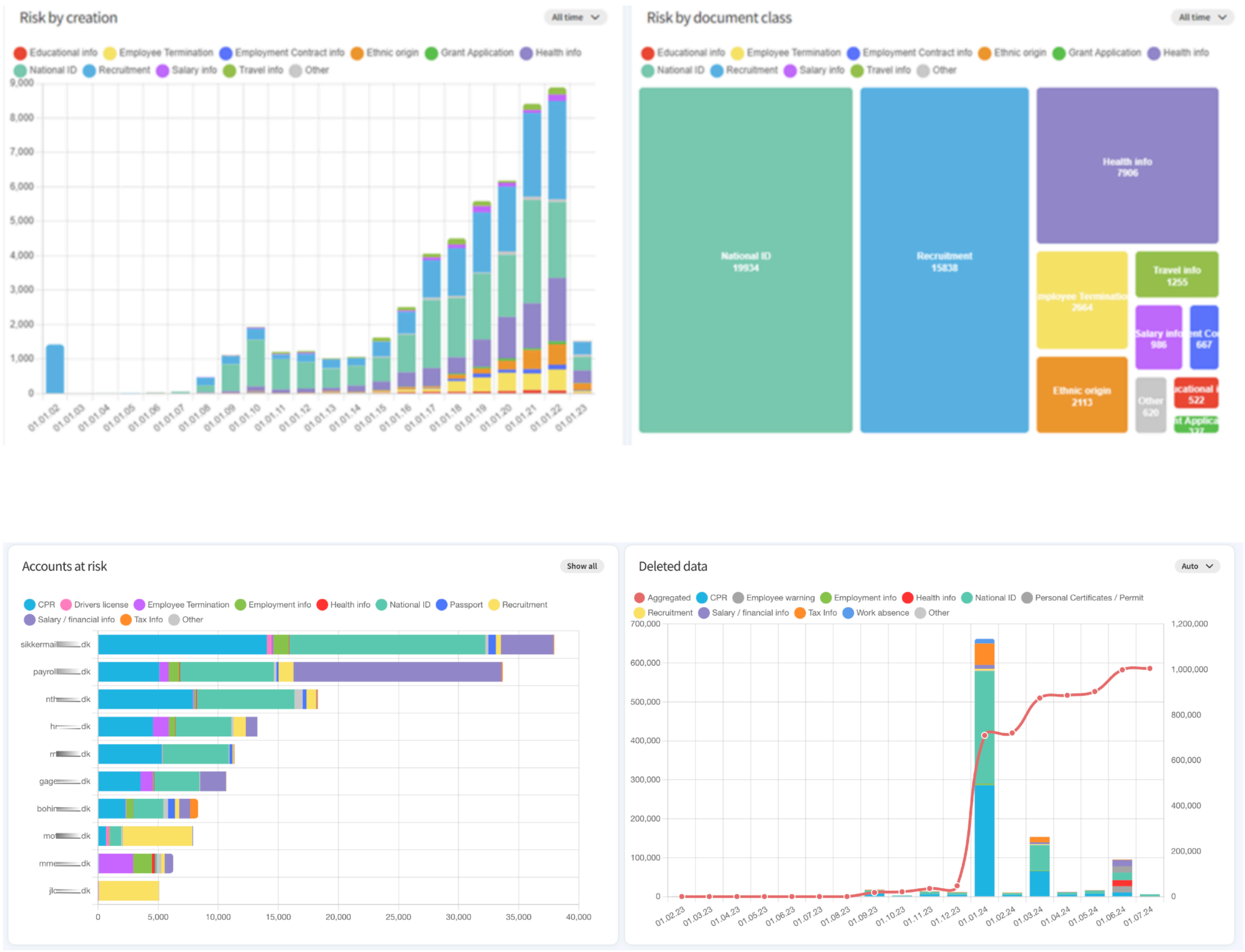
Non-compliant data

Deletions

High risk Data Sources

High risk document types

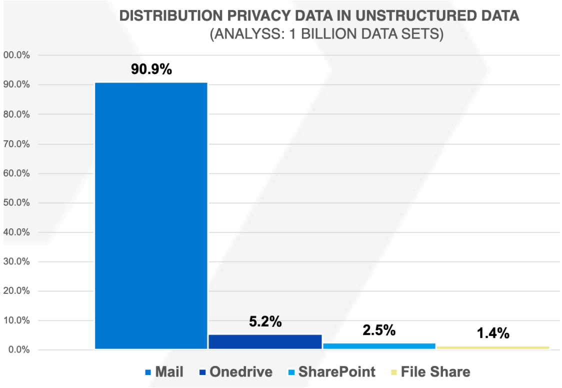
Examples of Compliancy Analytics Graphs:



In Compliance Analytics, the report can be filtered by AD Groups or specific policies or tags. The report can be used to show particular document classes or company-wide but will never show the actual content data.

