

# GDPR Compliance

## What Is the [GDPR](#)?

The General Data Protection Regulation ([GDPR](#)) is one of the biggest legislative changes made since 1975. To be effective from May 25, 2018, the primary goal of these changes is protection of personal data and rights of EU residents.

## Our Commitment toward [GDPR](#)

We are fully committed to upholding the privacy and rights of our customers and their customers. The essence of the [GDPR](#) is in direct alignment with our core values of customer trust and data privacy. With that in mind, we are actively working toward defining our road map for [GDPR](#) to overhaul our systems and processes in accordance with the standards. We are committed to achieving [GDPR Compliance](#) well before the May 25, 2018 deadline.

## How Are We Preparing for [GDPR](#)?

Over the last 18 months, we have made steady progress toward understanding and analyzing how [GDPR](#) will impact our customers. This was made possible with the help of a focused group comprising of experts on Corporate [Security](#) and [Compliance](#), and members from our senior leadership. Here's a glimpse of our analysis and the steps we are undertaking to ensure [Compliance](#):

### Establishing the Governance Structure

- Start the [GDPR Compliance](#) initiative with a dedicated focus group. - Completed
- Create a comprehensive Privacy Management Framework that incorporates 130+ best practices and organizational measures, divided into 13 data privacy management categories. - Completed
- Appoint a Data Protection Officer/Official (DPO) in an independent role. - Completed
- Conduct an assessment on product and business impact. - Completed
- Initiate the internal Privacy and [Security](#) Awareness program. - Completed
- Conduct Data Protection Impact Assessment (DPIA) (Internal). - Completed
- Conduct Data Protection Impact Assessment (External). - Completed
- Implementing Policies and Procedures
  - Data Protection Policy - Completed
  - Change Privacy Policy - Completed, to be published soon
  - Change Terms and Conditions - Completed, to be published soon
  - Data Protection and Information [Security](#) Policy - Completed, to be published soon
  - Data Breach and Incident Response Plan - Completed
- Risk management framework to assess and manage threats across the organization and real-time personal data - Completed
- Embedding of personal data protection requirements within contracts and agreements with third-party service providers - Completed
- Customer-facing Data Protection Addendum (DPA) - Completed, to be published soon
- Third-Party Supplier Data Protection Addendum (DPA) - Completed, to be published soon
- Embedding and Implementing Data Privacy into Operations
- Prepare a detailed inventory of data and data-flows within our systems - Completed
- Establish procedures and policies to restrict processing of personal data - Completed
- Set up mechanisms to automatically track flow of all data within and outside our systems - In Progress
- Information [Security](#) and Privacy [Compliance](#) Certifications

**We are on course to attaining following certifications to ensure [GDPR](#) preparedness:**

BS 10012:2017 Personal Information Management System [PIMS] & [GDPR](#) Regulation [Compliance](#): - BS

10012 helps organizations in managing risks to the privacy of personal data and implementing necessary policies, procedures, and controls to help ensure [Compliance](#) with data protection legislation.

ISO 27001:2013 Information [Security](#) management systems [ISMS]: ISMS ensures a systematic approach to managing sensitive company information so that it remains [secure](#). ISMS includes people, processes, and IT systems by applying a risk management process.

### **Existing Product Features Geared toward [GDPR Compliance](#)**

We take utmost care to ensure that our customer data is [secure](#) and easily accessible. While we are constantly working toward enhancing our [Security](#) parameters under the [GDPR](#) guidelines, Centralpoint includes the following out-of-the-box [capabilities](#) geared toward protecting personal data and privacy:

Anonymize IP address: By default, Oxcyon/Centralpoint never captures the full IP address of any of the visitors on your website. The last octet of the IP addresses is deleted to ensure that these are rendered completely anonymous.

Consent: Web Push Notifications already require website visitors to give explicit consent by turning on the browser-level permission.

Subscriber data: After accepting to receive notifications, the push notification service of the browser creates a randomly generated ID for the subscriber. This ID cannot be used to identify a particular individual.

New additions:

Privacy settings: We have added a new privacy settings page inside every Oxcyon/Centralpoint account which gives you full control over your account access. Read more about it [here](#).

Granular control over the subscriber data collected.

Enable subscribers to exercise their rights with regards to their personal information stored by you on Oxcyon/Centralpoint servers:

Right to access personal information

Right to get (any) personal information deleted

Right to withdraw consent

Opt-in: You can now enable consent for website activity tracking on the opt-in form. Read more about it [here](#)

### **FAQs**

#### **When is the [GDPR](#) coming into effect?**

The [GDPR](#) was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two-year transition period and, unlike a Directive, it does not require any enabling legislation to be passed by the government; meaning it will be effective from May 25, 2018.

#### **Whom does the [GDPR](#) affect?**

The [GDPR](#) applies not only to organizations located within the EU but also to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the location of the companies.

#### **What is the difference between a data processor and a data controller?**

A controller is an entity that determines the purposes, conditions, and means of processing of personal data, while a processor is an entity that processes personal data on behalf of the controller.

Where can I know more about the [GDPR](#)?

You can refer to the following links for more information on the [GDPR](#) and how you can prepare for it.