

Contents

Implementation Guide	2
Organization Setup	3
Key Terms	4
Privacy Officer	5
Home Page	5
Data Mapping	6
Data mapping is done in phases:	7
Governance	10
Privacy Notices	10
Integration	11
Training & Awareness	11
Security Measures	11
Record of Processing (also referred to as Record of Processing Activities - ROPA)	11
Stakeholder Comms	12
Compliance Audit	14
Monitoring Compliance	16
Service Providers	17
Subject Access - Data Subject Access Requests	19
Requests	20
Received	20
In progress	21
Breach Management	22
Privacy Impact Assessment	24
Screening Questions	25
Purpose	25
Processing justification	26
Individual's rights	26
Risks and Mitigations	27
Final Approval	27
Dashboard	28
User Maintenance	29
Glossary	30

Implementation Guide

This guide may be used for organizations who manage privacy management in a comprehensive manner, adopting Privacy by Design and Default. DataProtection Dynamix (DPDx) is a privacy framework which incorporates requirements common to one or more leading privacy compliance regulations and laws.

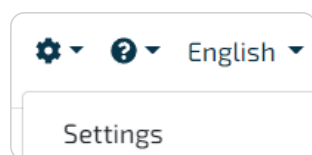
Your organization is the Controller of data you collect and process for your customers, employees and other data subject types, e.g. job applicants. We suggest you adopt the following approach to rolling out your privacy compliance program.

1. Understand the organization's activity by asking:
 - what are the core activities?
 - how many employees?
 - do you outsource the processing of personal data?
 - do you disclose personal data to other organization?
 - do you transfer personal data outside your country or region?
 - who heads up departments, e.g., HR, Sales and others that deal with personal data?
 - who is leading the privacy program?
 - in what US states do we do business and serve customers?
2. Heads of departments (Data Owners or Information Owners) to formulate a list of ALL processing activities that involve personal data; including any informal activities. If possible, record the sources of the personal data, in which applications do they process personal data, where the information is stored in their departments, and to whom the information is disclosed. Include physical media as well.
3. Heads of IT / Procurement to compile a list of all Vendors involved with processing of personal data, the country in which they are located, the expiry date of those contracts.
4. Inform the CEO / head of organization of the data protection program.
5. Appoint the Data Protection Officer, where appropriate (this is a requirement for the EU's General Data Protection Regulation (GDPR). DPDx has a section to appoint a Chief Privacy Officer or Privacy Lead.
6. Register with the Relevant Authority, where required.
7. Ensure your Organization Settings are complete. (See next section).
8. Add the relevant heads of departments and the program lead as users with the system role of Administrator. (Compliance User and Task Owner must be added via the Compliance sections)
9. Following point 2. above, Information Owners to review and understand ALL processing of personal data in their respective departments. Be aware of and record all informal processing too. For example, populating spreadsheets to manage processes outside of the formal, networked and security protected systems and apps.
10. Begin the data mapping exercise, using the prep work done by the Data Owners and record any work to be done beyond this session. The head of IT could provide valuable insight or guidance especially around any processing of personal data that may be outsourced to Service Providers (aka Processors) as well as the processing done by IT. Set a date for a follow-up data mapping session. Use the follow-up session to complete the data mapping exercise.

Follow the steps as indicated by the various sections below –
remember, **compliance is on-going.**

Organization Setup

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



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

Under '**Your Location**' enter your physical and postal addresses. Ensure that you select the relevant supervisory authority. (Only in GDPR) Ensure that a time zone is selected.

Under '**Your Officers**' enter the organization lead's (e.g., the CEO) name and email address as well as the Privacy Officer's details (CPO or DPO), where available.

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

Features required

- ☒ My organization shares **personal information** with Third Parties
- ☒ My organization is likely to transfer **personal information** outside of country
- ☒ My organization consists of multiple legal entities
- ☒ My organization is a Service Provider for Third Parties
- ☒ My organization does **data mapping** by department
- ☒ My organization may be required to carry out **privacy** impact assessments

Key Terms

These key terms are essential to the proper interpretation of Privacy Management regulations from around the world and to maintain the PrivIQ-DPDx application.

Controller – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data e.g., your organization.

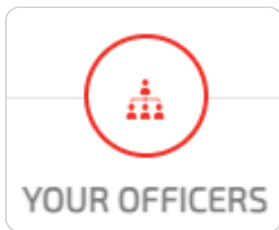
Service Provider or Processor – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller e.g., the external payroll company that does your monthly payroll run.

Personal Data – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject – means the person to whom personal data relates.

Data Owner – an individual that has approved management responsibility for controlling the maintenance, use and security of the personal data. Also sometimes called the "Information Owner".

Privacy Officer



There are two roles available in terms of Privacy Officers. These designates will display on reports such as your Records of Processing and Privacy Policy.

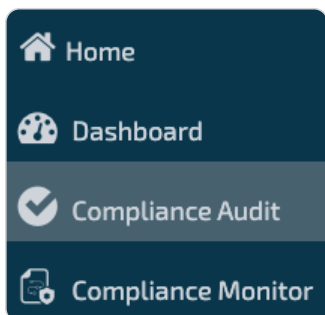
Specify the person in your organization who leads your data protection program. This could be your CEO, COO, compliance officer or program director, etc. In the second section, enter the details of your Privacy Officer.

The organization lead may be the same as your designated Privacy Officer (CPO) or Data Protection Officer (DPO), but it may not be. If it is the same person, please enter the information for that person in each section. The application will use these contacts to populate certain policies and documents in other modules, e.g., the Privacy Notice.

Complete the questionnaire, then the checklists, and if not already done under Settings, enter the Privacy Officer details. Even you don't appoint a DPO, there are 2 checklist items you must complete in the Business Environment and Governance checklist.

Home Page

The features you see on the home page will be those that were selected under Your Plan in the Organization 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 'Information Security, Response and Privacy by Design (PbD)'.

Compliance / **Information Security, Response and Privacy by Design (PbD)** / Incident Response

Data Mapping



Remember that saying regarding risk – “you can't manage it if you can't see it”? If people make inquiries about their personal data, or there's an incident, you need a detailed map to help you respond. *Data mapping is much more than producing an inventory.*

Mapping your personal data represents the first step towards building a proper foundation of your privacy management and demonstrating compliance. Data mapping covers the who, why, when, where and what of processing. You can select from pre-populated drop down lists to make your mapping exercise quick and easy. You may also add your own data items throughout the process, if one or more of the default items not apply to your organization.

Data owners must direct the data mapping and be involved throughout the process. In addition to mapping the “obvious” systems, identify any informal processing and record it in the data mapping, including 'unstructured' and paper records you hold. These are typically the areas of vulnerability, and any risks or issues should be documented and managed in the relevant compliance section.

Before you begin, a word on granularity

Granularity is important when describing your processing purposes. Don't crowd many types of processing into a singular description, especially where there are different types of personal data, and different **Service Providers**, as they are known in the US (elsewhere known as **Processors or Data Processors**). At the same time, you don't want to be overly granular when entering personal data types. Rather than recording every data element in a passport, would it not be better to say, “Passport details”?

Granularity is also important when it comes to Information Assets (in-house processing locations). You don't want to use 'Application Server' when that could be meaningless to someone who manages subject access requests. Add a location that is more descriptive, that enables the person to search the relevant systems or apps when searching for personal data to be used in response to a subject access request.

If there are commercial sensitivities around having the names of **Processors or Controllers** on your privacy notices then, add them as category names here and then add them individually in the Processors or Data Sharing sections, respectively. For example, you might not want to use 'Paula's Payroll Services', but rather use 'Payroll Processing Company' instead.

