cassie

Path to Compliance

An overview

STEP .1
Establishment

Create an actionable plan, draft a strategy, understand privacy laws, review privacy notices and governance as well as individuals' rights.

MORE DETAIL

STEP .2
Data Identification

Create a central inventory of data flow and processes.

MORE DETAIL

STEP .3
Data Processing

Introduce a centralized DPIA process and work-flow.

MORE DETAIL

STEP .4
Cookies

Ensure that your first interaction with your customers and prospects is compliant.

MORE DETAIL

STEP .5
Consent Collection

Consent and Preference Management data collection.

MORE DETAIL

STEP .6
Transparency

Data Subject Portal, Offline integration with your customer service teams and Data Subject Access Requests.

MORE DETAIL

STEP .7
Regulation

Audit and Reporting.

MORE DETAIL

STEP .1
Establishment

1.1

Create an actionable plan.

Preparation and making a plan are the keys to achieving compliance.

1.2

Establish privacy governance by drafting a strategy, forming a team and building awareness.

Accountability is one of the data protection principles: it makes you responsible for complying with the relevant data privacy legislation and says that you must be able to demonstrate your compliance.

1.3

Understand the individual privacy laws that affect your organizations. This is determined by customers' location, not the business.

Syrenis have partnered with leading Data Privacy Practices globally. Having local experts in key territories enables you to be abreast of legislation local to you and your customers.

1.4

Carry out review on privacy notices and governance, identify gaps and update to relevant compliance legislations.

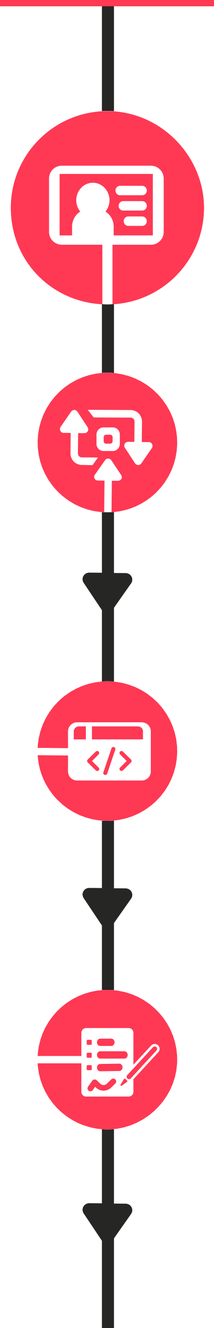
You must review the measures you implement at appropriate intervals to ensure that they remain effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data, or the types of information that you collect, you should review and update your measures frequently, and document what you do and why.

1.5

Make sure procedures cover all individuals rights, including what data you can and cannot keep and how long you can keep it.

Accountability is not just about being answerable to a regulator; you must also demonstrate your compliance to individuals.

Individuals have the right to be informed about what personal data you collect, why you use it, how long you hold this for and who you share it with.



STEP .2
Data Identification

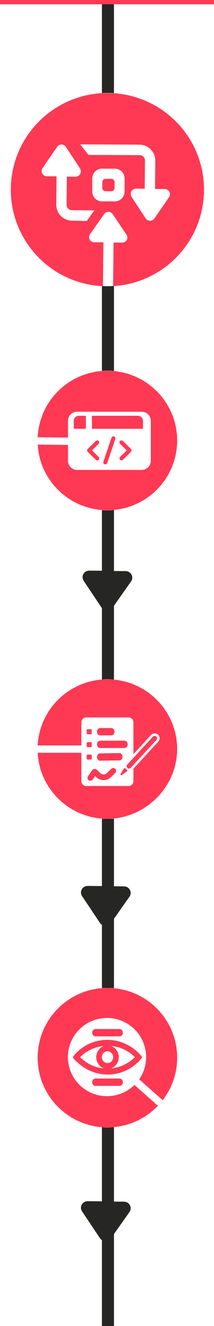
Create a central inventory of data flow and processes.

