Dear all,

Given the importance for us of our relations with the research and education community, GÉANT is fully dedicated and committed to ensure ongoing and continued compliance with data protection legislation ensuring the adequate contractual relationships with our service providers and partners. Considering that, GÉANT is acting as a facilitator in this particular partnership, we provide to the NREN's a detailed report with our internal conclusions regarding the Privacy and Security measures in place to protect data subjects' personal data by Sectigo – Digital Certificates Provider.

Please feel free to contact GÉANT's GDPR team to clarify any questions regarding this subject - gdpr@geant.org

Kind regards,

GDPR Team

Sectigo Report
Data Privacy and Security compliance

Introduction

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS/SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers worldwide and over 20 years' experience providing online trust solutions, Sectigo partners with businesses of all sizes to provide automated public and private trust solutions for securing webservers, user access, connected devices, and applications.

Company headquarters: New Jersey, USA

Sectigo has appointed – in line with art. 27 GDPR - a EU representative for Europe: Sectigo Limited Unit 7 & 9. Listerhills, Science Park, Campus Road. Bradford, BD7 1 HR United Kingdom UK. (email provided: DPOfficer@sectigo.com

Relevant Documents

Website Terms of Use:

https://sectigo.com/terms-of-use

Certification Practice Policies and Practices

https://sectigo.com/uploads/files/Sectigo-CPS-v5.1.7.pdf

Certificate Subscriber Agreement

https://sectigo.com/uploads/files/Certificate-Subscriber-Agreement-v2.2-click.pdf

Privacy Notice

Privacy Notice (called privacy policy in this case): https://sectigo.com/privacy-policy

Privacy Notice (Policy) analysis

The Article 13 from the General Data Protection Regulation determines the specific requirements to build up a privacy notice (or policy). Taking this into account, GÉANT analysed Sectigo Privacy Policy updated on January 1st 2020.

Requirement	Included in Privacy Policy	Conclusion
Art.13 p.1 lett. a) GDPR: the identity and the contact details of the controller and, where applicable, of the controller's representative	US OFFICES – Headquarters **Sectigo, Inc.** **5 Becker Farm Road, Suite 300** **Roseland, NJ 07068** **United States** UK OFFICES Sectigo Limited 26 Office Village, Exchange Quay, Trafford Road 3rd Floor Salford, Manchester M5 3EQ United Kingdom Sectigo Limited Unit 7 & 9 Listerhills, Science Park, Campus Road, Bradford, BD7 1HR United Kingdom privacy@sectigo.com	This requirement is met
Art.13 p.1 let. b) GDPR: the contact details of the data protection officer, where applicable	Contacts from US Headquarters provided, as well the European Representative – UK offices.	This requirement is met
Art. 13 p. 1 let. c) GDPR: the purposes of the processing for which the personal data are intended as well as the legal basis for the processing	In the section "How we use your information" of Privacy Policy there are enumerated the different sources where they can collect personal data from data subjects and the purpose of processing it.	This requirement is met

Art. 13 p.1 let. d) GDPR: when processing is based on legitimate interest - the legitimate interests pursued by the controller or by a third party	Also, in the section "How we use your information", Sectigo has very explicit and detailed groups/types of information they are going to collect from data subjects and the legal basis for it.	This requirement is met
Art. 13 p.1 let. e) GDPR: the recipients or categories of recipients of the personal data, if any	Sectigo provides this information in the following section "Sharing of information collected".	This requirement is met
Art. 13 p.1 let. f) GDPR: where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	This information is provided in detail in section International Transfer of Information. Sectigo ensures that "If your data is transferred to a server outside of Europe, we will ensure that it is protected and transferred in a manner consistent with legal requirements and applicable laws". Sectigo also makes available a channel to be used by data subjects if they require more details about transfers of information outside of Europe: "You can obtain more details of the protection given to your information when it is transferred outside Europe (including a sample of the model contractual clauses) by contacting us at the mailing address or email address below - privacy@sectigo.com"	This requirement is met
Art. 13 p.2 let. a) GDPR: the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period	Retention periods of each group of information that Sectigo may collect from data subjects, are described in section "How we use your information" – Necessary Retention Periods (right column).	This requirement is met

Art. 13 p.2 let. b) GDPR: the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;"	The rights of data subjects are provided in the following section of the Privacy Policy "Your Rights to Your Information"	This requirement is met
Art. 13 p.2 let. c) GDPR: where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.	Sectigo will collect and process data subject's information as described in Privacy Policy. In case of a different purpose, Sectigo will ask for your consent and you can freely withdraw. More details on section "Processing and Customer Consent"	This requirement is not applicable
Art. 13 p.2 let. d) GDPR: the right to lodge a complaint with a supervisory authority	This information is provided in the following section of the Privacy Policy "Your Rights to your Information".	This requirement is met
Art. 13 p.2 let. e) GDPR: whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; "	Sectigo identified each type of information collected and processed by them and have a specific and detailed legal base for the effect, as for e.g. **Information you submit to us when sending us an inquiry form or other communication** - Processing is based on your consent that we will obtain prior to sending you any communications.	This requirement is met

	Information that you provide us to issue a Certificate - Processing is for the legitimate interests of Sectigo and third parties, including compliance with our legal obligations and Industry Standards, network and informational security purposes, audit purposes, and fraud prevention purposes For more details consult the section "How we use your Information".	
Art. 13 p.2 let. f) GDPR: the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject	As there is no automated decision making nor profiling, this is not required.	This requirement is not applicable.
Art. 13 p.3 GDPR: Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph	Sectigo Privacy Policy is very specific detailing the personal data and the purposes. Setigo reserves on section "Amendments to this Privacy Policy", the right to amend the Privacy Notice at any time and also " If we make a material change to this Privacy Policy, or materially change the way we use or disclose your previously collected information, we will notify you by sending you an email to the primary point of contact we have on file or by posting the changes to the Sectigo website for at least 30 days before the change takes effect".	This requirement is not applicable.

GEÁNT concludes that Sectigo Privacy Policy is aligned with the requirements from art. 13 of General Data Protection Regulation.

Security

Sectigo develops, implements, and maintains a comprehensive security program designed to protect its networks and to safeguard the information it collects and stores. Sectigo protects information both online and off-line. Below are some of the many measures that Sectigo implements:

- Transmission of information, including any payment information, is encrypted and protected using TLS/SSL technology.
- Stored customer information is kept in a secure environment where access is restricted to employees who need the information to perform a specific job (for example, billing administration or the development team).
- Employees are required to use password-protected screen-savers and keep their computers up-to-date.
- Implementing detection and prevention controls to guard against viruses and malicious software.
- Security procedures are audited in accordance with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria,

More information about which security measures are in place to protect data subjects' personal data can be found on chapter 6 (six) of Sectigo Certification Practice Statement: https://sectigo.com/uploads/files/Sectigo-CPS-v5.1.7.pdf

Conclusion

Considering the documentation available and requested that was analysed by GÉANT, we consider that Sectigo is providing sufficient level of security, is presenting compliance with the applicable law and the Privacy Policy is aligned with the requirement (13) from GDPR.

With that and always considering the documentation and analysis that was presented in this report, GÉANT concludes that Sectigo can be considered as a recommendable contractor.