Data mapping is done in phases:

In our example, we're doing **data mapping by department**. Organizations may choose to not use the department feature and begin with Data subject type. Be thoughtful in your setup because if you decide to change the data mapping approach, the application will delete your prior mappings.

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).

Department	Data subject type	Processing purpose	Lawful Basis		
Department ▾ +	Data subject type ▾ +	Processing purpose ▾ +	Lawful Basis ▾	Add New	Cancel
Human Resources	Applicant	Employee recruitment	It is in our organization's legitimate interest	Edit	Delete

Select the department, 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'.

Add New

Cancel

NOTE: If you select the lawful basis – ***'it's in our organization's legitimate interest'***, in the next section you must indicate the type of legitimate interest and, you should use the template to complete a legitimate interest impact assessment. This is done to ensure that your organization's interests don't outweigh those of the data subject.

Legal basis

6(1)(f) - it's in our legitimate interest ▾

Fraud detection and prevention ▾

Describe the 'what' and 'where'

Data Mapping

Collection Sources

Edit

Visualise

Human Resources / Applicant / Employee recruitment

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

For this example 'purpose', ...Employee recruitment...

Enter the Retention Period (you may add your own by selecting 'Other')

Retention period

Until consent withdrawn ▾

Enter the **Personal Data** types

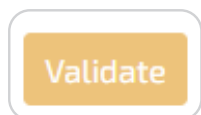
Enter the **Special Category Personal Data** types, including that **second lawful basis**

Enter the **Processing locations**, In-house (within the organization) and, externally by any **Service Providers / Processors** (See the earlier note on granularity)

Under **Data Sharing**, add any **Controllers** to whom you disclose personal data (these are NOT your Service Providers)

Add relevant **Notes and Files**

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



If you see 'OK', then you're done with this piece of data mapping. If not, the system will tell you what's missing to help you complete your data mapping.



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

Data mapping Collection Sources

Filter

Department ▼

Data subject type ▼

Processing purpose ▼

Legal basis ▼

OR, go to Collection Sources.

Identify the collection source

Data mapping

Collection Sources

Filter

Human Resources ▼

Employees / Prospective Employees ▼

Employment History ▼

Collection source	Directly	Third party
Blog or forum	<input type="checkbox"/>	<input type="checkbox"/>

After successfully validating each section under Data Mapping, indicate the Collection Source/s for each of the 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., Recruiting Site, Credit Bureau, etc.

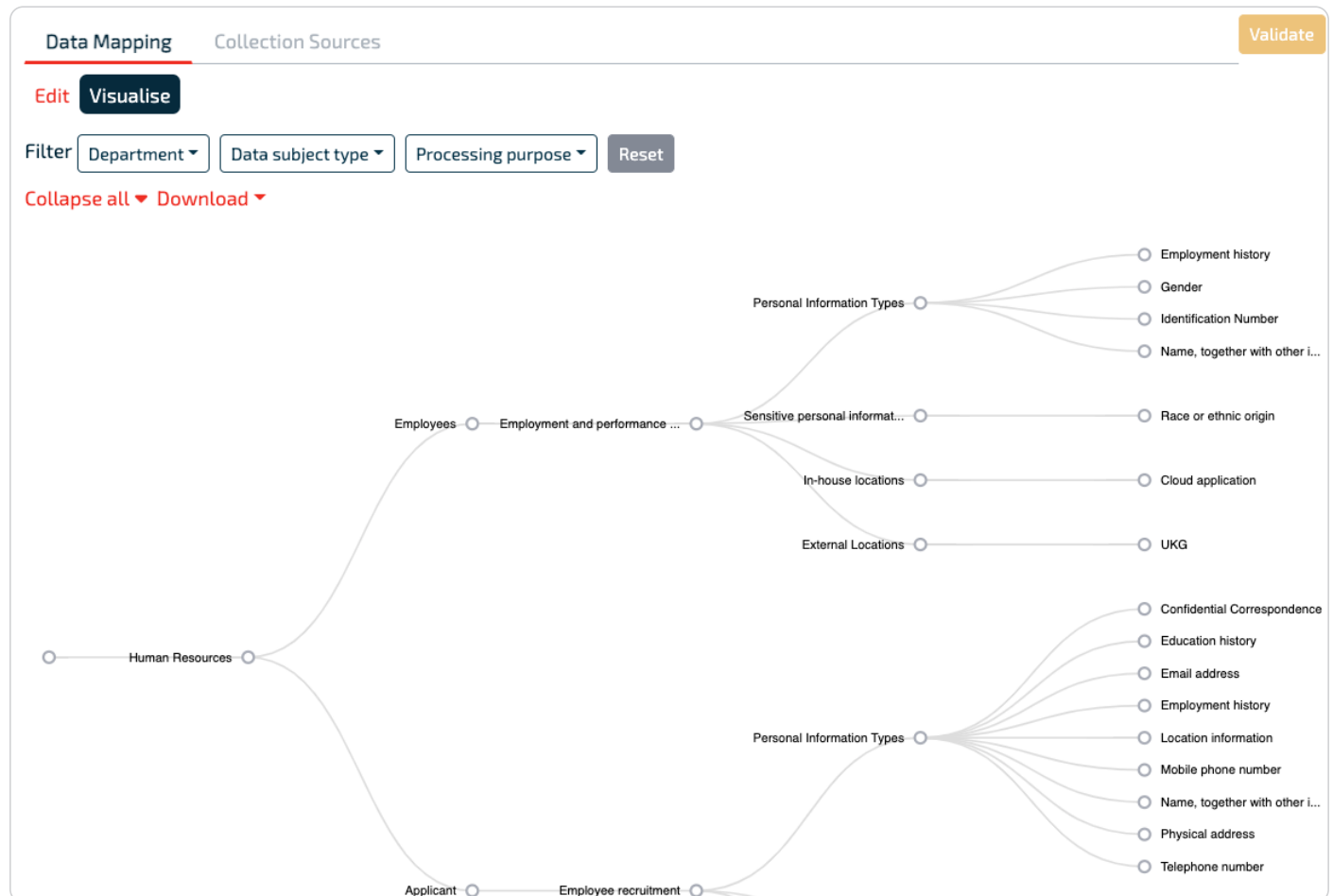
Click Validate. If there are issues, the validation will inform you as to where the issues are. If you see 'OK', move on to the next set of collection sources.

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

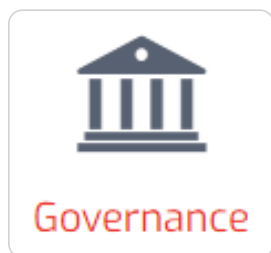
HINT: In Data Mapping and Collection Sources, click 'Visualise' to get an overview of your progress.

Edit Visualise

Example Data Map:

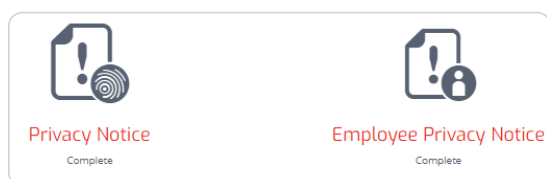


Governance

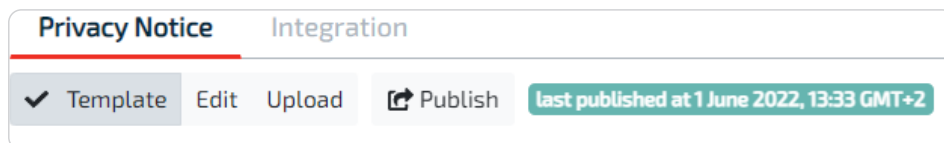


Every organization that collects and uses (processes) personal information of individuals must publicly disclose their privacy practices in one or more Privacy Notices. For example, organizations may have a web privacy notice, a product privacy notice, a cookie notice and an employee privacy notice. You may start with the privacy notice template and once you complete your data mapping and organization settings, the system automatically populates information by data subject and business process, along with the responsible privacy officer for your organization. In the Governance module, you can find the Record of Processing (ROPA) – an inventory of processes and systems that collect / process personal data – along with policies, procedures and other documents that you may share with employees and contractors. Refer to **Stakeholder Communications** section below for further information on acknowledgement tracking of documents.