To comply with legislations and to have good governance, it is important to identify all areas of your business that store and process PII (Personally Identifiable Information). This inventory of data and processing will be key to later stages of the compliance project.

Whilst producing an audit is required for your records, it is more important to tie the actual processing activity to your data. Most solutions allow you to document the process but don't verify the process.

Cassie's RoPA (Records of Processing Activities) module allows clients to produce an inventory of PII and the processes. Critically though, these processes are tied to the actual data processing. All Cassie's data collection points integrate into RoPA providing a real-time view of your data.

ROPA



STEP .3
Data Processing

Introduce a centralized DPIA process and workflow.

Alongside the identification of processing activities, each time data is being processed, a Data Processing Impact Assessment (DPIA) must be undertaken. Globally there are differing requirements for this process. Once this workflow process has been undertaken and agreed, the DPIA should be associated with the processing activities.

Cassie firstly allows you to define the Impact Assessment workflow and then attach that agreed process to the data processing activities throughout the solution.

DPIA Module

STEP .4
Cookies

Ensure that your first interaction with your customers and prospects is compliant.

Regulation requires website owners to gain consent before the pre-loading of cookies. This consent should be available at a granular level and include other tracking technology such as beacons and pixel tracking.

Cassie is designed to manage the complete consent journey of your data subjects from their first anonymous visit to your website.

The Cassie Cookie Module manages how your business can implement a compliant Cookie Banner to manage the consent prior to loading any cookies.

Cookie Management

STEP .5
Consent Collection

Consent and Preference Management data collection.

Cassie is designed to manage the PII and Consent and Preferences that are collected by an organization across their entire eco system. Cassie consolidates this into a singular virtual record of the truth but with the added advantage that every change to this information is captured in real time also.

Cassie then plays a pivotal role in supplying this data to all other systems that need that data. This includes CRM, Marketing platforms and e-mail providers, etc. The Cassie Connector service manages all of this centrally and within the control of our clients.

Cassie CMP | Connector Service | API

STEP .6
Transparency

1.1

Data Subject Portal.

Ensure your customers have full control of their data by creating a Public Portal, this will further the compliance journey and enable you to create brand trust through consent.

Cassie's Public Portal allows your customers to manage their own preferences in a dedicated portal in real time. The Cassie Public Portal is fully customisable with your CSS skins, creating a consistent brand experience.

Preference Centre

1.2

Offline integration with your customer service teams.

Real-time management of information and preferences for internal teams is integral when picking an auditable CPM solution. Considering how the solution will integrate with your current CRM systems is just as crucial.

Adding the Customer Service Portal to the Cassie platform will allow you to reduce the risk of data exposure or overwriting by configuring it to your requirements. Cassie's advanced integrations with your CRM systems will ensure your siloed databases are accurate and in sync in real time.

Customer Service Portal

1.3

Data Subject Access Requests.

Global regulations grant individuals the right to access their personal information from organisations so they can understand what data is held and how it's used, for lawful processing.

With Cassie you can manage DSARs and consolidate all consumer requests into one centralised portal. Easily manage and process requests from multiple regions and deliver personal information efficiently to your data subjects.

DSARs

STEP .7
Regulation

Audit and Reporting.

Compliance Data Protection audits are prevalent in the current security threat landscape. With the everchanging regulatory privacy laws and industry standards becoming more complex, audit and reporting can be the most challenging part of compliance.

Our consent management platform enables your customers to update their data in real time, granting your organisation the benefit of a live, transparent audit history. Consequently, any Subject Access Requests can quickly be addressed in line with Privacy Law requirements.

Book a discovery call:

- We want to understand your company and its structure.
- We want to understand how you currently manage your consent and preferences, and what challenges you face.
- We want to understand your goals around consent management and preferences.
- We want to show you how Cassie can help.

Contact details:

Igor Lopez
Head of Sales

Igor.Lopez@trustcassie.com

UK
Freephone 0800 368 7842
or +44 20 4551 9501

USA/Canada
(Toll-Free) +1 844 585 6264

cassie