ALTHAMMER & KILL

Compliance Check d.velop sign Management Summary

Inhalt

Dienstbeschreibung

Bei dem Dienst „d.velop sign“ handelt es sich um eine cloudbasierte Software mit der eine oder mehrere Personen Dokumente mit einer qualifizierten elektronischen Signatur versehen können. Dies kann für Angebote, Bestellungen, Vertragsabschlüsse, Bescheinigungen, Urkunden und weitere Dokumente genutzt werden, welche einer Signatur bedürfen.

Im Signaturprozess werden von d.velop sign-Kunden Dokumente in die Cloud hochgeladen und den Personen, welche Ihre Signatur setzen sollen, via Link zugänglich gemacht. Die Dokumente können dabei beliebig lange in der Cloud hinterlegt werden. Durch d.velop sign findet keine inhaltliche oder technische Prüfung der Dokumente statt. Die Höchstspeicherdauer der Dokumente beträgt 12 Monate. Eine Wiederherstellbarkeit durch Backups ist hiernach weiteren 30 Tage möglich.

Mit Kunden wird ein Auftragsverarbeitungsvertrag (AVV) geschlossen, bei dem die d.velop AG als Auftragnehmerin verpflichtet wird. Die d.velop AG nutzt ihrerseits AWS als Cloud-Dienstleister. Mit der AWS EMEA Sarl (Luxemburg) wurden ein AVV, Standardvertragsklauseln und zusätzliche vertragliche Garantien vereinbart. Überdies wurden zusätzliche technische Sicherheitsmaßnahmen implementiert, wie z.B. die Verschlüsselung der abgelegten Daten.

Juristische Analyse

Zur juristischen Analyse werden die zur Verfügung gestellten Dokumente sowie die beschriebene Ausgangsituation unter datenschutzrechtlichen Aspekten analysiert.

Jeder Prüfungspunkt wird nach dem Ampelsystem bewertet. Dabei stehen die Symbole für folgendes Ergebnis in Kurzform:

⛔ Die geprüften Unterlagen weisen eklatante datenschutzrechtliche Mängel auf

⚠ Die geprüften Unterlagen weisen im geringen Maße datenschutzrechtliche Mängel auf

✅ Die geprüften Unterlagen weisen keine Mängel auf

d.velop store AGB

Die “d.velop store AGB” liegen in der Fassung vom 15.04.2021 vor. Über die AGB wird ebenfalls der AVV, das NDA, die CCP, die Leistungsbeschreibung, die SLA und die Support Richtlinie einbezogen. Dies dürfte nach der aktuellen Rechtslage zulässig sein. Eine Subsumption von weiteren Dokumenten, die vertragsähnlich sind oder eine ergänzende Leistungsbeschreibung beinhalten, wie der AVV und das NDA unter die Allgemeinen Geschäftsbedingungen, wird bislang ohne Widerspruch von Aufsichtsbehörden und Verbraucherschutzbehörden auch von anderen Unternehmen wie zum Beispiel „Google Inc.“ praktiziert.

In Punkt 3.5 wird der Kunde vertraglich zu einer Meldung von unautorisierter Passwortnutzung durch Dritte verpflichtet. Zudem findet eine Verschiebung der Verantwortlichkeit für die Kundenkontonutzung auf den Kunden statt. Beides stellen zulässige und sinnvolle Maßnahmen dar.

Customer Conditions Cloud Services Plattform

Die CCP in der Fassung vom 13.04.2021 enthält die vertragliche Untersagung, schadhafte Dokumente oder Daten in die Cloud zu laden. Diese Verpflichtung dürften neben den gesetzlichen Pflichten aus §§ 241 Abs. 2, 242 BGB eher deklaratorischer Natur sein, ist jedoch im Grundsatz nachvollziehbar und sinnvoll.

d.velop cloud Plattform Leistungsbeschreibung

Die d.velop cloud Plattform Leistungsbeschreibung in der Fassung vom 13.04.2021 beschreibt in Punkt 2.3, dass die Löschung von Daten durch Kunden in Textform verlangt werden kann. Diese Löschung würde sodann nach 30 Tagen erfolgen.

Dieser Prozess wird dahingehend überarbeitet, dass bei konkreten Löschersuchen durch Kunden oder betroffenen Personen, die Löschung der entsprechenden Dateien nach Prüfung des Sachverhalts unmittelbar erfolgt. Der Notwendigkeit einer unverzüglichen Löschung wird damit nachgekommen.

Bei einer Löschung von Dokumenten durch Initiatoren innerhalb von d.velop sign erscheint der Hinweistext, dass damit Beteiligten das Dokument entzogen wird. Es ist damit für die Prozessbeteiligten nicht mehr verfügbar. Innerhalb des Systems besteht dennoch für eine Dauer von 30 Tagen ein Back-Up, innerhalb derer das zur Löschung freigegebene Dokument auf expliziten Wunsch des Kunden wiederhergestellt werden kann.