Privacy Notices

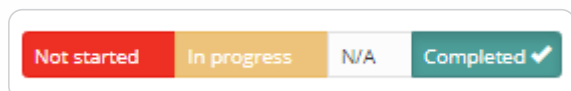


Privacy regulations and laws in the US have specific requirements for notifying individuals when collecting their personal data. The keyword being – *collecting*. Your notice must be displayed at or near the point of collection. Notice the external Privacy Notice as well as one for Employees. Click 'Privacy Notice'.



There are 3 options. The template – based on data you enter in the organization settings and data mapping; the editable version where you create your own content; or the option to upload your own PDF. However you decide to create your notice, you must remember to **Publish** the privacy notice whenever you update the template or the underlying data. Once you have completed your notice update, click on the Publish icon.

Once published, set the status to Completed – this will update your dashboard.



Remember to publish the employee privacy notice too.

Integration

The integration tab is next to the privacy notice tab. Here you will find the **code that you can embed in your websites** so that when people click on your privacy notice link, they will see whatever you have published here. There is also the option to download your published version in case you share the privacy notice other than via your websites. It is unlikely that you will present your employee privacy notice on your websites, but you must publish it before you share with your employees.

Training & Awareness

Internal

Optional

Document Library

One of the ways to demonstrate compliance is to show how you have promoted the relevant training & awareness within your organization. In these tabs you can find documents to share with various employees. Some of them have the 'template', 'own version', 'upload' options. If you are going to share a document with employees and other stakeholders, **you MUST set the document status to 'Complete'**. If you don't want to share them, mark them as N/A.

In the Document Library you can edit or upload your own documents. If you want to share them, you must tick 'Share with Employees?'

Name	Description	Show in employees
AML Manual	AML Manual	<input checked="" type="checkbox"/>

Security Measures

Technical and Organisational Security Measures

To maintain your Records of Processing Activities report, provide a general description of the measures adopted by your organisation which ensure a level of security that is appropriate to the risks of the processing of personal data. Where your organisation processes personal data on behalf of other organisations (and makes you a processor), provide a general description of the organisational security measures that might relate specifically to those categories of processing activities.

Template ☒ Edit

Record of Processing (also referred to as Record of Processing Activities - ROPA)

Record of Processing

To demonstrate compliance with various privacy laws around the world, e.g. GDPR, POPIA and in US, the controller or service provider / processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the Authority / Regulator and make those records, on request, available to it, so that it might serve for monitoring those processing operations. This report is automatically updated from having completed your data mapping and the security measures outlined above.

If you have not completed your data mapping, the system will alert you with the following message:

Please note that the Record of Processing report depends on the Data Mapping being complete. Your Data Mapping has not been completed.

[Complete Data Mapping](#)

Automated Decision Making (GDPR Version)

[Automated Decision Making](#)

Profiling' involves (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Automated processing implies the exclusion of any human intervention in any decisions which may be taken about such profiling. This is where you inform data subjects of their associated rights as well as the suitable safeguards. Content captured here will update the Template Privacy Notice.

Stakeholder Comms

Employees, contractors and other key stakeholders, e.g. trustees, retirees, are individuals directly involved in the organization. Each of these groups likely processes personal data on behalf of the organization and are often data subjects themselves. One key way you and your entire organization demonstrates privacy compliance and Privacy by Design (PbD) awareness and skill is by keeping all employees / stakeholders informed of their data privacy roles and responsibilities.

In the Governance section you would first select the relevant documents that you will share with your employees, contractor workers, and other stakeholders. Once you make sure that your documents are published in the Governance section, you then go to Stakeholders/ Compliance to assign and send documents to employees and other groups, e.g. contractors, etc.

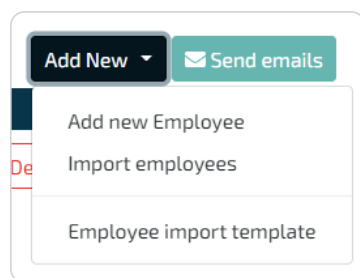
DPDx / DPDx DEMO ▼
[Stakeholders](#) / [Compliance](#)

Go to the Compliance section.

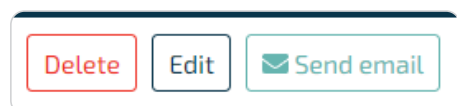
First name	Last name	Job title	Email address
Timmy	Thomas	None	timmyt@geemail.com

NOTE: You will only be able to select documents that have been set as 'Complete' in the Governance section.

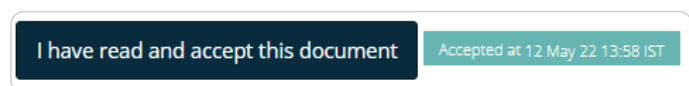
You may add an employee individually or use the template to upload. You may send emails globally, i.e., to everyone, by clicking 'Send emails'...



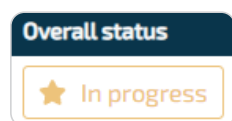
Or you can email individually by clicking 'Send email' next to the employee's name. You can also customise your message to the individuals.



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'.



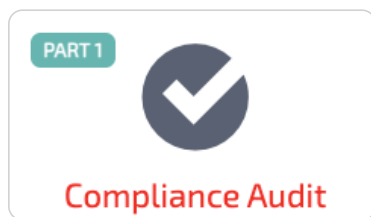
The overall status appears next to each employee name.



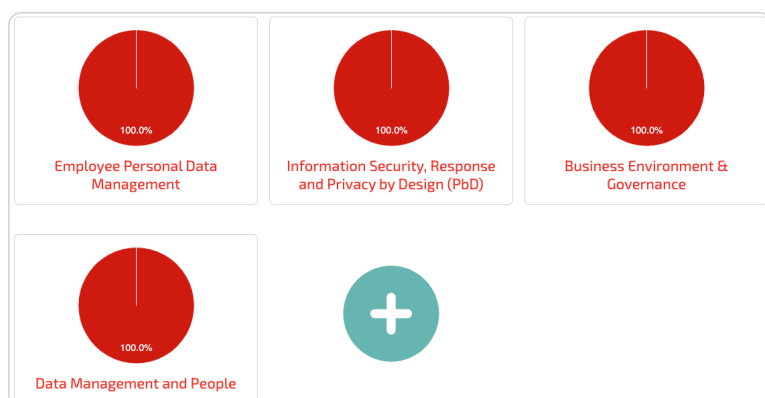
If you click on an employee, you will see the status of each document. A red star means the document has not been sent. An orange star means it has been sent but there is no response. A green star means the employee has accepted the document. Hover over the stars to see the meta-data.

Document	Status
Data Protection Program Announcement	★ Complete
Employee Privacy Notice	★ Complete
POLICY: Working From Home	★ In progress
POLICY: Personal Data Breach	★ Not started

Compliance Audit



Since your organization processes personal data as part of its operations, you should regularly review, assess, and maintain your personal data management and privacy practices. Depending on your organization's structure, you may need to get others involved – the Data Owners, e.g., your HR Manager, Marketing Manager, IT Manager, Sales Manager etc. When you do your initial data mapping you will almost certainly uncover operational risks and issues that you need to mitigate and manage. If these are not covered by the default sections and tasks, you may add your own sections and tasks.



