



Revolutionizing Risk Management

Data Privacy & Tailored Risk

Your customizable Compliance and Risk Solution

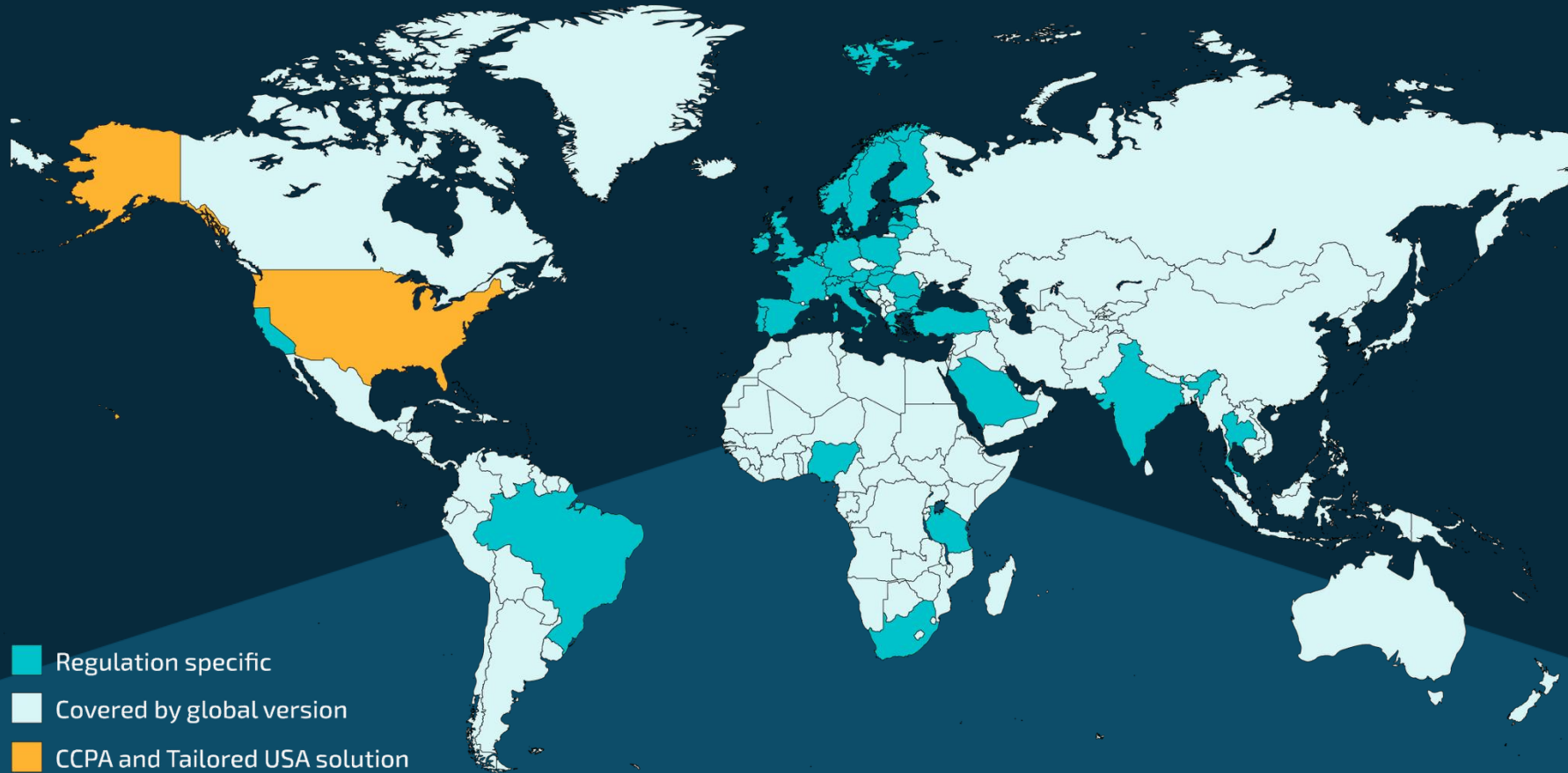
AI-Assisted / Human Verified

Contact us

Customers

Countries

Data Privacy Regulations



**Flexible, bespoke risk solutions, simple to deploy, offering exceptional value.
Data Privacy, GRC, HSSE, Operational, EIA, Cyber-Security.
The only limit is your imagination.**

Tell us your story

PrivIQ's Data Privacy Risk Management offers a globally trusted solution. With broad client appeal from SMB to enterprise. It is highly customizable to meet specific organizational requirements.

Explore Data Privacy



We get your headspace



Features -> Outcomes -> Feeling

Feature	Outcome (What it Delivers)	Feeling it Creates
Unified privacy governance & controls	Real-time visibility of gaps, clear owners, closed-loop follow-up	In control, nothing slipping
Data mapping & flow visualisation (ROPA, vendors, purposes)	End-to-end view of personal data; ROPA and Privacy Notices generated accurately	Clarity and confidence
Vendor & processor management	Structured due-diligence, contract tracking, ongoing compliance checks	Assurance your supply chain is safe
Policy & notice management	Consistent documents, quick updates, proof of communication	Credibility with stakeholders
Risk assessments (DPIA, TIA, LIA)	Prioritised risks with severity x likelihood scoring and clear mitigations	Decisiveness and safety
DSAR workflow & portal	On-time, well-documented responses with full audit trail	Calm compliance, responsiveness
Breach response & register	Fast triage, ready-to-use comms, lessons learned captured	Composed under pressure
Monitoring & alerts for standards adherence	Early detection of discrepancies; fewer surprises	Proactive peace of mind
Evidence & audit reporting	One-click packs; immutable records for regulators and clients	Audit-ready confidence
Stakeholder communications (staff & data principals)	Tracked acknowledgements and training; transparent engagement	Trust and accountability
Tailorability (controls, policies, assessments)	Fit-for-purpose framework that matches your reality	Ownership and alignment
Embedded scoring & mitigation planning	Current and projected post-mitigation risk, with tasks to close gaps	Progress you can feel and show

