Stellungnahme zu den Datenschutzhinweisen von GÉANT zur Nutzung von Sectigo-Diensten

Im Rahmen der Umstellung in der DFN-PKI wird der DFN-Verein statt auf ein Root-Zertifikat der Telekom in Zukunft auf den Trusted Certificate Service von GÉANT zurückgreifen. Während der 31. Sitzung des Ausschusses für Recht und Sicherheit wurde die Frage um die Einhaltung der Datenschutzgesetze in diesem Zusammenhang thematisiert.

GÉANT bedient sich seinerseits für die Bereitstellung des PKI-Dienstes der Dienstleistungen des Unternehmens Sectigo Limited. GÉANT ist sich der datenschutzrechtlichen Risiken bewusst und veröffentlichte daher ein Dokument, welches die Einhaltung des Datenschutzes nach Maßgabe der DSGVO von Sectigo bewertet.[1] Im Ergebnis kommt GÉANT zum Ergebnis, dass Sectigo die personenbezogenen Daten datenschutzkonform verarbeitet und die Nutzung der Dienste empfohlen werden kann. Nachfolgend überprüft die Forschungsstelle Recht im DFN anhand dieser Datenschutzhinweise die datenschutzrechtliche Einordnung des PKI-Dienstes von Sectigo.

Inhalt

[1] *GÉANT*, Sectigo GDPR Report 2020, abrufbar unter https://wiki.geant.org/display/TCSNT/TCS+2020+FAQ?preview=/133771845/148088484/GE%CC%81ANT_Sectigo_GDPR_Report_2020%20.pdf (zuletzt abgerufen am 31.03.2022).

A. Zusammenfassung und Ergebnisüberblick

Die Nutzung der Dienste von Sectigo ist nach der Analyse der Datenschutzhinweise von GÉANT aus datenschutzrechtlicher Sicht zulässig.

GÉANT kommt in ihrem Datenschutzhinweis zum Ergebnis, dass Sectigo mit seinen Diensten „ein ausreichendes Sicherheitsniveau bietet, die geltenden Gesetze einhält und die Datenschutzrichtlinie mit der Anforderung (13) der Datenschutz-Grundverordnung in Einklang steht. Vor diesem Hintergrund und unter Berücksichtigung der in diesem Bericht vorgelegten Dokumentation und Analyse kommt GÉANT zu dem Schluss, dass Sectigo als empfehlenswerter Vertragspartner angesehen werden kann“ (durch die FR übersetzt aus GÉANT Sectigo GDPR Report 2020[2], S. 7).

Diesem Ergebnis schließt sich die Forschungsstelle Recht im DFN an. Zwar ist Sectigo in seiner Datenschutzerklärung bei der Benennung der Rechtsgrundlagen nicht präzise, doch sind diese Ungenauigkeiten unbedenklich. Die Datenverarbeitungen können stets auf eine Rechtsgrundlage gestützt werden. Insbesondere mit Blick auf die vertraglichen Verbindungen zu den Nutzenden ist anzunehmen, dass die Datenverarbeitungen durch eine wirksame Rechtsgrundlage legitimiert sind.

B. Was ist Sectigo und was macht das Unternehmen?

Sectigo ist ein international agierendes Unternehmen, das im Bereich Cybersicherheit unter anderem PKI-Management für über 700.000 Unternehmen seit über 20 Jahren übernimmt. Verantwortlicher Datenverarbeiter ist die Sectigo Limited mit Sitz in Manchester, UK, diese gibt in der Datenschutzerklärung als Vertreter im Sinne des Art. 27 DSGVO die Sectigo Limited unter einer Adresse in Bradford, UK an. Im Übrigen hat Sectigo in weiteren Städten Standorte, unter anderem in die Sectigo Inc. in Roseland, New Jersey, USA, die Sectigo (Canada) Ltd. in Kanata, Canada oder die SSL247 SAS in Lille, Frankreich.

Das DFN bezieht über GÉANT einen *Trusted Certificate Service* (TCS), also ein PKI-Angebot (*public key infrastructure*), welches dazu dient, teilnehmenden Forschungsorganisationen Zugang zu Zertifizierungsmöglichkeiten zu geben, die von Sectigo bereitgestellt werden. Die Zertifikate können verwendet werden, um die Sicherheit von Websites anzuzeigen, um einzelne Teilnehmende bei elektronischer Kommunikation zu identifizieren oder um Software und entsprechende Dokumente zu authentifizieren. Sectigo dient dabei als Zertifizierungsstelle (CA) innerhalb der PKI.

Innerhalb dieser Dienstleistung kommt es zur Verarbeitung personenbezogener Daten in Form von beispielsweise E-Mail-Adressen oder IP-Adressen.