By way of example, let's look at 'Incident Response' which you will find under 'Information Security, Response and Privacy by Design (PbD)'.



A screenshot of the 'Incident Response' checklist interface. It shows a breadcrumb trail: 'Compliance / Information Security, Response and Privacy by Design (PbD) / Incident Response'. Below this, there's a 'Person responsible' field with 'Nalini Indorf Kaplan' and a green plus icon (1). The 'Checklist' tab is active, with a 'Background' tab (2). An 'Expand all' toggle and 'Add New' button (3) are on the right. A checklist item is shown: 'We have working and current incident response plans for personal data breaches.' with radio buttons for 'Low Risk', 'Risk', and 'High Risk' (6). An 'Assign' button with a green plus icon (4) is at the bottom left. At the bottom right, there are five colored circles representing progress: red (5), red with a checkmark, yellow, grey, and teal.



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. Click to 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, if appropriate, after you set your Status (in 5.).

We have working and current incident response plans for **personal data breaches**. [Add tag](#)

☐ Low Risk
 ☐ Risk
 ☒ High Risk

Notes




Oct 20, 2022 15:16   - Status updated: In progress

Oct 20, 2022 15:16 N   - Assigned to: N Compliance

[Add note](#)

Files

[Add file](#)

N Compliance 
 Due 2022-10-27  Review every Select 
[Remove](#) [Set for all](#)

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.

When you change the status of the item, assign it to someone or add notes and files, the system will enter a log with a data and time stamp of each entry.

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.

Monitoring Compliance

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.

Download the report in PDF or Excel format. It's good practice to regularly run and print the full report.

PART 2



Compliance Monitor

Please select the items you wish to include in the report

Sections	Status	Compliance
<input type="radio"/> all	<input type="radio"/> all	<input type="radio"/> all
<input type="radio"/> Organization Features	<input type="radio"/> Only incomplete	<input checked="" type="checkbox"/> CIS 8.0 IG1
<input type="radio"/> Organization Setup	<input checked="" type="checkbox"/> Complete	<input checked="" type="checkbox"/> CIS 8.0 IG2
<input type="radio"/> Data Mapping	<input checked="" type="checkbox"/> In progress	<input checked="" type="checkbox"/> CIS 8.0 IG3
<input type="radio"/> Governance	<input checked="" type="checkbox"/> Not started	<input checked="" type="checkbox"/> Employee Personal Data Management
<input type="radio"/> Stakeholders	<input checked="" type="checkbox"/> N/A	<input checked="" type="checkbox"/> Information Security, Response and Privacy by Design (PbD)
<input checked="" type="checkbox"/> Compliance		<input checked="" type="checkbox"/> Business Environment & Governance
<input type="radio"/> Service Providers		<input checked="" type="checkbox"/> Data Management and People
<input type="radio"/> Data Sharing		<input checked="" type="checkbox"/> ISO 27001 Control Objectives
		<input checked="" type="checkbox"/> PCI DSS Requirements v3.2.1

Tasks

☐ Filter by review due date

☐ Show overdue reviews

Notes

☒ Show Notes

Load report

Load report **Download**

Download PDF

Download Excel

DPDx D

Here's a sample from a report that you may download as either a PDF or as an Excel spreadsheet.

DPDx DEMO - Compliance overview

Compliance status

Employee Personal Data Management

8.7% complete

Not started

In progress

N/A

Complete

HR Data - Recruitment

High Risk

1. We only collect and use any sensitive personal data for specific recruiting-related purpose. We do this with a clear lawful basis. **Not started**

Medium Risk

1. We ensure all applicants are aware of what personal data we collect, how we use it and how we protect it. **Not started**

2. We collect and use personal data in recruiting only for processing the job application. **Not started**

Service Providers



A Service Provider (Processor) is a person/organization that processes personal data on your behalf, under contract. They cannot use the personal data for their own purposes. An example would be a company that does payroll processing on behalf of your company.

Copy Processor from Template ▾

Add New ▾

Contract

Processor - SC

Signed contrac

↑ Upload

Add New

Import processors

Processor import template

Privacy regulations and laws do not generally say who must draw up the contract, only that the Controller (your organization) must ensure that the written contract stipulates the appropriate security measures that the Service Provider / Processor must establish and maintain. You might well find that some Service Providers / Processors already have the relevant contract *template*.

Legal Basis	Contract Status	Contract
	<div><div>2</div><div></div><div></div><div>✓</div></div>	<div>Processor - SCCs</div> <div>Signed contract</div> <div>↑ Upload</div> <div>1</div> <div>Edit</div> <div>Delete</div>
46(2)(c) or 46(2)(d)- Standard approved EU data transfer contractual clauses	<div><div></div><div></div><div>✓</div></div>	<div>3</div> <div>SCCs - Exports ex EEA</div> <div>Signed contract</div> <div>↑ Upload</div> <div>4</div> <div>Edit</div> <div>Delete</div>

Edit the form (1) by completing the contact details, the contract start and end date. Set the status and Save the form. The status will display here (2), Once you have the signed contract or DPA, upload it here (4)

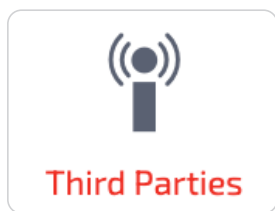
You would have noticed that there is nothing under Lawful basis for our first Service Provider (Processor). That's because, in this example, they are based within the EU. However, the lawful basis in the second example (3) is 'SCCs – Exports ex EEA'. The link (3) takes you to the EDPB site that has the standard contractual clauses. will display a suggested template for BCRs. What is this about? – **it's important for you to understand Chapter V of GDPR** (or the relevant section in your Data Privacy or Protection law or regulation dealing with international transfers)

New feature – when you Edit a Service Provider you may now add Notes and Files to every Service Provider.

Details

Notes and files

Third Parties (Data Sharing)



Unlike the 'sharing' of personal data between Controller and Processor (which is under written contract), here we speak of the sharing (or, disclosure) of personal data between *Controllers*. An example might be the organization providing medical insurance to your employees. In most cases there should already be some sort of agreement acknowledged between the two organization. Simply upload a copy and set the status to Signed.

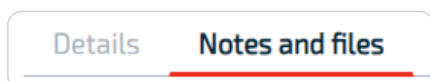
The functionality within the app is identical to the Service Provider section, except that the external links are relevant to controller-to-controller relationships.

It might help to look at a simple example.

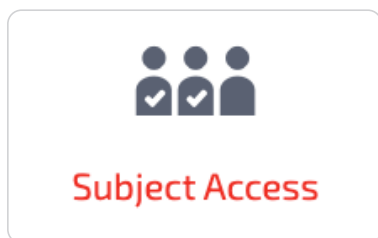
Let's say that a travel agent makes bookings on behalf of its clients with an airline and hotel chain. It's unlikely that the hotel chain and airline would be considered Processors. They are Controllers in their own right. But what if the three companies got together to develop a system or app that would be of value to ALL their clients? Now we're talking of *further* processing that brings about a **JOINT** sharing relationship – and will almost definitely require data subjects' consent. In fact, all the other Conditions (principles) come into play. It's important the data subject knows who to approach.

A more sophisticated and potentially, more-risky scenario of personal data sharing will be that of the world of data brokers.

New feature – when you Edit a Controller you may now add Notes and Files to every Controller.