AI-Assisted / Human Verified



“Perfect support for a complex and high responsibility job”

Ensuring compliance with data Protection laws within organisations is challenging, complex and sometimes frightening when one considers the breadth of scope it demands. I suppose my favourite aspect of PrivIQ is how it simplifies the complexity by laying out very clearly all the items one has to go through, as a DPO, to go from compliance assessments to compliance sustenance including the facilitation of everyday responsibilities like managing DSARs or performing DPIAs.

Jose R. (EU)



“Easy to Use Robust Privacy Management Platform”

PrivIQ is an elegant, easy-to-use and robust solution that is well-suited to support organizations in the complex and ever-evolving US data privacy landscape. We needed a platform that could easily tailor and extend to include compliance requirements from various US states, US Federal Laws and regulations and accommodate information security framework as well.

Nalini K. (USA)



“I use PrivIQ as a privacy advisor to accelerate client success and simplify ongoing compliance”

PrivIQ is an excellent value that is unmatched in the current privacy software marketplace. Overly complex and overpriced tools prevent companies from advancing their compliance programs. PrivIQ is an excellent antidote. It's very easy to set up and start using right away without a lot of ongoing support. It's technology that actually makes things easier.

KARENS. (USA)



Read our reviews on



Leveraging ChatGPT 03Mini

Extensive content library with seamless integration into our solution.

Compliance Checklists & Risk Controls

Prompt based generation for any regulation or use case, editable and verifiable.

Policies & Documents

Generate tailored policy documents, communicate these to stakeholders for reading and acceptance.

Risk Assessments (RA)

Generate qualitative RA questions & Quantitative Threat Analyses with Severity and Likelihood Influencers.

Auto-creation of remediation tasks

Working with Pre-Mitigation and Post-Mitigation Risk scores for each threat to generate tasks required.

Demonstrate Compliance.

Data privacy management requires a comprehensive approach across HR, IT & Security, and Marketing. Our solution helps you navigate data privacy regulations, ensuring adherence to standards, mitigating risks, and enhancing transparency and accountability. Monitor and enforce data privacy standards effectively and respond promptly to discrepancies.

Our platform provides thorough data mapping, offering a clear overview of data flows within your organization enabling your ROPA and Privacy Notices and identifying vendors.

Governance is at the heart of our solution. Manage privacy notices, policies, and stakeholder communications seamlessly, maintaining robust data privacy practices.

Manage third-party vendors and processors with ease. Monitor and assess their data privacy practices to ensure compliance with your standards and regulatory requirements.

Conduct comprehensive risk assessments, including DPIA and TIA, among others. Identify and mitigate potential privacy risks, ensuring compliant data handling practices.

Handle Data Subject Access and data breach reporting efficiently. Streamline these processes to ensure timely and accurate responses to regulatory requirements.

A solution you can tailor to your requirements.



- Home
- Dashboard
- Reports
- Real Time Audit
- Compliance Audit**
- Data Mapping
- Compliance Monitor
- Governance
- Employee Comms
- Processor/Service Provider
- Controller/Third Party
- DPIA
- Subject Access
- Incident Response
- Consent Management
- Risk Assessments

Home

Real Time Audit
Real Time Audit

Compliance Audit
Assess, mitigate and review operational risk of your personal data processing practices

Data Mapping
Maintain the inventory of processing of personal data / information. Establish whose data you're collecting, why it's collected, the lawful bases, what data is collected and to whom it is disclosed.

Compliance Monitor
Monitor the progress of your personal data protection program

Governance
Publish a Record of Processing. Build integrated privacy notices. Establish a library of policies, procedures, and training & awareness material.

Employee Comms
Socialize privacy and security training material. Track employees' understanding, engagement and document reviews and acknowledgements.

Processor/Service Provider
Assess your Data Processor / Service Provider management practices. Document and manage personal data / information outsourced to Processors / Service Providers. Record signed contracts.

Controller/Third Party
Document and manage personal data / information shared with or disclosed to other Controllers. Record signed sharing agreements.

DPIA
Complete Data Protection / Privacy Impact Assessments for planned data processing activities that could result in risk to individuals.

Subject Access
Manage the life-cycle of data subject access requests.

Incident Response
Evaluate, monitor and record responses to security incidents.

Consent Management
Consent Management

Risk Assessments
Risk assessments

AI-Assisted / Human Verified

Real Time Audit

Our Real Time Audit module takes a detailed “point in time” snapshot of your entire privacy program, allowing you to create audits for any area of your organization and address findings immediately.

It examines all aspects of data privacy in depth, assigning Compliance Scores, Compliance Risk Scores, Impact Scores, and distinguishing between mitigated and unmitigated risk.

Upon completion, each audit is saved so you can compare it against past or future audits.