Sollte für dieses Back-Up ein Löschverlangen durch den Kunden oder betroffene Personen eingehen, würde nach Prüfung des Einzelfalls das Back-Up unverzüglich gelöscht werden. Punkt 2.3 der Leistungsbeschreibung bezieht sich lediglich auf die kundenseitige Löschung und nicht den Umgang mit Löschersuchen gemäß Artikel 17 DSGVO.

Gemäß Punkt 3.1 wird die d.velop cloud platform im Großraum Frankfurt betrieben. Der Betrieb auf Severn im Großraum Frankfurt am Main ist sinnvoll, da hierdurch eine Datenverarbeitung auf den AWS-Servern innerhalb der EU durch AWS zugesichert wird.

Vertrag über die Auftragsverarbeitung

Der Vertrag über die Auftragsverarbeitung in der vorgelegten Fassung (20210510) wurde juristisch geprüft. Die Regelung aus Nr. 5 zur Übertragung von personenbezogenen Daten in ein Drittland unter der Einhaltung der Art. 44 ff. DSGVO ist derzeit eine der wenigen für Auftraggeber rechtssicheren Formulierungen, um die Drittlandsübermittlung zu regeln. Dies würde im Falle einer Drittlandsübermittlung jedoch bedeuten, dass d.velop als Auftragnehmer, einen bestimmten Maßnahmenkatalog durchzuführen hat, um die Art. 44 ff. DSGVO auch tatsächlich einzuhalten. Hierzu gehören der Abschluss von AVV, Standardvertragsklauseln, zusätzliche Garantien sowie die technische Implementierung weiterer Garantien zur Herstellung der Datensicherheit. Diese sind auf Verlangen der Auftraggeber vorzulegen.

Zu den Subunternehmern von d.velop gehören laut Anlage 1 die Amazon Web Services. Auch wenn es sich bei AWS um die europäische Dependance handelt, ist eine Übertragung personenbezogener Daten in die USA, welche ein Drittstaat ohne Angemessenheitsbeschluss sind, aufgrund des Cloud Acts nicht ausgeschlossen. Es sind folglich die entsprechenden Vorkehrungen zur Einhaltung der Art. 44 ff. DSGVO zu treffen. Gemäß dem von d.velop übersandten Antwortkatalog wurden Standardvertragsklauseln sowie zusätzliche Garantien vereinbart. Sämtliche der zur Verfügung stehenden technischen Garantien wurden durch d.velop im Rahmen von Ziffer 5.2 des AWS GDPR KMS implementiert.

Einzelne Vertragsdetails könnten zu Gunsten der Auftraggeber nachgeschärft werden, wie zum Beispiel der Umfang der Mitwirkungspflichten. Eine Verletzung von geltendem Datenschutzrecht ist jedoch nicht erkennbar.

Die gesetzlichen Vorgaben der DSGVO wurden ausreichend berücksichtigt.

Allgemeine Geschäftsbedingungen für das Produkt d.velop sign

Es wurden die AGB für d.velop sign in der Fassung vom 13.04.2021 geprüft. In Punkt 19 werden vorfallabhängige Dokumentenaudits geregelt. Hierbei handelt sich um einen Prozess der Bundesdruckerei zur Auditierung des Dokumentationsprozesses. Eine Verarbeitung personenbezogener Daten findet hierdurch nicht statt.

d.velop sign Leistungsbeschreibung

Die d.velop sign Leistungsbeschreibung wurde in der Fassung vom 13.04.2021 geprüft. Hieraus ergeben sich keine datenschutzrechtlichen Besonderheiten oder Probleme.

d.velop sign cloud Plattform Service Level Agreements (SLA)

Die SLA wurde in der Fassung vom 13.04.2021 geprüft. Hieraus ergeben sich keine datenschutzrechtlichen Besonderheiten oder Probleme.

Datenschutzerklärung

Es ist eine Datenschutzerklärung unter https://www.d-velop.de/datenschutz verfügbar. Hierunter finden sich Informationen und Hinweisen zur Verarbeitung personenbezogener Daten bei dem Besuch der d.velop Website und weiter Online-Präsenzen.

Eine gesonderte Datenschutzerklärung für die „d.velop Cloud Apps" Produkte, zu denen auch d.velop sign gehört, findet sich unter https://s3.eu-central-1.amazonaws.com/mediamanager.cloudcenter.service.d-velop.cloud/056044d5-178c-4328-8f23-fdec4529326b, welche über die Verarbeitung personenbezogener Daten bei der Nutzung dieser Produkte informiert. Die Informationspflichten gemäß Artikel 13 DSGVO werden damit umfassend erfüllt.

Juristische Analyse der Ausgangssituation

Aufgrund der beschriebenen Ausgangslage ergeben sich keine datenschutzrechtlichen Herausforderungen. Die Einführung einer Begrenzung der Speicherdauer von Dokumenten auf den Servern von d.velop sign ist sinnvoll. Hochgeladene Dokumente können potenziell personenbezogene Daten, mitunter auch besondere Kategorien personenbezogener Daten gem. Artikel 9 DSGVO, beinhalten. Die zeitlich unbegrenzte Speicherung dieser personenbezogenen Daten in einer Cloud wäre nicht von den Vorgaben der DSGVO gedeckt, welche sich die Datenminimierung gem. Artikel 5 Abs. 1 lit. c) DSGVO zum Ziel gesetzt hat. Durch die zeitlich begrenzte Speicherung wird dieser Grundsatz eingehalten. Hierdurch werden unnötige Risiken für die Rechte und Freiheiten von betroffenen Personen minimiert, indem Daten nicht unnötig lange aufbewahrt werden und damit im Fall eines IT-Sicherheitsvorfalles unbefugten Dritten zugänglich gemacht werden könnten.