[2] *GÉANT*, Sectigo GDPR Report 2020, abrufbar unter https://wiki.geant.org/display/TCSNT/TCS+2020+FAQ?preview=/133771845/148088484/GE%CC%81ANT_Sectigo_GDPR_Report_2020%20.pdf (zuletzt abgerufen am 31.03.2022).

C. Datenschutzhinweise von GÉANT

Als direkter Partner des DFN hat sich GÉANT bereits mit der Rechtmäßigkeit implementierter Sicherheitsstandards von Sectigo nach Maßgaben der DSGVO auseinandergesetzt, insbesondere bezüglich der Maßnahmen, die nach Art. 13 DSGVO notwendig sind. [3]

Sectigo hat auf ihrer Webseite eine eigene *privacy policy*[4] veröffentlicht. Diese Datenschutzerklärung ist neben den *Nutzungsbedingungen*[5], den *Best Practice Policies*[6] und der *Zertifikat-Nutzenden-Vereinbarung*[7] Grundlage für die Datenschutzhinweise von GÉANT. Die Datenschutzhinweise analysieren die Datenschutzerklärung von Sectigo anhand der erforderlichen Vorgaben aus Art. 13 DSGVO.

I. Anforderungen nach Art. 13 Abs. 1 DSGVO

Als Namen und Kontaktdaten des Verantwortlichen sowie Kontaktdaten ihres Vertreters gemäß Art. 13 Abs. 1 lit. a) DSGVO gibt Sectigo seine Büros in Manchester, Bradford, Roseland, Kanata und Lille an. Dies ist für die Erfüllung der Vorgaben durch die DSGVO überobligatorisch. Sectigo stellt zu Beginn seiner Datenschutzerklärung klar, dass Sectigo Limited als Verantwortliche, bzw. bei Diensten von SSL247 SAS diese Verantwortliche ist. Die Angabe der Adressen der anderen Büros ist nach der DSGVO nicht erforderlich.

Als Kontaktdaten des Datenschutzbeauftragten gibt Sectigo seine Adresse in Bradford, UK an. Anders als noch in den Datenschutzhinweisen von GÉANT hat Sectigo an dieser Stelle seine Datenschutzerklärung geschärft und nicht mehr nur die allgemeinen Kontaktdaten angegeben.

Art. 13 Abs. 1 lit. c) DSGVO verlangt die Benennung der Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die entsprechende Rechtsgrundlage für die Verarbeitung. Unter dem Abschnitt „*How we use your information*“ stellt Sectigo in seiner Datenschutzerklärung anhand einer sehr ausführlichen Tabelle dar, welche Verarbeitungszwecke für welche personenbezogenen Daten relevant sind. Auch die Rechtsgrundlagen benennt Sectigo in der dritten Spalte dieser Tabelle, doch fällt auf, dass Sectigo die meisten Datenverarbeitungsvorgänge auf das „*legitimate interest*“ stützt, also auf das berechtigte Interesse nach Art. 6 Abs. 1 lit. f) DSGVO. Obwohl bei einigen Verarbeitungsvorgängen wohl auch alternative Erlaubnistatbestände einschlägig sind (z.B bei der Verarbeitung personenbezogener Daten zur Ausstellung eines Zertifikats dient diese Verarbeitung der Erfüllung des geschlossenen Vertrages nach Art. 6 Abs. 1 lit. b) DSGVO), nutzt und unterscheidet Sectigo in seiner Datenschutzerklärung nicht zwischen diesen Tatbeständen. Dies ist für eine

---

[3] *GÉANT*, Sectigo GDPR Report 2020, abrufbar unter https://wiki.geant.org/display/TCSNT/TCS+2020+FAQ?preview=/133771845/148088484/GE%CC%81ANT_Sectigo_GDPR_Report_2020%20.pdf (zuletzt abgerufen am 31.03.2022).
[4] Privacy policy, abrufbar unter https://Sectigo.com/privacy-policy (zuletzt abgerufen am 31.03.2022).
[5] Website Terms of Use, abrufbar unter https://Sectigo.com/terms-of-use (zuletzt abgerufen am 31.03.2022).
[6] Certification Practice Policies and Practices, abrufbar unter https://Sectigo.com/uploads/files/Sectigo-CPS-v5.1.7.pdf (zuletzt abgerufen am 31.03.2022).
[7] Certificate Subscriber Agreement, abrufbar unter https://Sectigo.com/uploads/files/Certificate-Subscriber-Agreement-v2.2-click.pdf (zuletzt abgerufen am 31.03.2022).

