

Cloudflare support for ENS compliance — Spain's national security scheme

ENS: Protection for public sector entities

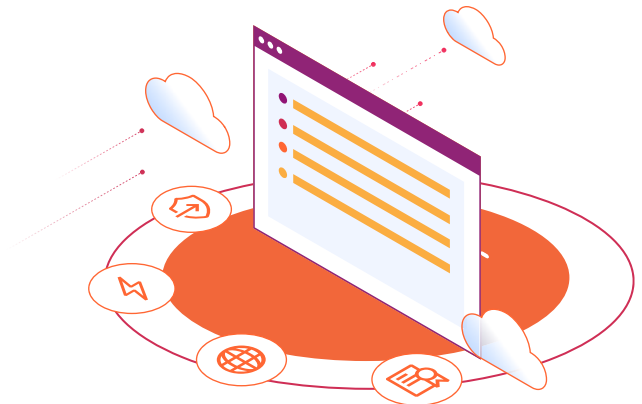
When handling private information, Spanish public sector entities and their IT service providers must comply with Esquema Nacional de Seguridad (ENS). The national security scheme for Spain, established by the Entidad Nacional de Acreditación (ENAC), is based on Royal Decree 311/2022 and provides a framework that establishes the security principles and standards to adequately protect information for Spanish public sector entities.

To receive authorization to process data for Spanish public services — such as governments and public organizations — service providers that process classified information must implement measures to comply with ENS requirements. The framework applies to all public sector entities in Spain as well as private entities and their supply chain partners that provide services to public sector entities.

Cloudflare security measures to support ENS compliance

To support customers who need to comply with ENS, Cloudflare achieved the designation of High accreditation ENS status. Before achieving this accreditation, Cloudflare had already taken steps to comply with other regulations pertaining to the protection of private information. This includes applying security controls across all of our network services:

- Keyless SSL allows customers to store and manage their own private keys, which Cloudflare never sees.
- Geo Key Manager provides customers with granular control over the data centers in which their private keys are stored.
- Payload inspection boundary inspects traffic at the network edge and identifies and routes security threats from any location across the global Cloudflare network.



- Regional Services permits customers to choose where to terminate TLS connections for decrypting encrypted data.
- Customer Metadata Boundary keeps end-user traffic metadata that can identify a customer within the country of origin.



Additional Cloudflare certifications for protecting personal data

- European Union General Data Protection Regulation (GDPR)
- ISO/IEC 27701:2019
- ISO 27001/27002
- Payment Card Industry Data Security Standards (PCI DSS)
- SSAE 18 SOC 2 Type II

Cloudflare validates these certifications annually with third-party auditors. In addition to providing assurance to organizations that transfer sensitive data through Cloudflare services, these certifications help organizations meet their own compliance obligations.

The Cloudflare commitment to privacy

The designation of High accreditation ENS status aligns with the Cloudflare mission to help our customers and their customers work more securely on the Internet. Cloudflare defined this privacy stance long before governments across the globe started regulating privacy. As a privacy-first company, we built our network and our products with data protection in mind.



- We will not sell personal data or track customer end-users across Internet properties.
- We will not profile customer end-users to sell advertisements.
- We retain personal data only as necessary to provide services to customers.

Cloudflare never provides customer encryption keys or a feed of customer content transiting our network to any third party or government. We exhaust all legal remedies before complying with such requests.

In addition, Cloudflare pursues legal remedies to contest any government request for data we identify as subject to protection. We also notify customers of any legal process requesting their information before disclosure of such information.

A global cloud network built on customer trust

Trust is the foundation of Cloudflare's business. We earn customer trust by respecting the sanctity of personal data transiting our network and being transparent about how we handle and secure that data.

Learn more about our policies, technologies, and third-party certifications that make this trust possible at the [Cloudflare Trust Hub](#) or [contact us today](#).