privIQ

PrivIQ Product Overview

2021

Intelligent Compliance, Simply

Gartner

"By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today."

"By 2023, companies that earn and maintain digital trust with customers will see 30% more digital commerce profits than their competitors."

"By 2024, more than 80% of organizations worldwide will face modern privacy and data protection requirements."

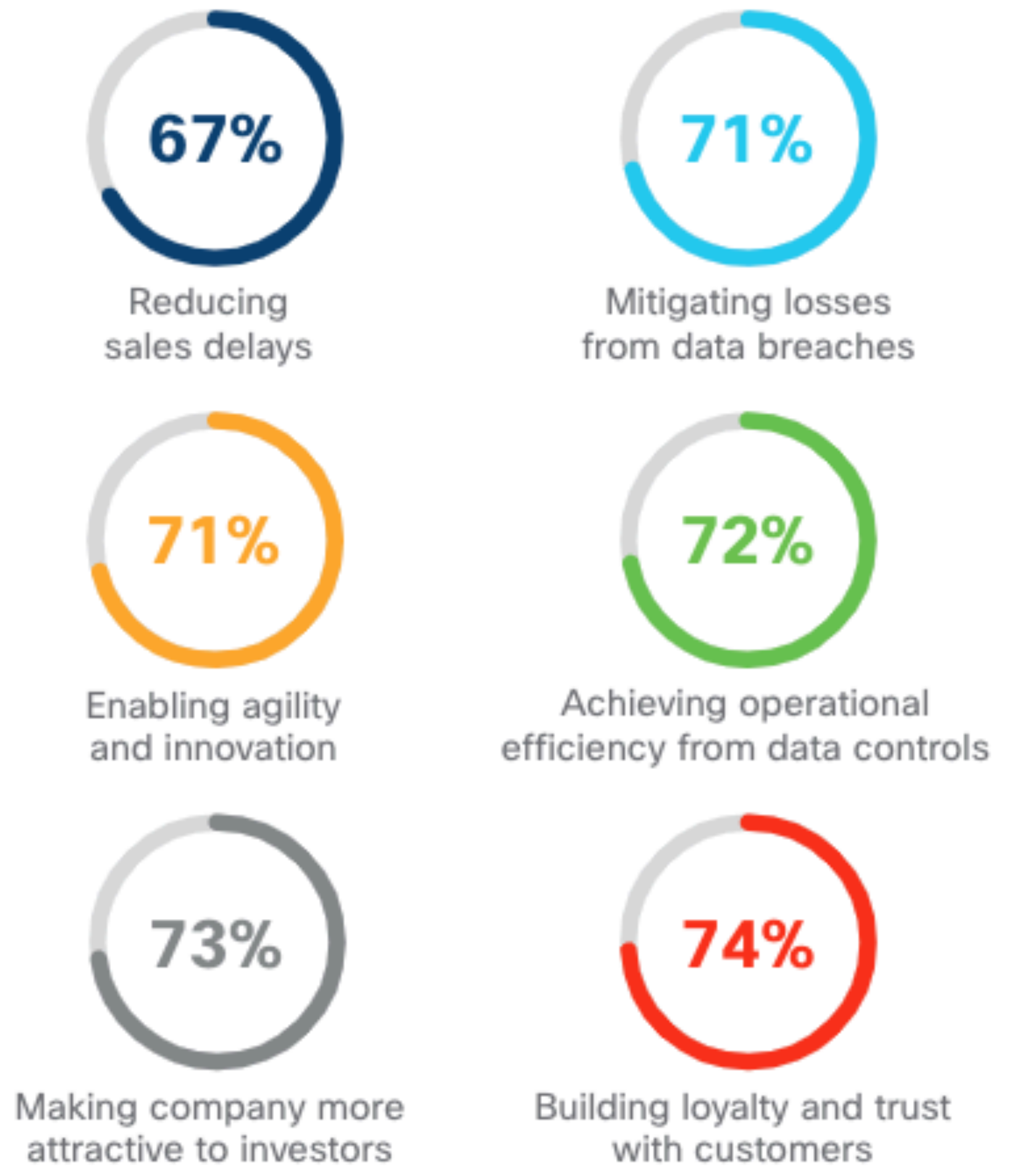
From Privacy to Profit

Achieving positive returns on privacy investments

“Most organizations are seeing very positive returns on their privacy investments, and more than 40% are seeing benefits at least twice that of their privacy spend.”

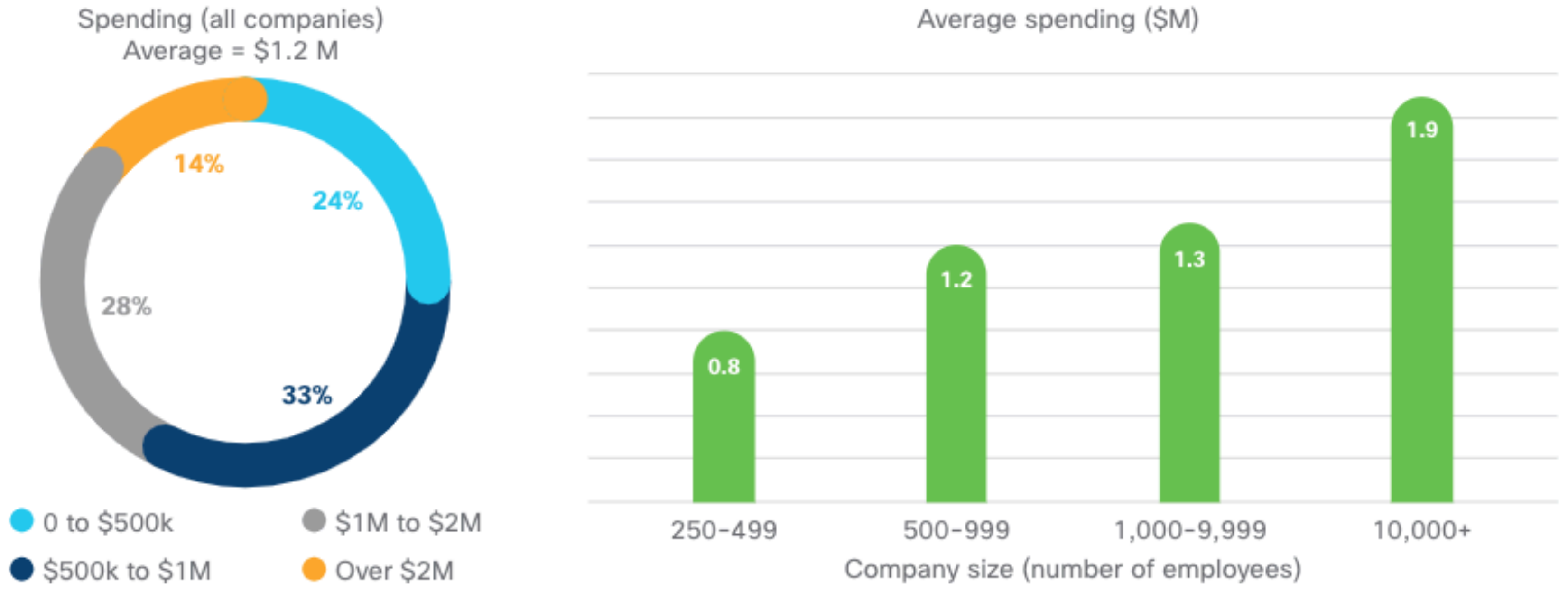
*Cisco Data Privacy Benchmark Study 2020

Business impact of privacy
Percentage of companies getting significant benefits in each area, N=2549



