DigiCert

Privacy, Controller Status, and Trusted Public Third-Party Certification Services

Frequently Asked Questions ("FAQs")

Last updated 15 March 2024

These FAQs apply to DigiCert, Inc. and its subsidiaries, including DigiCert Ireland Limited, (collectively referred to in these FAQs as "DigiCert"), and have been prepared to answer certain frequently asked questions about DigiCert's role under the General Data Protection Regulation ("GDPR"), where DigiCert is acting as a Trusted Third-Party Public Certification Authority.

Overview: When does DigiCert act as a controller and when does it act as a processor?

i) To the extent that DigiCert is acting as a Trusted Third-Party Public Certification Authority, DigiCert is acting as an independent controller.

ii) To the extent that DigiCert is *not* acting as a Trusted Third-Party Public Certification Authority in respect of services to customers and instead processes customer personal data solely under the instruction of the customer, then it will be acting as a processor.

DigiCert's customer data processing addendum reflects this hybrid categorisation, providing the GDPR-required processor commitments where DigiCert acts as a processor and controller-controller commitments where it acts as controller, ensuring customers get the commitments they need to stay compliant with GDPR.

Why is DigiCert a controller for some processing when the majority of technology vendors are just a processor?

DigiCert is a controller where it is acting as a Trusted Third-Party Public Certification Authority because those services involve DigiCert doing something that most technology and services vendors never do – using personal data to make an independent assessment of whether its customers align with third party standards.

That assessment of its customers against third party standards, and the independent decision-making it involves, sets DigiCert apart from most technology vendors, and puts DigiCert clearly in the controller category.

On the other hand, DigiCert is a processor of personal data in providing products or support services that are not related to the issuance of publicly trusted digital certificates.

What is a Trusted Third-Party Public Certification Authority?

A Trusted Third-Party Public Certificate Authority is an independent organization that acts to validate websites, domains, PKI, code signing, secure email, applications and IoT devices and other entities according to validation rules set by the Certificate Authority / Browser (CA/B) Forum, a third-party standards body that governs issuance of publicly trusted digital PKI certificates. To do this, DigiCert needs to collect certain information including personal data, for the purposes of assessing and verifying identity and trustworthiness as required by the independent standards before it can issue or validate trusted certificates. For more information about Certificate Authorities see DigiCert blog - 'What is a Certificate Authority?'.

What does the GDPR have to say about certification?

The European Data Protection Board ("EDPB") acknowledges the principle within EC law[1] that the purpose of accreditation is to provide an authoritative statement of the competence of a body to perform certification (conformity assessment activities). This acknowledgment can be found within published EDPB guidelines[2] relevant to certification mechanisms for demonstrating compliance with the GDPR. These guidelines make clear that a certification from the perspective of the EDPB, can only be issued by the independent assessment of evidence by an accredited certification body.

In reaching this view, the EDPB guidelines more generally consider the role of certification, making clear that whilst the GDPR does not define "certification", the International Standards Organisation (ISO) universal definition is relevant and applies to:

"*the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements".*[3]

The EDPB further refers to ISO vocabulary regarding certification as a:

"*third party conformity assessment" involving "third party attestation…related to products, processes, and services*".

Key here is that the object of certification has been:

"independently assessed in a certification procedure and conforms to specified requirements".

The independence of a certification process is therefore in the view of the EDPB, necessary for valid certification processes.

What is the difference between a controller and a processor?

It is important that the correct processing role is determined for specific data processing activities as this is central to the proper allocation of responsibilities and obligations under the GDPR. If the categorisation is wrong, DigiCert and its customers will be non-compliant with GDPR.

A controller determines the purposes for which and the means of the processing of personal data. In other words, they decide why and how personal data is processed. An organisation's influence over *why* processing is taking place can be based on legal drivers, (e.g. if a body is obligated by law

[1] 1 Recital 15 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8. 2008, pp. 30–47).

[2] Guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 1/2018. file:///C:/Users/sannereau/Documents/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

[3] ISO Conformity Assessment https://www.iso.org/conformity-assessment.html#:~:text=Certification%20is%20the%20provision%20by,as%20third%20party%20conformity%20assessment.

to carry out certain activities) or by the factual circumstances. The factual circumstances are particularly relevant in the context of performing roles that entail individual, standalone responsibility or the exercise of professional independence and/or expertise.