When viewing an audit it compares it’s scores with the prior audit and graphically shows improvements or downgrades.

This function provides a clear, data-driven picture of your organization’s improvements over time.

April 2024

Created by Russ Raizen, Date created 9 Dec 2024 17:05 GMT+2

Last calculated 9 Dec 2024 17:07 GMT+2

Recalculate 

Mark as complete 

Download Excel 

Risk Report 

Compliance Data Mapping Other  Notes  Files

Section	Compared to	Item count	Not Assigned	No Review Dates	Overdue Tasks	Not started	In progress	Complete	N/A	% NA	Compliance score	Compliance risk	Impact	Mitigated risk	Unmitigated risk
Data Controller / Data Controller Russ Raizen	Jan 2024	9	9	0	0	4	1	3	1	11	2.75	3.25	5	8.75	16.25
Data Processors / Service Providers / Data Processors / Service Providers Russ Raizen	Jan 2024	7	7	0	0	7	0	0	0	0	1	5	5	0	25
Data Protection Officer / Data Protection Officer Russ Raizen	Jan 2024	8	8	0	0	1	1	3	3	37	3.8	2.2	5	14	11
Data Sharing / Data Sharing Russ Raizen	Jan 2024	12	12	0	0	7	0	5	0	0	2.67	3.33	5	8.33	16.67
Data Subject Consent / Data Subject Consent Russ Raizen	Jan 2024	9	9	0	0	1	0	8	0	0	4.56	1.44	5	17.78	7.22
Direct Electronic Marketing & Profiling / Automated Decision Making and Profiling Russ Raizen	Jan 2024	11	11	0	0	1	2	8	0	0	4.27	1.73	5	16.36	8.64
Direct Electronic Marketing & Profiling / Existing customers Russ Raizen	Jan 2024	10	10	0	0	2	2	6	0	0	3.8	2.2	5	14	11
Direct Electronic Marketing & Profiling / Prospective customers Russ Raizen	Jan 2024	12	12	0	0	2	3	7	0	0	3.83	2.17	5	14.17	10.83
Employees / Employees Russ Raizen	Jan 2024	10	10	0	0	10	0	0	0	0	1	5	5	0	25
GDPD Demo RA / Data Privacy Breaches		0	0	0	0	0	0	0	0	0					
HR Practices / Employees' Health Information Russ Raizen	Jan 2024	5	5	0	0	1	1	3	0	0	3.8	2.2	5	14	11
HR Practices / Employment records Russ Raizen	Jan 2024	10	10	0	0	1	0	9	0	0	4.6	1.4	5	18	7
HR Practices / Monitoring at work Russ Raizen	Jan 2024	4	4	0	0	1	1	2	0	0	3.5	2.5	5	12.5	12.5
HR Practices / Recruitment Russ Raizen	Jan 2024	7	7	0	0	1	0	6	0	0	4.43	1.57	4.14	13.71	7
Information Use & Security / Information Quality Russ Raizen	Jan 2024	12	12	0	0	3	5	4	0	0	3.17	2.83	5	10.83	14.17
Information Use & Security / Retention and Restriction Russ Raizen	Jan 2024	9	9	0	0	1	2	6	0	0	4.11	1.89	5	15.56	9.44
Information Use & Security / Security Controls Russ Raizen	Jan 2024	20	20	0	0	3	4	12	1	5	3.95	2.05	5	14.74	10.26

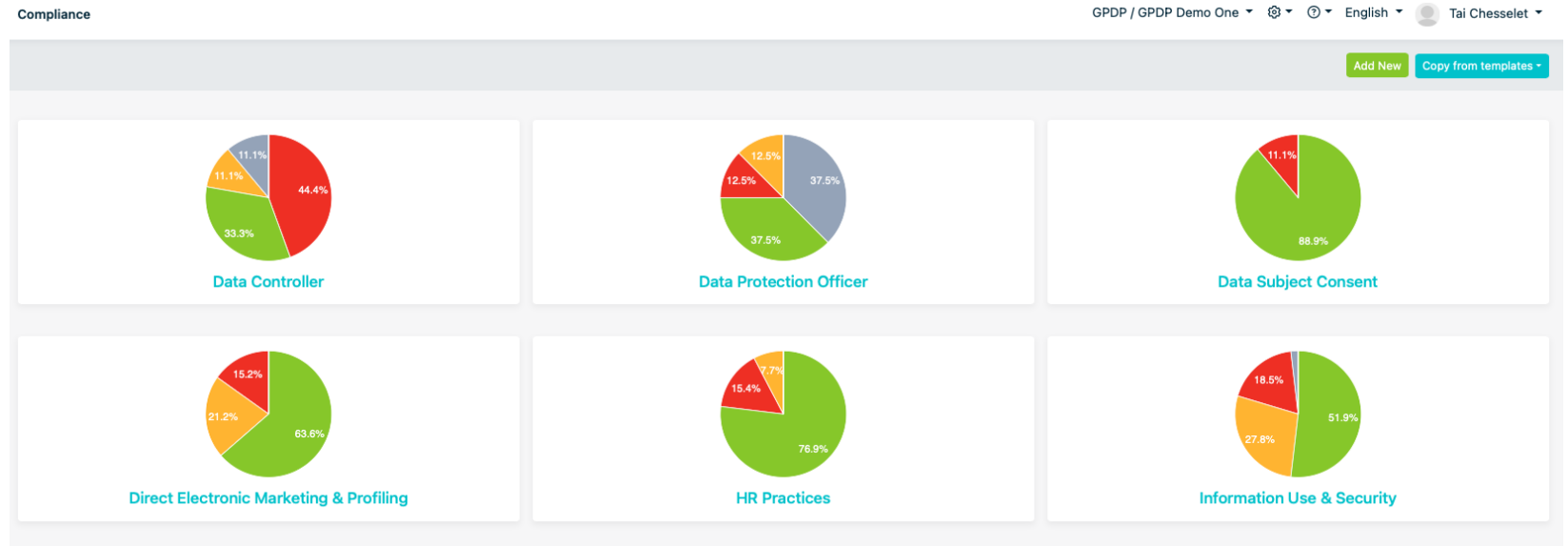
Operational HR, IT & Security and Marketing compliance.

