



CCPA

Onboarding Guide

Contents

Welcome Email	3
Organization Settings	3
Users	4
Home Page	4
Data Mapping	5
Data mapping is done in phases:	5
Governance	7
Privacy Policy	7
Training & Awareness	8
Document Library	8
Employee Awareness	8
Assessment Report	9
Compliance Audit	10
Consumer Requests	11
Consent Management	12
Do Not Sell My Personal Information	12
Opt-In	13
Opt-Out	13

The California Consumer Privacy Act (CCPA) gives California consumers certain privacy rights. This means that a business that collects, uses, or sells consumers' personal information needs to implement policies and procedures that enable the business to comply with the various provisions in the Act. These include having to inform consumers through various notices, responding to consumers' requests, and implementing mechanisms for managing consent.

Although there are many terms, understanding the following key terms is essential to correctly setting up your PrivIQ account. (See the *Definitions* link, under *Support* in the upper navigation bar)

Business

Consumer

Household

Verify

Verifiable consumer request

Sale

Personal information – (see 1798.140 for the full description)

Data subject – the person to whom personal information relates (A generally accepted definition)

Let's get started!

Welcome Email

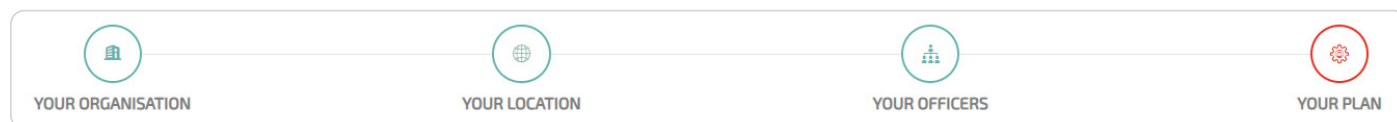
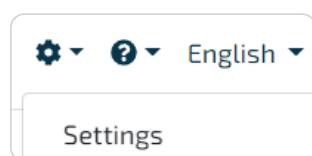
If it's your first PrivIQ account, you will receive a temporary password. Click 'Log in', enter your username and copy and paste the temporary password. (Looks something like this fdABCDb#777bZ). Change your password and sign in.

Log in

We suggest you skip any MFA setup now, rather set that up once you have signed in. Simply hover over your name in the top right corner and select MFA. To sign-in to subsequent accounts, you won't need a temporary password. Simply sign in as normal and you will see additional accounts in the list.

Organization Settings

To get to Settings, click the wheel in the upper navigation bar.



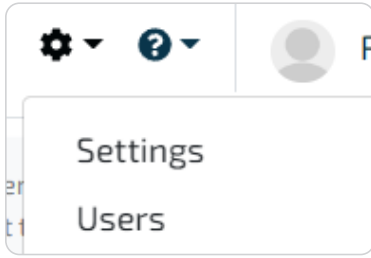
Under '**Your Organisation**' enter your contact details and upload your logo.

Under '**Your Location**' enter your physical and postal addresses.

Under '**Your Officers**' enter the organization lead's (e.g., the CEO) name and email address.

Under '**Your Plan**' you will find the settings and features that determine your package size

Users



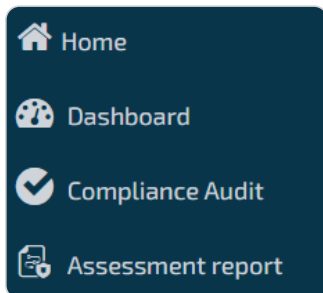
Add and manage users under Users. If you add Compliance Users here, you must ensure that they have been assigned as the person responsible in the relevant Compliance sections.

To provide an extra layer of security, we've added multi-factor authentication (MFA).

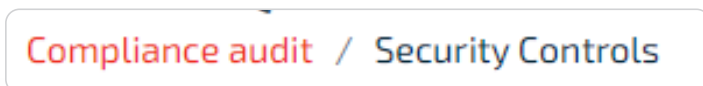
New users will receive a welcome email, inviting them to login with a temporary password and then changing their password. You can choose to either receive a verification code via SMS which you will enter along with password. Or, preferably, you can use an authenticator, such as Authy, Google Authenticator (iOS/Android) or Microsoft Authenticator, that will generate the verification code to enter with your password.

Home Page

The features you see on the home page will be those that were selected under Your Plan in the Organisation Settings. When switching between different sections you are encouraged to use the sidebar.



At other times it might be convenient to click on the breadcrumb, as in the below picture where you're simply moving 1 level back to 'Compliance audit'



Data Mapping



Data mapping

Data mapping informs the Privacy Policy (template) and the Consumer Requests section. This is where we answer the 'who', 'why', 'what', and 'where' of processing of consumers' personal information. Throughout the data mapping you may add your own data element, should the default list not suffice.