Source: Cisco 2020 Data Privacy Benchmark Study

Annual privacy spending overall and by company size
N=2549



Source: Cisco 2020 Data Privacy Benchmark Study

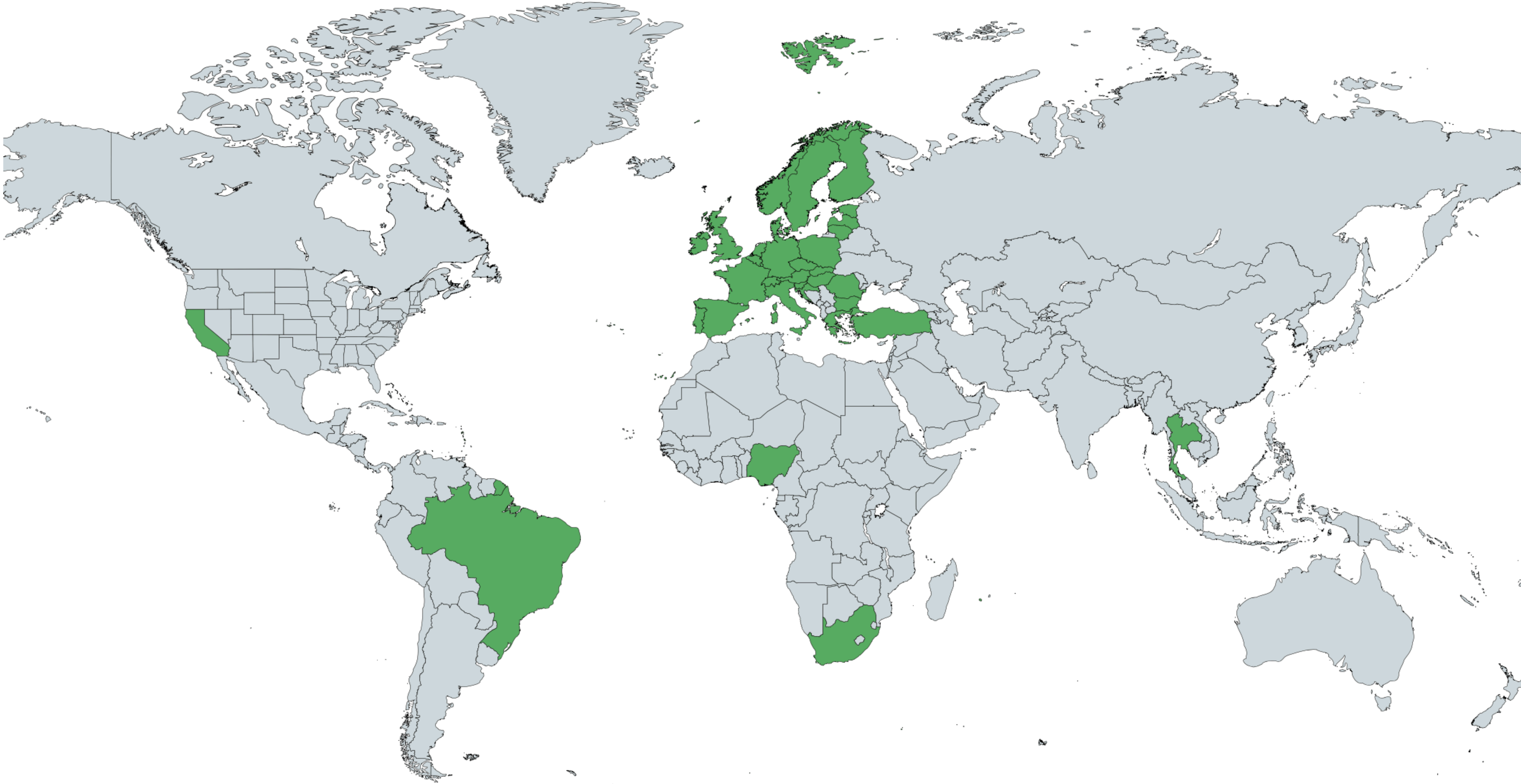
Our Purpose

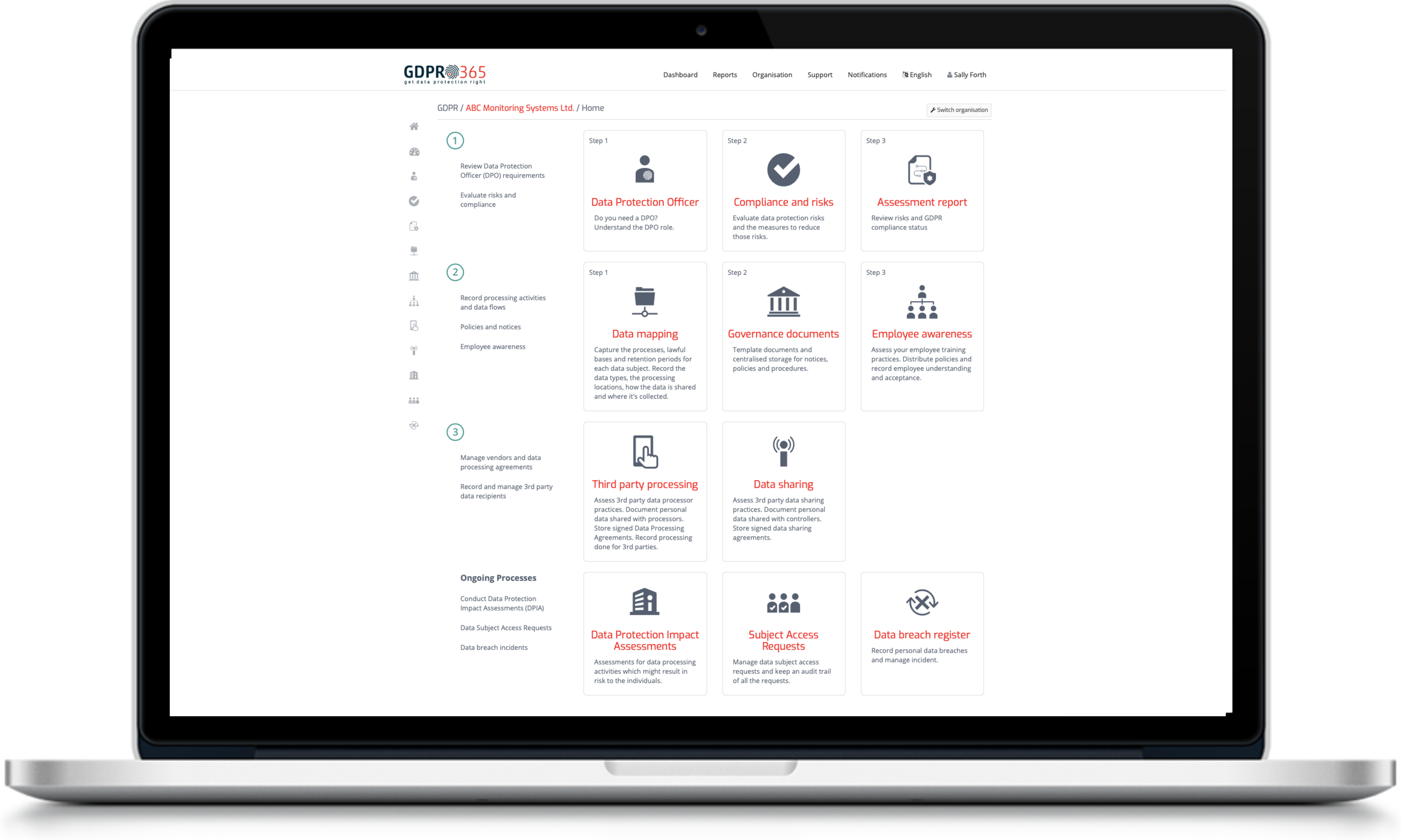
To provide privacy compliance management SAAS solutions as a cloud-based offering to a broad base of organisations covering various legal regulations worldwide.

Intelligent Compliance, Simply

Our reach - 8 Regulations worldwide, 23% of global economy.

privIQ





GDPR / ABC Monitoring Systems Ltd. / Home

1

Review Data Protection Officer (DPO) requirements

Evaluate risks and compliance

Step 1 – Data Protection Officer: Do you need a DPO? Understand the DPO role.

Step 2 – Compliance and risks: Evaluate data protection risks and the measures to reduce those risks.

Step 3 – Assessment report: Review risks and GDPR compliance status

2

Record processing activities and data flows

Policies and notices

Employee awareness

Step 1 – Data mapping: Capture the processes, lawful bases and retention periods for each data subject. Record the data types, the processing locations, how the data is shared and where it's collected.

Step 2 – Governance documents: Template documents and centralised storage for notices, policies and procedures.

Step 3 – Employee awareness: Assess your employee training practices. Distribute policies and record employee understanding and acceptance.

3

Manage vendors and data processing agreements

Record and manage 3rd party data recipients

Third party processing: Assess 3rd party data processor practices. Document personal data shared with processors. Store signed Data Processing Agreements. Record processing done for 3rd parties.

Data sharing: Assess 3rd party data sharing practices. Document personal data shared with controllers. Store signed data sharing agreements.

Ongoing Processes

Conduct Data Protection Impact Assessments (DPIA)

Data Subject Access Requests

Data breach incidents

Data Protection Impact Assessments: Assessments for data processing activities which might result in risk to the individuals.

Subject Access Requests: Manage data subject access requests and keep an audit trail of all the requests.

Data breach register: Record personal data breaches and manage incident.

PrivIQ – Intelligent Compliance, Simply.

Global privacy law compliance service.