Our Operational Compliance module simplifies data privacy compliance across HR, IT & Security, and Marketing. It provides comprehensive checklists tailored to each department's specific needs, ensuring that all areas of your organization meet regulatory requirements. By breaking down compliance tasks into manageable steps, our module helps departments maintain a clear focus on their responsibilities.

The module includes assignable tasks, enabling teams to collaborate effectively. Each task is clearly defined and can be assigned to specific team members, ensuring accountability and streamlined workflows. This collaborative approach fosters a culture of shared responsibility and ensures that compliance efforts are coordinated across departments.

Risk reports generated by our module offer insights into compliance status and highlight areas needing attention. These reports enable proactive risk management, allowing departments to address potential issues before they become critical. With our Operational Compliance module, your organization can achieve and maintain compliance efficiently and collaboratively.

Using AI you can tailor checklists to your specific needs and add entire sections with sub-sections to manage other regulation controls and criteria.



Compliance / Information Use & Security / Security Controls

GDPP / GPDP Demo One English Tai Chesselet

Person responsible: Russ Raizen

Security Controls

Checklist Background

Expand all Edit

We manage the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers

High Risk Add tag

We actively manage all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access

High Risk Add tag

Assign +

Notes

Jun 15, 2023 12:50 Russ Raizen - Status updated: Complete

+ Add note

Files

+ Add file

We actively manage all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution

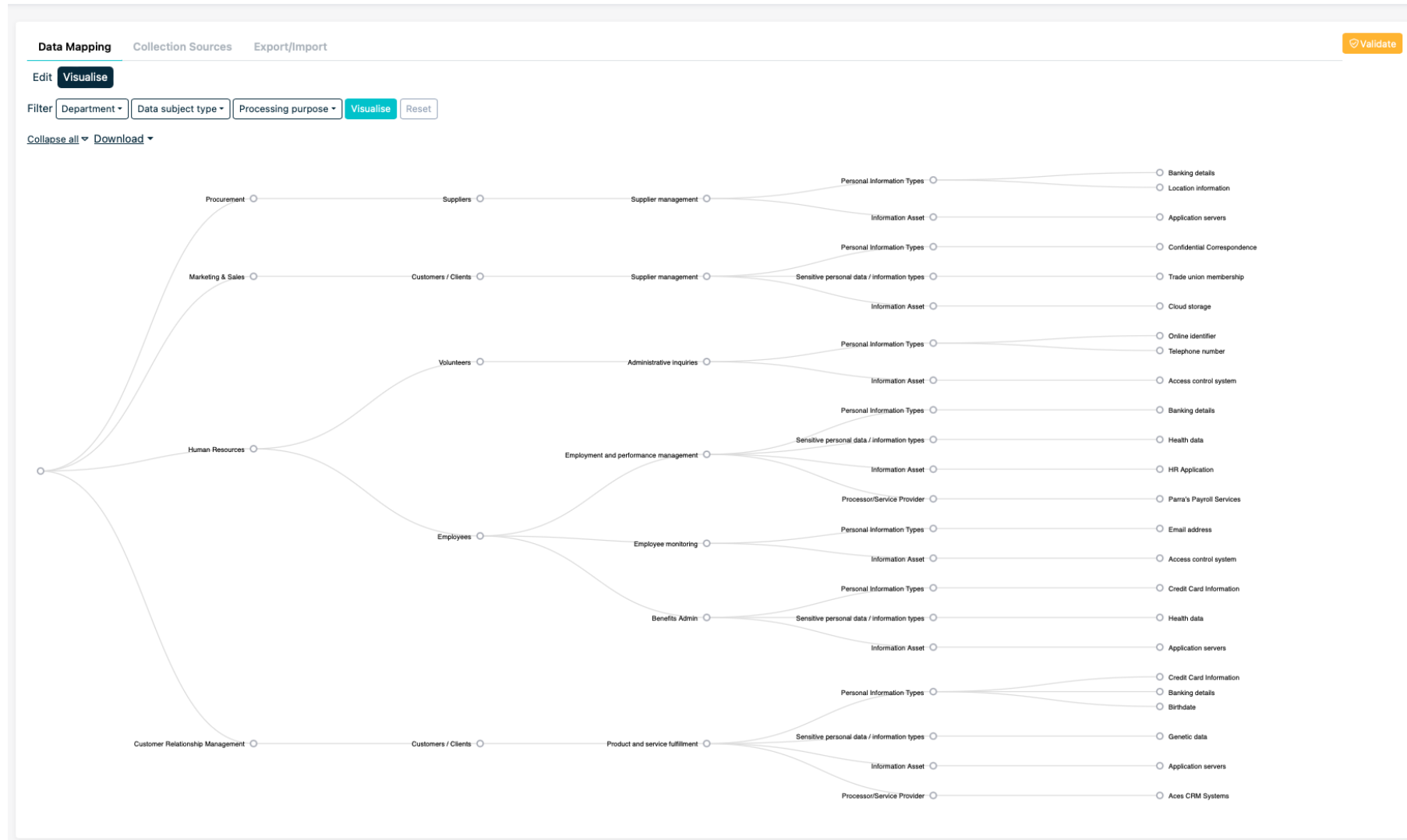
High Risk Add tag

AI-Assisted / Human Verified

Data Mapping.

