Data & More | Key Features

Protecting digital privacy and minimizing the risk, cost, and liability of processing unstructured data

Table of Contents

Overview

Data & More | Privacy Platform supports the following core privacy compliance processes

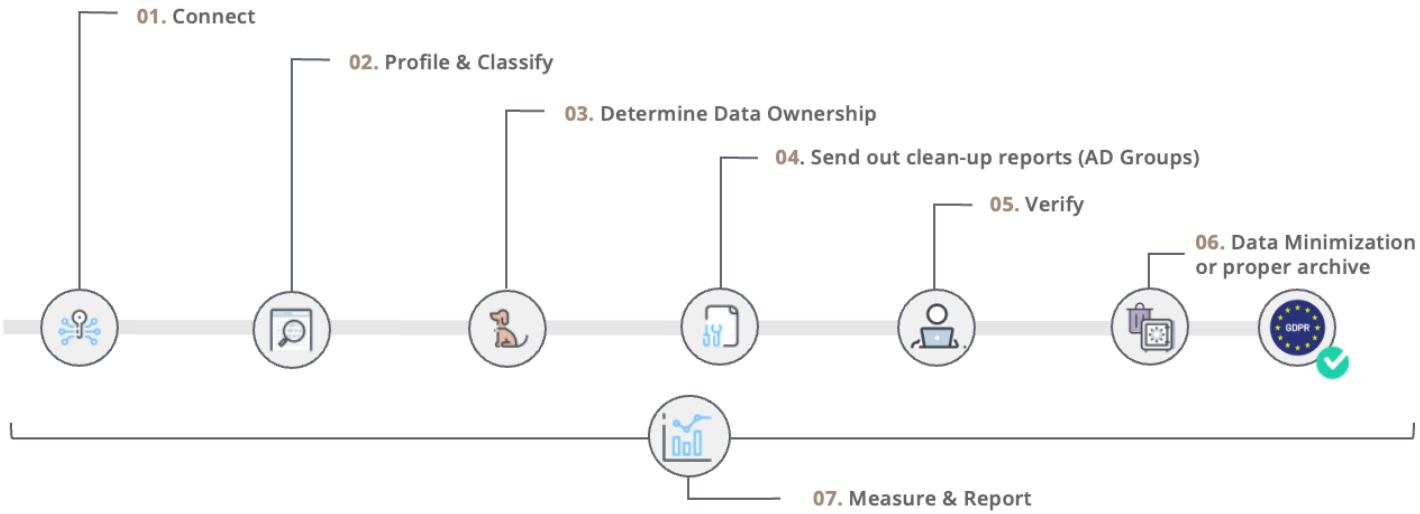
- Data Minimization (Deletions, Encrypting & Archiving),
- Data Subject Management (DSAR, RFI, Data Breach Mitigation)
- Microsoft Copilot Protection (AI Privacy Protection)
- Microsoft Purview Classification & Verification

Data & More | Privacy Platform key features that differ from all other Privacy GRC software:

1. We support the complete privacy lifecycle from data creation to data minimization
2. Our comprehensive Privacy Classification and Data Identification is **ready to use**. It is based on the local compliance regulations covering **28 languages.**
3. We identify both the **Data Subjects** and the **Privacy Data** in the source data
4. The solution can include the relevant employee (data owner) for final approval of their non-compliant data before the solution deletes the data.
5. We have more than **150.000 users** in more than **50 countries**
6. Our solution accuracy is tested every day and has a false positive ratio of less than 1%
7. The solution can be set up to handle both the regulatory data deletion policies and the organization's own deletion & retention policies
8. The most essential unstructured data sources are taken care of
9. Instant data search across all connected data sources, for e.g. request for insight
10. Automatical generated dashboards and reports with fact-based insights

Data & More provides comprehensive Infrastructure and Security capabilities, as outlined below, alongside its core process support features.

Automated Data Minimization



A successful data minimization process requires following the seven steps outlined in the diagram above. The Key Features section highlights how the D&M Privacy Platform facilitates each step.

1. Connect | Key features

Connect is the process of connecting unstructured data sources like mail, OneDrive, SharePoint, and file shares to the Data Privacy Platform.

1. High-Speed Data Connectors
   - Exchange Online & Exchange On-Premise
   - OneDrive & Teams Documents
   - SharePoint Online & SharePoint On-Premise
   - Filshare, NAS, Azure AWS, and other Storage types
2. Authentication via App registration Secret or Certificate
3. Graph, EWS, and SharePoint API Support
4. Scoping via AD Groups and select accounts or paths
5. Full encryptions of all data in transit
6. Massive parallel processing with up to 200.000 documents per hour (or more) for large enterprises with a fully scaleable set-up.