Designed:

- Multi-lingual
- Multiple-regulation
- Collaborative

For:

- Mid-Tier
- Enterprise

Current Regulations:

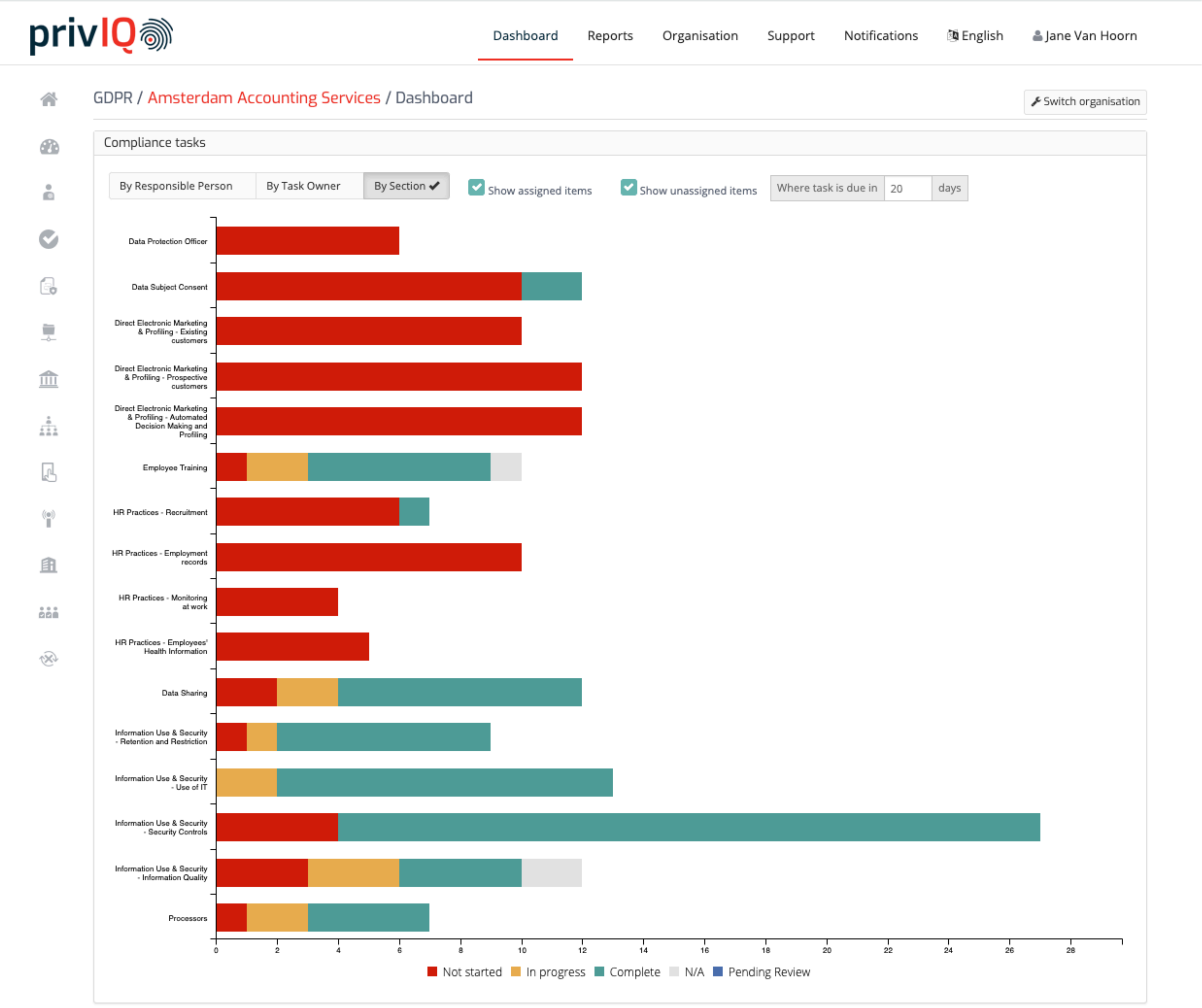
EU / UK / Turkey / South Africa / Nigeria / Brazil / Thailand / California*

- In development

The following slides are using the GDPR version.

Software Features

- ✓Easy to use
- ✓Collaboration and notification
- ✓Dashboards
- ✓Reporting Tools
- ✓SAAS Service



GDPR / Amsterdam Accounting Services / Dashboard

Compliance tasks

By Responsible Person | By Task Owner | By Section ✓

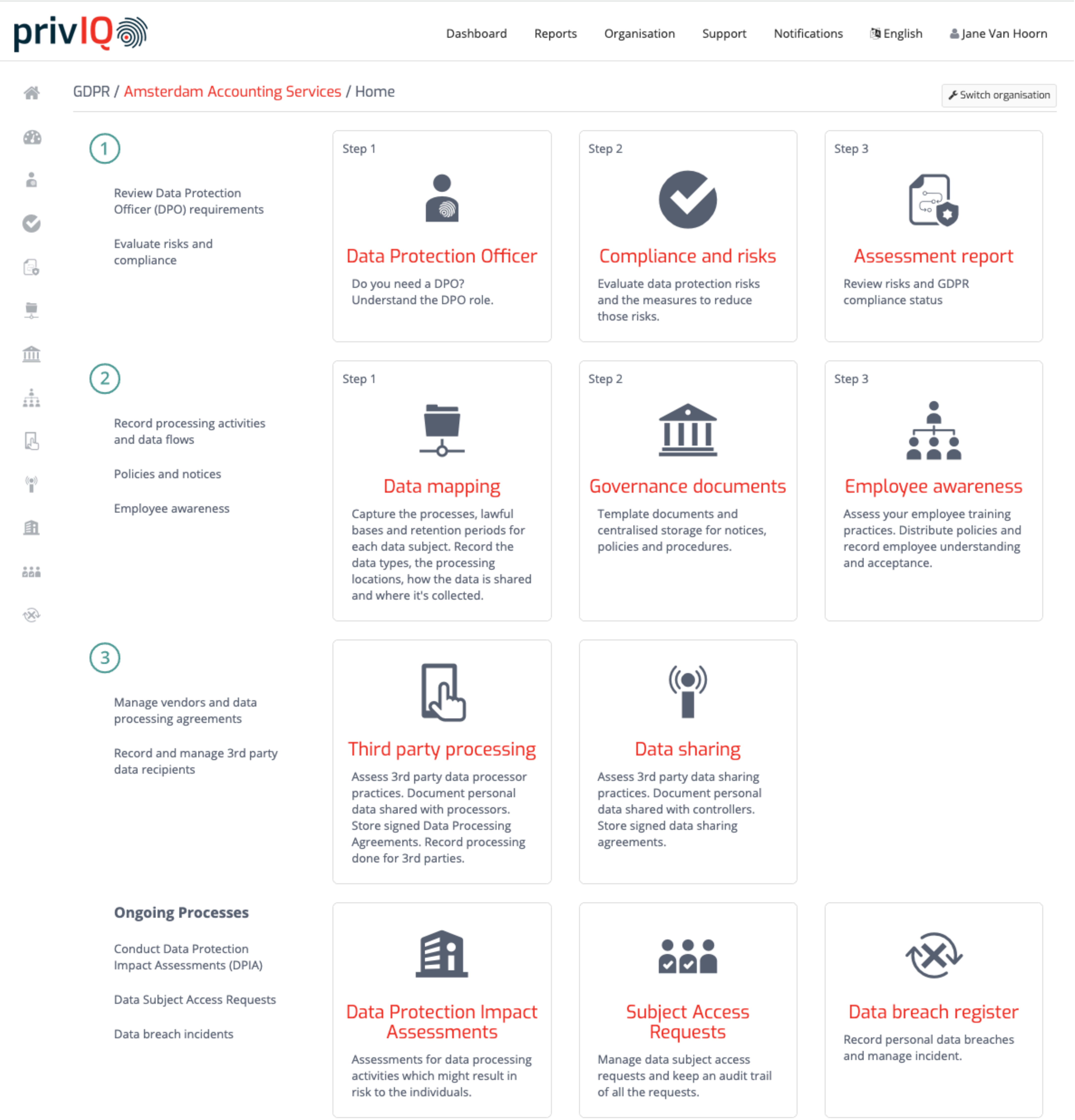
☑ Show assigned items ☑ Show unassigned items

Where task is due in 20 days

privIQ
Dashboard
Reports
Organisation
Support
Notifications
English
Jane Van Hoorn
Switch organisation
Data Protection Officer
Data Subject Consent
Direct Electronic Marketing & Profiling - Existing customers
Direct Electronic Marketing & Profiling - Prospective customers
Direct Electronic Marketing & Profiling - Automated Decision Making and Profiling
Employee Training
HR Practices - Recruitment
HR Practices - Employment records
HR Practices - Monitoring at work
HR Practices - Employees' Health Information
Data Sharing
Information Use & Security - Retention and Restriction
Information Use & Security - Use of IT
Information Use & Security - Security Controls
Information Use & Security - Information Quality
Processors
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28
Not started
In progress
Complete
N/A
Pending Review

Home Screen layout

- **Home screen** with all functionality available.
- All text specific to regulation of company.
- Section 1
  - Information officer.
  - Ongoing compliance reviews.
  - Readiness Assessment of compliance areas.
- Section 2
  - Data Mapping of data subjects, processing purposes and legitimate basis.
  - Governance – Privacy Notices, Governance documents, Document library.
  - Employee training and notification.
- Section 3
  - Operators and data sharing agreements.
- Ongoing processes
  - Data Protection Impact Assessments, Subject access requests and security compromise recording



privIQ

Dashboard | Reports | Organisation | Support | Notifications | English | Jane Van Hoorn

GDPR / Amsterdam Accounting Services / Home

Switch organisation

1

Review Data Protection Officer (DPO) requirements

Evaluate risks and compliance

Step 1 — **Data Protection Officer**: Do you need a DPO? Understand the DPO role.