Die Verarbeitungsprozesse innerhalb des Dienstes d.velop sign wurden gemäß der Angaben des von d.velop übersandten Antwortkatalogs in das Verarbeitungsverzeichnis übernommen.

Sicherstellung von Betroffenenrechten

Die Artikel 12 – 23 DSGVO beschreiben die Rechte betroffener Personen gegenüber den verantwortlichen Stellen. Besonders hervorzuheben sind dabei das Auskunftsrecht nach Art. 15 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO und das Recht auf Datenportabilität gem. Art. 20 DSGVO. Bei den aufgeführten Artikeln handelt es sich um Rechte, welche potentiell vermehrt von betroffenen Personen gegenüber der d.velop AG in Bezug auf d.velop sign geltend gemacht werden können.

Hierzu liegt ein eingeübter und dokumentierter Prozess zur Reaktion auf die Geltendmachung von Betroffenenrechten vor.

Technische Analyse

Sicherheit und Integrität der gespeicherten Daten

Die Inhalte der d.velop Plattform werden in Deutschland in einem zertifizierten Rechenzentrum gespeichert. Dabei werden ruhende Daten („Data at rest“) mit dem vom BSI (vgl. BSI TR-02102-1, Absatz 2.1) empfohlenen Algorithmus AES-GCM mit 256-bit Schlüssellänge verschlüsselt.

Der AES-Algorithmus bietet nach aktuellem Stand der Technik ein hohes Maß an Sicherheit und die GCM-Betriebsart bietet außerdem zusätzlich eine Datenauthentisierung. Des Weiteren werden unterschiedliche Schlüssel für verschiedene Speicher benutzt und der Zugriff auf die Schlüssel protokolliert. Die Schlüssel selbst werden vom Cloud-Betreiber aufbewahrt und verwaltet.

Unterschiedliche Mandanten und die von ihnen verwendeten Apps werden voneinander getrennt gespeichert. Es gibt ein Backupkonzept, Versionierung/Snapshots und regelmäßige Widerherstellungstests dieser. Firewalls werden benutzt, um die Systeme zu sichern. Es werden dabei nur die notwendigen Ressourcen verfügbar gemacht.

Sicherheit bei Übertragungen

Die d.velop Cloud implementiert eine Microservice-Architektur, bei der einzelne Dienste über ein Netzwerk miteinander kommunizieren. Bei dieser Kommunikation wird stets jede Übertragung nach dem Stand der Technik verschlüsselt. Von außen erreichbare Dienste und Schnittstellen übertragen Informationen ebenfalls nur in verschlüsselter Form. Voneinander unabhängige Systeme und Netzwerke sowie Entwicklungs-, Test- und Produktivumgebungen sind voneinander isoliert.

Bei einer On-Premise Installation der Plattform ist eine Fernwartung möglich, bei der standardmäßig TeamViewer zum Einsatz kommt. Auf eine ausreichende Sicherheit bei Authentifizierung und Übertragung bei einer solchen Fernwartung wird geachtet.

Authentifizierung

Die gebotenen Authentifizierungsmöglichkeiten bei den verschiedenen Systemen folgen einer Sicherheitsrichtlinie, in der unter anderem eine Kennwortrichtlinie und Zugangsberechtigungen beschrieben sind. Zugriffe auf die Cloud-Systeme werden protokolliert und bei administrativem Zugriff wird eine Mehrfaktor-Authentifizierung benutzt, um die Sicherheit zu erhöhen. „Privilege-Escalation“ durch Mitarbeiter wird mittels technischer Maßnahmen verhindert. Mehrere Personenkreise müssen eine Anpassung von Berechtigungen eines Mitarbeiters absegnen. Des Weiteren ist es möglich, externe Identitätssysteme mittels des Standards „OpenID Connect“ zu benutzen.

Maßnahmenplan

Aufgrund der vorgenommenen Prüfung ergeben sich aus datenschutzrechtlicher Perspektive keine weiteren Maßnahmen zur Verbesserung der datenschutzrechtlichen Ausgangslage.

Fazit

Die rechtlichen Dokumente und Verfahren können nach eingehender juristischer und technischer Prüfung nicht bemängelt werden. Die wenigen vorhandenen Schwachstellen wurden von der d.velop AG nach entsprechender Beratung durch Überarbeitung von Dokumenten oder Prozessen beseitigt.

Auf der technischen Seite entspricht, nach Analyse, die Informationssicherheit der Plattform dem Stand der Technik. Es wurde auf mehreren Ebenen auf Verschlüsselung und Datenintegrität geachtet.

November 2021