46. Jahrgang
datenschutz-berater.de
DSB 01/2022

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Alexander Weidenhammer und Max Just

Datenschutzrechtliche Herausforderungen im Zusammenhang mit „Schatten-IT“

Verantwortliche Stellen haben dafür Sorge zu tragen, dass sowohl die internen Abläufe und Prozesse als auch die dabei eingesetzte Hard- und Software den Anforderungen der DSGVO entsprechen. Dies umfasst neben der vollständigen datenschutzrechtlichen Dokumentation insbesondere die Sicherstellung der Grundsätze für die Verarbeitung personenbezogener Daten sowie die Gewährleistung der Sicherheit der Verarbeitung. Die konforme Umsetzung dieser Verpflichtungen stellt zahlreiche Unternehmen regelmäßig vor erhebliche Hürden. Hinzu treten weitere datenschutzrechtliche Herausforderungen, wenn innerhalb der verantwortlichen Stelle einzelne Fachbereiche oder Beschäftigte im Rahmen ihrer täglichen Arbeit nicht-freigegebene Endgeräte oder Anwendungen nutzen.

Problemaufriss

Unter dem Begriff der Schatten-IT sind sämtliche informationstechnische Systeme, Prozesse, Anwendungen und Endgeräte zu verstehen, welche durch einzelne Fachbereiche oder Beschäftigte einer verantwortlichen Stelle ohne Freigabe oder gar Kenntnisnahme der IT-Abteilung beziehungsweise der Leitungsebene angeschafft und eingesetzt werden. Erfasst werden hierbei sowohl individuelle Datenverarbeitungen mit Tabellenkalkulationen, Nutzung einfacher Applikationen wie Messenger-Dienste oder Cloud-Dienste sowie Eigenbeschaffung mobiler Endgeräte, insbesondere Speichermedien.

Die Anschaffung von Schatten-IT stellt heute für Beschäftigte keine besonders hohe Herausforderung mehr dar. Bieten insbesondere zunehmend zahlreiche Angebote im Bereich der Open-Source-Software einfache Möglichkeiten zur eigenständigen Nutzung von Anwendungen, wobei hier allem voran cloudbasierte Dienste zu nennen sind. Neben lizenzrechtlichen oder kostentechnischen Fragestellungen ergeben sich Problemfelder insbesondere in den Bereichen Datenschutz und Datensicherheit. Dies beginnt bereits mit der Anschaffung von Schatten-IT und zieht sich über den weiteren Betrieb bis zur Entsorgung fort: Aufgrund mangelnder Transparenz ist weder die Einbeziehung des Fachwissens der IT-Abteilung noch die des Datenschutzbeauftragten gewährleistet. Notwendige datenschutzrechtliche Überprüfungen der Anwendungen oder Dienstleister werden nicht durchgeführt, mit der Datenverarbeitung einhergehende Risiken nur unzureichend betrachtet und erforderliche Dokumentationen nicht angelegt.

Besondere Herausforderungen liegen zudem bei Anwendungen und Diensten vor, die im Zusammenhang mit einer Datenübermittlung an Drittländer stehen. Doch darüber hinaus schwächt unzureichend überprüfte Hard- und Software unter Umständen das gesamte Sicherheitsniveau der verantwortlichen Stelle. Cyberkriminellen wird mittels Schatten-IT unter Umständen Tür und Tor zum ansonsten gut geschützten Unternehmensnetzwerk geöffnet.

Allerdings ermöglicht Schatten-IT für verantwortliche Stellen unter Umständen auch neue Chancen, bspw. um die Motivation der Beschäftigten bei der Aufgabenerfüllung zu steigern, denn der Einsatz kann den Arbeitsalltag effektivieren. Dennoch steht die Steigerung der Effektivität meist in keinem Verhältnis zu den aufgezeigten Risiken.