Step 2 — **Compliance and risks**: Evaluate data protection risks and the measures to reduce those risks.

Step 3 — **Assessment report**: Review risks and GDPR compliance status

2

Record processing activities and data flows

Policies and notices

Employee awareness

Step 1 — **Data mapping**: Capture the processes, lawful bases and retention periods for each data subject. Record the data types, the processing locations, how the data is shared and where it's collected.

Step 2 — **Governance documents**: Template documents and centralised storage for notices, policies and procedures.

Step 3 — **Employee awareness**: Assess your employee training practices. Distribute policies and record employee understanding and acceptance.

3

Manage vendors and data processing agreements

Record and manage 3rd party data recipients

Third party processing: Assess 3rd party data processor practices. Document personal data shared with processors. Store signed Data Processing Agreements. Record processing done for 3rd parties.

Data sharing: Assess 3rd party data sharing practices. Document personal data shared with controllers. Store signed data sharing agreements.

Ongoing Processes

Conduct Data Protection Impact Assessments (DPIA)

Data Subject Access Requests

Data breach incidents

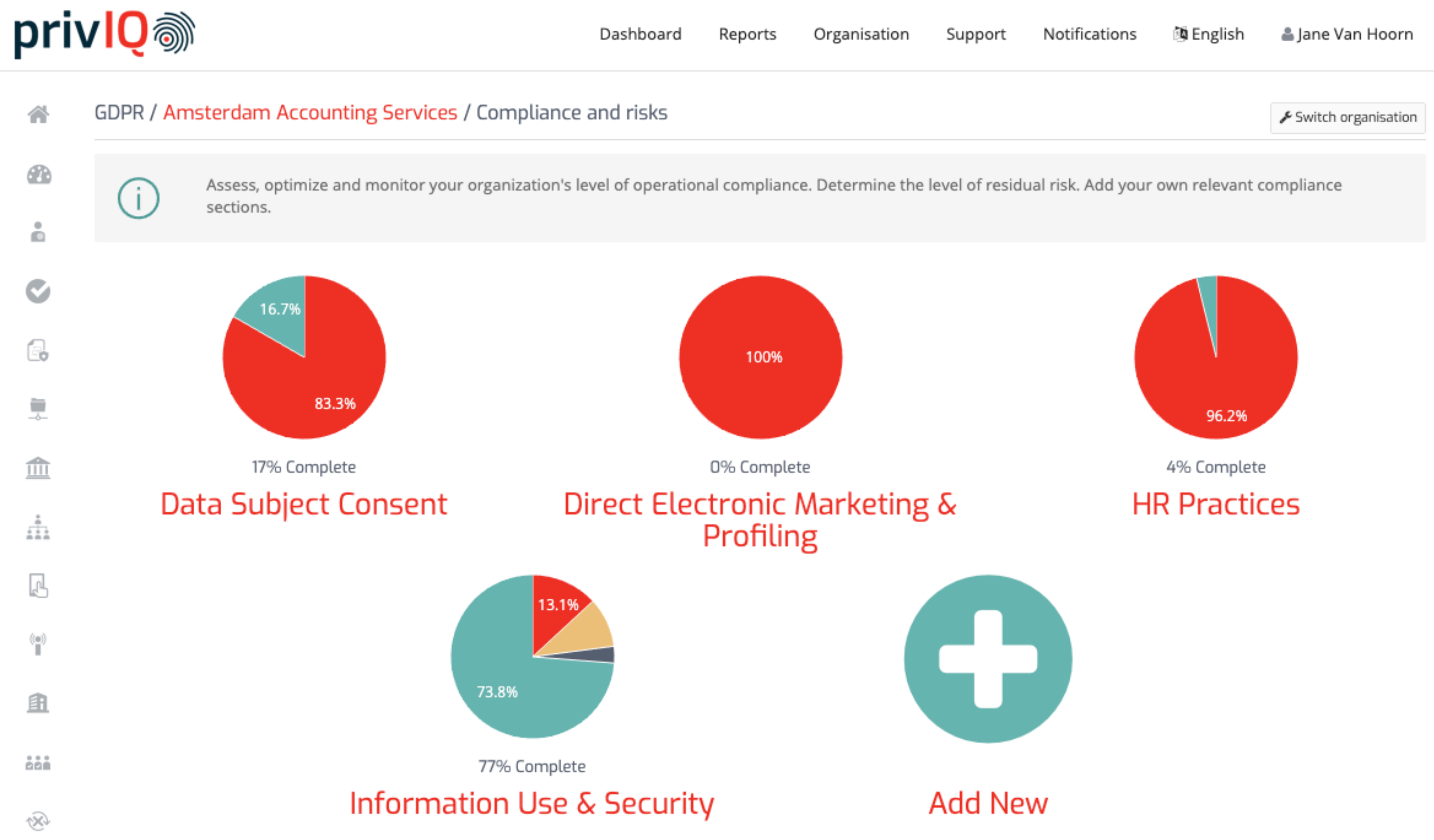
Data Protection Impact Assessments: Assessments for data processing activities which might result in risk to the individuals.

Subject Access Requests: Manage data subject access requests and keep an audit trail of all the requests.

Data breach register: Record personal data breaches and manage incident.

Compliance Section

- Predefined or add your own.
- Main Areas – Data subject consent, Marketing, HR, IT & Security.
- Add your own compliance areas for specific regulation for example, Anti-Money Laundering, PCI, Own Practices.



GDPR / Amsterdam Accounting Services / Compliance and risks

Assess, optimize and monitor your organization's level of operational compliance. Determine the level of residual risk. Add your own relevant compliance sections.

