



Centralpoint GDPR Compliance

Our Ongoing Commitment to EU Data Protection

Overview

The General Data Protection Regulation (GDPR) has governed the protection of personal data and the rights of EU residents since it took effect on May 25, 2018. It remains the primary framework we design our systems, contracts, and internal processes around when we handle personal data belonging to EU data subjects, and it continues to inform how we build Centralpoint.

This document is a plain-language summary of our data protection program. It is not a substitute for legal advice — organizations evaluating their own GDPR obligations should consult qualified counsel about their specific processing activities.

Our Commitment to GDPR

Data privacy and customer trust are core to how we operate. We maintain a standing privacy and security program rather than treating GDPR as a one-time project, and we review that program on a recurring basis as regulatory guidance, case law, and our own product evolve.

The European Commission has also proposed changes to GDPR itself. In November 2025, the Commission introduced the Digital Omnibus package, which would adjust several GDPR provisions — including the definition of personal data, breach notification timing, and how cookie consent is governed — alongside changes to the ePrivacy Directive and the AI Act. As of mid-2026 this package is still moving through the European Parliament and Council and has not been adopted. We are tracking it and will update our program if and when it becomes law.

Governance and Organizational Measures

Our data protection program rests on a set of standing organizational controls, established as part of our original GDPR readiness effort and maintained on an ongoing basis since:

Control	Status
Dedicated data protection governance function	Established and maintained
Privacy Management Framework spanning our data privacy management categories	Established; reviewed periodically
Data Protection Officer (DPO) or equivalent designated role	In place — see Assumptions for publication of current contact details
Product and business impact assessments for new processing activities	Ongoing, triggered by new features and integrations
Internal privacy and security awareness training	Ongoing, recurring program
Data Protection Impact Assessments (DPIAs), internal and external-facing	Performed as required for higher-risk processing

Policies and Procedures

The following policies and procedures form the backbone of our compliance posture:

- Data Protection Policy
- Privacy Policy

- Terms and Conditions, including data protection provisions
- Data Protection and Information Security Policy
- Data Breach and Incident Response Plan
- Enterprise risk management framework covering threats to personal data
- Data protection requirements embedded in contracts and agreements with third-party service providers
- Customer-facing Data Protection Addendum (DPA)
- Third-party supplier Data Protection Addendum (DPA)

These documents are reviewed on a recurring cycle and updated when our processing activities, sub-processors, or applicable law change.

Data Privacy in Operations

- A maintained inventory of personal data and data flows across our systems, including a formal Record of Processing Activities (ROPA)
- Documented procedures restricting and governing the processing of personal data
- Ongoing work to automate tracking of data flows within and outside our systems
- Defined data retention schedules tied to the purpose each category of data was collected for

Data Subject Rights

Individuals whose personal data we process have the right to:

- Access the personal data we hold about them
- Correct inaccurate or incomplete personal data
- Request erasure of their personal data (the "right to be forgotten")
- Restrict how their personal data is processed
- Receive their personal data in a portable format
- Object to processing, including for direct marketing
- Withdraw previously given consent at any time
- Not be subject to decisions based solely on automated processing that produce legal or similarly significant effects

Requests to exercise these rights can be submitted through the privacy settings available in every Oxcyon/Centralpoint account, or directly to our Data Protection Officer.

Legal Bases for Processing

We process personal data only where we can point to a valid legal basis under Article 6 of GDPR — most commonly performance of a contract, consent, compliance with a legal obligation, or our legitimate interests in operating and securing the platform, weighed against the rights of the individuals involved.

International Data Transfers

Where personal data moves outside the European Economic Area, we rely primarily on the European Commission's Standard Contractual Clauses (SCCs), supported by transfer impact assessments for the receiving jurisdiction.

Some organizations also rely on the EU-U.S. Data Privacy Framework (DPF) for transfers to certified U.S. entities. That framework's legal footing has come under renewed scrutiny in 2026 following U.S. Supreme Court and EU court proceedings touching the independence of its U.S. oversight mechanisms. We treat SCCs, not the DPF alone, as our primary transfer mechanism, and we are monitoring developments closely given that history — Safe Harbor and Privacy Shield, the DPF's two predecessors, were each invalidated by the Court of Justice of the EU.

Data Breach Notification

We notify the relevant supervisory authority of a qualifying personal data breach within the 72-hour window required by Article 33 of GDPR, and notify affected individuals directly where the breach is likely to result in a high risk to their rights and freedoms. The pending Digital Omnibus proposal would raise the reporting threshold and extend this window to 96 hours; until that change is adopted, we continue to apply the current 72-hour standard.