Data mapping is done in phases:

Record the 'who' and 'why'

To begin, select the relevant data elements from the drop-down lists (or add new elements by clicking the green cross).

Data subject type	Processing purpose
Data subject type ▾ +	Processing purpose ▾ +
Consumer	Detecting security incidents
Consumer	Providing customer service

A data subject is the person to whom personal information relates. Select the data subject type (WHO), processing purpose (WHY) and lawful basis. Then, clicking 'Add New' will take you to the next step where you describe the 'what' and 'where'.

Describe the 'what' and 'where'

Clicking 'Add New' earlier will open the above box where you will need to:

Personal information types Processing locations Information sharing Notes and files

Enter the **Personal information types**

Enter the **Processing locations**, Information assets (within the organisation) and, externally by any Service Providers

Under **Information sharing**, add any Third Parties to whom you disclose personal information

Add relevant **Notes and files**

Once you're happy with your input, click 'Validate'

Validate

If you see 'OK', then you're done with this piece of data mapping. If not, you will be informed as to where to complete your data mapping.

Data mapping validation

OK

Continue data mapping for the next new set of data subject types, purposes. Use the Filter if you are editing existing entries.

Filter

Data subject type ▾

Processing purpose ▾

Reset

OR, go to Collection Sources.

Identify the collection source

Data mapping

Collection Sources

Edit

Visualise

Filter

Consumer ▾

Address, telephone number, other contact details ▾

Collection source	Directly	Third party
Advertising networks	☒	☐
Data analytics providers	☐	☐

After successfully validating each section under Data Mapping, indicate the Collection Source/s for each of the personal data or special category types you selected in the data mapping.

Use the Filter to select the department, data subject type and personal data type. Select the collection source/s and if it's from a Third Party, enter the category of the third party e.g., Credit Bureau.

Click Validate. If there are issues, the validation will inform you as to where the issues are. If you see 'OK', move on to the next set of collection sources.

Data mapping will integrate with the **Records of Processing Report** which you will find under Governance.

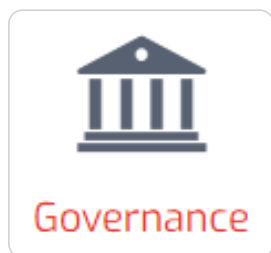
HINT: In Data Mapping and Collection Sources, click 'Visualise' to get an overview of your progress.

Edit

Visualise

Remember that data mapping is not a once-off but should be revisited as circumstances change within the business.

Governance

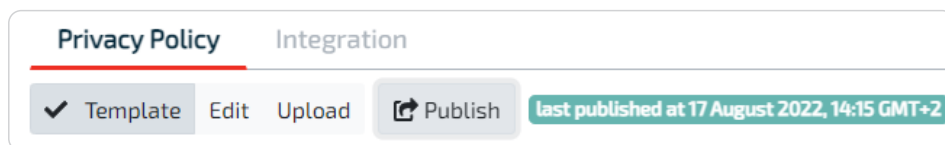


Now that the data mapping is complete, it's time to setup the Privacy Policy, select any training & awareness documents you wish to send to your employees and to populate the document library.



Privacy Policy

The purpose of the Privacy Policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. Additionally, the CCPA Regulations provide for a Notice at Collection (999.305). PriviQ combines both these documents into the Privacy Policy.



Note the three options. The Template is informed by the completed data mapping, you may Edit your own, or you may upload a PDF. You must Publish the document each time you refresh your data mapping or each time you change an option.

Publishing will reveal the script which you can embed behind a link named 'Privacy Policy'. The link must be displayed on any website where you collect personal information.



Add all domains from where you will be calling the widget.

You may also download a PDF version.

Training & Awareness

In the Internal tab you will find 2 default documents. If you're going to share them with employees, **set them to Complete**. We'll discuss later where you may send them to employees.

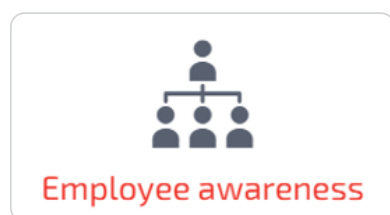
Name	Description	Show in employees
AML Manual	AML Manual	☒

Document Library

Here you may upload or edit your own documents. There's also the option to share or not to share with employees.

Description	Show in employees
User Manual	☒

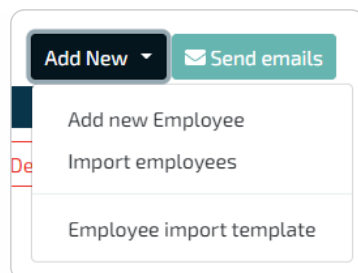
Employee Awareness



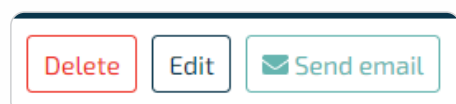
Employees are directly involved in the organisation – managers, employees, directors, trustees etc. One of the ways in which to demonstrate compliance is by keeping all employees informed of their roles and responsibilities. In the Governance section you would have selected the relevant documents that you would need to share with your employees, contractor workers, and the like. Go to the Compliance section.