17% Complete
Data Subject Consent

0% Complete
Direct Electronic Marketing & Profiling

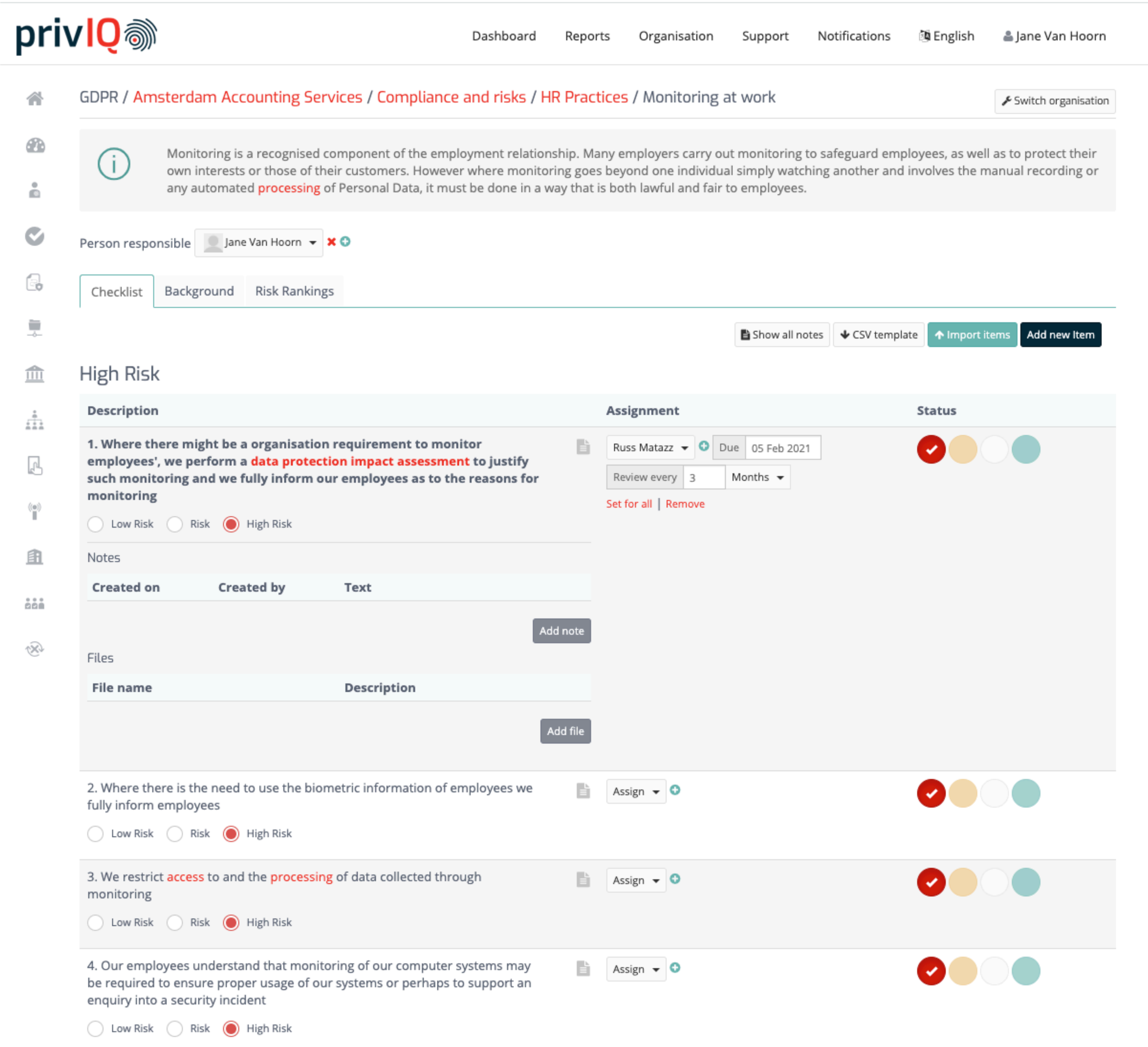
4% Complete
HR Practices

77% Complete
Information Use & Security

Add New

Compliance Items

- Predefined or add your own.
- Assign to task owner, specify review periods, due dates.
- Set Task status – Not started, in progress, N/A, Completed.
- Set risk level.
- Add notes and files to each item as required.



GDPR / Amsterdam Accounting Services / Compliance and risks / HR Practices / Monitoring at work

Monitoring is a recognised component of the employment relationship. Many employers carry out monitoring to safeguard employees, as well as to protect their own interests or those of their customers. However where monitoring goes beyond one individual simply watching another and involves the manual recording or any automated processing of Personal Data, it must be done in a way that is both lawful and fair to employees.

Person responsible: Jane Van Hoorn

High Risk

Description	Assignment	Status
1. Where there might be a organisation requirement to monitor employees', we perform a data protection impact assessment to justify such monitoring and we fully inform our employees as to the reasons for monitoring ○ Low Risk ○ Risk ● High Risk	Russ Matazz · Due 05 Feb 2021 Review every 3 Months Set for all | Remove	✓
2. Where there is the need to use the biometric information of employees we fully inform employees ○ Low Risk ○ Risk ● High Risk	Assign	✓
3. We restrict access to and the processing of data collected through monitoring ○ Low Risk ○ Risk ● High Risk	Assign	✓
4. Our employees understand that monitoring of our computer systems may be required to ensure proper usage of our systems or perhaps to support an enquiry into a security incident ○ Low Risk ○ Risk ● High Risk	Assign	✓