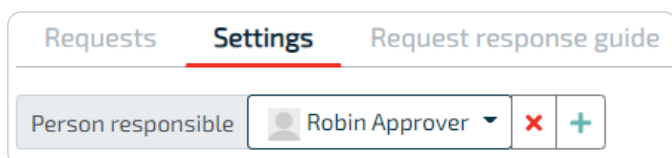
Subject Access - Data Subject Access Requests



There are several reasons why individuals might want to gain access to their personal data and several ways in which they can make these requests for access. Equally, there are several different responses that could come from your organization.

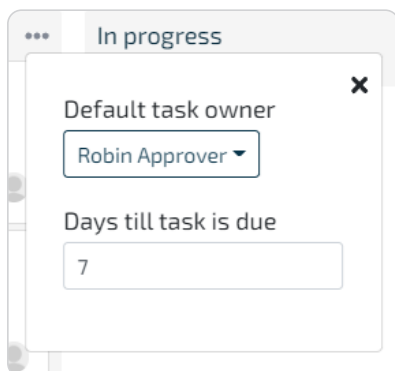
DataProtection DynamiX provides requesters with an online link and allows you to receive or capture the requests, delegate them as appropriate, navigate and understand the rules and gain oversight of progress via a dashboard.

Settings



Click Settings and set the 'Person responsible' for receiving online requests. If not in the drop-down, click the green cross to add new persons. The 'Person responsible' **must set the Notification Preference to be notified** when an online subject access request is received. To do this, click the drop-down under the username in the top right corner.

The 'Received' and 'In progress' sections have 3 dots. Set the default task owner and the number of days within which the default task owner must respond.



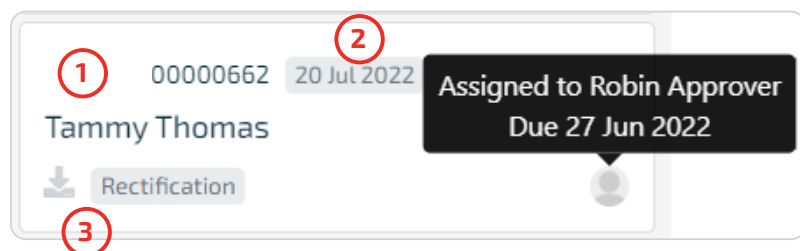
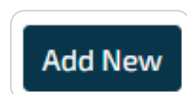
Online subject access request form

Still under Settings – ask your web developer to embed the code behind a link on your website – name it something relevant like 'Subject Access Requests'. Add the domains from where you will be calling this link. Click 'Preview' to see how it will present to the requester.

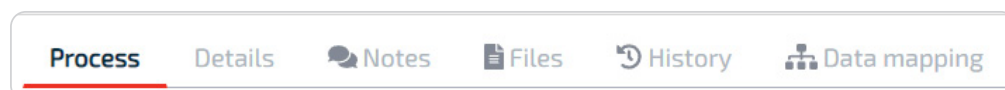
Requests



Online requests are auto-received here. You may add requests manually by clicking Add New

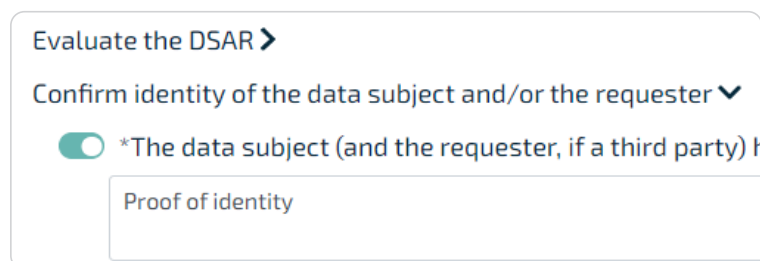


Looking at the panel above, we can see the automatically assigned reference number (1), the due date (2) and the download button, (3)



Click a panel to enter. When you click on Process you will notice the 3 stages – **Received, In Progress, and Complete.**

Received



Evaluate the DSAR as there may be reasons why you wish to reject it. If it's a legitimate request, indicate how you have proven the identity of the requester. As soon as you tab out of that field, the Move to In Progress button is revealed.

In progress

Process Details Notes Files History **Data mapping**

If your data mapping is accurate and current, it should give you clear indication of where to search. If you think any of the data mapping appears vague, inform your privacy manager. For example, if a processing location suggested 'Application Server', it might be useful to name the application instead.

Once you have all the data to support your decision, step through the rules. Any rule with a star * is mandatory. Hover over the text to see supporting information. The blue text indicates the request is successful and the red text means it has failed.

Rectification ▼



***Where practical, we have informed all recipients of the personal data of the rectification subject about those recipients. See below for details**

Where practical, we have informed all recipients of the personal data of the rectification request.

2022-06-24



The personal data will not be rectified. It is either accurate as it stands or there is a legal i

If you have followed the steps correctly, you'll be able to move the request to the Complete column.

Move to Complete →

Breach Management



Incident Response & Management

A personal data breach could lead to the accidental or unlawful use, destruction, loss, alteration, or disclosure of that information – in other words, a breach. A breach, not appropriately responded to, could result in physical, material, or non-material stress to data subjects and could well have a financial and/or reputational impact on your organization.

A Controller must inform the Authority / Regulator as soon as reasonably possible after becoming aware of a security compromise. The Controller also needs to communicate with data subjects, especially where the exposure presents a high-risk to them. They should also consider the possibility that law enforcement authorities may need to be involved e.g., where there are safety concerns or perhaps, where early disclosure to data subjects could hamper investigations.

Use this section to capture and manage your responses to any incidents as well as communications with the Authority / Regulator and data subjects. Ensure that your Service Providers / Processors have a similar process in place. Doing table-top exercises fosters good practice that keeps the relevant staff aware of the processes involved in breach response management. Print those documents as evidence of training and then remove the incidents so that they don't obscure your dashboard.

Status	Documents
<div><div>✓</div><div></div><div></div></div>	<div>Letter to Supervisory Authority</div> <div>↓ Download</div> <div>Subject notification</div> <div>↓ Download</div> <div>Incident</div> <div>↓ Download</div> <div>Edit</div> <div>Delete</div>
<div>Reported</div> <div><div>✓</div><div></div><div></div></div>	<div>Incident</div> <div>↓ Download</div> <div>Edit</div> <div>Delete</div>

In the above example we have two types – the first where the incident was contained, there was no need to report it and we only needed the incident report. The second is where it had to be reported to both the Regulator and the data subjects impacted – in some cases you may be prevented from informing the data subjects.

Click Add New

Add New

Read the Introduction, followed by some background into Containment & Recovery.

Fill in the details required for the Incident title, followed by the Incident details.

Next, we're at the Risk Assessment step.

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

What measures are in place to contain the incident?

These are the measures that were in place.

Move to the final step which is the Incident evaluation and response. Clicking 'Finish' takes you back to the register and you will notice that it is only the Incident Report that is produced.

However, if the incident *hasn't* been contained you will move through the steps until you get Notification to the Authority / Regulator. Here you will find all the content which is based on your prior input. Use this information in your engagement with the Authority.

The next page is the content based on your prior input and should inform your communications with those data subjects who may be affected by the incident.

NOTE: Law enforcement – If you had selected this item under the Risk Assessment, the content you would normally use to communicate with data subjects will not be displayed.

☐ Law enforcement prevents you from informing the **data subjects** involved

Privacy Impact Assessment



Conducting a Privacy Impact Assessment (PIA), also called a Data Protection Impact Assessment (DPIA) in some jurisdictions, is a legal requirement to help meet privacy and data protection expectations of customers, employees, and other stakeholders. A PIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project. This section allows you to identify why a PIA is relevant for this project.