Der Problemaufriss zeigt, welche umfangreichen Risiken mit Schatten-IT einhergehen. Bereits mit Beginn des Beschaffungsprozesses von Hard- und Software gelten besondere Anforderungen im Bereich des Datenschutzrechts, die es grundsätzlich zu beachten gilt, im Zusammenhang mit Schatten-IT jedoch in das Hintertreffen geraten.

Datenschutzrechtliche Anforderungen

Der Verantwortliche ist nach Maßgabe des Art. 5 Abs. 2 DSGVO zur Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO verpflichtet und muss im Rahmen seiner Rechenschaftspflicht die Einhaltung nachweisen können. Die in Art. 5 DSGVO niedergelegten Grundsätze werden durch weitere Vorschriften der DSGVO entsprechend konkretisiert. Mit Blick auf den technischen Datenschutz betrifft dies insbesondere den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO (Art. 25 DSGVO) sowie den Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f DSGVO (Art. 32 DSGVO). Daneben tritt insoweit nach Art. 24 Abs. 1 DSGVO die Pflicht des Verantwortlichen geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO erfolgt.

Von USB-Sticks und Messenger-Diensten

Schatten-IT kann im Unternehmen viele Gesichter haben, welche in unterschiedlichen Ausprägungen potenziell dazu geeignet ist, die dargelegten Grundsätze und Schutzziele zu beeinträchtigen:

Die Nutzung von nicht-freigegebenen portablen Speicher-

medien, insbesondere von USB-Sticks und externen Festplatten, ist dazu geeignet die Sicherheit der Verarbeitung erheblich zu gefährden. Oftmals werden diese genutzt, um Daten untereinander auszutauschen, gemeinsam an Dokumenten zu arbeiten oder um Dateien zwischen unterschiedlichen Endgeräten zu transportieren. Zum einen kann eine Gefährdung der Vertraulichkeit bei einem Verlust des in der Regel unverschlüsselten Speichermediums eintreten. Zum anderen kann hierdurch versehentlich Schadsoftware von netzwerkfremden Endgeräten in das Netzwerk des Unternehmens eingebracht werden.

Die Entwicklung und der Betrieb von Anwendungen durch die Fachabteilungen und Beschäftigten in Eigenregie ist grundsätzlich dazu geeignet, die datenschutzrechtlichen Grundsätze außer Acht zu lassen. Derartige Eigenentwicklungen orientieren sich zwar meist an den durch das Unternehmen vorgegebenen Verarbeitungszwecken. Jedoch liegt der Fokus meist auf der Umsetzung des maximal technisch Möglichen und weniger auf dem – datenschutzrechtlich gebotenen – zwingend erforderlichen Minimum. Ein Risiko besteht sowohl im Hinblick auf den Umfang der verarbeiteten personenbezogenen Daten als auch auf die technische und organisatorische Umsetzung der Betroffenenrechte. Zum Beispiel: Ist in der Anwendung eine maximale Speicherfrist hinterlegt? Kann in der Anwendung grundsätzlich eine Löschung kompletter Datensätze vorgenommen werden? Mag die Datenlöschung noch vermehrt Berücksichtigung finden, kann das hinsichtlich der Datenportabilität bereits anders aussehen.