Notes

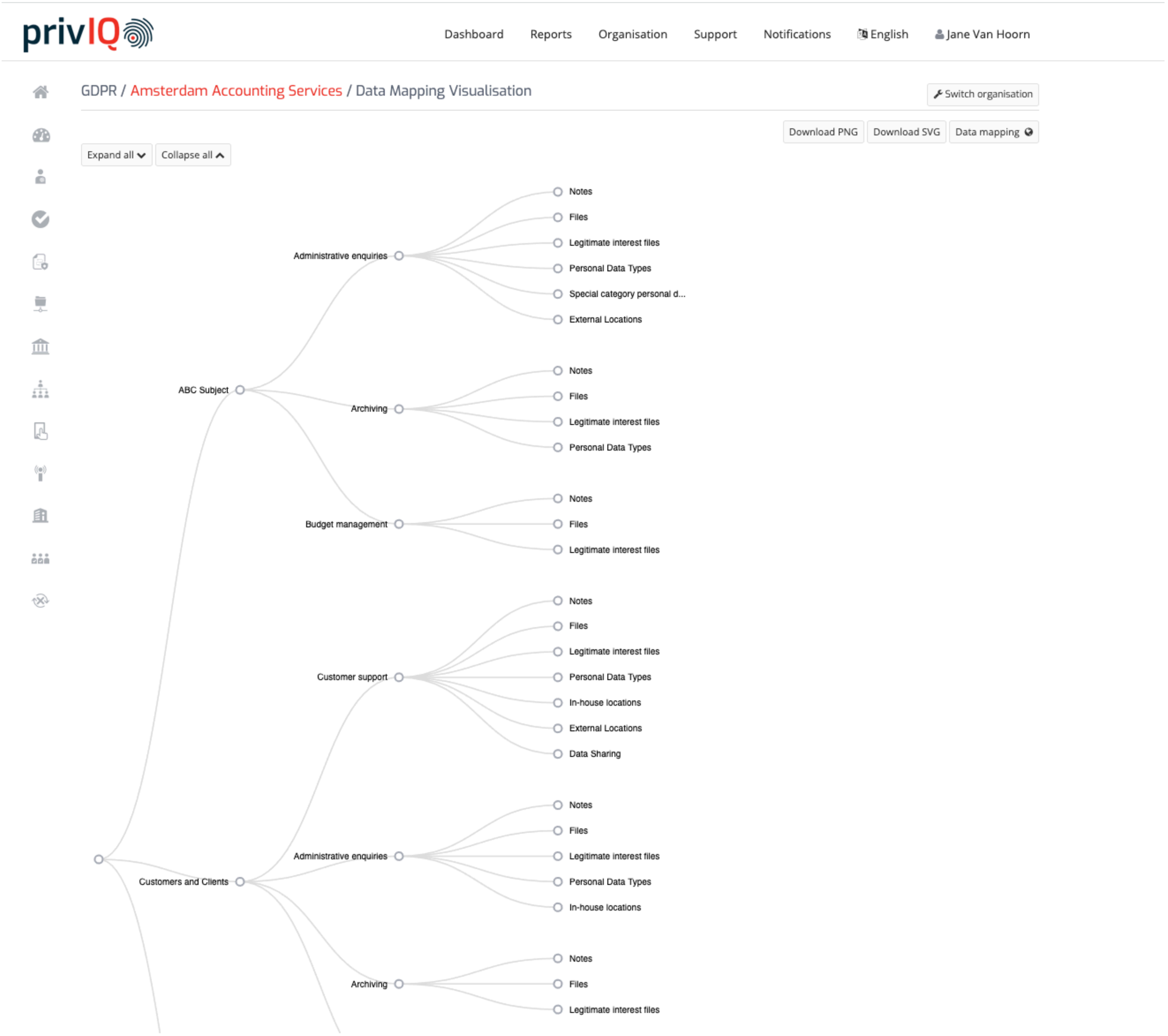
Created on	Created by	Text

Files

File name	Description

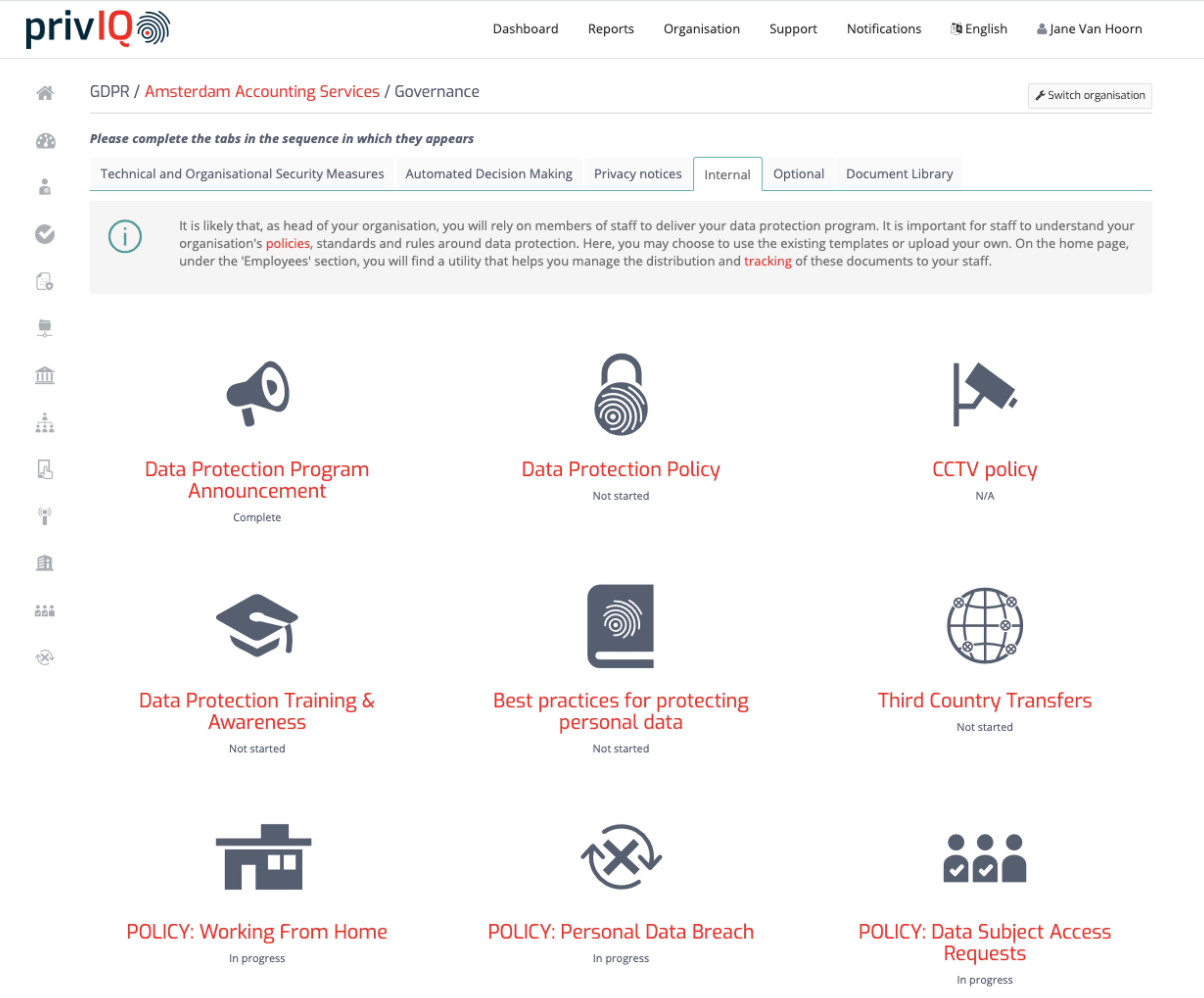
Data Mapping

- Personal and sensitive personal information inventory.
- Understand whose information you hold, for what purpose, under which lawful basis and for what duration.
- Assists in generating privacy notices, Records of Processing, defines 3rd parties to whom data is sent or shared with.
- Enable LIA's (Legitimate Interest Assessments), store all artifacts of data mapping.



Governance

- Manage Privacy Notices
- Tailor pre-loaded governance policies to your organisation.
- Upload your own documents and further policies to the document library.
- Communicate policies to all stakeholders and obtain “Read and Accepted” confirmations.



GDPR / Amsterdam Accounting Services / Governance

Please complete the tabs in the sequence in which they appears

It is likely that, as head of your organisation, you will rely on members of staff to deliver your data protection program. It is important for staff to understand your organisation's policies, standards and rules around data protection. Here, you may choose to use the existing templates or upload your own. On the home page, under the 'Employees' section, you will find a utility that helps you manage the distribution and tracking of these documents to your staff.

Data Protection Program Announcement
Complete

Data Protection Policy
Not started

CCTV policy
N/A

Data Protection Training & Awareness
Not started

Best practices for protecting personal data
Not started

Third Country Transfers
Not started

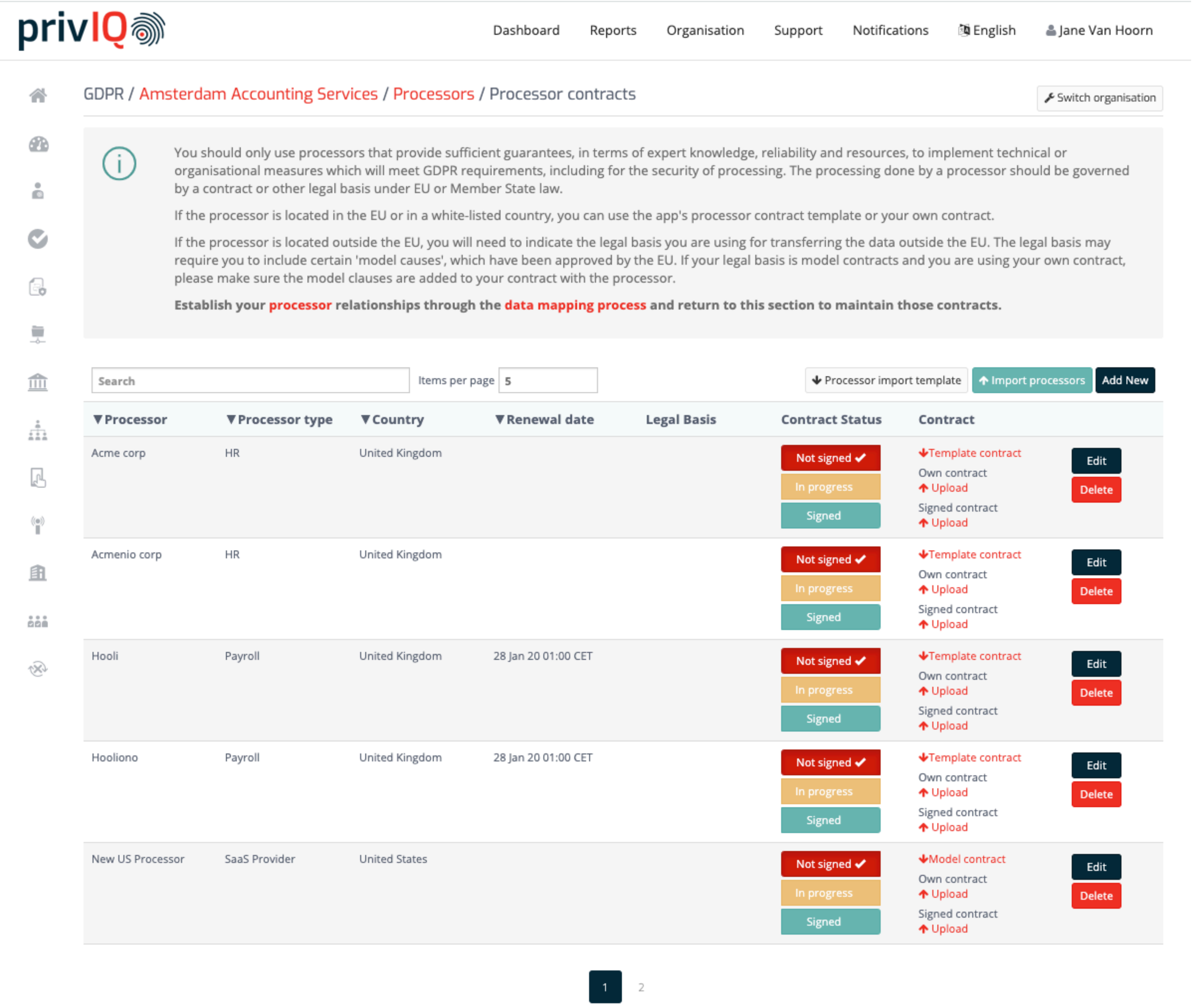
POLICY: Working From Home
In progress

POLICY: Personal Data Breach
In progress

POLICY: Data Subject Access Requests
In progress

3rd Party contracts and data sharing

- Manage 3rd party and data sharing contracts.
- Ensure 3rd parties confirm their compliance
- Store signed contracts



GDPR / Amsterdam Accounting Services / Processors / Processor contracts

You should only use processors that provide sufficient guarantees, in terms of expert knowledge, reliability and resources, to implement technical or organisational measures which will meet GDPR requirements, including for the security of processing. The processing done by a processor should be governed by a contract or other legal basis under EU or Member State law.

If the processor is located in the EU or in a white-listed country, you can use the app's processor contract template or your own contract.

If the processor is located outside the EU, you will need to indicate the legal basis you are using for transferring the data outside the EU. The legal basis may require you to include certain 'model causes', which have been approved by the EU. If your legal basis is model contracts and you are using your own contract, please make sure the model clauses are added to your contract with the processor.