ordnungsgemäße Datenschutzerklärung zunächst nicht schädlich. Doch führt diese Angabe im nächsten Schritt dazu, dass das berechtigte Interesse in der Datenschutzerklärung ausgeführt werden muss, siehe Art. 13 Abs. 1 lit. d) DSGVO. Die Datenschutzhinweise von GÉANT bejahen das Vorliegen der Ausführungen zum legitimen Interessen. Doch ist dies in der Datenschutzerklärung von Sectigo meist nur spärlich bzw. gar nicht der Fall. Dass andere Rechtsgrundlagen einschlägig sind, wird von GÉANT ebenfalls nicht angemerkt. Die fehlenden Ausführungen zum berechtigten Interesse bedeuten nicht automatisch, dass die entsprechenden Datenverarbeitungen rechtswidrig sind. Dennoch ist die Datenschutzerklärung von Sectigo an dieser Stelle unpräzise.

Soweit eine Einwilligung für die Datenverarbeitungen erforderlich ist, verweist Sectigo darauf, dass diese im Vorfeld eingeholt wird.

Bezüglich der erforderlichen Angaben zur Weitergabe von Empfängern oder Kategorien von Empfängern der personenbezogenen Daten stellt Sectigo in einem Abschnitt die Kategorien der Empfänger entsprechend nach Vorgabe der DSGVO dar.

Art. 13 Abs. 1 lit. f) DSGVO verlangt eine Angabe über die Absicht des Verantwortlichen, die personenbezogenen Daten außerhalb des Geltungsbereichs der DSGVO zu verarbeiten und im Falle eines solchen Vorhabens die dafür geeigneten Garantien zu benennen. Sectigo stellt diese Absicht unter dem Abschnitt „*International Transfer of Information*“ dar und versichert die rechtmäßige Verarbeitung der personenbezogenen Daten nach geltendem Recht. Zudem statuiert Sectigo, dass für Datenverarbeitungen außerhalb des Geltungsbereichs der DSGVO mit den Auftragsverarbeitern die Standarddatenschutzklauseln der Europäischen Kommission vereinbart sind, um das Datenschutzniveau sicherzustellen. Um weitere Informationen hierzu zu erhalten bzw. um eine Kopie der vereinbarten Vertragswerke zu bekommen stellt Sectigo eine entsprechende Kontaktmailadresse (*privacy@sectigo.com*) zur Verfügung. Dies entspricht den Vorgaben der DSGVO. Die Verwendung von Standarddatenschutzklauseln stellt eine geeignete Garantie nach Art. 46 DSGVO dar. Doch ist seit der Rechtsprechung des EuGH zu Schrems II[8] bei der Verwendung von Standarddatenschutzklauseln zu beachten, dass die Verwendung der Klauseln allein nicht ausreichend ist, wenn Sicherheitsbehörden im EU-Ausland Zugriffsrechte auf die personenbezogenen Daten haben. Der EuGH stellte insofern fest, dass entsprechende technische und organisatorische Maßnahmen (TOMs) vorgenommen werden müssen, um das Datenschutzniveau sicherzustellen und entsprechende Zugriffe zu verhindern. Doch verlangt die DSGVO keine Darstellung dieser TOMs in der Datenschutzerklärung. Dennoch stellt Sectigo die getroffenen TOMs sowohl in der Datenschutzerklärung in einer Übersicht im Abschnitt „*Information security*“ als auch ausführlich in dem zusätzlichen Dokument „*Certification Practice Policies and Practices*“ dar (s.u.).[9]

[8] EuGH, Urteil v. 16. Juli 2020, C-311/18, Schrems II.

[9] Certification Practice Policies and Practices, abrufbar unter https://Sectigo.com/uploads/files/Sectigo-CPS-v5.1.7.pdf (zuletzt abgerufen am 31.03.2022).

II. Anforderungen nach Art. 13 Abs. 2 DSGVO

Des Weiteren verlangt die DSGVO eine Darstellung über die Speicherdauer der personenbezogenen Daten. Sectigo nimmt dies in seiner Datenschutzerklärung zu jeder beabsichtigten Datenverarbeitung entsprechend vor.

Sectigo nimmt ebenfalls die erforderlichen Hinweise über das Bestehen des Rechts auf Auskunft gegenüber den Verantwortlichen über die betreffenden personenbezogenen Daten, auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung, des Widerspruchsrechts gegen die Verarbeitung, des Rechts auf Datenübertragbarkeit sowie auf desjederzeitigen Widerrufsrechts einer gegebenen Einwilligung und des Beschwerderechts bei der Aufsichtsbehörde unter dem Abschnitt „*Your rights to your information*“ vor.

Da Sectigo in ihren Diensten nach eigenen Angaben keine automatisierten Entscheidungen im Sinne der DSGVO vornimmt, ist eine Angabe hierüber nicht erforderlich.