Die Inanspruchnahme externer Dienstleister kann je nach Anwendungsbereich ebenfalls enorme Auswirkungen auf die datenschutzrechtliche Konformität der verantwortlichen Stelle haben. In Vergessenheit gerät hierbei oftmals, dass eine Beauftragung eines Dienstleisters unter Umständen auch form- und geräuschlos erfolgen kann. Nicht zwingend geht eine solche mit der Unterzeichnung eines Vertrages oder der Bezahlung einer entsprechenden Vergütung einher. Insbesondere im Bereich kostenloser Softwarelösungen, beispielsweise in Form von Cloud-Services oder Messenger-Diensten im weitesten Sinne ist eine einfache Zustimmung zu den Nutzungsbedingungen meist ausreichend. Darin enthalten sind oftmals Regelungen hinsichtlich der weitreichenden Verarbeitung von Metadaten, die eine Finanzierung des ansonst kostenfreien Produkts sicherstellen soll. Damit einher gehen datenschutzrechtliche Problematiken im Zusammenhang mit der Rechtmäßigkeit und Transparenz der Datenverarbeitung, der Vertraulichkeit personenbezogener Daten aufgrund unzureichender Verschlüsselung oder der Übermittlung personenbezogener Daten an Drittländer. Im Besonderen der letztgenannte Punkt stellt nahezu sämtliche verantwortliche Stellen auch abseits des Problemfeldes Schatten-IT vor große Herausforderungen. Auch eine grundsätzliche Prüfung der Geeignetheit und des datenschutzrechtlichen Bewusstseins des Dienstleisters findet meist nicht statt.

Hinsichtlich sämtlicher beispielhaft dargestellter Sachverhalte kommt erschwerend hinzu, dass neben einer fehlenden Überprüfung der zur Anwendung kommenden Schatten-IT auch die datenschutzrechtliche Dokumentation zur Erfüllung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nicht oder ausschließlich lückenhaft erfolgt.

Risiken aufgrund lückenhafter Dokumentation

Die datenschutzrechtlichen Folgen können mitunter massiv sein. Bereits die einzelnen Fachbereiche dürften ohne Unterstützung der IT-Abteilung und/oder des Datenschutzbeauftragten bzw. -koordinators nicht oder nur äußerts selten in der Lage sein, die Anforderungen an die datenschutzrechtlichen Prüfungen und Dokumentationen zu durchdringen, welche unter anderem bei Einführung eines neuen Systems, einer neuen Anwendung oder eines neuen Dienstes zu erfüllen sind. Vorrangig zu nennen ist hier die Feststellung und Klassifizierung schutzbedürftiger Datenkategorien, unabhängig davon, ob es sich hierbei um besondere Kategorien personenbezogener Daten i. S. v. Art. 9 DSGVO handelt. Nicht weniger komplex gestalten sich die Fälle in denen gar eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO erforderlich ist.

Besondere Anforderungen gelten zudem mit Blick auf den risikobasierten Ansatz. Dieser stellt ein prägendes Element der DSGVO dar, welches an vielen Stellen verankert ist, so u. a. in Art. 24, Art. 25, Art. 32, Art. 33 und 34 sowie Art. 35 DSGVO. Erforderlich ist in insoweit die Durchführung einer Risikoanalyse, wobei i. d. R. Aspekte der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen sind. Schwierigkeiten ergeben sich bereits dadurch, dass die DSGVO keine abschließende Definition des Risikos oder einer Risikobeurteilung bzw. -analyse bereitstellt. Angeführt werden als Bewertungskriterien lediglich Eintrittswahrscheinlichkeit und Schwere der Risiken. Unter Zugrundelegung bekannter Standards wie bspw. dem BSI-Standard 200-3 können – verkürzt dargestellt – die Identifikation der Risiken, Bestimmung möglicher Schäden und deren Eintrittswahrscheinlichkeit sowie Schadenshöhe bzw. -auswirkung und eine anschließende Risikobewertung durchzuführen sein. Daran schließt sich eine Risikobehandlung z. B. durch die Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen an.

Weitergehende Probleme ergeben sich, wenn eine Risikoanalyse im Rahmen der Melde- und Informationspflichten der Art. 33 und Art. 34 DSGVO aufgrund des Eintritts einer Verletzung des Schutzes personenbezogener Daten i. S. v.

Art. 4 Nr. 12 DSGVO erforderlich wird. Vorausgesetzt es gelingt die Feststellung und Klassifizierung einer derartigen Verletzung, bedarf es gleichsam einer entsprechenden Behandlung des Vorfalls unter Feststellung des Bestehens oder Nichtbestehens eines Risikos für die Rechte und Freiheiten natürlicher Personen sowie des Ergreifens daran anschließender Handlungs- und/oder Dokumentationspflichten. In der Regel wird dies nur dann durch die verantwortliche Stelle zielführend vorgenommen werden können, sofern zu den Verarbeitungstätigkeiten bereits vollumfängliche Dokumentationen vorliegen.

