

Trust, Privacy and Digital Sovereignty for Europe

Helping customers meet evolving regulatory requirements with local infrastructure, regulated trust services, strong data protections, and customer control



How DigiCert supports you

We are a global provider of intelligent trust with a strong European presence. For supported European services, we provide region-specific infrastructure and service delivery, business presence and personnel across Europe, locally regulated trust-service operations, and EU/UK/Swiss-compliant data protection and security controls. Our commitment is straightforward: we give our European customers clear information about where their data resides, how and where our services are provided, what safeguards apply, and what additional deployment choices are available when their sovereignty requirements demand greater control.

Our European customers increasingly evaluate technology providers across several dimensions at once: data residency, operational sovereignty, regulated trust, data protection and security. We take responsibility for addressing those requirements through a layered approach to trust, privacy and sovereignty, not through a single claim about where data is hosted. We help you select the right combination of deployment, access and legal controls for your business.

What matters	How DigiCert supports you
Data residency	Regional DigiCert ONE environments and in-Europe storage for supported data.
Operational sovereignty	Agents running in your environment receive trusted identities and secure connections. Before they can operate, their digital signatures and declared software components are verified.
Regulated trust	EU and Swiss qualified trust-service entities under local supervisory regimes.
Data protection & security	GDPR-compliant safeguards, documented TOMs, encryption, access controls and transfer mechanisms.

Data residency

We provide regional DigiCert ONE production environments, including our Netherlands environment at one.nl.digicert.com. When you select a supported regional environment, you can choose regional hosting to support your residency requirements.

For supported European deployments, the region you select determines the location of the production environment. We designed this architecture to give you a concrete regional boundary backed by technical implementation, not just contractual language about location.

Additional control through private CA deployments

Some customers require stronger isolation than regionally hosted SaaS. For those use cases, DigiCert Private CA can support customer-controlled deployment models, including on-premises designs in which you choose the hosting location, key-management architecture, backup destinations and disaster-recovery approach. These models can keep sensitive CA functions and key material within your infrastructure, including highly restricted or disconnected environments when required by the deployment design.

We offer options ranging from regional SaaS to customer-controlled private CA deployment, so you can choose the architecture that best fits the sensitivity, regulatory requirements, and operating model of your workload.

Operational Sovereignty

We maintain registered business presence, offices, infrastructure and specialist teams across Europe. Our platform and qualified trust-service businesses are supported by in-region operations, as part of our global service model.

We operate DigiCert-owned infrastructure and dedicated regional service instances in Europe. Our European teams support sales, validation, fulfilment and trust-service operations. European customers can also receive PKI engineering from personnel located in the region, and EU-based PKI engineers can perform ceremonies on cryptographic assets located in Europe. By maintaining these capabilities in Europe, we reduce dependence on personnel outside the region for activities that may be sovereignty sensitive.

Regulated trust

In Europe, we do more than provide services from the region. Through our qualified trust-service entities, we operate inside European trust-service regulatory frameworks. Our public legal documentation identifies our qualified trust-service entities on the Netherlands and Belgium Trusted Lists, with local supervisory authorities. We also maintain a qualified trust-service presence in Switzerland under Swiss law.

Our qualified trust-service commitments

For the services provided by our Qualified Trust Service Providers (QTSPs), we operate under the requirements of the EU eIDAS framework for qualified trust services, including independent assessment and ongoing audit. Our Netherlands qualified trust-service provider is supervised in the Netherlands, while DigiCert Europe Belgium B.V. is supervised in Belgium. Our public audit materials describe annual qualified-trust-service audits against applicable ETSI standards and eIDAS requirements.

This oversight gives you assurance beyond our own statements: the relevant DigiCert trust services are operated within established European regulatory and independent-audit regimes.

European trust anchors and documented PKI operations

We publish the applicable Certificate Policies and Certification Practice Statements (CP/CPS), PKI Disclosure Statements and related trust-service documentation in our European legal repository. These materials explain how we identify applicants, issue and revoke certificates, protect CA infrastructure, and govern physical, personnel, technical and operational controls.

For customers using our qualified or regionally operated trust services, this provides a documented chain from the service to its governing practices, independent audit regime and supervisory jurisdiction. We make this evidence available so regulated organizations can evaluate our controls directly rather than relying solely on high-level assurances.

Independent assurance you can verify

We submit our certificate-authority and trust-service operations to extensive independent assurance. Our public materials identify WebTrust audits, SOC 2 reporting and European qualified trust-service audits among our assurance mechanisms. Our FY24 Security and Sustainability Report stated that we undergo more than 30 audits annually and highlighted eIDAS, SOC 2 and multiple WebTrust audit programs. We also publish privacy documentation, TOMs, subprocessor information, European CP/CPS materials and audit information so you can examine the controls, operating practices and legal frameworks behind our services.