Information Security and Certifications

Our security program is built around recognized information security management frameworks, including:

- ISO/IEC 27001:2022 — Information Security Management Systems (ISMS). Note: ISO retired the 2013 edition of this standard on October 31, 2025; any certification referenced publicly should point to the current 2022 edition.
- BS 10012:2017 — Personal Information Management System (PIMS), supporting GDPR compliance specifically.

See the Assumptions section below — current certificate numbers, audit dates, and scope statements should be confirmed with our certification bodies before this document is published externally.

Product Features Supporting GDPR

Centralpoint includes the following out-of-the-box capabilities geared toward protecting personal data and privacy:

- IP anonymization — the last octet of a visitor's IP address is dropped by default, so full IP addresses are never captured or stored
- Consent-gated web push notifications, requiring explicit browser-level permission before any subscription is created

- Randomly generated subscriber IDs for push notifications that cannot on their own identify an individual
- An account-level privacy settings page giving administrators full control over account access
- Granular control over which subscriber data is collected
- Built-in workflows for subscribers to exercise their rights to access, delete, or withdraw consent for personal information stored on Oxcyon/Centralpoint servers
- Opt-in consent controls for website activity tracking, configurable directly on the opt-in form

Frequently Asked Questions

Is GDPR still in effect?

Yes. GDPR was adopted by the EU Parliament in April 2016 and has applied directly across EU member states, without national enabling legislation, since May 25, 2018.

Who does GDPR affect?

GDPR applies to any organization processing or holding the personal data of individuals residing in the EU, regardless of where the organization itself is located, if it offers goods or services to those individuals or monitors their behavior.

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

A controller determines the purposes, conditions, and means of processing personal data. A processor processes personal data on the controller's behalf and under its instructions.

Is GDPR changing?

The European Commission's Digital Omnibus proposal, introduced in November 2025, would amend parts of GDPR alongside the ePrivacy Directive and AI Act. It remains under negotiation between the European Parliament and Council as of mid-2026 and is not yet law.

Assumptions

This document summarizes our data protection program at a point in time. Before it is published externally or shared with a customer, the items below should be confirmed:

- Current name and contact details for the designated Data Protection Officer (or equivalent role) for publication
- Current certificate numbers, scope, and audit dates for ISO/IEC 27001:2022 and BS 10012:2017, confirmed directly with the certification bodies
- An up-to-date sub-processor list and the transfer mechanism (SCCs, DPF, or both) in place for each
- Legal review and sign-off by data protection counsel prior to external publication or use in a customer contract
- Confirmation of which product features described here reflect the current release, since product capabilities evolve between releases

Change Tracking and Scope Control

Updates to this document and to the underlying compliance program are logged in Oxcyon's issue management system and tagged to the assigned Production Manager, keeping every revision auditable. The system is available at <https://oxcyoninc.aceproject.com>

Glossary of Terms

Data Controller — The entity that determines the purposes, conditions, and means of processing personal data.

Data Processor — The entity that processes personal data on behalf of, and under instruction from, a data controller.

DPA (Data Protection Addendum) — A contractual document setting out how personal data is protected between two parties — used here for both customer- and supplier-facing relationships.

DPF (EU-U.S. Data Privacy Framework) — A 2023 adequacy mechanism allowing personal data transfers from the EU to self-certified U.S. organizations; successor to the invalidated Privacy Shield and Safe Harbor frameworks.

DPIA (Data Protection Impact Assessment) — A structured assessment of the risk a processing activity poses to individuals' rights, required under GDPR for higher-risk processing.

DPO (Data Protection Officer) — An independent role responsible for overseeing an organization's data protection strategy and compliance with GDPR.

Digital Omnibus — A European Commission legislative proposal, introduced November 2025, that would amend GDPR, the ePrivacy Directive, and other digital regulations; not yet adopted as of mid-2026.

GDPR — The General Data Protection Regulation (EU 2016/679), in effect since May 25, 2018, governing the protection of personal data and the rights of EU residents.

ISMS — Information Security Management System — the systematic approach to managing sensitive information defined by ISO/IEC 27001.

PIMS — Personal Information Management System — the systematic approach to managing personal data defined by BS 10012.

ROPA (Record of Processing Activities) — The documented inventory of what personal data an organization processes, why, and how, required under Article 30 of GDPR.

SCCs (Standard Contractual Clauses) — European Commission-approved contract terms used to lawfully transfer personal data outside the EEA.