Trefflich muss daher die Frage gestellt werden, ob einzelne Fachabteilungen überhaupt in der Lage sein können, derartige Prüfungen durchzuführen und zu dokumentieren. Insofern erscheint es ohne Weiteres nachvollziehbar, dass die Anforderungen, an denen bereits Fachabteilungen scheitern dürften, für einzelne Beschäftigte schlichtweg nicht zu bewältigen sind.

Die Folgen für die verantwortlichen Stellen sind nicht zu unterschätzen. Zwar ordnet Art. 5 DSGVO im Einzelnen keine unmittelbaren Rechtsfolgen bei einem Verstoß an. Jedoch kann bereits ein Verstoß gegen die Konkretisierungsvorschriften des Art. 25 DSGVO bzw. Art. 32 DSGVO gemäß Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt sein. Daneben ist ebenfalls ein Verstoß gegen Art. 5 DSGVO gemäß Art. 83 Abs. 5 lit. a DSGVO sanktionsfähig.

Strategien zum Umgang mit Schatten-IT

Besonders aufgrund der drohenden Gefährdung der Sicherheitsziele nach Art. 32 DSGVO sowie den möglichen datenschutzrechtlichen Sanktionen, aber auch im Interesse der verantwortlichen Stelle selbst, bedarf es eines strategischen Umgangs mit der Thematik. Dabei können definierte Prozesse hinsichtlich der Anschaffung informationstechnischer Systeme, Anwendungen und Endgeräte oder bezüglich der Erweiterung bestehender Prozesse bzw. Verarbeitungstätigkeiten eine wesentliche Rolle einnehmen. Wie jedoch im Zusammenhang mit vielen Themen des Datenschutzes und der IT-Sicherheit, gelingt dies nicht ohne angemessene Einbeziehung und Berücksichtigung der Belange der Beschäftigten.

Definierte Prozesse sind nur ein Teilaspekt

Zu Beginn ist es sinnvoll, sich mit den bereits vorhandenen Ressourcen auseinanderzusetzen und durch die IT-Abteilung eine Übersicht über die im Einsatz befindlichen Endgeräte und Anwendungen sowie deren Verwendungszwecke erstellen zu lassen. Gegebenenfalls sind auch bereits einzelne nicht-freigegebene Ressourcen bekannt, die in der Übersicht als solche bereits Eingang finden können, d. h. es besteht die Möglichkeit einen ersten Schritt hin zur Identifizierung möglicher Schatten-IT zu machen. Darüber hinaus sollte ebenfalls erörtert werden, welchen Anforderungen die einzelnen Ressourcen genügen müssen. Dies können allgemeine Anforderungen der verantwortlichen Stelle oder einzelner Fachabteilungen, lizenzrechtliche Besonderheiten, aber eben auch datenschutzrechtlich bedeutsame Kriterien sein. Die Übersicht sowie der Katalog an Anforderungen bilden dann die Grundlage für die Anschaffung und den Betrieb weiterer Ressourcen. Ferner können nunmehr etwaige Mehrfachanschaffung von Anwendungen bzw. Systemen ausgemacht und minimiert werden.

Spätestens an diesem Punkt wird klar, dass es bezüglich der Anschaffung und des Betriebs von Ressourcen der Einbeziehung verschiedenster Akteure bedarf. Um für die gesamte verantwortliche Stelle eine einheitliche Bewertung sowie einen geregelten Ablauf zu sorgen, ist die Etablierung eines definierten Prozesses anzuregen. Dieser sollte grundsätzlich so aufgebaut sein, dass eine Eingabe etwaiger Bedürfnisse an zusätzliche Hard- oder Software auch durch einzelne Beschäftigte ermöglicht wird, die Einbeziehung verschiedener Akteure zur Bewertung der Erfüllung der zuvor definierten Anforderungen erfolgt sowie letzten Endes eine Freigabe zur Beschaffung bzw. des Betriebs durch die Leitung der verantwortlichen Stelle vorgenommen wird.