First name	Last name	Job title	Email address
Timmy	Thomas	None	timmyt@geemail.com

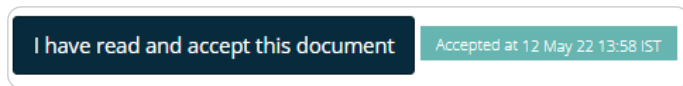
You may add an employee individually or use the template to upload. You may send emails globally, i.e., to everyone, by clicking 'Send emails'...



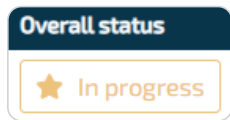
Or you can email individually by clicking 'Send email' next to the employee's name. You can also customise your message to the individuals.



They will need to open that document by clicking the link in the email, reading the document, and then clicking 'I have read and accept this document'.

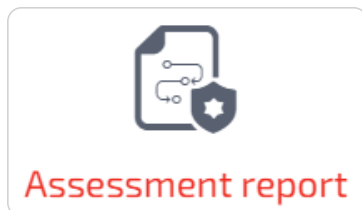


The overall status appears next to each employee name.



If you click on an employee, you will see the status of each document. A red star means the document has not been sent. An orange star means it has been sent but there is no response. A green star means the employee has accepted the document. Hover over the stars to see the meta-data.

Assessment Report

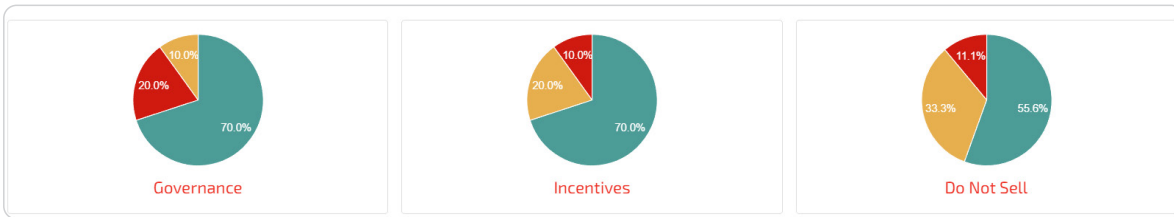


Run this report to keep track of and report on your compliance journey. Use the filter to target specific sections. Download the report in PDF or Excel format. It's good practice to regularly run and print the full report.

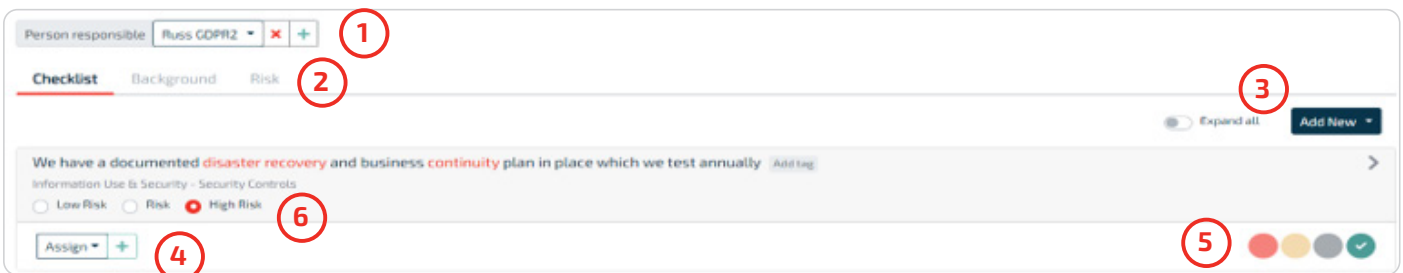
Compliance Audit



As compliance is both a collaborative and continual process, you will find a suite of compliance sections which require regular updating. Note that you may add any new sections which might be relevant to your business. The objective is to assign sections to what we call Compliance Users and then for the section owners to assign tasks to Task Owners.



By way of example, let's look at the first item under 'Security Controls'.



The screenshot shows the 'Checklist' tab for 'Security Controls'. It includes a 'Person responsible' dropdown (1), a 'Background' tab (2), an 'Add New' button (3), a checklist item 'We have a documented disaster recovery and business continuity plan in place which we test annually' (4), a risk level selector (5) currently set to 'High Risk', and an 'Assign' button (6).

