Beitrag aus
4/2023

www.dud.de

DuD
Datenschutz und Datensicherheit
EXTRA

DSGVO-Haftungs- und Sicherheitsrisiken durch Protokoll und Diagnosedaten im IT-Betrieb

Horst Speichert

Springer Gabler

Horst Speichert

DSGVO-Haftungs- und Sicherheitsrisiken durch Protokoll- und Diagnosedaten im IT-Betrieb

IT-Diagnose- und Protokoll-Daten enthalten häufig große Mengen an personenbezogenen und sicherheitskritischen Daten, ohne dass die Verantwortlichen davon in der Praxis ausreichend Kenntnis nehmen oder rechtlich überprüfen. Die Protokoll- und Diagnosedaten werden vom IT-Betrieb zu Analyse- und Service-Zwecken in Form von Dumps und Logs an die weltweiten Supporteinheiten der internationalen Software-Hersteller versendet und von diesen – auch für eigene Zwecke – verarbeitet. Dadurch drohen in vielen Fällen Datenschutzverletzungen und damit Haftungsfallen für Unternehmen und Behörden sowie die dortigen Datenschutz- und IT-Verantwortlichen.

1 Überhänge beim Export von Diagnose- und Protokolldaten

Der IT-Betrieb begeht potentiell – häufig ohne es zu wissen – Rechtsverstöße durch das Erstellen, Verarbeiten und Versenden von Protokoll- und Diagnosedaten. In Security-Monitoring-Lösungen, wie zum Beispiel einem SIEM, werden diese System-Logs für Analyse, Absicherung und Qualitätsverbesserung genutzt. Im Falle von Computer- oder Applikationsabstürzen sind es die Giga-Byte-großen Diagnosedateien in Form von DUMPs, also Speicherauszügen, die zu Supportzwecken an Dienstleister oder Software-Hersteller übermittelt werden. Entsprechend verletzen IT-basierte Consumer-Produkte, wie Autos, Smart Meter, IoT-Produkte oder Heimwerker-Geräte, Fitness-Tracker, Apps usw. potentiell die DSGVO, denn es werden Daten zu Nutzungs-, Diagnose-, Service- oder Weiterentwicklungszwecken – ggf. pauschal und kontinuierlich – an den Hersteller übertragen.

Die genannten Datenexporte enthalten standardmäßig „Überhänge“, also „zu viele“ Daten, die gemäß der Datenschutzanforderungen wegen fehlendem „Zweck“ und „Notwendigkeit“ nicht an Dritte weitergeleitet werden dürfen. Diese in ihrer Struktur „mehrdimensionalen Überhänge“, in denen sich auch hoch-sensible Personendaten befinden, sind oftmals unverhältnismäßig und demnach rechtswidrig.

Auch dürfen diese Daten nur unter besonderen Voraussetzungen in unsichere Drittländer übermittelt werden, die im Sinne des Datenschutzes kein gleichwertiges Schutzniveau wie die EU besitzen. Seitdem der EuGH1 am 16.07.2020 das Privacy Shield für ungültig erklärt hat, gilt auch die USA als „unsicheres Drittland“, das kein der EU gleichwertiges Schutzniveau besitzt. In Drittländern haben allerdings die meisten großen weltweit agierenden IT-Anbieter ihren Hauptsitz und somit auch ihre System-Support-Einheiten. Schickt nun zum Beispiel ein europäisches Unternehmen seine DUMPs mit den Überhängen an den US-amerikanischen Hersteller seiner Systeme, oder übermittelt es seine System-Logs an einen Security-Monitoring- Dienstleister in Indien oder China, begeht es potentielle Datenschutzverstöße. Davon haben die wenigsten IT- Verantwortlichen Kenntnis und riskieren hohe Bußgelder bedingt durch diese Übertretung des Datenschutzrechtes. Aber auch nach einer möglichen Einigung der EU und USA über ein neues Privacy Shield[1] blieben DSGVO-bezogenen Risiken, die sich mit Protokoll- und Diagnosedaten verbinden, weiterhin bestehen, da die resultierenden Verstöße von grundsätzlicher Natur sind.