Unter Berücksichtigung der zuvor aufgeführten datenschutzrechtlichen Implikationen sowie der Aufgaben eines Datenschutzbeauftragten nach Art. 39 DSGVO kann es nur selbstverständlich sein, dass der Datenschutzbeauftragte einer der vorbenannten Akteure zur Bewertung der Erfüllung datenschutzrechtlicher Anforderungen sein muss. Gleiches gilt – soweit vorhanden – auch für den IT- bzw. Informationssicherheitsbeauftragten hinsichtlich der Aspekte der Daten- und Informationssicherheit.

Ferner sollte in Abstimmung der vorbezeichneten Akteure eine Richtlinie oder vergleichbare interne Vorgabe erarbeitet und implementiert werden, um eine langfristige Lösung zu schaffen. Ein Aspekt sollte die Aufnahme künftiger Kontrollmöglichkeiten – auch unter Mitwirkung der Beschäftigten – sein, um effektiv die aufgezeigten Risiken minimieren zu können. Ein solch definierter Prozess allein genügt in der Regel jedoch nicht. Grundsätzlich erfordert es Bewusstsein und Verständnis sämtlicher Beschäftigten für die Thematik und Problematik.

Einbeziehung der Beschäftigten

Es darf grundsätzlich nicht das Ziel der Organisation sein den Einsatz sämtlicher, aus Sicht der Beschäftigten effektiven, Systeme und Anwendungen zu untersagen oder eine Einführung durch Aufbürden umständlicher sowie langwieriger Prozesse faktisch unmöglich zu machen. Insbesondere die IT-Abteilungen müssen dazu angehalten werden, nicht „von vornherein“ jegliches Ersuchen

von Fachabteilungen und Beschäftigten abzulehnen, sondern, mitunter nach entsprechenden Dialogen, im Rahmen der vor allem eng begrenzten zeitlichen Ressourcen, in Prüfungen die Einsatzmöglichkeiten der Anwendungen und Systeme betreffend, einzusteigen. Dass dies insbesondere in Ausnahmesituationen wie einer pandemischen Lage inflationäre Ausmaße annehmen kann, ist hierbei bestenfalls gleichwohl zu beachten. Um andererseits eine Überlastung von IT-Abteilungen vorzubeugen, kann bspw. proaktiv – nach Prüfung der zuständigen Stellen – eine Aufstellung freigegebener Anwendungen und Dienste erfolgen, welche für die Beschäftigten zentral einsehbar sind und zur konkreten Nutzung „lediglich" eines Freigabeersuchens bei der IT-Abteilung bedarf. Gleichfalls muss es im Interesse der Beschäftigten liegen, dass die verantwortliche Stelle den erforderlichen datenschutz- und sicherheitsrechtlichen Prüfumfang durchführen kann. Diese Belange sind nach Möglichkeit in Ausgleich zu bringen.

Weiterhin ist durch eine angemessene Sensibilisierung der Beschäftigten die Problematik der Schatten-IT aufzuzeigen und für Verständnis für die Regulierung durch unternehmensinterne Prozesse zu sorgen. Der Umfang und das Ausmaß möglicher Sensibilisierungsmaßnahmen hängt dabei grundsätzlich von der Größe der verantwortlichen Stelle, den wesentlichen Sicherheitsanforderungen und gegebenenfalls existierenden Sensibilisierungskonzepten ab (siehe hierzu auch Weidenhammer/Just, DSB 2021, 128 ff.). Ziel muss es jedoch auf jeden Fall sein, dass ein offener Umgang der verantwortlichen Stelle mit der Thematik dazu führt, dass das Ausmaß an nicht-freigegebener Hard- und Software abnimmt. Dies kann nur gelingen, wenn Fachbereiche oder einzelne Beschäftigte über die Möglichkeit verfügen, einen Bedarf an zusätzlichen Mitteln zu kommunizieren.