1. You MUST assign all compliance sections to Compliance Users. If not in the drop-down list, add users by clicking the green cross. A compliance user only sees sections assigned.
2. Find useful information in the Background tab.
3. Add your own relevant checklist items individually, or upload using the csv template.
4. Assign checklist items to Task Owners and, **most importantly, set a review cycle** which triggers notifications to the task owners.
5. Assess your organization's progress against each checklist item. (Not started; In progress; N/A; Complete)
6. Reset the residual risk level after you set your Status (in 5.)

NOTE: By clicking the drop-down arrow on the right, the task owner can add audit notes and upload documents in support of the review.

BIG TIP: By clicking the white cross in the green circle, you may add your own sections and checklist items in each section. This feature is especially useful where you need to manage risks and issues you identify during the onboarding procedure or during normal operations.

Consumer Requests



Consumer Requests

A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or more designated methods for submitting requests to know or requests to delete, including, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

[Requests](#) **Settings** [Request response guide](#)

Person responsible

Russ CCPA ▾ ✕ +

Integration Customisation

Under Settings, you will find a script which you must embed behind a link on your websites called 'Consumer Requests'. Add the domains from where you will be calling the widget

Code to include on your site

```
<script>(function (w,d,s,o,f,js,fjs) {w['365Compliance']
```

Click the '**Preview**' button to see how the form will present to a consumer making a request. Note, the person may also attach documents to the request. Online requests are received by the 'person responsible' in the Requests tab but you can add requests manually by clicking Add New.

Add New

Process [Details](#) [Notes](#) [Files](#) [History](#) [Data Mapping](#)

●

RECEIVED

[Evaluate >](#)

[Verify >](#)

First evaluate the request – e.g., it's possible it might not be for your business or might not involve personal information. Then verify the requester before moving to the next step.

Observe the Data Mapping for this particular type of data subject making the request. Proceed through the request, taking note of any **mandatory** items denoted by a star, and reading the supporting notes behind the info buttons. A failed request is indicated by the red text and a successful one, by the blue text.

Don't forget to update the Consumer Requests checklist!

Consent Management

There are several instances where consent management is provisioned in the CCPA. For example, consumers must be allowed to opt out of the sale of the personal information. In some cases, consumers must be allowed to opt-in to the sale of their personal information, e.g., where a consumer is less than 16 years of age. PrivIQ enables you to setup a workflow and link for each scenario.



Consent Management

Do Not Sell My Personal Information

The CCPA states that "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary *or other valuable consideration*.

So, there doesn't necessarily need to be an exchange of money. Examples of *other valuable consideration* could be where you use advertising technology to improve your site's performance or sharing within your family of companies, where those companies are separate entities, yet they benefit from sharing personal information.

Consent Setup

Consent Dashboard

Consent Queries

In Consent Setup, click Add New.

Consent Type

Consent Type ▾

search

CCPA-DNSMPI

CCPA-DNSMPI-SIMPLE

Select CCPA-DNSMPI.

(Note – there is also CCPA-DNSMPI-SIMPLE for when you don't require the detail as in the regular one)

The **Header** field is what appears on your website. Ensure that the content you insert in the **Body** field complies with regulation **999.306**. # days to expiry is for your own internal reference.

Preview

Code Snippet

Edit

Delete

Click Preview to see the flow of the request, add some data which will then appear as a request under Consent Queries. Try both options – for yourself, and on behalf of someone else.

Form widget

Unsubscribe

Click Code Snippet. Add the domains from where you will be calling the widget. Here you will also find code to include on your site. Use the script to embed behind your 'Do Not Sell My Personal Information' link.

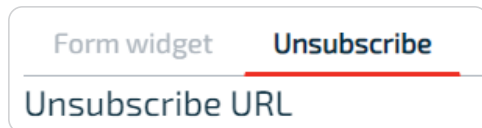
Opt-In

A consumer could potentially:

- opt-in to a financial incentive – see **999.307** (Notice) and **Article 6** (Non- discrimination) of the Regulations
- opt-in after opting out of the sale of personal information – Regulation **999.316**
- as someone under 16 years of age, opt-in to the sale of personal information – **Article 5**

In Consent Setup, click Add New, select GENERIC-OPT-IN and follow the same procedure as above.

Click Code Snippet.

A screenshot of a web form widget. It has a light gray border and rounded corners. Inside, there are two tabs: 'Form widget' and 'Unsubscribe'. The 'Unsubscribe' tab is selected and highlighted with a red underline. Below the tabs, the text 'Unsubscribe URL' is displayed.

You will find the unsubscribe URL that you may include in your communication with consumers. This URL will be specific to each opt-in form you create. If you don't want the user to be redirected to a generic thank you page when they click the unsubscribe link, you can provide your own unsubscribe success page.

Opt-Out

Besides the 'Do Not Sell My Personal Information' opt-out, there may be other scenarios where you might want to use the opt-out functionality.

In Consent Setup, click Add New, select GENERIC-OPT-OUT and follow the same procedure as above.