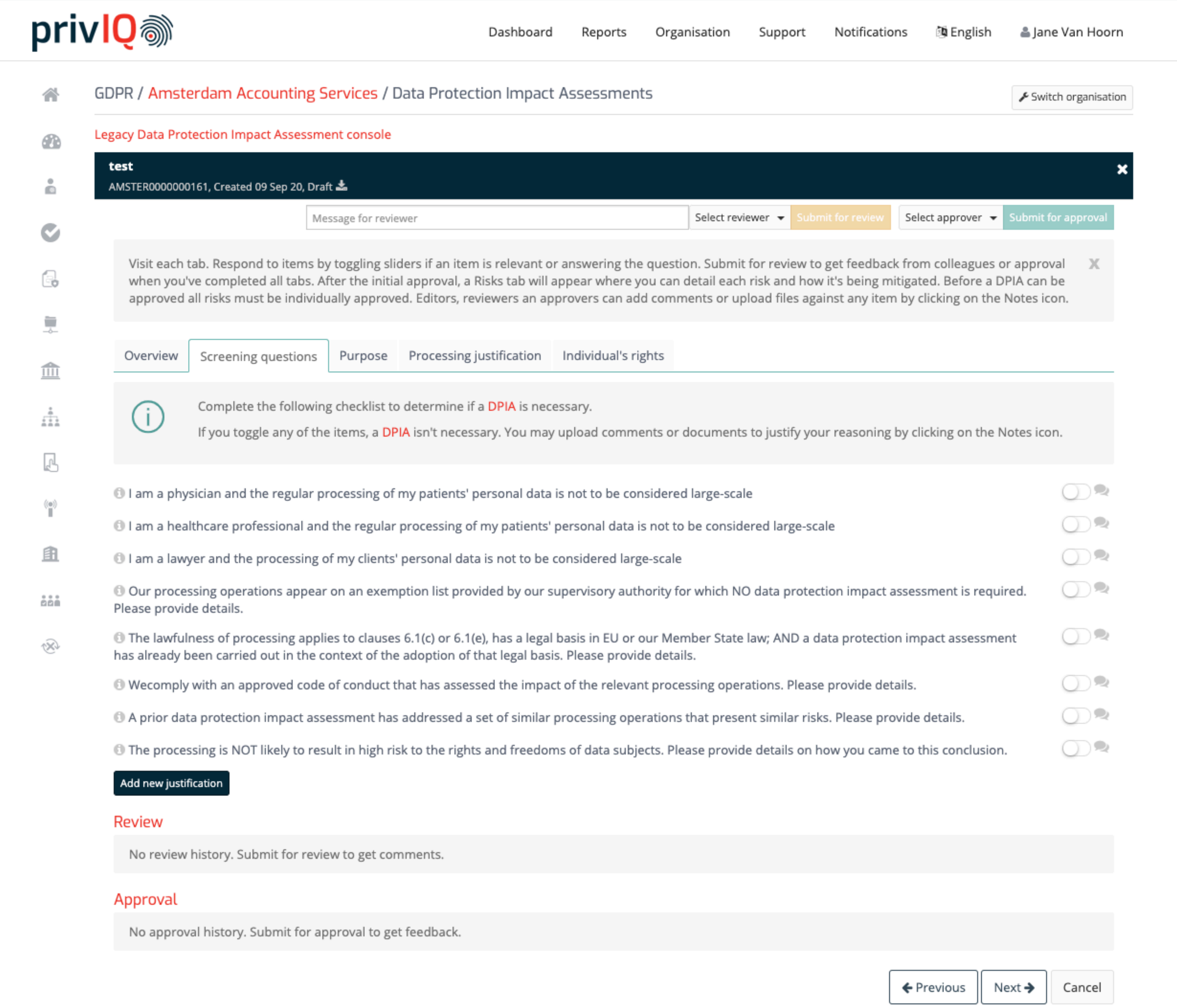
Establish your processor relationships through the data mapping process and return to this section to maintain those contracts.

▼Processor	▼Processor type	▼Country	▼Renewal date	Legal Basis	Contract Status	Contract	
Acme corp	HR	United Kingdom			Not signed ✓ In progress Signed	↓Template contract Own contract ↑ Upload Signed contract ↑ Upload	Edit Delete
Acmenio corp	HR	United Kingdom			Not signed ✓ In progress Signed	↓Template contract Own contract ↑ Upload Signed contract ↑ Upload	Edit Delete
Hooli	Payroll	United Kingdom	28 Jan 20 01:00 CET		Not signed ✓ In progress Signed	↓Template contract Own contract ↑ Upload Signed contract ↑ Upload	Edit Delete
Hooliono	Payroll	United Kingdom	28 Jan 20 01:00 CET		Not signed ✓ In progress Signed	↓Template contract Own contract ↑ Upload Signed contract ↑ Upload	Edit Delete
New US Processor	SaaS Provider	United States			Not signed ✓ In progress Signed	↓Model contract Own contract ↑ Upload Signed contract ↑ Upload	Edit Delete

Data Protection Impact Assessments

Organisations need to assess any personal data processing that might result in high risk to individuals. Pre-defined screening and purpose questionnaires.

- Wizard for justifying processing and documenting individual's rights are protected
- Workflows to get feedback from stakeholders and manage the approval process
- Analyse risks and record mitigation records using automation rules
- Easily run reports for stakeholders and regulators



GDPR / Amsterdam Accounting Services / Data Protection Impact Assessments

Legacy Data Protection Impact Assessment console

test
AMSTER0000000161, Created 09 Sep 20, Draft

Visit each tab. Respond to items by toggling sliders if an item is relevant or answering the question. Submit for review to get feedback from colleagues or approval when you've completed all tabs. After the initial approval, a Risks tab will appear where you can detail each risk and how it's being mitigated. Before a DPIA can be approved all risks must be individually approved. Editors, reviewers an approvers can add comments or upload files against any item by clicking on the Notes icon.

Complete the following checklist to determine if a DPIA is necessary.

If you toggle any of the items, a DPIA isn't necessary. You may upload comments or documents to justify your reasoning by clicking on the Notes icon.

- I am a physician and the regular processing of my patients' personal data is not to be considered large-scale
- I am a healthcare professional and the regular processing of my patients' personal data is not to be considered large-scale
- I am a lawyer and the processing of my clients' personal data is not to be considered large-scale
- Our processing operations appear on an exemption list provided by our supervisory authority for which NO data protection impact assessment is required. Please provide details.
- The lawfulness of processing applies to clauses 6.1(c) or 6.1(e), has a legal basis in EU or our Member State law; AND a data protection impact assessment has already been carried out in the context of the adoption of that legal basis. Please provide details.
- Wecomply with an approved code of conduct that has assessed the impact of the relevant processing operations. Please provide details.
- A prior data protection impact assessment has addressed a set of similar processing operations that present similar risks. Please provide details.
- The processing is NOT likely to result in high risk to the rights and freedoms of data subjects. Please provide details on how you came to this conclusion.

Review

No review history. Submit for review to get comments.