Eine solche Kommunikationsmöglichkeit darf nicht nur auf zukünftig eintretende Bedürfnisse zugeschnitten sein, sondern sollte gleichfalls dazu führen, dass Fachbereiche und Beschäftigte bereits im Einsatz befindliche Anwendungen bzw. Endgeräte offenlegen. Selbstverständlich ist dabei auch, dass die verantwortliche Stelle nicht dazu verpflichtet sein kann, auf sämtliche Bedürfnisse und Anforderungen einzugehen. Jedoch ermöglicht der dargestellte Umgang die Verschaffung eines Überblickes hinsichtlich der Notwendigkeit bestimmter Ressourcen. Nur unter diesen Umständen kann es gelingen, die zuvor dargelegten Prüfungen und Prozesse im Alltag zielführend und erfolgsversprechend umzusetzen.

Handlungsempfehlungen

Für die verantwortliche Stelle können aus einer Existenz von Schatten-IT erhebliche Risiken hervorgehen. Dies betrifft einerseits die Abschwächung der Sicherheit der Verarbeitung aufgrund unzureichender technischer und organisatorischer Maßnahmen. Andererseits gehen die Einführung und der Betrieb nicht-freigegebener Hard- und Software oftmals mit einer mangelhaften datenschutzrechtlichen Dokumentation einher. Eine solche kann nicht nur durch entsprechende Bußgelder sanktioniert werden, sondern führt auch im Falle einer Datenschutzverletzung zu erheblichen Umsetzungsschwierigkeiten der weiteren datenschutzrechtlichen Verpflichtungen. Ursprung dieser erheblichen Risiken bildet im Kern die fehlende Einbeziehung der wesentlichen Akteure.

Entsprechende Strategien können dazu beitragen, vorhandene Schatten-IT zu reduzieren und deren zukünftige Entstehung vorzubeugen. Festzuhalten ist dabei, dass Schatten-IT ein wichtiger Indikator für Bedürfnisse der Beschäftigten zur Optimierung von Prozessen sein kann. Eine Einbeziehung der Beschäftigten ist demnach ein elementarer Bestandteil einer solchen Strategie. Daneben können insbesondere die folgenden Punkte weitere Teilaspekte der benannten Strategie sein:

- Bestandsaufnahme der bereits vorhandenen Ressourcen innerhalb der verantwortlichen Stelle sowie Implementierung eines Anforderungskatalogs bezüglich Neuanschaffungen unter Berücksichtigung der bestehenden Bedürfnisse von Fachbereichen oder einzelnen Beschäftigten.
- Einbeziehung wesentlicher Akteure, insbesondere zur Gewährleistung der Berücksichtigung datenschutz- und datensicherheitsrelevanter Kriterien.
- Implementierung eines definierten Prozesses zur Anschaffung von Hard- und Software unter Berücksichtigung einer Eingabemöglichkeit auch durch einzelne Beschäftigte.
- Sensibilisierung der Beschäftigten im Hinblick auf die vielfältigen Chancen und Risiken, welche mit Schatten-IT für die verantwortliche Stelle einhergehen.

Autoren: **Alexander Weidenhammer ist Rechtsanwalt im Dresdner Institut für Datenschutz, spezialisiert im IT-Sicherheits- und Datenschutzrecht und als externer Datenschutz- und Informationssicherheitsbeauftragter tätig.**

Max Just, LL.M. ist Wirtschaftsjurist im Dresdner Institut für Datenschutz, insbesondere auf öffentliche Stellen spezialisiert und als externer Datenschutz- und Informationssicherheitsbeauftragter tätig.