DigiCert also maintains ISO/IEC 27001 certification for the operations defined within the scope of its certificate. This provides independent assurance that we operate a systematic, risk-based information security management system. ISO 27001 supports the security controls expected under European frameworks such as GDPR and NIS2, but it does not by itself establish compliance with those regulations or replace the eIDAS and ETSI assessments applicable to our qualified trust services.

Data protection and security

We design and operate our data protection program to support applicable data-protection laws, including the GDPR. Through our public Privacy Center, we explain our roles in different processing contexts, including circumstances in which we act as a controller when operating as a trusted third-party public Certification Authority. We also provide information about data protection rights, processing and storage locations, subprocessors, and the technical and organizational measures we use to protect personal data.

How we safeguard cross-border processing

We know that you need clarity not only about where product data is stored, but also about circumstances in which personal data may be processed or accessed across borders. Where relevant, we use data-processing agreements and recognized transfer safeguards. Our public subprocessor documentation states that our agreements with subprocessors incorporate safeguards including the EU Standard Contractual Clauses (SCCs) to support GDPR-compliant cross-border transfers.

We maintain a public list of subprocessors and provide a subscription mechanism so you can receive notice when that list changes. We make this information available because regional product residency and broader corporate processing are not always the same thing. Depending on the service, analytics, support, validation, security, billing, and other processes may involve DigiCert entities or approved service providers outside the selected region, subject to applicable contractual and legal safeguards.

Security you can see and verify

European customers should not have to rely solely on a provider's claims about its security practices. DigiCert publicly documents the technical and organizational measures we use to protect customer information. Our baseline controls cover the full security lifecycle, including the following:



Network segmentation and perimeter protections



Logging and monitoring of database access



Encryption of stored and transmitted data using industry-recommended ciphers



Role-based access controls and authentication



Personnel confidentiality, background checks and role-specific training



Physical security for offices and data-center areas



Vulnerability scanning and patching



Independent penetration testing



Security and privacy requirements for third parties with access to our systems or data

We also maintain, review and test policies and plans covering information security, business continuity, disaster recovery and incident response.

For customers evaluating trust providers, the difference is not simply whether security controls exist. It is whether those controls are clearly documented, independently tested, and supported by operational practices customers can evaluate. That transparency is part of DigiCert's approach to security, privacy, resilience, and digital sovereignty.

Accountability for access

We require individual authentication and approved, role-based access. Our published controls provide for periodic access reviews, separation of duties, logging and monitoring of database access, and prompt removal of access when personnel leave.

Our platform also supports role-based access control for customer accounts, allowing your administrators to define what users and groups can access and do within supported DigiCert solutions. These controls help you apply least-privilege principles while giving both you and us clearer administrative accountability.

Legal controls

We reinforce technical controls with contractual safeguards. Personnel with access to our systems or data are subject to confidentiality obligations, and our agreements with service providers address security, privacy, and permitted processing. Our customer data-processing terms distinguish our responsibilities as a controller from those that apply when we process personal data on your behalf.

We require review of the legality of disclosure requests, challenge the requests where there are reasonable grounds to consider a request unlawful, and provide notification subject to applicable legal restrictions. These safeguards complement our technical access controls and the transfer protections described above.

Scope of our commitments

We define our European commitments precisely. The term “European” may refer to the contracting entity, hosting or support location, regulatory jurisdiction, or data-processing boundary, and these are not interchangeable. The applicable agreement, including any service documentation incorporated into it, specify the binding commitments for each service, the operational access model, and any exceptions or ancillary processing. This allows you to understand both the controls we provide and their boundaries.

We want our commitments to be clear and usable. Residency, access and transfer commitments are specific to the product and configuration you purchase. Your agreement and applicable data processing terms define the contractual scope; our privacy notice explains our processing practices. This document describes our overall EMEA trust posture; it is not intended to imply that every DigiCert service or every category of personal data is processed exclusively within the EEA.

Our trust and privacy commitment to European customers

We combine our global scale with regional technology, local people, regulated trust-service operations, and documented privacy and security governance. Our responsibility is to give European customers clear answers about where their information resides, who can operate the service, what safeguards govern access and transfer, what external assurance applies, and how much control they retain. When you entrust DigiCert with high-value identities, certificates, keys, software and connected systems, we take responsibility for earning and maintaining that trust through our architecture, people, operating practices, legal safeguards, technical controls and published evidence.

Evidence and documentation

[DigiCert Privacy Center](#)

[DigiCert Technical and Organizational Measures](#)

[DigiCert Subprocessor List](#)

[DigiCert Europe Legal Repository](#)

[DigiCert WebTrust and European audit information](#)

[DigiCert ONE environments and base URLs](#)