Die Funktionalität der IT- und Datensysteme ist auf die Unterstützung Dritter, also externer Dienstleister und Hersteller, angewiesen. Demzufolge müssen die Protokolldaten zu Analysezwecken an deren Labore und Systemexperten übermittelt werden. Diese befinden sich weltweit in verschiedenen Lokationen. Um

Horst Speichert

Rechtsanwalt, spezialisiert auf IT-Recht und Datenschutz, Partner der Kanzlei esb Rechtsanwälte, Geschäftsführer der esb data GmbH, Lehrbeauftragter für Informationsrecht der Universität Stuttgart. Langjährige Praxiserfahrung als Seminarleiter, Autor und Datenschutzbeauftragter.“
E-Mail: horst@speichert.de

1 Die Europäische Kommission hat am 13.12.2022 einen Beschlussentwurf vorgelegt, der an ein US-Dekret Präsident Bidens vom 07.10.2022 anschließt und das Verfahren eines Angemessenheitsbeschlusses für sichere EU-USA Datenströme einleitet, mit dem die vom EuGH in der Schrems II-Entscheidung geäußerten Bedenken ausgeräumt werden sollen.

zu vermeiden, dass die IT-Verantwortlichen und Unternehmen Datenschutzverstöße begehen, müssen die Daten für den Transport bereinigt werden, zum Beispiel durch Tools zur Anonymisierung und Pseudonymisierung. Das heißt, dass nur diejenigen Daten übermittelt werden, die für die Analyse und Beseitigung der Problemursache notwendig sind, also ohne personenbezogene Daten, die sich zweckfremd in den Logfiles oder DUMPs befinden. Nur so erfüllen IT-Betreiber die Anforderungen der Datenminimierung, Verhältnismäßigkeit und Zweckbindung nach der DSGVO.

2 Dump- und Log-Files verletzen Datenschutz- und Sicherheitsbestimmungen

Rechtliche Fallstricke verbergen sich in den täglichen Routine-Abläufen der Unternehmens-IT in ungeahntem Ausmaß. Die zentrale Gefahr pauschalisierter, großzügiger Datenfreigaberoutinen liegt im unverhältnismäßigen und zweckwidrigen „Zuviel" an Daten und Verarbeitungsinstanzen. Die „mehrdimensionalen Überhänge" sind aus Sicht der Betroffenen nicht statthaft. Sie schwächen darüber hinaus die entlastende juristische Wirksamkeit der getroffenen Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO zwischen IT und Dienstleister. Sie stellen diese legitimierenden Verträge in Frage, weil die großvolumigen Datenübermittlungen überwiegend im Fremdinteresse erfolgen, also vom Auftragszweck nicht gedeckt sind und damit das Unternehmen juristisch angreifbar machen, weil für eine Übermittlung im Fremdinteresse die Rechtsgrundlage fragwürdig ist.

Ein Vorwurf der Verletzung der DSGVO aber auch der Sicherheitsbestimmungen kann deshalb pauschal ausgesprochen werden. So könnte praktisch jeder betroffene Kunde oder Arbeitnehmer eines Unternehmens mühelos und mit hoher Trefferquote einen Anfangsverdacht äußern. Denn die nachfolgend beschriebenen und täglich praktizierten Routine-Abläufe sind fester Bestandteil jeder Unternehmens-IT. Es bedarf praktisch keinerlei aufwendiger Nachforschung, um den Nachweis von Verstößen zu führen.

Die Verantwortung für dieses Missverhältnis zwischen notwendiger und tatsächlicher Datenmenge, dem Überhang, trägt zunächst der Verantwortliche bzw. Übermittler der Log- und Diagnose-Daten, denn die Hersteller und Dienstleister lehnen in vielen AGB-Gestaltungen proaktiv jede Verantwortung für die Rechtmäßigkeit der Übermittlung ab und weisen sie stattdessen dem Übermittler zu. Sie übernehmen damit zwar vertraglich keinerlei Haftung für die Zulässigkeit des Datentransfers, sind aber nach der Haftungsverteilung der DSGVO für rechtswidrige Datenübermittlungen mitverantwortlich.

3 Allgemeine DSGVO-Anforderungen an Diagnose- und Protokolldaten

In Art. 5 der DSGVO sind die tragenden Grundsätze der Verarbeitung personenbezogener Daten geregelt. Das Kernanliegen der DSGVO besteht in Datenvermeidung, Zweckbindung und Verhältnismäßigkeit.