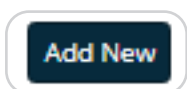
A PIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to individuals' resulting from the processing of personal data, by assessing them and determining the measures to address them. PIAs are important tools for accountability, as they help a controller to demonstrate that appropriate measures will be or have been taken to ensure compliance with applicable data privacy and protection laws, e.g. CPRA, CPA, GDPR, etc.

The EU's new Transfer Impact Assessment workflow is being added to the PIA procedure and this document will be updated accordingly.

Some examples of where a DPIA may be required:

- A hospital processing its patients' genetic and health data
- The use of a camera system to monitor driving behavior on highways. The data controller wants to use an intelligent video analysis system to single out cars and automatically recognize license plates
- A company monitoring its employees' activities, including the monitoring of the employees' workstation, internet activity, etc
- The gathering of public social media profiles data to be used by private companies generating profiles for contact directories
- In some instances where the processing might require prior consultation with the Regulator

Click:



Enter the PIA Name, Description and Project due date. Click **Save**.

Overview

PIA Name

Project due date

2022-11-19

Project status

Draft

Description of assessment

PIA owner

+

Reviewers

Reviewers

+

Approvers

Approver

+

Save

Cancel

The Project owner is *usually* the person compiling and editing the PIA.

Select the **Reviewer(s)** or add any not in the drop-down list (click the green cross). Reviewers can only be Compliance Users or Task Owners.

Select the **Approver(s)**. Approvers must be Administrator type users.

The DPO's comments in the PIA will be recorded as such. Indicate which user is the DPO under Organization /Users.

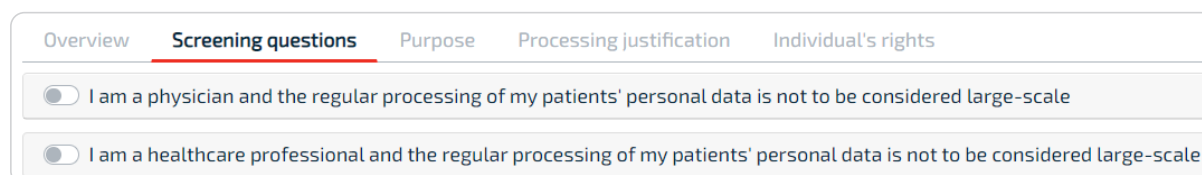


Active

Is DPO

Screening Questions

By selecting an option under screening questions, you're suggesting that a PIA is not relevant or required. The rest of the PIA falls away. However, you still need to submit it for approval.

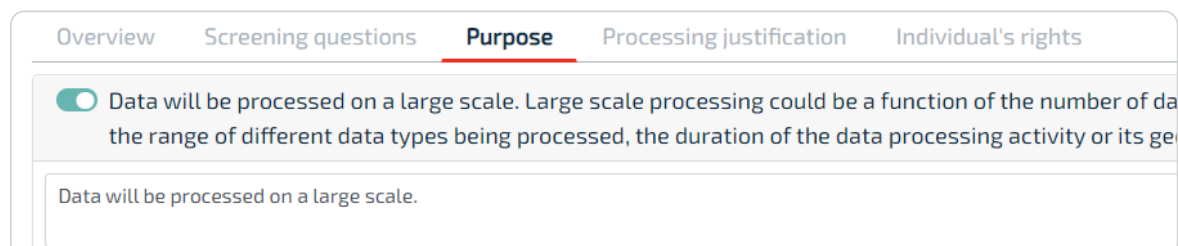


Overview **Screening questions** Purpose Processing justification Individual's rights

☐ 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

Purpose



Overview Screening questions **Purpose** Processing justification Individual's rights

☒ Data will be processed on a large scale. Large scale processing could be a function of the number of data subjects, the range of different data types being processed, the duration of the data processing activity or its geographical scope.

Data will be processed on a large scale.

In this section, you indicate why the PIA is relevant to this project or planned processing of personal data. Add comments or upload documents by clicking 'Notes and Files'. You may add your own reason for conducting a DPIA.

Processing justification

Overview	Screening questions	Purpose	Processing justification	Individual's rights
Department	Data subject type	Processing purpose	Legal basis	
Department ▾ +	Data subject type ▾ +	Processing purpose ▾ +	Legal basis ▾	
Human Resources	Employees / Prospective Employees	Employee monitoring	6(1)(a) - we have the data subject's consent	

Select the relevant department / data subject type / processing purpose and legal basis. Then click **Save**.

Save	Cancel
Edit	Delete

In the next panel, complete the mandatory fields (highlighted in red), enter the relevant personal data types, add any notes and files, and then click Close.

Legal basis	Personal data types	Special category data types	Notes and files
--------------------	---------------------	-----------------------------	-----------------

Individual's rights

Overview	Screening questions	Purpose	Processing justification	Individual's rights
<input type="checkbox"/> Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)?				
<input type="checkbox"/> Are the data accurate and kept up to date?				

This section concerns data subjects' rights and **how those rights will be protected**. Once you have completed this section, you're now ready to submit the PIA for Review (first) and for Approval (last). The reviewer and approver will receive notifications informing them of the task. After inserting their comments, the reviewer may return the PIA for improvement or the Approver can approve the sections.

Submit for review ▾	Submit for approval ▾
---------------------	-----------------------

Risks and Mitigations

This then reveals the Risks and mitigations tab to the PIA owner.

Overview	Screening questions ✓	Purpose ✓	Processing justification ✓	Individual's rights ✓	Risks and mitigations Limited ✓
Description	Risk type	Impact to individuals	Risk Likelihood		
<input type="text"/>	<input type="text" value="Risk type"/>	<input type="text" value="Impact to individuals"/>	<input type="text" value="Risk Likelihood"/>		
Risk One	Illegitimate access	Minimal	Remote		

The PIA owner will then add a relevant risk and click Save.

Description	Risk type	Impact to individuals	Risk Likelihood
<input type="text" value="Risk Two"/>	<input type="text" value="Unwanted modification"/>	<input type="text" value="Significant"/>	<input type="text" value="Possible"/>

Then add an associated mitigation.

NOTE: If a mitigation has been added, it cannot be edited – it must be deleted and then replaced by the correct mitigation.

Overview	Mitigations	Notes and files
Measure	Effect	Phase
<input type="text" value="aaa"/>	<input type="text" value="Acceptable"/>	<input type="text" value="Existing"/>

When all risks and mitigations are captured, submit the PIA for approval.

Overview	Screening questions ✓	Purpose ✓	Processing justification ✓	Individual's rights ✓	Risks and mitigations Limited ✓	Approval ✓
<input type="checkbox"/> Does this DPIA require changes to be made to compliance documentation or data mapping ?						
<input type="checkbox"/> Residual risks remain high and we are consulting with our supervisory authority						
<input type="checkbox"/> Even though we did not consult the Supervisory authority they require a copy of the DPIA and we have submitted it.						

Final Approval

Approve each risk individually by clicking Approve to the right. Click Close and return to the main approval page.

Maximum	Approval
---------	----------

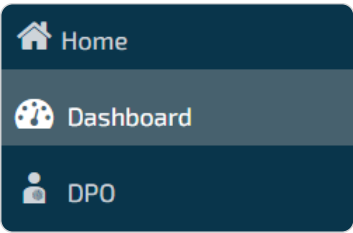
Then approve the risks overall by adding comments and the approval at the bottom of the page and submit to the owner.