Our Data Mapping module enables the visualizing data flows within your organization. It allows data mapping by department, processing purpose, and data subject types, giving you a detailed understanding of how data is handled across your operations. This granularity ensures that all aspects of data processing are transparent and easily manageable.

The module also facilitates the generation of essential documents such as Privacy Notices, Records of Processing Activities (ROPA), and vendor/processor contracts. Additionally, it provides critical information for conducting Data Protection Impact Assessments (DPIAs). By streamlining these processes, our Data Mapping module enables efficient compliance management and supports your organization in maintaining data privacy practices.



Compliance Monitor

Our Compliance Monitor module offers a comprehensive snapshot of your personal data protection program across key areas such as Organization Setup, Data Mapping, Governance, Stakeholders, Compliance, Data Processors, and Data Sharing.

It reports on the current status of each area so you can keep everything in one place.

You can download the data to PDF or Excel for building reports, assigning tasks, or integrating with project management tools.

This streamlined approach ensures everyone has an up-to-date view of your compliance progress.

Please select the items you wish to include in the report



Sections

- ☐ all
- ☐ Organization Features
- ☐ Organization Setup
- ☐ Data Mapping
- ☐ Governance
- ☐ Stakeholders
- ☒ Compliance
- ☐ Service Providers
- ☐ Data Sharing

Status

- ☐ all
 - ☐ Only incomplete
 - ☒ Complete
 - ☒ In progress
 - ☒ Not started
 - ☒ N/A
- ### Notes
- ☐ Show Notes

Compliance

- ☐ all
- ☒ Data Controller
- ☒ Data Protection Officer
- ☒ Data Subject Consent
- ☒ Direct Electronic Marketing & Profiling
- ☒ HR Practices
- ☒ Information Use & Security

Tasks

- ☐ Filter by review due date
- ☐ Show overdue reviews

Load report

Download 

GDPD Demo One - Compliance overview

Compliance status

Data Controller

44.44% complete

Not started 4 In progress 1 N/A 1 Complete 3

Data Controller

High Risk

1. We understand the definition of Data Controller.	Complete
2. Where required, we are appropriately registered with the relevant regulator.	Complete
3. We remain committed to working with the regulator on matters concerning complaints, breaches, investigations, or as may be required by the regulator.	Not started
4. Where required, we have appointed a representative and have informed the regulator of the representative's name and contact details.	Not started
5. We are committed to developing, implementing, monitoring, and maintaining the appropriate compliance framework. This includes designating a data protection officer, where required.	N/A
6. Our compliance framework is guided by the relevant data protection standards / principles / processing conditions that uphold the rights of data subjects.	Complete
7. We implement appropriate organizational and technical security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction, or disclosure of personal data / information.	Not started
8. We maintain relevant records as may be required by regulation.	In progress
9.	Not started

AI-Assisted / Human Verified

Governance

The Governance module enables you to publish and maintain a Record of Processing, build integrated Privacy Notices, and establish a comprehensive library of policies, procedures, and training materials.

With built-in AI assistance, you can generate and review these documents before distributing them to staff and contractors.

This organized approach provides a strong foundation for data protection across the organization.

Governance

DPDPA / DPDPA Company

Tai Chesselet

Please complete the tabs in the sequence in which they appear

Security MeasuresRecord of ProcessingPrivacy noticesInternalOptionalDocument Library

Privacy notices / Privacy Notice

Please note that the Privacy Notice depends on the Data Mapping being complete. Your Data Mapping has not been completed. Complete Data Mapping

Privacy NoticeIntegration

Use templateUse my own contentUse my own documentPublishHas never been published

Not startedIn progressN/ACompleted

English

Has not been published.

Has not been published.

Download

DPDPA Company - Privacy Notice

This Privacy Notice provides details of the personal data we collect and use, what we do with it, how we look after it, and who it might be shared with. It also provides information on the individuals' rights concerning their personal data and how they might access that information.

Our Organization

DPDPA Company
123 Privacy Way
Mumbai
12345
India
Mobile: +9112015550123
Telephone: +9112015550123
Organisation email: raizenrrr+sapopia@gmail.com

What we do with your personal data

We process personal data only for the purpose for which they are collected. The purpose is dependent on whether you use only our website, or additionally, our services. If you use our services, you are required to register, and we collect your personal data. We use this personal data for the provision of the service or the performance of the contract. We may use your personal data for other similar purposes, including marketing and communications, but that will only occur in the case we have your consent or another legal justification for doing so.

From our Customers / Clients we collect, use and retain personal data for the following purposes and periods, with the applicable lawful basis..

upload your own. Only documents that are marked as Complete will be available for distribution to employees. Documents that should not be shared must be marked as N/A.