In vielen Fällen sind Diagnose- und Protokolldaten mit natürlichen Personen (z.B. Kunden, Mitarbeitern, Kontaktpersonen von Kunden, Angestellten von IT-Dienstleistern usw.) unmittelbar verbunden oder lassen sich mit einem vertretbaren Aufwand auf solche natürlichen Personen zurückführen. Somit sind personenbezogene oder personenbeziehbare Daten gegeben, welche zur Anwendbarkeit der gesetzlichen Datenschutzbestimmungen insbesondere der DSGVO führen.

Personenbezogene Diagnose- und Protokolldaten müssen demnach folgende Anforderungen erfüllen. Sie müssen u.a. gemäß Art. 5 DSGVO[2]:

- 1. in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Transparenzgebot);
- 2. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Zweckbindungsgebot);
- 3. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Grundsatz der Datenminimierung und Verhältnismäßigkeit)
- 4. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Grundsatz der Speicherbegrenzung)

Das verarbeitende Unternehmen ist für die Einhaltung dieser Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können (Grundsatz der Rechenschaftspflicht).

Diese von der DSGVO in Art. 5 vorgegebenen strengen Datenschutzgrundsätze werden im Zusammenhang mit umfangreichen Protokolldateien und Diagnosedaten in vielen Fällen nicht eingehalten.

4 Datentransfer in unsichere Drittländer – Aktualität durch EuGH-Schrems II

Die Einschaltung von IT-Dienstleistern im Rahmen von IT-Systemen und ISMS-Lösungen bedeutet in der Regel die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung), so dass die Vorgaben von Art. 28 DSGVO erfüllt sein müssen. Danach ist insbesondere ein Vertrag mit dem Dienstleister abzuschließen (sog. AV-Vertrag), der dem umfangreichen Anforderungskatalog des Art. 28 DSGVO entspricht.

Detailliert geregelt wurde auch eine Kontrollpflicht beim Dienstleister. Der Auftraggeber hat sich gemäß Art. 28 Abs. 3h DSGVO vor Beginn der Datenverarbeitung (bereits vor Vertragsschluss bei der Auswahl, siehe Art. 28 Abs. 1 DSGVO) und sodann regelmäßig von der Einhaltung der beim Dienstleister getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.[3]

Nach der Entscheidung des EuGH vom 16.07.2020 (Aktenzeichen C-311/18, Schrems II [4]) ist eine Neubewertung des Transfers personenbezogener Daten in unsichere Drittländer erforderlich, insbesondere bezüglich des Datentransfers in die USA. Für die vorliegend in Frage stehenden Protokolldateien aus IT-Syste-

2 vgl. im Detail z.B. bei Gola, DS-GVO, BDSG, 3. Auflage 2022 Art. 5 Randnr. 11 ff.; Kühling/Buchner, DS-GVO, BDSG, 3. Auflage 2020 Art. 5 Randnr. 18 ff.

3 siehe zur Kontrollpflicht Gola, BDSG, 3. Auflage 2022, DS-GVO, Art. 28 Randnr. 11; dagegen abschwächend Kühling/Buchner, DS-GVO, BDSG, 3. Auflage 2020 Art. 28 Randnr. 60, 78, der aber letztlich im Ergebnis die regelmäßige Kontrollpflicht ebenso bejaht

4 siehe die Entscheidung im Volltext: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

men und ISMS-Lösungen ist dies aufgrund der Übermacht der US-Anbieter in besonderem Maße relevant.

Nach den Feststellungen des EuGH ist der Angemessenheitsbeschluss 2016/1250 der europäischen Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) unwirksam. Die Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield ist deshalb künftig unzulässig und muss unverzüglich eingestellt werden. Zum Datenexport in diesem Sinne gehören auch bloße Zugriffsmöglichkeiten von Stellen in unsicheren Drittländern, z.B. ein Supportzugriff eines Dienstleisters aus den USA. Der EuGH hat das Privacy Shield für ungültig erklärt, weil das US-Recht kein gleichwertiges Schutzniveau bietet, insbesondere wegen der nachrichtendienstlichen Erhebungsbefugnisse nach Section 702 FISA und Executive Order 12333.

Die Entscheidung 2010/87/EG der Kommission über Standarddatenschutzklauseln (Standard Contractual Clauses, SCC) war nach den Feststellungen des EuGH weiterhin gültig, so dass die SCC auch grundsätzlich weiterhin genutzt werden können. Die verantwortlichen Datenexporteure und Datenimporteure müssen jedoch prüfen, ob das Drittland im Datenschutzsinne ein gleichwertiges Schutzniveau wie die EU besitzt. Dieses angemessene Schutzniveau wird für die USA sowohl vom EuGH wie auch von den Datenschutzbehörden verneint. Bei fehlendem Schutzniveau müssen die Akteure deshalb zusätzliche Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus ergreifen.

Nach dem Urteil des EuGH reichen also bei Datenübermittlungen in die USA die SCC ohne zusätzliche Maßnahmen nicht mehr aus. Die SCC können die Behörden des Drittlandes nicht binden und stellen daher bei unzureichendem Schutzniveau ohne zusätzliche Maßnahmen der Vertragspartner keinen angemessenen Ausgleich dar. Sofern der Verantwortliche auch mit zusätzlichen Maßnahmen kein angemessenes Schutzniveau herbeiführen kann, muss er den Datentransfer einstellen.

5 Die neuen Standarddatenschutzklauseln

Die europäische Kommission hat am 04.06.2021 die finale Fassung der neuen Standardvertragsklauseln (SCC) für die Übermittlung personenbezogener Daten in unsichere Drittländer sowie für Verarbeitungen innerhalb der EU angenommen und veröffentlicht.[5] Die neuen Standardvertragsklauseln lösen die bislang noch geltenden alten Fassungen der Standardvertragsklauseln aus 2001 und 2010 ab. Sie sehen eine ganze Reihe von Änderungen gegenüber den bislang geltenden Vertragsmustern vor. Insbesondere können sie gemäß eines modularen Ansatzes sowohl für Übermittlungen zwischen Verantwortlichen als auch für Datentransfers zu Auftragsverarbeitern und zwischen Auftragsverarbeitern verwendet werden.

Nach Auffassung der EU-Kommission berücksichtigen die neuen Standardvertragsklauseln auch bereits die Anforderungen des EuGH aus der Schrems II-Entscheidung. Allerdings können auch die neuen Vertragsklauseln aufgrund ihrer Natur als vertragliche Vereinbarungen etwaige Konflikte mit gesetzlichen Bestimmungen für Durchgriffsrechte von Ermittlungsbehörden und Geheimdiensten nicht abschließend lösen. Die EU-Kommission weist in ihrem Beschluss deshalb ausdrücklich darauf hin, dass der Transfer personenbezogener Daten auf Basis der neuen Standardvertragsklauseln nur stattfinden darf, wenn die gesetzlichen Bestimmungen und Rahmenbedingungen in den Drittstaaten den Datenimporteur nicht daran hindern, seinen vertraglichen Verpflichtungen nachzukommen.[6]

Die datenexportierenden Unternehmen müssen also trotz der neuen Standardvertragsklauseln die konkreten Übermittlungen im Einzelfall prüfen, um festzustellen, welche gesetzlichen Bestimmungen für den Datenimporteur gelten und welche Zusatzmaßnahmen, z.B. zusätzliche Vertragsregelungen, Monitoring- und Verschlüsselungsmaßnahmen, zu ergreifen sind (sog. Datentransferfolgenabschätzung oder Data Transfer Impact Assessment).

6 Sicherheit der Verarbeitung und der internen und externen Richtlinien

Gemäß Art. 32 DSGVO müssen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um die Sicherheit und den Schutz der Daten zu gewährleisten.[7] Dies gilt nicht nur für personenbezogene Daten, sondern auch für sicherheitskritische Informationen in Dumps und Logs. Denn es befinden sich Zertifikate, User-IDs, Security Controls, Passwörter, Schlüssel, etc. in IT-Diagnose-Daten. Diese können die Sicherheit der Datenverarbeitung gefährden, wenn sie an Personen mit betrügerischen Absichten gelangen.

Die technischen und organisatorischen Maßnahmen können u.a. Pseudonymisierung und Verschlüsselung sowie Anonymisierung personenbezogener Daten beinhalten.