09 Data & More | Purview Integration (add-on)

Microsoft Purview is an excellent tool for MS 365 compliance, Including Data Loss Prevention and in-document tagging. However, more is needed if you want to be compliant with any Data Protection legislation. Let's take a look at what D&M Purvew integrated adds to Purview.
[1]



1. Purview can protect less than 10% of Privacy Data because it's located in old mail or nonaccessible file types. ([See data and more for Purvew for a complete analysis](#))

2. With Data & More Purview integration, you will be able to identify and minimize +99.99% of any privacy data in Microsoft 365

3. Purview gives you the option to build a Privacy Classification based on some preexisting libraries and regex. However, creating an entire Privacy Classification in Purview has never been done and would take a dedicated team multiple years (if at all posible). Luckily, the D&M Privacy Classification can be transferred to Purvew via Sensitivity Labels, which enables the full potential of Privacy Protection in Purview, including DLP, Oversharing monitoring, and deletion of legacy data in emails.

4. Finally, by using the Data & More Verification Report, data owners will be able to see what data that have been classified as up for deletion. No matter if data have been classified by Puruview automatically, manually by an end user, or by the Data & More Classification Engine. When a data owner can verify that data can be deleted using the Verification Repor, the responsibility for deletion is moved from the IT department to where it belongs.

From a Privacy Perspective, Data & More gives the Purview “Super Powers” and unluck a suite of functionality that are based on correct classification and validation, like DLP, sharing control, and Retention policies.

[1] Analyses of 1 billion datasets conducted by D&M 2024

10 Data & More | Copilot Privacy Protection (add-on)

If you subscribe the the Data & More Privacy Platform, use can add Copilot Privacy protection. In short, D&M | CPP prevents Microsoft Copilot from accessing Personal Sensitive Data by adding sensitivity labels to the data, with the above limited as outlined in sectional 08.

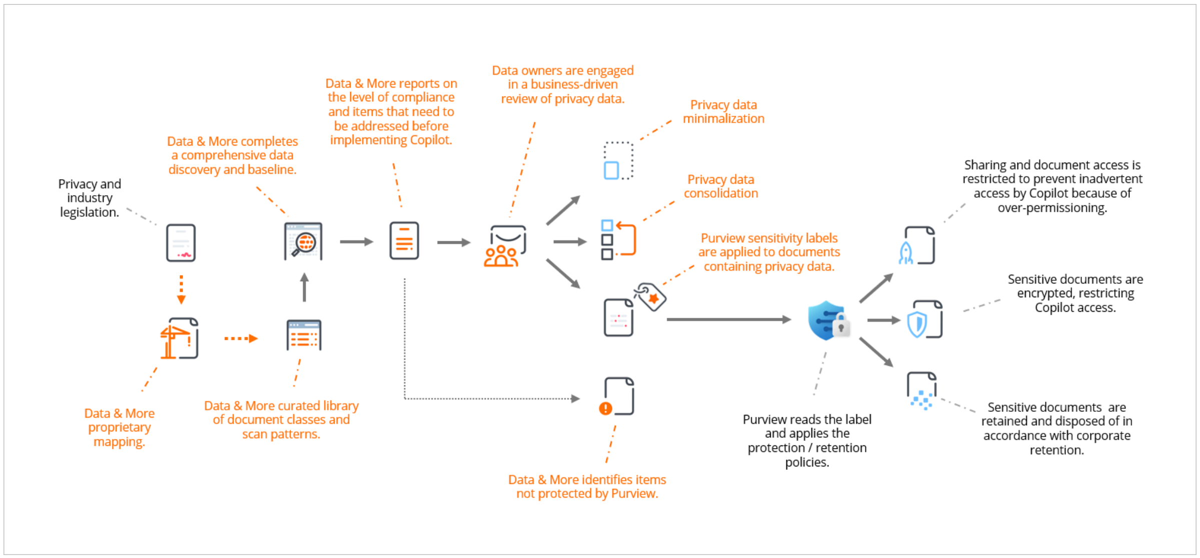
The high-level methodology developed by Data & More for ensuring Copilot data readiness consists of the following steps:

1. **Deploy D&M | CPP and complete a data discovery**. As mentioned in this architecture section, this requires the creation of an App Registration in Azure. It also requires a location to host the software. This can be the Data & More cloud or a server, physical or virtual, that you host.
2. **Identify items to be remediated**. D&M | CPP will provide a summary of all documents containing privacy data, the type of privacy data identified, the location of each document and its age. It will also provide additional insights, like the occurrence of duplicates and the level of access. This information can be curated into a Copilot Data Readiness Baseline and used to determine the best option for addressing each set of privacy data.
3. **Conduct a business-driven privacy data review**. Data owners and custodians are the best people in an organization to make decisions about privacy data. D&M | CPP automates the engagement of these individuals, distributing information about documents containing privacy data to each data owner and custodian, allowing them to mark documents for deletion, retention, relocation, and labeling.
4. **Configure Purview labels and data protection policies**. The labels needed for encryption and content analysis blocking can be configured along with the policies to implement these services on labeled content.
5. **Remediate identified data**. Once reviewed by business owners, D&M | CPP can:
   a. Purge items marked for deletion,
   b. Transfer items marked for relocation to the appropriate approved storage location and
   c. Apply Purview sensitivity labels to documents so content analysis blocking and file-level encryption can be applied to those documents.

   It may also be necessary to adjust permissions and content sharing should any ‘gaps’ be identified as part of the remediation.

6. **Enable Content Analysis Blocking and Restricted SharePoint Search**. This establishes the scope of Copilot's access to data in alignment with organizational content management practices and data governance, both of which need to support the organization's legal and regulatory requirements.
7. **Complete a Copilot Data Readiness Review and certify the environment as Copilot Ready**. This step reviews the results of the remediation and configuration against the Copilot Data Readiness Baseline to ensure all privacy data has been properly addressed. Once confirmed, the environment is Copilot-ready.
8. **Proceed with Copilot adoption**. At this point, the organization has met the Phase One requirement in Microsoft's Copilot for Microsoft 365 Adoption Playbook of reviewing security and data settings. The organization is now in a position where it can proceed with the remainder of Phase One and subsequent phases of the Copilot adoption.

This workflow can be visualized as follows:



Privacy and industry legislation.
Data & More completes a comprehensive data discovery and baseline.
Data & More reports on the level of compliance and items that need to be addressed before implementing Copilot.
Data owners are engaged in a business-driven review of privacy data.
Privacy data minimalization
Privacy data consolidation
Purview sensitivity labels are applied to documents containing privacy data.
Sharing and document access is restricted to prevent inadvertent access by Copilot because of over-permissioning.
Sensitive documents are encrypted, restricting Copilot access.
Sensitive documents are retained and disposed of in accordance with corporate retention.
Purview reads the label and applies the protection / retention policies.
Data & More identifies items not protected by Purview.
Data & More proprietary mapping.
Data & More curated library of document classes and scan patterns.

The four key outcomes of this workflow are in the middle of the diagram:

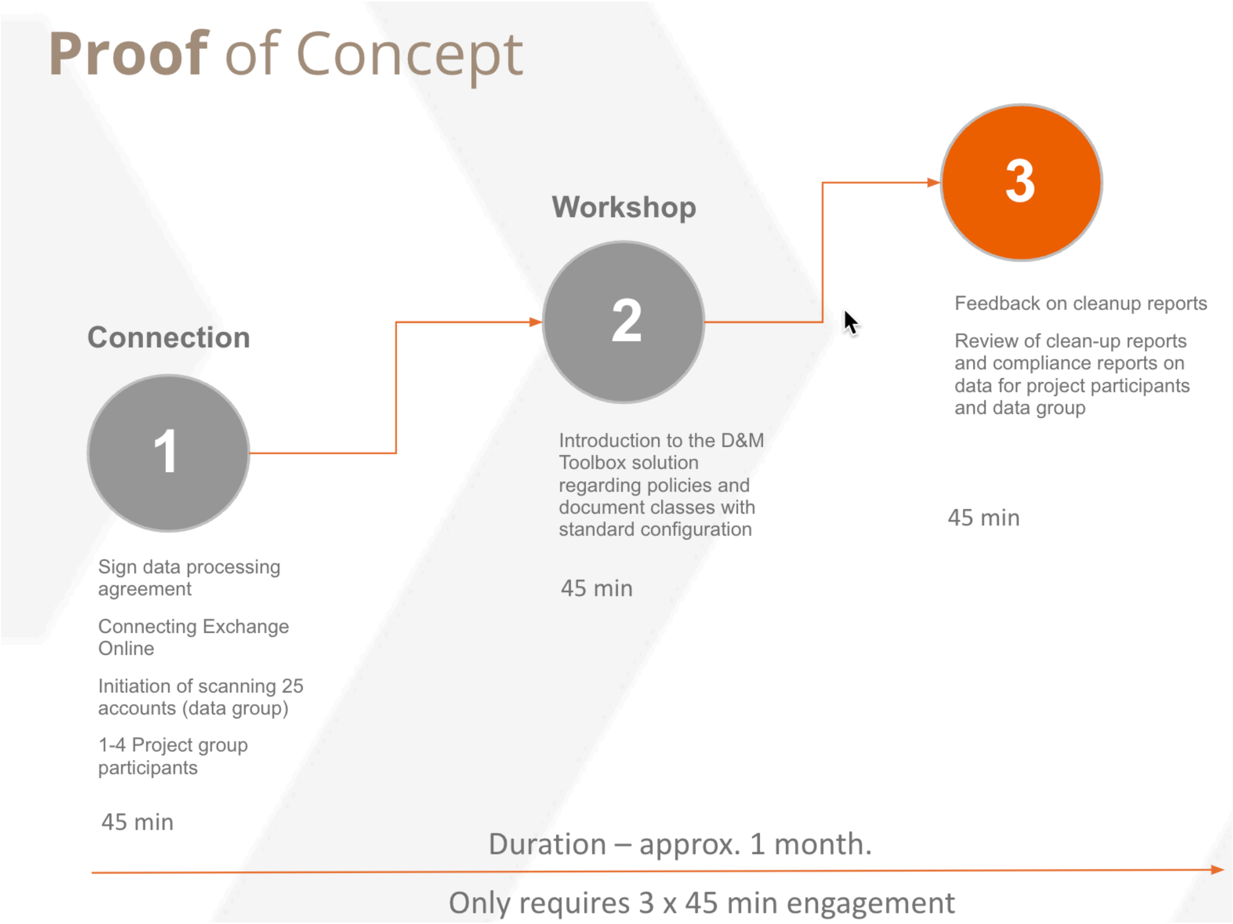
a. Privacy data minimization,
b. Privacy data consolidation,
c. Privacy data labeling and
d. Identifying privacy data not protected by Purview.

These items are facilitated, at scale, by Data & More Copilot Privacy Protection.

11 Get a Sponsered PoC

There is nothing like a hands-on evaluation of a white paper. If you want a demo of our software, you can try demo.dataandmore.com. It will give you five users out of the box.

If you send an email stating that you would like to evaluate Data & More, we will provide you with 20 more users to test and a free compliance workshop if your organization has more than 200 employees.



Proof of Concept

Connection

1

Sign data processing agreement

Connecting Exchange Online

Initiation of scanning 25 accounts (data group)

1-4 Project group participants

45 min

Workshop

2

Introduction to the D&M Toolbox solution regarding policies and document classes with standard configuration

45 min

3

Feedback on cleanup reports

Review of clean-up reports and compliance reports on data for project participants and data group

45 min

Duration – approx. 1 month.

Only requires 3 x 45 min engagement

w: dataandmore.com // m: support@dataandmore.com //

Denmark: *+45 4290 1070 - Flaesketorvet 68, 1711 Copenhagen V, Denmark*
Germany: *+49 151 59422362 - Am Steinebrück 29, 40589 Düsseldorf, Germany*
Canada: *+1.587.966.9070 - 500 - 4th Avenue SW, Calgary, Alberta, Canada*