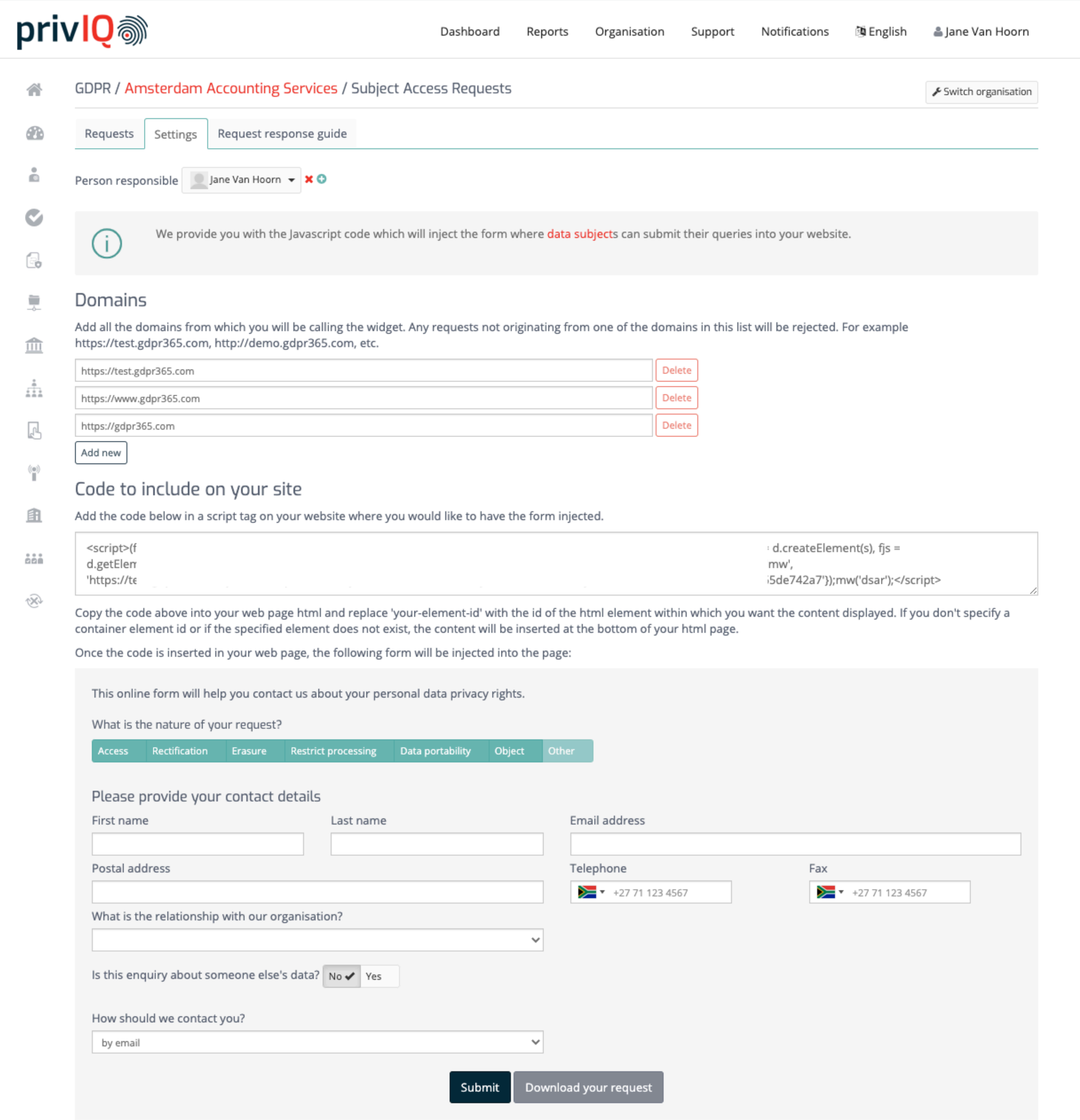
Approval

No approval history. Submit for approval to get feedback.

Subject Access requests

A subject access request is a request made by a data subject for the information that your organisation holds about them

- A pre-built brandable form you can link to from any website or application.
- Real-time alerts and reminders.
- A case management system that records and stores your SAR responses in one location.
- The option to add written and verbal requests manually.
- Guidance to ensure you respond correctly.
- Multilingual forms.
- Workflow to ensure you validate and respond before deadlines.



GDPR / Amsterdam Accounting Services / Subject Access Requests

Person responsible: Jane Van Hoorn

We provide you with the Javascript code which will inject the form where data subjects can submit their queries into your website.

Domains

Add all the domains from which you will be calling the widget. Any requests not originating from one of the domains in this list will be rejected. For example https://test.gdpr365.com, http://demo.gdpr365.com, etc.

https://test.gdpr365.com — Delete
https://www.gdpr365.com — Delete
https://gdpr365.com — Delete

Add new

Code to include on your site

Add the code below in a script tag on your website where you would like to have the form injected.

```
<script>(f                                  d.createElement(s), fjs =
d.getElem                                   mw',
'https://te                                 5de742a7'});mw('dsar');</script>
```

Copy the code above into your web page html and replace 'your-element-id' with the id of the html element within which you want the content displayed. If you don't specify a container element id or if the specified element does not exist, the content will be inserted at the bottom of your html page.

Once the code is inserted in your web page, the following form will be injected into the page:

This online form will help you contact us about your personal data privacy rights.

What is the nature of your request?

Access | Rectification | Erasure | Restrict processing | Data portability | Object | Other

Please provide your contact details

First name:
Last name:
Email address:
Postal address:
Telephone: +27 71 123 4567
Fax: +27 71 123 4567
What is the relationship with our organisation?
Is this enquiry about someone else's data? [✓ No] Yes
How should we contact you? by email

Submit | Download your request

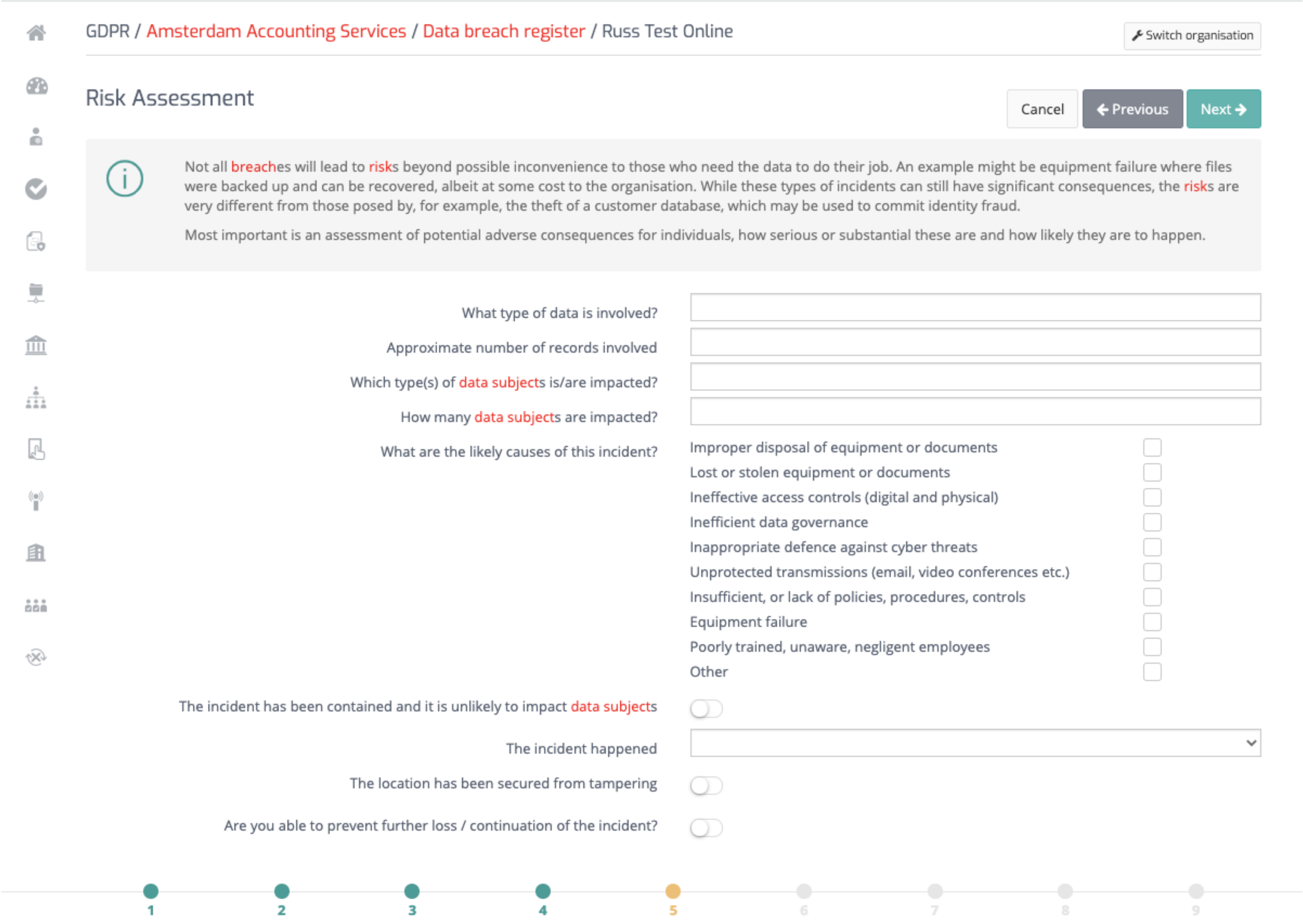
privIQ

Breach Management

The high incidence of data breaches means that avoiding a personal data breach is no longer good enough for small to medium-sized organisations.

We enable you to prepare for data breaches by having a system in place to manage your response to them, from assessing and documenting to reporting them within the stipulated time of becoming aware.

- Manage your responses to personal data breaches.
- Report personal data breaches to the authorities.
- Protect your business from the risk of a bad reputation.



GDPR / Amsterdam Accounting Services / Data breach register / Russ Test Online

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 organisation. 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?

Approximate number of records involved

Which type(s) of data subjects is/are impacted?

How many data subjects are impacted?

What are the likely causes of this incident?

- Improper disposal of equipment or documents ☐
- Lost or stolen equipment or documents ☐
- Ineffective access controls (digital and physical) ☐
- Inefficient data governance ☐
- Inappropriate defence against cyber threats ☐
- Unprotected transmissions (email, video conferences etc.) ☐
- Insufficient, or lack of policies, procedures, controls ☐
- Equipment failure ☐
- Poorly trained, unaware, negligent employees ☐
- Other ☐

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

The incident happened

The location has been secured from tampering ○

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

privIQ

Let’s Connect

Book a demo with us.

Go to our website.

THANK YOU