Auch müssen die IT-Verantwortlichen die internen IT-Sicherheitsrichtlinien sowie die vertraglichen Pflichten gegenüber den Kunden respektieren.

Qualitätsstandards wie ISO 27001 oder regulatorische Vorgaben wie MaRisk oder BAIT verlangen ebenso den Schutz sicherheitsgefährdender Informationen im IT-Betrieb.

7 Zusammenfassendes Fazit

Die dargestellten Problemlagen haben die Gefahr von Datenschutzverletzungen aufgrund von evidenten Verstößen gegen das Zweckbindungs-, Datenminimierungs- und Transparenzgebot sowie gegen das Verhältnismäßigkeitsprinzip durch einen Überhang bei den Protokoll- und Diagnosedaten eindeutig zu Tage gefördert.

Die Frage ist nun, welche Lösungsansätze weiterhelfen können, die gleichzeitig auch revisionssicher sind. Dies muss für die verschiedenen Kategorien von Datenschutzverstößen unterschiedlich beantwortet werden. So können Verletzungen der Transparenzpflicht durch eine detailliertere Ausgestaltung der Datenschutzhinweise nach Art. 13, 14 DSGVO relativ problemlos behoben werden. Schon wesentlich aufwendiger sind Fortschritte bei der Datenminimierung umzusetzen. Hierfür müssen in mü-

5 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=DE

6 siehe u.a. Erwägungsgrund 19 des Beschlusses der EU-Kommission vom 04.06.2021, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=DE

7 Gola, BDSG, 3. Auflage 2022, DS-GVO, Art. 32 Randnr. 7; Kühling/Buchner, DS-GVO, BDSG, 3. Auflage 2020 Art. 28 Randnr. 71

hevoller Kleinarbeit die verschiedenen Datenquellen durchforstet und jeweils entschieden werden, ob und wie lange die personenbezogenen Daten benötigt werden. Dieser Aufwand wird sicherlich möglich sein, aber voraussichtlich erst dann investiert werden, wenn die Protokoll- und Diagnosedaten aus den Tiefen der IT-Systeme ihr Schattendasein durch ein höheres Maß an Aufmerksamkeit verlieren.

Pauschale Lösungsansätze, die alle Kategorien von Datenschutzverstößen abstellen könnten, wie die Anonymisierung oder die Einholung von Einwilligungen der Betroffenen, sind sicherlich stark von der konkreten technischen und organisatorischen Situation im Einzelfall abhängig. So sind legitimierende Einwilligungen von betroffenen Kunden in der Regel rechtlich leichter einzuholen als von Arbeitnehmern, bei denen die Freiwilligkeit ihrer Zustimmung stets kritisch zu hinterfragen ist. Einwilligungen von Arbeitnehmern sind z.B. im Zusammenhang mit der erlaubten Privatnutzung (wirtschaftlicher Vorteil) ohne weiteres möglich, während sie bei rein dienstlichen Prozessen häufig an der Freiwilligkeit oder Widerruflichkeit (durch einzelne Arbeitnehmer) scheitern.

Die lokale, automatisierte Anonymisierung der sensiblen Daten in Dumps und Logs würde das Datenschutzproblem technisch lösen und präventiv vermeiden.

IT-Betrieb, Revision, Risiko-Management und Datenschutz müssen die Risiken der versteckten und unkontrollierten Weiterleitung personenbezogener Daten vor dem Hintergrund der DSGVO neu bewerten. Sie stehen in der Verantwortung, Schutzmaßnahmen und Kontrollen zu implementieren und die Datenschutzlücken zu schließen. Andernfalls drohen grobe Datenschutzverstöße und Bußgelder, verbunden mit möglicher persönlicher Haftung leitender Mitarbeiter.

IMPRESSUM
Sonderdruck für ENTERPRISE- IT-SECURITY.COM Seestrasse 3a, CH-6300 Zug;
Springer Fachmedien Wiesbaden GmbH, Postfach 1546, 65173 Wiesbaden,
Amtsgericht Wiesbaden, HRB 9754, USt-IdNr. DE81148419

GESCHÄFTSFÜHRER:
Stefanie Burgmaier I Andreas Funk I Joachim Krieger