GDPP / GPP Demo One

English

Tai Chesselet

policies, standards and rules around information protection. Here, you may choose to use the existing templates or

Privacy Program AnnouncementComplete

Privacy PolicyComplete

CCTV PolicyN/A

Data Protection Training & AwarenessComplete

Best Practices for Protecting Personal DataComplete

Transborder Information FlowsNot started

Working from Home PolicyComplete

Personal Data Breach PolicyIn progress

Data Subject Access Requests PolicyIn progress

AI-Assisted / Human Verified

Employee Communications

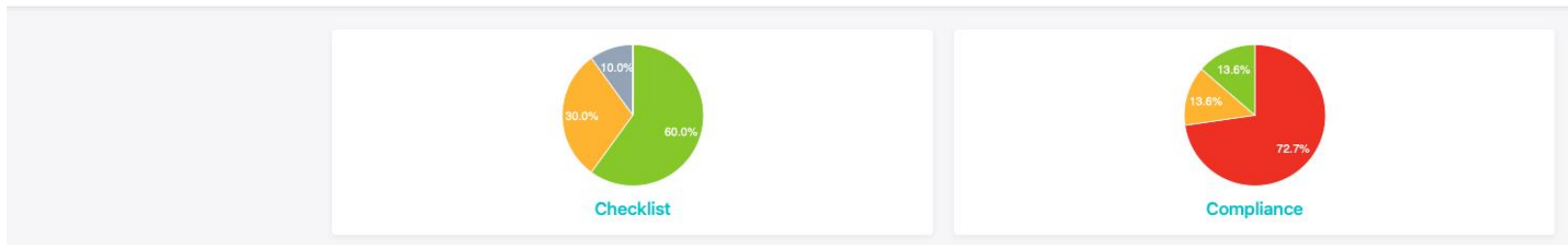
The Employee Communications module provides a dedicated utility for managing staff communications.

You can add employees one by one, use bulk uploads with a provided template, or integrate with Microsoft Active Directory.

Once their details are in place, you can selectively send policies and documents, along with a link for each employee to complete assigned tasks.

The system tracks whether employees have read and acknowledged the content, helping you monitor understanding and engagement.

Customizable controls ensure that all communications meet compliance standards.



Department	Location	Status							
search									
2 results found									
First name	Last name	Job title	Email address	Department	Location	Is active			
April	Showers	CEO	raizenrrrr@gmail.com			✓	Send email	In progress	
Robin	Woods	DPO	raizenrrrr-sapopia@gmail.com			✓	Send email	In progress	

Send compliance emails

Please note, before sending. You may only select documents from the Governance section that have been set as 'Complete'. Documents set to N/A will not be displayed here.

Send to

☐ All employees

☒ To employees where the current status is 'Not started'

☐ To employees where the current status is 'In progress'

☐ To employees where the current status is 'Complete'

Department Location

Documents to send

Governance Governance

Document Library Document Library

Customise your email

Language English

Subject Compliance training and awareness

Message

The following is important information from our data protection program. Please click on the link/s in this email to take you to the relevant document. When you have completed the task, click on the button which says 'I have read and accept this document'.

Send emails Cancel




Data Processors

The Data Processors module helps you assess and document how your organization manages external data processors.

You can track personal data that has been outsourced, record signed contracts, and review compliance practices against a defined set of controls.

This ensures your organization handles Data Processor relationships in a consistent and compliant manner.

Data Processors/Service Providers / Processor/Service Provider Contracts

GPDP / GPDP Demo One   English  Tai Chesselet

search




Copy Processor/Service Provider from Template Add New

3 results found

Processor/Service Provider	Service type	Country	Renewal date	Lawful basis	Contract Status	Contract
Aces CRM Systems	CRM System	Ireland		To conclude or perform a contract with a data controller in the interest of the data subject	<div><div></div><div></div><div></div></div>	GPDP Sharing Guide <div><div></div><div></div></div> <div>Signed contract</div> <div><div>↑</div>Upload</div>
Amazon Web Services	Hosting	United States			<div><div></div><div></div><div></div></div>	GPDP Sharing Guide <div><div></div><div></div></div> <div>Signed contract</div> <div><div>↑</div>Upload</div>
Parra's Payroll Services	Payroll processor	United States			<div><div></div><div></div><div></div></div>	GPDP Sharing Guide <div><div></div><div></div></div> <div>Signed contract</div> <div><div>↑</div>Upload</div>

Items per page 50

Data Processors/Service Providers / Processor/Service Provider Contracts / Aces CRM Systems

GPDP / GPDP Demo One   English  Tai Chesselet

DetailsData MappingNotes and files

Name

Aces CRM Systems


Processor/Service Provider type

CRM System


Website

Email address

Telephone number

 (201) 555-0123

Mobile number

 (201) 555-0123

Address

Postal address

City

Postal code

Country

Ireland

Lawful basis ⓘ

To conclude or perform a contract with a data controller in the interest of the data subject

Description of service

Bots Processor

Contract start date

Contract end date

Contract renewal period

monthly, annually..

Frequency of processing

hourly, monthly, annually..

Estimated # of records

Methods of transmission

Save

Cancel

Data Subject Access

The Data Subject Access module manages the entire lifecycle of data access or grievance requests through a structured workflow that updates status at each step.

You can set up an online link to make it easy for individuals to submit their requests and embed forms wherever needed—such as on your website or intranet—to ensure a smooth intake process.

This centralized approach helps track and resolve each request efficiently while maintaining compliance with data privacy requirements.

Requests

Settings

Integration

Customisation

Request response guide

GPDPNU0000015417, Naomi Chesselet, Created 17 Feb 2025, Due 19 Mar 2025

Process

Details

Notes

Files

Data Mapping

What is the nature of your request?

Access / Copies

Objection

Correction ☒

Deletion

I would like to make corrections to or delete portions of my personal data / information in your possession or under your control. (Please specify below, details of the personal data / information that must be corrected or deleted as well as the reasons why you are making this request) *

aaa

Received date

2025-02-17

Particulars of the person making the request

First name *

Naomi

Last name *

Chesselet

Email address *

raizenrrr@gmail.com

Unique identifier/identity number

Postal address

PO Box

Telephone number

12015550123

Fax number

Person's relationship with our organization *

Customers / Clients

Are you applying on behalf of another person? *

☒ No ☐ Yes

How would you prefer our response and any information to be presented to you? *

Via email

Close

Breach Response

Use the Breach Response module to evaluate, monitor, and record responses to security incidents.

It also assists in preparing communications for both the Board and any affected individuals, ensuring all stakeholders are informed promptly.

Once the incident details are compiled, you can download a comprehensive report as a PDF for a clear audit trail and compliance record.

Breach

GDPP / GDPP Demo OneEnglishTai Chesselet

search

Add New

Name	Date	Investigator	Status	Documents
GDPP Contained Incident	15 Jun 23 09:19 CAT		<div><div></div><div></div><div></div></div>	Incident Download
GDPP Reported Breach	06 Jun 23 09:11 MDT	aa	<div><div></div><div></div><div></div></div>	Comms content for the relevant authority Download Subject notification Download Incident Download

Items per page50

Breach / GDPP Reported Breach

GDPP / GDPP Demo OneEnglishTai Chesselet

1

2

3

4

5

6

7

8

9

Risk Assessment

Not all breaches will lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be equipment failure where files were backed up and can be recovered, albeit at some cost to the organization. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, which may be used to commit identity fraud. Most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

What type of data is involved?

Contact details

Approximate number of records involved

111

Which types of data subjects are affected?

aa

How many data subjects are impacted?

111

The incident has been contained and it is unlikely to impact data subjects

What measures are in place to contain the incident?

The incident happened

Internally

The location has been secured from tampering

Are you able to prevent further loss / continuation of the incident?

What are the likely causes of this incident?

cause.generic.name.1

cause.generic.name.6

☒ cause.generic.name.3

cause.generic.name.4

cause.generic.name.2

cause.generic.name.9

cause.generic.name.5

cause.generic.name.0

cause.generic.name.8

cause.generic.name.7

Cancel

Previous

Next

Notes and files

Notes

+ Add note

Files

+ Add file

Consent Management

The Consent Management module provides a comprehensive workflow enabling you to create, preview, and manage opt-in or opt-out forms.

You can integrate these forms into your websites, emails, or apps, and attach custom notices that clarify how data is collected and used.

The module then synchronizes consent responses with your chosen system, making it straightforward to track, verify, and update user permissions as needed.

Additionally, **immutable, time-based consent records** are maintained to ensure each user's consent status is securely logged and cannot be altered.

This structured ensures a clear audit trail of user consent activities.

Consent Management

Responsible Person Russ Raizen

At its most basic level, a person can either agree to a particular arrangement (OPT-IN) or request that a particular arrangement be cancelled (OPT-OUT). Some laws, such as California's CCPA, will be specific in naming the arrangement e.g., 'Do Not Sell or Share My Personal Information' but essentially, it's an OPT-OUT request.

In 'Consent Setup' you can create these consent types, preview them to confirm the expected results, and integrate the links with your websites or emails. Responses to the consent types can be viewed under 'Consent Queries', downloaded in JSON or CSV format to be incorporated into your relevant programs or campaigns.

Consent Setup

Consent Dashboard

Consent Queries

search

Add New

7 results found

Consent Item	Date Added	Last edited by	Consent Type				
Campaign One	21 Jun 2023	Russ	GENERIC-OPT-OUT	Preview	Code Snippet	Edit	Delete
Campaign Two	21 Jun 2023	Russ	GENERIC-OPT-OUT	Preview	Code Snippet	Edit	Delete
CCPA-Limit Use	15 Jun 2023	Tai	CCPA-Limit the Use of My Sensitive Personal Information	Preview	Code Snippet	Edit	Delete
GDPD Generic Opt In	15 Jun 2023	Russ	GENERIC-OPT-IN	Preview	Code Snippet	Edit	Delete
Generic Do Not Sell	15 Jun 2023	Russ	GENERIC-Do Not Sell or Share My Personal Information	Preview	Code Snippet	Edit	Delete
GDPD Opt Out	6 Jun 2023	Russ	GENERIC-OPT-OUT	Preview	Code Snippet	Edit	Delete
Medical Consent	16 Jun 2023	Russ	GENERIC-OPT-IN	Preview	Code Snippet	Edit	Delete

Items per page

50

Data Privacy Risk Assessments.

Our Data Privacy Risk Assessment module ensures compliance with requirements like DPIA and TIA. In addition it allows you to assess and monitor the data privacy practices of third-party vendors and processors, ensuring they meet regulatory standards.

Beyond statutory assessments, our module includes AI use risk management. As AI adoption grows, it’s vital to mitigate privacy risks associated with AI technologies. Our risk assessments allow you to evaluate these risks, ensuring responsible AI use and regulatory compliance.

A standout feature is the flexibility of our AI-assisted, human-verified technology, allowing you to create custom risk assessments. This combination of AI efficiency and human insight ensures comprehensive and accurate risk assessments, tailored to your specific needs. Stay ahead of potential threats and maintain clear data privacy practices with our versatile module.

AssessmentsRisk registersMy templatesSystem templates

Tai test

DetailsRequest for Risk AssessmentCaptureThreat AnalysisReviewApproval

Organizational Roles and Responsibilities

Has a Privacy Officer been appointed to oversee HIPAA privacy compliance?

Please provide the name and contact information of the appointed Privacy Officer.

Are staff roles and responsibilities regarding PHI clearly defined and documented?

Policies and Procedures

Does the organization have written policies and procedures that comply v

When were the HIPAA privacy policies and procedures last reviewed or u

Are there procedures in place for handling patient requests for access to

Do you have a process for documenting policy changes and communicati

PHI Flow Mapping

Has the organization mapped the flow of PHI internally and externally?

List all departments that handle PHI within the organization.

Identify all external entities with whom PHI is shared.

Are Business Associate Agreements (BAAs) in place with all external entit

Failure to Conduct HIPAA Privacy Risk Assessment

Risk categories

Compliance, Legal, Financial, Reputational

Monetary risk

5000000

Cost of Control

100000

Pre-Mitigation Threat Scoring

Post-Mitigation Threat Scoring

Severity influencer

Severity level

Degree of non-compliance with HIPAA Privacy Rule

Potential fines and penalties imposed

Impact on organization's reputation due to regulatory violations

Extent of PHI handled by the organization

Likelihood influencer

Likelihood level

Lack of awareness of HIPAA privacy requirements

Absence of an appointed Privacy Officer

Complexity of organizational workflows

Frequency of changes in operations without assessment

Risk

Formula

13 / 25

((5 + 4 + 3 + 4) / 4) * ((3 + 3 + 4 + 3) / 4)

Pre-Mitigation Risk

Post-Mitigation Risk

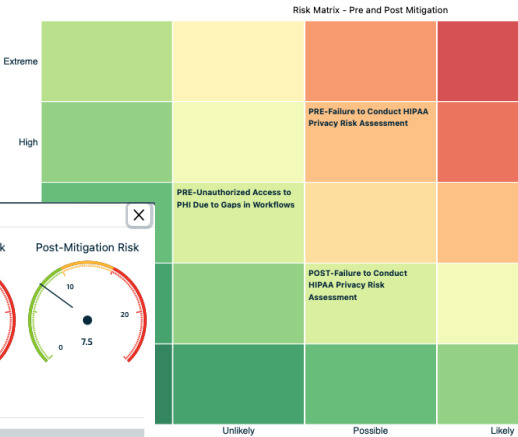
01020

13

01020

7.5

Name	Monetary risk	Cost of Control	Pre-mitigation severity	Pre-Mitigation likelihood	Pre-Mitigation Risk	Pre-Mitigation risk exposure	Pre-Mitigation monetary risk	Post-mitigation severity	Post-Mitigation likelihood
Failure to Conduct HIPAA Privacy Risk Assessment	5,000,000	100,000	4	3.25	13	52%	2,600,000	2.5	3
Unauthorized Access to PHI Due to Gaps in Workflows	0	0	3.5	2.75	9.63	38.52%	0		
Total	5,000,000	100,000	3.75	3	11.32	45%	2,250,000	2.5	3



Detailed risk description. Define the event.

The organization faces the risk of failing to conduct a HIPAA Privacy Risk Assessment, which encompasses Compliance, Legal, Financial, and Reputational categories. This failure can lead to significant negative outcomes.

Severity: Extreme (5)

The potential severity of this risk is rated as Extreme (5) due to:

- Degree of non-compliance with HIPAA Privacy Rule: Extreme (5) – Represents substantial violations that could result in severe legal consequences.
- Potential fines and penalties imposed: High (4) – Indicates substantial financial losses from regulatory penalties.
- Impact on organization's reputation due to regulatory violations: Medium (3) – Could lead to loss of trust among patients and partners.
- Extent of PHI handled by the organization: High (4) – A larger amount of Protected Health Information increases the potential impact of non-compliance.

Likelihood: Likely (4)



Industries we serve

- Banking & Finance
- IT & Security / Internet
- Telecoms
- Government
- Accounting
- Healthcare/Medical/Pharmaceutical
- Insurance
- Mining
- Manufacturing
- Chemical
- Testing, inspection and certification Services



500+

Customers

36+

Countries

12

Data Privacy Regulations



Reasons to find out more

- Global Data Privacy & Tailored Risk SAAS
- AI-Integrated for a tailored, flexible and scalable solution
- Broad Client Appeal (SMB to Enterprise)
- Clients can build bespoke Risk solutions
- Multi-lingual & Multi Regulation
- Price / Performance

Next Actions

- On a scale of 1-10 how interested are you in a deep dive in our solution?
- What are your timescales / contract periods?
- Who are the decision makers?
- Can we schedule a deep dive meeting?



Thank you

Contact us