III. Anforderungen nach Art. 13 Abs. 3 DSGVO

Soweit der Verantwortliche beabsichtigt, im Sinne des Art. 13 Abs. 3 DSGVO die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so muss er der betroffenen Person vor dieser Weiterverarbeitung Informationen über den anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung stellen. Sectigo verpflichtet sich unter dem Abschnitt „*Amendment to this privacy policy*“ im Falle einer Verarbeitung der erhobenen personenbezogenen Daten zu einem anderen Zweck, die betroffene Person über diese neue Verarbeitung mindestens 30 Tage zuvor in Kenntnis zu setzen und die erforderlichen Informationen zur Verfügung zu stellen.

IV. Technische und organisatorische Maßnahmen

Sectigo stellt in seiner Datenschutzerklärung die vorgenommenen TOMs in einer Übersicht dar. Hierzu gehören u.a. folgende Maßnahmen:

- Die Übertragung von Informationen, einschließlich aller Zahlungsinformationen, wird mit TLS/SSL-Technologie verschlüsselt und geschützt
- Gespeicherte Kundendaten werden in einer sicheren Umgebung aufbewahrt, in der der Zugang für solche Mitarbeiter beschränkt ist, die die Informationen für die Ausführung einer bestimmten Aufgabe benötigen (z. B. die Abrechnungsverwaltung oder das Entwicklungsteam)
- Mitarbeiter sind verpflichtet, passwortgeschützte Bildschirmschoner zu verwenden und ihre Computer auf dem neuesten Stand zu halten.
- Implementierung von Erkennungs- und Präventionskontrollen zum Schutz vor Viren und bösartiger Software
- Die Sicherheitsverfahren werden gemäß den AICPA/CICA WebTrust for Certification Authorities Principles and Criteria geprüft, deren Ergebnisse durch Anklicken des WebTrust-Siegels auf sectigo.com abgerufen werden können

Zusätzlich informiert Sectigo über seine TOMs ausführlich im Dokument „*Certification Practice Policies and Practices*“.[10]

Die TOMs werden in dem Datenschutzhinweis von GÉANT zu Recht nicht weiter beanstandet. Sectigo nimmt umfassende Maßnahmen vor, um die Datensicherheit zu gewährleisten. Ob die eingesetzten Dienste den Datenschutzbestimmungen im Detail genügen, ist einzelfallabhängig und kann anhand der Datenschutzerklärung allein nicht festgestellt werden.

D. Ergebnis

Der Datenschutzhinweis von GÉANT kommt anhand der vorliegenden Dokumente zum Ergebnis, dass Sectigo mit seinen Diensten „ein ausreichendes Sicherheitsniveau bietet, die geltenden Gesetze einhält und die Datenschutzrichtlinie mit der Anforderung (13) der Datenschutz-Grundverordnung in Einklang steht. Vor diesem Hintergrund und unter Berücksichtigung der in diesem Bericht vorgelegten Dokumentation und Analyse kommt GÉANT zu dem Schluss, dass Sectigo als empfehlenswerter Vertragspartner angesehen werden kann“ (durch die FR übersetzt aus GÉANT Sectigo GDPR Report 2020, S. 7).

Diesem Ergebnis schließt sich die Forschungsstelle Recht im DFN an. Zwar ist Sectigo in seiner Datenschutzerklärung bei der Benennung der Rechtsgrundlagen nicht präzise, doch sind diese Ungenauigkeiten unbedenklich. Die Datenverarbeitungen können stets auf eine Rechtsgrundlage gestützt werden. Insbesondere mit Blick auf die vertraglichen Verbindungen zu den Nutzenden ist anzunehmen, dass die Datenverarbeitungen durch eine wirksame Rechtsgrundlage legitimiert sind.

Es ist abschließend darauf hinzuweisen, dass sich die rechtliche Lage ändern kann. Die besondere Situation des Brexit und der damit verbundenen rechtlichen Entwicklung bleibt zu beobachten. Im Zentrum der Beobachtungen muss dabei der derzeit geltende europäische Angemessenheitsbeschluss für das Vereinigte Königreich stehen. Sollte dieser von der Kommission zurückgenommen werden, ist eine rechtliche Bewertung erneut vorzunehmen.

Münster, März 2022

Forschungsstelle Recht im DFN

Die Forschungsstelle Recht ist ein Projekt an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung unter Leitung von Prof. Dr. Thomas Hoeren, Leonardo-Campus 9, D-48149 Münster, E-Mail: recht@dfn.de

[10] Certification Practice Policies and Practices, abrufbar unter https://Sectigo.com/uploads/files/Sectigo-CPS-v5.1.7.pdf (zuletzt abgerufen am 31.03.2022).