A processor on the other hand acts only on a controller's behalf such as where a processing activity is delegated to it and where the service provider acts under the controller's direct instruction, authority and control. Notably, whereas processors must "allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller," independent controllers do *not* have to allow for such inspections/audits.[4]

What is the significance of independence to a controller role?

The EDPB guidelines on the concepts of controller and processor in the GDPR identify independent decision-making as a key factor that distinguishes a controller from a processor. These factors include[5]:

- Where, within a processing activity the processing entity decides independently from the other party on which data it needs to process to provide the service.
- The other party cannot have any influence on that decision making process.
- The processing activity is determined by separate criteria or provisions from those set by the other party.

The EDPB guidelines are clear that the mere fact that a service provider processes personal data in the course of delivering a service does not make it a processor. Rather determination of role rests upon its "*concrete activities in a specific context".* The nature of the service rather than the entity is overriding here.[6]

Where the key element of a service is the provision of the service, rather than the processing of personal data which forms part of the service, then the service provider may, in that context, independently determine the purpose and means of the processing that is necessary to provide the service. In such a situation, the service provider is viewed as a separate controller. This will be applicable to a service where the exercise of professional independence is a necessary function of the service.

What makes a Third-Party Public Certification Authority a data controller?

A Third-Party Public Certificate Authority acts as independent validation party. A certification issued by such an authority is therefore the result of a standalone assessment against separate

[4] See GPDR Article 28(h).

[5] See the Guidelines 07/20 on the concepts of controller and processor in the GDPR https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[6] Section 80 of the Guidelines states that "the EDPB recalls that not every service provider that processes personal data in the course of delivering a service is a 'processor' within the meaning of the GDPR." Rather, "the ***nature*** of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR" [emphasis added].

validation criteria and under a process that the recipient of certification is unable to influence or interfere with.

The necessary independence of the validation, assessment and certification activity against separate criteria means that the certification authority acts apart from the party seeking certification. The certification represents an attestation that the Certificate Authority has independently verified factors relevant to the certificated party and was not instructed or directed by the certificated party to reach that outcome.

How does DigiCert act as a Third-Party Public Certification Authority?

Customers use DigiCert public trust certification services for the purpose of seeking independent attestation of their digital products and services such as websites, domains, PKI, code signing, secure email, applications and IoT. The independence of the assessment and certification process is fundamental for customers in fostering trust and enabling user confidence in transactions involving digital products and services certified by DigiCert.

In this respect DigiCert is accredited under separate international standards for how a certification is validated, assessed and issued. These standards include the criteria to assess certificate authority controls against the CA/B Browser Forum (CAB) requirements[7] for the issuance and management of publicly trusted certificates. For this reason, clients are unable to instruct DigiCert as to the data DigiCert must take into account or the standards by which the client is assessed. Rather, DigiCert's certification policy and practice is directed by the separate standardisation body requirements.

Is there any circumstance where DigiCert issues certificates but is not a controller?

In certain limited cases a client may not be seeking a public trusted third-party certification for their public digital products and services but rather they may wish to use DigiCert technology within their internal business to issue private certificates for internal services within their control.

In those circumstances the client would be contractually prevented from using DigiCert technology outside the business and the client would set their own internal system validation requirements. To the extent DigiCert provides technology support services for client private internal use only, then DigiCert would be considered a processor in that context. However, for all accredited Third-Party Trusted Public Certification Authority services, DigiCert would act as an independent assessor and controller.

DigiCert also acts as processor for services and/or products that do not related to the issuance of digital certificates, such as DNS services and/or certain support services (as explained above).

If DigiCert is designated as a data controller, does that mean DigiCert customers have no control over how DigiCert processes customer personal data, such as third-party sharing, data-selling, etc.?

[7] CAB Webtrust WebTrust for CAs | CA/Browser Forum (cabforum.org)

Customers and data subjects are still in control over any personal data they provide to DigiCert. DigiCert does not use personal data provided by customers or data subjects for any purpose other than providing the services our customers have hired us to perform. Even if the nature of our services would be legally categorized as data controller activities, we do not exercise any independent control over customer personal data beyond providing certificate services. Our Public Privacy Notice and our standard data processing agreement explain how DigiCert customers and data subjects remain in control of any personal data provided to DigiCert, and detail the safeguards we put in place to ensure responsible processing of personal data provided to us.

For further information about DigiCert's data protection program or about its data processing responsibilities under GDPR, contact DigiCert's Data Protection Officer at dpo@digicert.com.