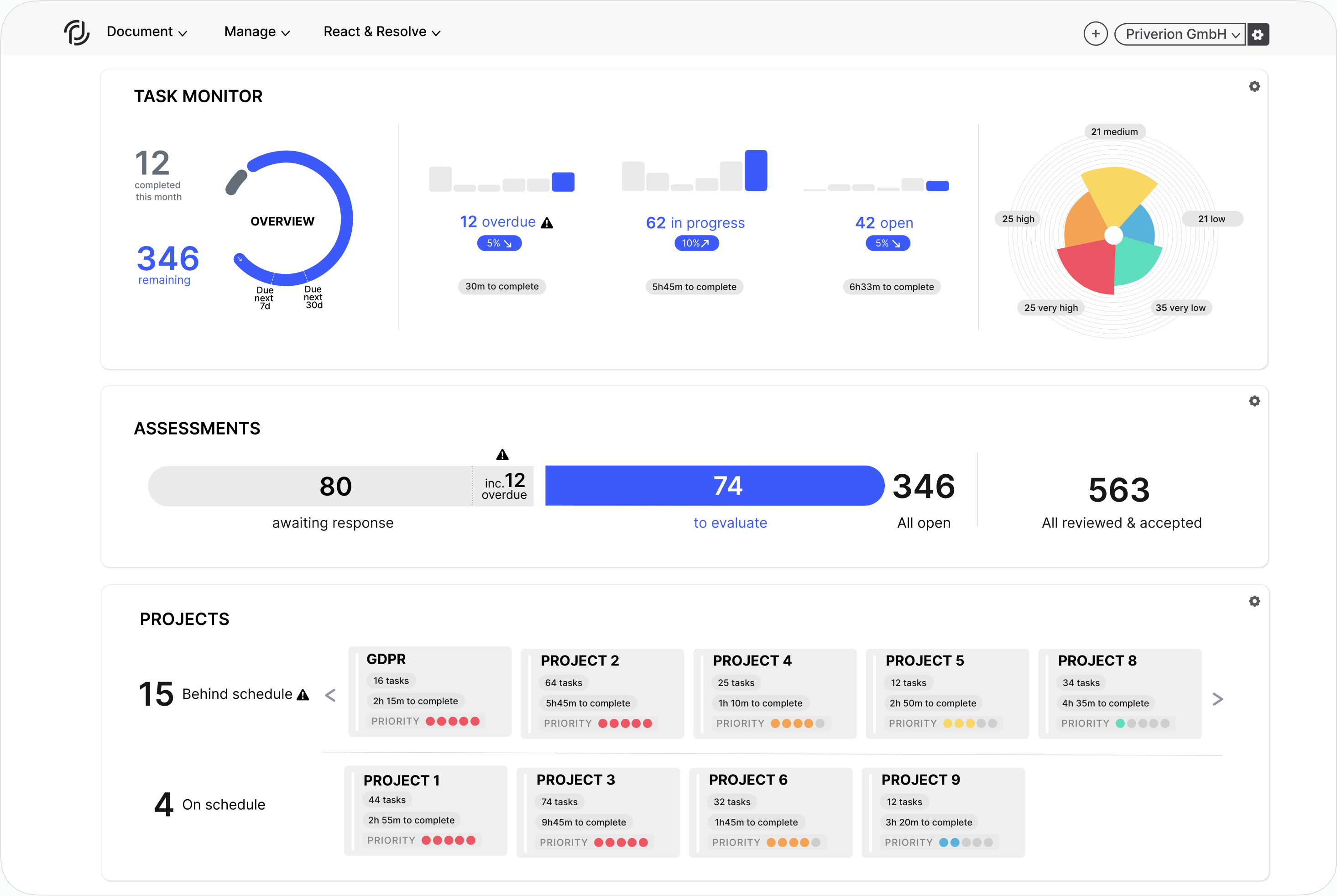
PRIVERION

One Platform.

SEPTEMBER 2023

One Platform.

Privacy and InfoSec covered.



TASK MONITOR

12 completed this month

346 remaining

OVERVIEW

Due next 7d

Due next 30d

12 overdue ⚠ 5% ↘ 30m to complete

62 in progress 10% ↗ 5h45m to complete

42 open 5% ↘ 6h33m to complete

21 medium

25 high

21 low

25 very high

35 very low

ASSESSMENTS

80 awaiting response

⚠ inc. 12 overdue

74 to evaluate

346 All open

563 All reviewed & accepted

PROJECTS

15 Behind schedule ⚠

GDPR
16 tasks
2h 15m to complete
PRIORITY ●●●●●

PROJECT 2
64 tasks
5h45m to complete
PRIORITY ●●●●●

PROJECT 4
25 tasks
1h 10m to complete
PRIORITY ●●●●●

PROJECT 5
12 tasks
2h 50m to complete
PRIORITY ●●●●●

PROJECT 8
34 tasks
4h 35m to complete
PRIORITY ●●●●●

4 On schedule

PROJECT 1
44 tasks
2h 55m to complete
PRIORITY ●●●●●

PROJECT 3
74 tasks
9h45m to complete
PRIORITY ●●●●●

PROJECT 6
32 tasks
1h45m to complete
PRIORITY ●●●●●

PROJECT 9
12 tasks
3h 20m to complete
PRIORITY ●●●●●

One logic. All angles covered.

Privacy.

Our privacy modules allow you to maintain all the necessary elements of privacy compliance.

InfoSec.

Our InfoSec modules empower and support InfoSec Officers in their daily tasks.

One logic. Three steps.

Document

One place to gather the documentation for your Privacy and InfoSec programs. From the Record of Processing Activities with a process based risk view to the Asset Register with an asset based risks view you are covered from all angles.

Manage

Manage your Privacy and InfoSec operations by triggering reviews and audits as well as creating risk reports based on standards or organizational units (such as departments).

React & Resolve

React to incidence, check notification requirements or simply create tasks and projects to keep your Privacy and InfoSec programs on track. Create corrective actions for standard related improvements.

Step 1. Document.

Privacy.

- Record of Processing Activities (ROPA)
- Data Protection Impact Assessments
- Reports & Downloads
- Legitimate Interests Documentation
- Retention & Deletion Periods
- Automated Decision Making and AI
- Technical & Organizational Measures (TOM)
- Assessments
- Vendors
- Policies
- Data Collection Points
- Privacy Center
- Meetings & Activities

InfoSec.

- International Standards
- Meetings & Activities
- Vendors
- Policies
- Reports & Downloads
- Automated Decision Making & AI
- Assets Register
- Technical & Organizational Measures (TOM)
- Assessments

Step 2. Manage.

Privacy.

InfoSec.

- Projects
- Vendor Risk
- Process Risk
- Privacy Audit

- Projects
- Vendor Risk
- Asset Risk
- Information Security Audit

Step 3. React & Resolve.

Privacy.

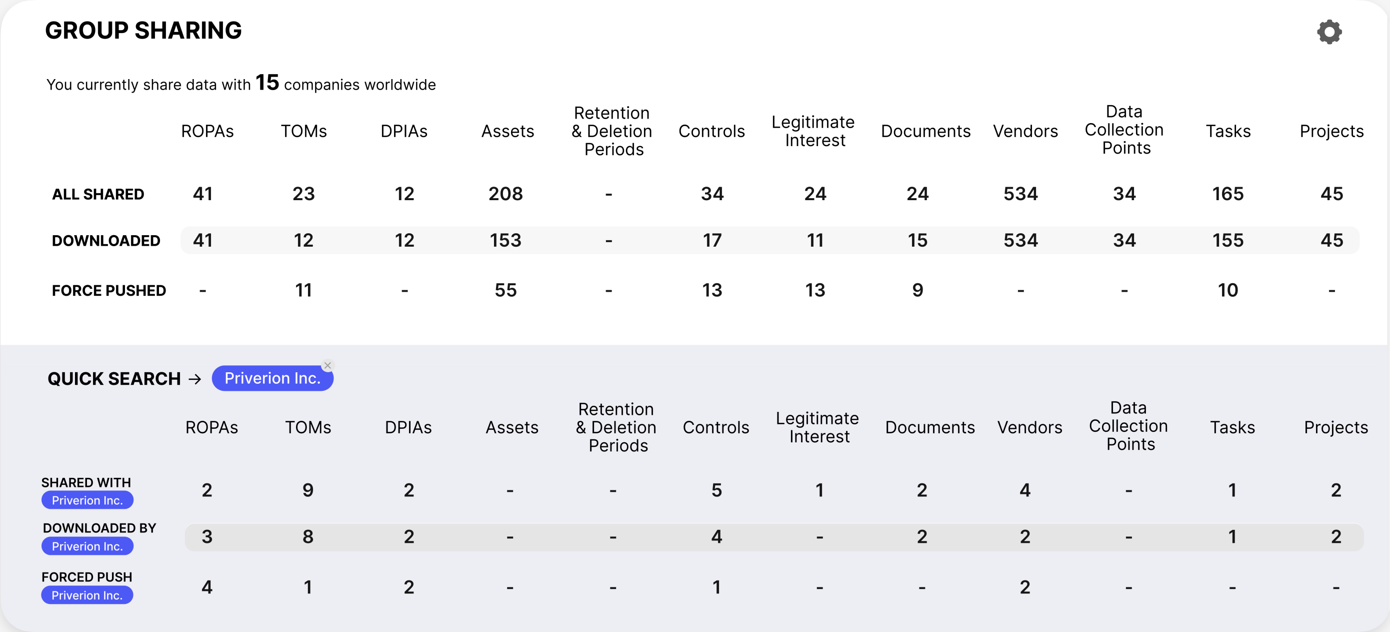
- Task Management
- Projects
- Incident Management
- Data Subject Requests

InfoSec.

- Task Management
- Projects
- Incident Management
- Corrective Actions & Immediate Measures

GROUP MANAGEMENT supports the standardization of privacy and Infosec topics.
Standardize your approach and gain insights into the maturity of your organizations within your corporate group.

Create **SHARED SERVICES** with one source of documentation.
Each organization can download shared services and use its documentation within their own organization. Customize the general documentation for your country specific needs.



GROUP SHARING

You currently share data with **15** companies worldwide

	ROPAs	TOMs	DPIAs	Assets	Retention & Deletion Periods	Controls	Legitimate Interest	Documents	Vendors	Data Collection Points	Tasks	Projects
ALL SHARED	41	23	12	208	-	34	24	24	534	34	165	45
DOWNLOADED	41	12	12	153	-	17	11	15	534	34	155	45
FORCE PUSHED	-	11	-	55	-	13	13	9	-	-	10	-

QUICK SEARCH → Priverion Inc.

	ROPAs	TOMs	DPIAs	Assets	Retention & Deletion Periods	Controls	Legitimate Interest	Documents	Vendors	Data Collection Points	Tasks	Projects
SHARED WITH Priverion Inc.	2	9	2	-	-	5	1	2	4	-	1	2
DOWNLOADED BY Priverion Inc.	3	8	2	-	-	4	-	2	2	-	1	2
FORCED PUSH Priverion Inc.	4	1	2	-	-	1	-	-	2	-	-	-

Highlights

Azure Active Directory

Connect your Azure Active Directory and immediately grant access to your employees, assign tasks and create momentum for your projects.

Servers in Switzerland or EU

We offer servers in Switzerland and as well as in Germany and other locations. From hyperscalers as well as local providers.

DPA Analyzer (Coming next)

Analyze a DPA within a minute and receive advice and recommendations on changes. Directly send your feedback to the vendor to enable fast implementation.

Privacy Center (Coming next)

One point of contact for all privacy and information security related information and requests.

Libraries

Retention & Deletion Periods Library

Load retention and deletion periods of over 150 countries. No more searching for deletion and retention periods in laws and regulations.

Vendor Library (Beta available)

No more manual creation of vendors. Load up to date vendor information from our database and get informed should changes in the vendor occur.

Policy Library (Coming next)

Need to implement a new Policy? Download templates and drafts from our library to get started fast.

ROPA Library (Coming next)

Most organizations have standard processes such as HR employee files and email systems. Download these processing activities into your system as templates from our library so you can focus on the more complex topics.

Module Index

● Privacy Modules

● InfoSec Modules

D Document (Step 1)

M Manage (Step 2)

R React & Resolve (Step 3)

D ● Automated Decision Making and AI

Automated decision making and artificial intelligence are becoming more and more important. Creating a sound documentation on these technologies and their effects on data subjects is paramount in complying with new regulations such as the AI Act.

D ● Assessments

Assessments are an important pillar of your privacy program. Assessments can be conducted internally on specific elements such as a ROPA or externally for example on vendors. Using our best practice templates or your own customized assessments we support the automatization of your yearly reviews.

D ● Automated Decision Making and AI

Keeping track of the information security measures for your automated decision making processes and artificial intelligence technologies allows your organization to pass external assessments. The more attention your AI technologies receive, the more stakeholders will seek documentation on its security and privacy compliance.

D ● Assessments

Assessing the maturity Level of your information security can be challenging. Using an assessment based approach to evaluate maturity levels supports you by automating most of the work for you. Automatically sending reminders and keeping track of deadlines enables a manageable InfoSec program.

D ● Asset Register

This register supports the information security officer and risk owners to determine the asset based risks. Using scenario based approaches and a damage and likelihood based approach the high risk assets can be identified. Easily create your risk mitigation plan on the basis of your asset risks.

M ● Asset Risk

Most international standards in information security take an asset based view on risk. Using risk scenarios the threat to your assets are identified. Afterwards based on your risk model, the likelihoods and damages of the risk scenario by assets are defined. Using technical and organizational measures these risks can then be continuously reduced.

R ● Corrective Actions & Immediate Measures

Mitigate identified risks in information security by creating corrective actions to reduce likelihood or damage of non-conformities. Document decisions taken by management on whether to carry out the proposed measures.

D

D ● Data Protection Impact Assessments

DPIA are necessary to evaluate the processing of specific data in a high risk context. These evaluations are necessary under many different laws, such as the GPDR or state law in the US. If you are planning to process sensitive or special categories of data you will likely need to conduct a DPIA.

D ● Data Collection Points

To comply with information requirements an organization must keep track of all interfaces from which personal data flows into the organization. These so called Data Collection Points are linked to Privacy Notices and automatically inform the responsible Person if a Privacy Notice is changed. This way you can be sure that your information requirements are fulfilled.

R ● Data Subject Requests

Manage your data subject requests and create cases, track progress and deadlines. Create one form for all requests and dynamically assign workflows depending on the applicable laws.

D

R ● Incident Management

Handling incidents according to country specific requirements is challenging. Using the Priverion incident management process allows you to cover all necessary information and notification obligations in one place. These steps are necessary under applicable laws, such as the GPDR or state law in the United States. If you are planning to process sensitive or special categories of data preparing for this process becomes even more crucial. Being prepared is the only way to handle incidents when they arise. We provide all necessary processes so you are ready when the case arises.

R ● Incident Management

Record, classify and mitigate incidents. From initial evaluation to reporting and notification requirements to data protection authorities or data subjects. The guided process supports information security officers and data protection officers in carrying out the required steps in accordance with best practices.

D ● International Standards

International Standards such as ISO27001, NIST or Cloud Security Standard are the basis for most InfoSec programs. Using the international standards module allows you to create all standard specific required elements such as the Statement of Applicability.

M ● InfoSec Audit

Depending on the applicable standards, regular information security audits are necessary. For example the internal audits according to ISO27001. Using the InfoSec audit module, standard specific or customized audits can be carried out in a fast and efficient manner.

D

Legitimate Interests Documentation

As an organization you might use your legitimate interests as basis to process personal data. For this it is essential to document the interests of the affected persons and balance these against your organizations interests. Using the Legitimate Interests module you can do this in a structured way and ensure that you have all required information.

L

D ● Meetings & Activities

Documenting meetings and any relevant activities is an important task in privacy compliance. As the burden of proof in most cases is on the organization, keeping a record of any privacy related activities will support your defense. The meetings & activities modules allows you to create the relevant records on the fly.

D ● Meetings & Activities

Documenting meetings and all relevant activities is an important task in privacy compliance. As the burden of proof in most cases is on the organization, keeping a record of all privacy related activities will support you in showing that appropriate controls are in place. The meetings & activities module allows you to create the relevant records on the fly.

M

D ● Policies

Version tracking and communicating your internal policies is important in implementing a efficient privacy management system. Using the policy module you can track new versions of documents and determine how well your organization is informed about each policy.

R ● Projects

Considering implementing a new CRM or starting to implement an international privacy standard? Create a project and break down the work into tasks. Conduct gap assessments before getting started, so you know what tasks have to be done and who will carry these out.

D ● Policies

IT Security Policies such as the BYOD Policy are important measures for Information Security. Using the Policy module the Information Security Officers can track the distribution of Policies within the organization, keep track of changes and update as required.

R ● Projects

Regularly occurring tasks can be bundled to reoccurring projects which re-create themselves each year. With this functionality you can put your internal reviews on autopilot.

P

M ● Privacy Audit

With our overview of all privacy topics, actions that Need to be taken and risks that have been assigned you are able to audit your current privacy state with the click of a button and identify areas in which further action is required.

D ● Privacy Center

The Privacy Center allows any organization to publish their Privacy and InfoSec information on one central page. This increases the sales cycles as customers can easily check compliance documentation. Additionally, data subject requests are directed through standardized best practice forms.

P

M ● Process Risk

The ROPA documents all processes within your company that use personal data. It aggregates all necessary legal information such as the purpose of processing as well as the legal basis for processing. Through intelligent linking to deletion and retention periods and your system landscape, you always know which deletion and retention periods apply to each system (on prem and in the cloud).

P

D ● Reports & Downloads

Create individual reports on the fly. Do you want to create a report with high risk vendors or open tasks? Using search and filter functionalities you can create your individual report to answer the specific question you might have. Standardized compliance reports supplement the individual reports.

D ● Reports & Downloads

Create individual reports on the fly. Do you want to create a report with high risk vendors or open tasks? Using search and filter functionalities you can create your individual report to provide you with a custom overview over the state of your data protection organisation. Standardized compliance reports supplement the individual reports.

D ● Register of Processing Activities (ROPA)

The ROPA contains a detailed documentation of all processes within your company that use personal data. It aggregates all necessary legal information such as the purpose of processing as well as the legal basis for processing. Through intelligent linking to deletion and retention periods and your system landscape, you always know which deletion and retention periods apply to each system and who is responsible.

R

D

● Retention & Deletion Periods

Keeping track of an organizations retention and deletion periods is an important task. By creating organization wide retention and deletion periods and applying these to your processes and assets, the operationalization for your IT admins becomes much easier.

R

D ● Technical and Organizational Measures

TOM are how your organization implements legal and regulatory requirements. Regular reviews and up to date documentation lets you keep track of the maturity and implementation level of your TOM. Using this information, reporting to the board is based on newest information and provides an up to date representation.

R ● Task Management

Create, manage and assign tasks in your organization. Track progress and automatically remind the users of deadlines. Determine workload of tasks to monitor the workload of your privacy program and to plan your resources accordingly.

D ● Technical and Organizational Measures

After evaluating the risks for an organization's assets TOM are implemented to reduce the identified risk. Linking TOM to risk scenarios and monitoring the implementation state on each assets makes sure that no gaps are missed.

R ● Task Management

Create, manage and assign information security tasks in your organization. Track progress and automatically remind the users of deadlines. Determine workload of tasks to monitor the workload of your Infosec program.

D ●

Vendors

Privacy risk in supply chains is becoming more and more important. Having insights into your vendors privacy posture as well as the hidden sub-processors helps your organization understand and monitor their risks and apply appropriate controls through Data Processing Agreements and assessments.

M ●

Vendor Risk

Each Vendor has their own specific risk profile. Using various different risk dimensions, the data protection or privacy officer can take a birds eye view on each vendor's privacy maturity. From regulatory to technical and organizational controls. Risk stems from a low maturity level of the necessary controls.

D ●

Vendors

Any data flowing in or out of your organization is a potential risk. Keeping track of the data flows and applying the right measures to your vendors is crucial for your information security. From your external law office to your external development partner. Every interface is important for your information security and should be regularly monitored.

M ●

Vendor Risk

Depending on the criticality of your vendor, the information security officers can decide on the level of maturity which is needed for a control. The vendor risk overview gives you a direct understanding of the vendor's information security posture.