To correct	Needs improving	Approved ✓
------------	-----------------	-------------------

There are 2 possible outcomes after final approval. The owner could move the PIA to Complete where those identified risks must be incorporated into your projects risk management framework. Or move it to the Submitted column where engagement with the Authority / Regulator is necessary.

Dashboard

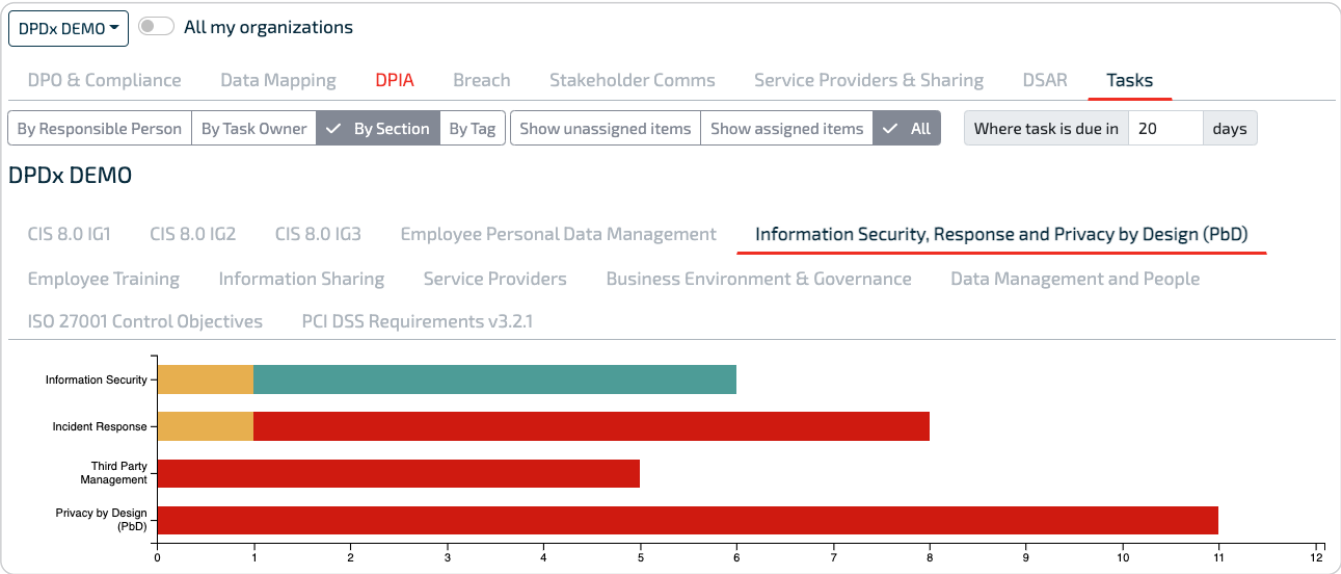
Find the dashboard icon in the sidebar.



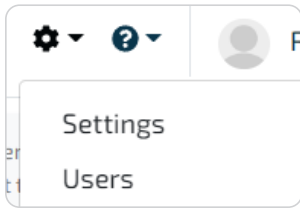
You may view across the various sections.



When you view tasks by task owner, click on the task owner to see which tasks have been assigned to the task owner.



User Maintenance



Add and manage users under Users. Click on the gear icon and select Users.

There are three roles:

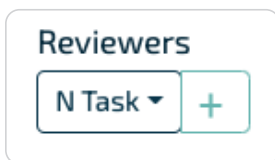
Administrator – has all access

Compliance User – will have access to the assigned compliance sections.

Task Owner – will have access to assigned tasks.

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

Typically, you would add your Compliance User or Task Owner within the Compliance Audit module or other specific area such as Privacy Impact Assessments. Click on the green plus sign to display the new user screen.

A screenshot of the 'New user' form. The form has a title 'New user' and three input fields: 'First name', 'Last name', and 'Email address'. The 'First name' field is highlighted with a blue border. At the bottom right, there are 'Save' and 'Cancel' buttons.

You may assign more than one person to an item or role, e.g. review, approval.

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.

Glossary

access

the right, the opportunity or the means of finding, using or retrieving information or data.

accountability

the condition that individuals, organizations and the community are responsible for their actions and may be required to explain them to others.

affirmative authorization-CCPA

an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer's personal information in accordance with the methods set forth in section 999.330. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

aggregate consumer information-CCPA

information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. Aggregate consumer information does not mean one or more individual consumer records that have been deidentified.

anonymous

process or data state that cannot be attributed to a specific identified or identifiable natural person.

anonymous information

information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.

anti-malware

software that is designed to identify and prevent malicious software, or malware, from infecting computer systems or electronic devices.

anti-virus

software designed to detect and destroy computer viruses.

Attorney General

The chief law officer and legal counsel of the government of a state or nation. Each US State elects its own Attorney General (AG). In some US states, the AG is the supervisory authority and enforces state data privacy statutes and regulations.

authorized agent-CCPA

a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.

automated decision making

decisions made by machine (computers), without human intervention. For example, to automatically accept or deny an online credit application or the automated processing of CVs that evaluates (profiles) personal aspects of individuals to determine if they will qualify for a position.

availability

the guarantee of reliable access to information by authorized people.

binding corporate rules

personal information processing policies, within a corporate group, which are adhered to by a responsible party or operator within that group when transferring personal information to a responsible party or operator within that same group in a foreign country.

biometric data-CCPA

an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

breach

a breach means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

business-CCPA

a legal entity that is organized or operated for the profit or financial benefit, collects consumers' personal information and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and (a) has annual gross revenues in excess of twenty-five million dollars (USD 25,000,000), (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices, OR (c) derives 50 percent or more of its annual revenues from selling consumers' personal information. Business also means any entity that controls or is controlled by a business as defined above and that shares common branding with the business. Common branding means a shared name, service mark, or trademark.

business purpose-CCPA

the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

categories of sources-CCPA

types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

categories of third parties-CCPA

types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

CCPA

the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 et seq.

child

a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

child-GDPR

per the GDPR, parental consent is required for children below 16 years. Member States may lower this age but not below 13 years.

classification

the process of assigning an appropriate level of classification to an information asset to ensure it receives an adequate level of protection.

collects

collected, or collection means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the data subject, either actively or passively, or by observing the data subject's behavior.

confidentiality

is managed by the set of rules that limits access to information.

consent

of the data subject means, any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

consumer-CCPA

a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

continuity

encompasses planning and preparation to ensure that an organization can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period.

controller

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law or regulation, e.g., US Federal, State or other jurisdiction.

COPPA

the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5.

core activities

the core activities of a controller relate to primary activities and do not relate to the processing of personal data as ancillary activities. An example of an ancillary activity would be a company paying the salaries of its workers. However, the core activity of a hospital is to provide health care and it could not provide healthcare safely and effectively without processing health data, such as patients' health records. Those activities cannot be considered ancillary and must be considered as core

cross-border processing-GDPR

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

data broker-CCPA

a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Data broker does not include any of the following:

- A consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.)
- A financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.
- An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 1791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).

data concerning health

personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

data mapping

the process used to identify what personal information you use, why you use it, how sensitive it is, how long you may retain it, where you process it and where you collect it.

data portability

the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services.

data protection impact assessment

a systematic process for evaluating the potential impact of data processing risks that are likely to affect the data protection rights of individuals.

data subject

the person to whom personal information relates.

de-identified

information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.

delete

the process of eliminating or deleting records beyond any possible reconstruction.

destroy

the process of eliminating or deleting records beyond any possible reconstruction.

direct marketing

to approach a data subject, either in person or by mail or electronic communication, for the purpose of promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject or requesting the data subject to make a donation of any kind for any reason.

disaster recovery

the process or actions for an organization to minimize the effects of a disruptive incident, to continue to operate or quickly resume mission-critical functions.

device

any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

disclosure

the transfer of a responsible party's data subjects' personal information to another responsible party or parties.