What makes D&M Connect features unique

D&M | Connect can best be described as SUPER Fast, Easy, and Secure to content, and it is unmatched by any other technology in the field.

2. Profile & Classify | Key Features

Profiling and classifications are the processes by which data is analyzed to find Data Subjects and Personal Information.

1. Automatic Identification of Data Subjects
2. Full Data Privacy Classification
3. Complete semantic analyses, not just RegEx and Libraries
4. Complete localization - including country-specific document classes, like local workers' unions, local religious orientations, local public certificates, local health information, and drug names
5. Custom classifications for unique organizational needs
6. Multilanguage support
7. Can differ between internal and external communication
8. Full AI-powered OCR for text and face recognition
9. AI power identification ID of ID Cards, Driver Licenses, and Passports
10. Identification of the number of people in pictures
11. Powerful multithreading allowing unlimited horizontal scaling
12. Integration with Microsoft Purview for Data Retention and Sensitivity labeling (optional)

What makes D&M Profiling & Classification features unique?

D&M's profiling and classification capabilities stand out with three unique advantages that set them apart from other tools in the industry. First, D&M is the only solution capable of automatically generating a comprehensive list of individuals whose data is contained within your data sources, often referred to as Data Subjects. Second, the extensive Data Privacy Classification system developed by the D&M language team is unmatched in scope and innovation, offering a level of precision that is unprecedented in the field. Finally, as an industry leader, D&M benefits from the feedback of over 150,000 users. This real-time feedback loop allows for immediate error detection and continuous refinement, ensuring the ongoing accuracy and reliability of our classifications.

3. Ownership / Custodian Mapping | Key Features

The solution automatically detects the data owner in most data sources and can address each data owner with their non-compliant data - but some data sources have no specific owner and must be handled in a specific way through establishing Data Ownership aka Custodian Mapping.

It is the process where rogue privacy data is assigned to a Data Owner. This process is essential for fileshares, SharePoint Sites, and Shared e-mails, as Data Owners can have left the organization or have never been mapped.

13. Identify rouge privacy data before Owners before assigning ownership - not assign owners to data with no privacy issues.
14. Assign ownership to Fileshares data via
    a. ACL,
    b. Folder naming conventions,
    c. D&M Custodian Mapping tool for file-share
15. Assign Ownership to ShareMailboxes via:
    a. Azure settings via "Manager" or "Other emails."
    b. D&M Custodian Mapping tool for Shared Mailboxes
16. Assign Ownership to SharePoint data via:
    a. Document Creator ID
    b. SharePoint Site Owners
17. Assign owners to Shared Mailboxes using bulk upload of CSV and individual settings.

What makes D&M Custodian Mapping features unique?
The D&M Custodian Mapping tools is a unique design to assign Data Owners to Privacy Data and is a Unique feature of the Data & More | Privacy Platform

4. Send-out & Notification

The Data & More Privacy Platform supports the notifications process by making it easy to schedule and send out notifications to the relevant Data Owners, Project Managers, and DPOs.

18. Email Notification can be sent via:
    a. Graph Authentication for email
    b. SMPT gateway
    c. Authenticated SMTP
    d. Postmark

19. All standouts are tracked and validated
20. Notifications can be resend with the original configuration
21. AD / SSO login to Verification Report
22. Microsoft Entry Login (AD)
23. Send out scheduling by fixed date or periods like X days or Y months
24. Exemptions from notifications can be managed centrally
25. Reporting groups can be managed via AD Groups, lists, or all users with PII data
26. Count down warnings for sending out

What makes D&M Send-out Notifications features unique?
The very flexible notification model for the privacy platform makes it easy for an Organization to use notifications within its security frame while maintaining **full control** of communications.

5. Privacy Data Verification Report

End-user verification is the process where data owners can review whether data should be minimized before the minimization is carried out. This process moves the responsibility for any irregular minimization from the IT department to the data owner.

27. Individual Verifications Reports of all Data Owners
28. Multilanguage support
29. Precise Classification of Personal Data
30. Filter option for fast deletion based on document
    - Classification (e.g. ID Card, Health Information, travel information)
    - Document Location
    - Document Age
    - Document creation data and last accessed
    - Filetypes
31. Multiselect for fast deletion
32. Custom tagging by ensure - like Archive or Move
33. Mark as Dispensation for data that should not be minimized due to actually
34. Mark as Private to exclude any of the Data Owners own Privacy Data
35. Mark Data as Misclassified, which helps us improve our Classification Precision
36. Fast preview of each identify document

What makes the D&M Privacy Data Verification Report features unique?
Usability—Usability—Usability. With over 150,000 users, the majority of whom have relatively modest computer skills, we have chosen **ease of use** as our number one design criterion. On average, we have less than one support case per 1000 users.

6. Data Minimization & Archiving

Data Minimization & Archiving is the process where the data is (finally) deleted, moved, or encrypted.

37. Delete data in all data repositories
38. Move data from one data source to another or within a data source
39. Archive data in the Compliance vault
40. Manual deletion via verification Report
41. Automatic deletion based on
    a. Document age
    b. Last access or edit
    c. Document Class or Type
    d. AD group scope
    e. Latest verification data
    f. Sensetivy label
    g. And a lot more...
42. Non-deletion / Exceptions based on
    a. All of the above
    b. Manual marking sources as | Private, Dispensations, Misclassified
    c. Location and time
    d. Folder name or path
    e. And a lot more...
43. Panic
    a. Automatically Move Data Back
    b. ~~Restore Deleted Data~~ | Sorry, we can't do that...
44. Audit trail
    a. Keep track of how the documents were deleted
        i. Manually, Automatically or InSouce
        ii. Where were the deleted documents located
        iii. Who owned the deleted documents
        iv. How was the deleted document classified

What makes the D&M Privacy Platform for Data Minimization & Archiving features unique?
It's not difficult to delete data... the trick is to delete the right data at the right time. The D&M Privacy Platform's unique ability to make it easy for end users to delete the **right** data can make the difference between compliance and catastrophe.

7. Measure & Report

The first part of compliance is to do the right thing. The second part is to document and report. The Data & More Privacy Dashboard is designed for **Auditors, DPOs, Project Managers, and Team Leaders**, each with their own unique needs.

45. **Total number of Data Subjects in the data**
46. Total number of monitored data sets and size
47. The total number of data sets analyzed
48. Total number of data sets with Privacy Data
49. Total number of non-compliance datasets, aggregated by
    1. AD group
    2. Data Owner
    3. Direct Manager
    4. Full Manager Hierarchy
    5. Data Policy
    6. Data Sources
    7. Data Location
    8. Data Age
    9. Creation date or period
    10. Data Type (msg, png, ext)
    11. Document Classification (Passport, Health information, etc.)
    12. Location
    13. User account
50. Upcoming non-compliant data
51. SQL synchronization of reporting data for PowerBI integration
52. Deleted data - aggregated by time, user, type, class
53. Notified data - aggregated by time, user, type, class
54. Data that used have been classified as Privat, Dispensation, or Misclassified
55. Custom reporting by any dimension you can model

What makes the D&M Privacy Platform Reporting features unique?
No other software can report on the actual Data Subjects in the data AND link it to the data Subjects' Personal data. Another unique feature decentralized - reporting by manager - that enables small teams to take responsibility for their compliance.

Infrastructure

Infrastructure… sooner or later, it matters. The Data & More Privacy Platform can be deployed anywhere as long as the servers are big and speak Ubuntu or Red-hat. The Data & More | Privacy Platform:

56. Can be installed On-Premise
57. Can be installed at a customer-designated cloud center
58. Can be delivered as SaaS - from individual secured designated servers
59. Can be configured to work with highly restricted security frameworks
60. Can scale horizontally and can analyze petabytes of data
61. Are extremely fast, with a current speed record of 200.000 documents / per hour. in a production environment

What makes the D&M Privacy Data Reporting features unique?
Nothing, really… besides the fact that the Platform does not have to run on expensive cloud infrastructure and that it does not rely on even more costly cloud services.

Security & transparency

Analyzing Privacy Data requires top-level security and transparency. The Data & More organisation and Privacy Platform suppers:

62. Natos requirement for logging
63. 256-bit encryption of all data in transit or at ease
64. Microsoft Entra Authentication
65. ISAE GDPR 3000 and ISAE 3403 Certification (ISO 2701 pending)
66. Open Code Review for Defence & Police Organisations
67. 24/7/365 surveillance for abnormal usage
68. And a lot more….

What makes the Data & More platform robust?
Data & More | Privacy Platforms are used by Defence, Police, and NIS2 Organizations and are widely considered the most secure platform for Data Discovery & Minimization.