DNSMPI

Do Not Sell My Personal Information.

DPIA

data protection impact assessment: systematic process for evaluating the potential impact of data processing risks that are likely to affect the data protection rights of individuals.

electronic communication

means any text, voice, sound, or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

employment benefits

retirement, health, and other benefit programs, services, or products to which individuals and their dependents or their beneficiaries receive access through the individual's employer.

employment-related information-CCPA

personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.

encryption

the process of converting information or data into a code, especially to prevent unauthorized access.

enterprise

a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity .

erasure

the process of eliminating or deleting records beyond any possible reconstruction.

filing system

any structured set of personal information which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. Can be digital or manual system.

financial incentive

a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.

genetic

personal information relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular DNA or RNA analysis.

genetic data

personal information relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Gramm Leach Bliley Act

An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes.

health

personal information related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

health

personal information concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.

health insurance information-CCPA

a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

high-risk

activities including, but not limited to, large scale data processing which could affect a large number of individuals; regular and systematic monitoring; the transfer of personal information to countries which don't have adequate privacy.

Homepage-CCPA

the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, 'About,' 'Information,' or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.135, including, but not limited to, before downloading the application.

household

a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.

identifiers

a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

infer

the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

information owner

an individual that has approved management responsibility for controlling the maintenance, use and security of the personal information; e.g., head of HR; head of Sales etc. Also called data owner.

Information Regulator

the Data Protection, Privacy or Consumer Regulator established in statutes and regulations in a jurisdiction.

integrity

the assurance that information is trustworthy and accurate.

international organization

an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

internet activity

including, but not limited to, browsing history, search history, and information regarding a individual's interaction with an internet website, application, or advertisement.

large-scale data processing

examples could include – patient data in the regular course of business by a hospital; travel data of individuals using a city's public transport system (e.g. tracking via travel cards); real time geo-location data of customers of an international fast food chain for statistical purposes by an Operator specialized in these activities; customer data in the regular course of business by an insurance organization or a bank; personal information for behavioral advertising by a search engine; data (content, traffic, location) by telephone or internet service providers.

main establishment-GDPR

- a controller with establishments in more than one EU Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment
- a processor with establishments in more than one EU Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the GDPR.

notice at collection-CCPA

the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in the regulations.

notice of financial incentive-CCPA

the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

notice of right to opt-out-CCPA

the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in the regulations.

operator

a natural or legal person, public authority, agency or other body which processes personal information on behalf of the Responsible Party. Also called Service Provider.

opt in

choose to participate in something.

opt out

choose NOT to participate in something.

person

means a natural person, individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

personal data

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

personal data breach

a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

personal information

information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

personal information impact assessment

a systematic process for evaluating the potential impact of information processing risks that are likely to affect the privacy rights of individuals.

PIA

Privacy Impact Assessment - a systematic process for evaluating the potential impact of processing risks that are likely to affect the privacy rights of individuals.

policies

clear and measurable statements of preferred direction and behavior to condition the decisions made within an organization.

policy

clear and measurable statement of preferred direction and behavior to condition the decisions made within an organization.

portability

the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services.

price or service difference

any difference in the price or rate charged for any goods or services to any individual related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; OR

any difference in the level or quality of any goods or services offered to any individual related to the collection, retention, or sale of personal information, including the denial of goods or services to the individual.

principles

accountability, purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, lawful basis for processing, processing of special category personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by binding corporate rules.

prior authorization

prior authorization that must be obtained prior to any processing of unique identifiers, information on criminal behavior, information for the purposes of credit reporting; the transfer of special personal information or the personal information of children to countries that do not provide an adequate level of protection of processing of personal information.

privacy

the right of a party to maintain control over and confidentiality of information about itself.

Privacy by Design (PbD)

Processes and engineering that ensures respect for privacy and good security is present for the data in question throughout its entire lifecycle, from collection to deletion. PbD also means that you inform your customers, employees and other data subject of your organization's privacy practices.

Privacy Officer

Persons responsible for data privacy or protection vary by title and duties. Some serve as executives internal to an organization; others are external. In the US, an organization may have these roles include Chief Privacy Officer (CPO), Data Protection Officer (DPO), Privacy Program Manager, and other assigned staff.

privacy policy-CCPA

as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information.

process

a set of interrelated or interacting activities that transforms inputs into outputs.

processing

any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

processor

a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

profiling

any form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

pseudonymization

the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

publicly available

information that is lawfully made available from federal, state, or local government records. Publicly available does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

recipient

a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

record

means any recorded information regardless of form or medium.

record of processing activities

information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. This must be completely made available to authorities upon request if subject to certain regulations, e.g., GDPR.

regular and systematic monitoring

examples include - operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g., credit scoring, fraud prevention or detection); location tracking (for example, by mobile apps); loyalty programs; behavioral advertising; fitness and health data via wearable devices; CCTV; connected devices.

re-identify

in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

relevant and reasoned objection-GDPR

an objection to a draft decision as to whether there is an infringement of the GDPR, or whether envisioned action in relation to the controller or processor complies with the GDPR, which clearly demonstrates the significance of the risks posed by the draft decision with regard to the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the European Union.

requester

in relation to a private body means any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body; or a person acting on behalf of the person.

request to know-CCPA

a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115.

Responsible Party

a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

restriction

to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information – for example – temporarily moving the data to another processing system, making the data unavailable to users, or temporarily removing published data from a website.

restriction of processing

the marking of stored personal data with the aim of limiting their processing in the future.

rights

of data subjects, including the right to be informed; to establish whether personal information is being held; to request correction, destruction, or deletion; to object to certain processing; to not be the target of unsolicited direct electronic marketing; to object to profiling; to submit a complaint to the Regulator; to institute civil proceedings.

risk

a threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided or mitigated through pre-emptive action.

ROPA

record of processing activities: information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. This must be completely made available to authorities upon request if subject to certain regulations, e.g., GDPR.

sale-CCPA

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.

security compromise

a compromise of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information transmitted, stored or otherwise processed.

service

work, labor, and services, including services furnished in connection with the sale or repair of goods.

service provider

a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

share

the transfer of a responsible party's data subjects' personal information to another responsible party or parties.

sharing

the transfer of a responsible party's data subjects' personal information to another responsible party or parties.

special personal information

personal information including religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal or biometric information.

technical and organizational measures

internal policies as well as measures which meet the conditions of privacy, inter alia - minimizing the processing of personal information; de-identifying personal information as soon as possible; transparency with regard to the functions and processing of personal information; enabling the data subject to monitor the data processing; using Operators who provide the appropriate guarantees; ensuring the appropriate security measures, including confidentiality; maintaining data quality; conducting privacy impact assessments; on-going training and awareness of staff.

third party

in relation to a request for access to a record of a private body means any person (including, but not limited to, a public body) other than the requester.

third party-CCPA

a person who is NOT any of the following: the business that collects personal information from consumers under the CCPA; a person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract. HINT: see the CCPA for further conditions relating to contracts.

track

creating, capturing and maintaining information about the movement and use of records.

tracking

creating, capturing and maintaining information about the movement and use of records.

unique identifier

means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

unique personal identifier-CCPA

means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

value-CCPA

of the consumer's data means the value provided to the business by the consumer's data as calculated under section 999.337.

verifiable consumer request-CCPA

a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.

verify-CCPA

to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian.