49187

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Datenschutz

1|2018

Rainer Seidlitz,
Datenschutzexperte bei der
TÜV SÜD Sec-IT GmbH

„Mit der DS-GVO bekommt der Datenschutz endlich den Stellenwert, den er längst verdient!“

DATAKONTEXT

www.itsicherheit-online.com

EU-DS-GVO UND BDSG-NEU SETZEN NEUE PRIORITÄTEN

DATENSCHUTZ AVANCIERT ZUM QUALITÄTSMERKMAL

Aufgrund des rasanten technischen Fortschritts, der damit einhergehenden Globalisierung und den resultierenden internationalen Verflechtungen, muss das Datenschutzrecht in Europa harmonisiert werden. Ziel ist es, das Schutzniveau bei der Verarbeitung personenbezogener Daten in der gesamten EU hoch und einheitlich zu gestalten. Dafür sorgt ab dem 25. Mai 2018 die Europäische Datenschutz-Grundverordnung (EU-DS-GVO). Ab diesem Stichtag wird die neue Verordnung in allen EU-Mitgliedstaaten anwendbares Recht und ersetzt in grundlegenden Bereichen das bislang bestehende Datenschutzrecht – in Deutschland insbesondere das Bundesdatenschutzgesetz (BDSG). An vielen Stellen bietet die Verordnung allerdings Öffnungsklauseln, die den einzelnen Ländern Spielraum für nationale Regelungsinhalte bieten. Der Deutsche Bundestag hat von dieser Möglichkeit Gebrauch gemacht und das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU verabschiedet, das ein die EU-DS-GVO ergänzendes Gesetz (BDSG-neu) darstellt und zeitgleich in Kraft tritt.

Obwohl die anstehenden Änderungen schon seit längerem bekannt sind, wirft deren konkrete Umsetzung nach wie vor viele Fragen auf, denen sich Unternehmen noch nicht mit dem gebotenen Ernst annehmen. Doch bis zum Stichtag bleibt nicht mehr viel Zeit und die Verantwortlichen für die Datenverarbeitung erkennen erst allmählich ihre umfangreichen Aufgaben und Rechenschaftspflichten, die mit den neuen Regelungen einhergehen. Wer angefangen hat, sich mit dem Thema zu beschäftigen, bemerkt die enormen Auswirkungen schnell – sowohl auf technischer als auch auf prozessualer Ebene. Die EU-DS-GVO stellt Unternehmen daher vor massive Herausforderungen, die diese bis zum Stichtag meistern müssen. Allerdings bietet diese große Aufgabe auch eine Chance: Die EU-DS-GVO fordert einen einheitlichen und geregelten Datenschutz und das kommt den Betroffenen entgegen. Die neue Verordnung bietet das Potenzial, Datenschutz als unabdingbares Qualitätsmerkmal zu etablieren, sichtbar zu machen und damit das Vertrauen von Kunden, Partnern und Mitarbeitern zu stärken und diese langfristig für sich zu gewinnen. Gleichzeitig werden bislang eventuell unterschätzte Risiken der Datenverarbeitung transparent und beherrschbar.

Datenschutz im Fokus – wichtige Änderungen

Mit Anwendung der EU-DS-GVO werden die Pflichten für Unternehmen im Hinblick auf den Datenschutz erweitert, vor allem was die systematische Auseinandersetzung der mit der Datenverarbeitung verbundenen Risiken betrifft. Auf Basis dieser Risikobewertung müssen Unternehmen geeignete technische und organisatorische Maßnahmen umsetzen und deren Wirksamkeit nachweisen können. Diese „Rechenschaftspflicht" fordert von Unternehmen, nachweisen zu können, dass sämtliche personenbezogenen Daten rechtskonform und gemäß EU-DS-GVO verarbeitet werden. Für mittlere und große Unternehmen ist diese Herausforderung am besten mit der Einführung eines Datenschutzmanagementsystems zu meistern, welches idealerweise mit bereits vorhandenen Managementsystemen verwoben wird. Synergien können damit optimal genutzt werden, sodass einer möglichen Prüfung durch die Aufsichtsbehörden gut vorbereitet entgegengesehen werden kann.

Eine zentrale Forderung der EU-DS-GVO (Art. 25) ist, IT-Systeme so auszulegen, dass die Einhaltung der Datenschutzgrundsätze durch Technik und datenschutzfreundliche Voreinstellungen gewährleistet wird. Das bedeutet, der Datenschutz muss als integraler und nachweisbarer Bestandteil in die Produkt- und Systementwicklung implementiert werden (Privacy by Design). In der Regel erfordert das eine Anpassung der entsprechenden Prozesse sowie die Einbindung von Datenschutzexperten. Ist bereits ein wirksames Qualitäts- und IT-Security-Management im Unternehmen etabliert, können die bestehenden Vorgehensweisen entsprechend erweitert werden, so dass im Idealfall ein integriertes Management entsteht. Gleichzeitig legt die EU-DS-GVO fest, dass der Datenschutz keine

Option mehr ist, die Unternehmen auswählen können oder nicht, sondern durch entsprechende Voreinstellungen zum Standard wird (Privacy by Default).

Das bisherige Bundesdatenschutzgesetz (BDSG) hat die Umsetzung von technisch-organisatorischen Maßnahmen gefordert, die je nach Art und Kategorie der zu schützenden Daten zu treffen waren. Die EU-DS-GVO hingegen fordert, diese Maßnahmen nun auch nach Verarbeitungszweck und Stand der Technik zu richten. Sie können beispielsweise so ausgelegt sein, dass eine Minimierung der Verarbeitung personenbezogener Daten vorgenommen wird oder dafür sorgen, dass personenbezogene Daten pseudonymisiert oder verschlüsselt werden.

Gemäß Art. 32 Abs. 1 d) EU-DS-GVO muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen eingeführt werden. Dieses Vorgehen entspricht ebenfalls der erforderlichen Vorgehensweise im Rahmen der Errichtung und Aufrechterhaltung von Managementsystemen. Bezüglich der Auseinandersetzung mit den Risiken der Datenverarbeitung fordert die EU-DS-GVO eine Datenschutz-Folgenabschätzung (DSFA), wenn für die Rechte und Freiheiten der betroffenen Person voraussichtlich ein hohes Risiko besteht. Auch für die DSFA gilt eine umfassende Dokumentationspflicht, welche insbesondere eine nachvollziehbare Bewertung dieser Risiken beinhaltet. Eine besonders große technische und organisatorische Herausforderung ist für viele Unternehmen das umfassende „Recht auf Vergessenwerden" gem. Art. 17 Abs. 1 EU-DS-GVO – ein grundlegendes Recht der betroffenen Personen. Demnach müssen Unternehmen für ihre Datenverarbeitungsprozesse wirksame Löschprozeduren erarbeiten, implementieren und diese auch nachweisen können. In diesem Zuge bedarf es vieler Klärungen, etwa zu Aufbewahrungspflichten, Speicherorten, Datenübertragung in vernetzten Systemen und zu Dritten, sowie die umfassend wirksame technische Löschung, die auch Archivsysteme betreffen kann.

Drohende Bußgelder rütteln wach

Ein Grund, warum viele Unternehmen das Thema Datenschutz bislang nicht priorisiert behandelt haben, war mangelndes Bewusstsein. Bußgelder drohten nur selten und waren – wenn verhängt – von vergleichsweise geringen Summen. Auch für den Umgang mit Datenpannen gab es bisher keine strengen Regelungen, da diese nur zu melden waren, wenn die betroffenen Daten besonders sensibel waren. Das wird sich mit der EU-DS-GVO ändern. Für Datenpannen gilt nach Art. 33 EU-DS-GVO eine regelmäßige Meldepflicht binnen 72 Stunden an die Aufsichtsbehörde. Geschieht diese Meldung nicht, können hohe Bußgelder fällig werden, die möglicherweise höher ausfallen als die Kosten, die durch die Datenpanne selbst schon anfallen. Daher sollten entsprechende Meldeprozesse mit der erforderlichen Detailtiefe und Effizienz bereits vorab installiert werden. Die EU-DS-GVO enthält einen Katalog von Kriterien, die Einfluss auf die Bußgeldverhängung und -bemessung haben. War das Nicht-Führen von internen Verarbeitungsübersichten bisher beispielsweise überhaupt nicht bußgeldbewehrt, droht nun ein Bußgeld von bis zu zehn Millionen Euro oder sogar bis zu zwei Prozent des weltweit erzielten Jahresumsatzes. In anderen Konstellationen kann sogar ein Bußgeld in Höhe von bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Jahresumsatzes verhängt werden. Diese Zahlen sind es, die das Unternehmensmanagement wachrütteln.

Interdisziplinäre Projektteams

Aufgrund der Komplexität des Themas und des nunmehr kurzen Zeitrahmens sollten Unternehmen umgehend entsprechende Umsetzungsprojekte initialisieren. Deren Erfolg hängt maßgeblich davon ab, welchen Reifegrad die Datenschutzorganisation bereits hat und mit welcher Intensität das Projekt vorangetrieben wird. Die Umsetzung muss dabei die volle Unterstützung des Managements erfahren und die Projektleitung sollte Hand in Hand mit Verfahrens- und Prozessverantwortlichen sowie mit technischen Ansprechpartnern für Applikationen und IT-Systeme arbeiten. Falls vorhanden, ist auch die Zusammenarbeit mit dem Datenschutzbeauftragten (DSB) und den IT-Security-Managern wesentlich. Die Unternehmensleitung sollte das Projekt mit ausreichend Ressourcen ausstatten, wodurch Datenschutz endgültig zur Chefsache wird.

Der Datenschutzbeauftragte: weiterhin zentrale Person

Eine wichtige Rolle spielt nach wie vor der DSB, den nichtöffentliche Stellen ergänzend zu Art. 37 EU-DS-GVO in Deutschland bestellen müssen, wenn sich in ihrem Betrieb in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 BDSG-neu). Die Aufgaben des DSB richten sich nach den Bestimmungen von Art. 39 EU-DS-GVO. Demnach berät er den Auftraggeber und die mit der Verarbeitung personenbezogener Daten Beschäftigten hinsichtlich ihrer Pflichten nach EU-DS-GVO, des novellierten BDSG und anderen Vorschriften über den Datenschutz und überwacht deren Einhaltung. Der DSB ist somit eine wichtige Person in einem DS-GVO-Projekt.

Datenschutz als Qualitätsmerkmal

Die hohe, mit der EU-DS-GVO einhergehende, Verantwortung sorgt aufgrund der vielfältigen anzugehenden Themen nach wie vor für Verunsicherung. Eine allumfassende Umsetzung bis zum 25. Mai 2018 werden wohl nur die wenigsten Unternehmen bewerkstelligen. In jedem Fall wichtig ist jedoch eine intensive Auseinandersetzung mit den Anforderungen und – sofern noch nicht erfolgt – der umgehende Start der Umsetzung, um im Bedarfsfall vorgenommene Maßnahmen nachweisen zu können. Wenn Unternehmen das Thema ernst nehmen und einen guten Datenschutz als nachhaltiges Qualitätsmerkmal erkennen, wird die EU-DS-GVO einen Beitrag zum Unternehmenserfolg leisten und eine notwendige Vertrauensbasis für die rasch voranschreitende Digitalisierung schaffen, die ohne integrierten Datenschutz zum unkalkulierbaren Risiko für alle Beteiligten wird. ■

RAINER SEIDLITZ,
Datenschutzexperte bei der
TÜV SÜD Sec-IT GmbH

„MIT DER DS-GVO BEKOMMT DER **DATENSCHUTZ** ENDLICH DEN STELLENWERT, DEN ER LÄNGST VERDIENT!“

*Interview mit **Rainer Seidlitz,** Datenschutzexperte bei der TÜV SÜD Sec-IT GmbH*

Kaum ein Unternehmen kommt heutzutage noch ohne personenbezogene Daten und deren Verarbeitung aus. Egal ob Kundendaten, Mitarbeiterdaten oder Daten von Partnern und Lieferanten – sie sind überall. Mit Anwendbarkeit der EU-Datenschutz-Grundverordnung (EU-DS-GVO) ab 25. Mai 2018 wird dem Schutz dieser Daten in Unternehmen europaweit eine höhere Priorität eingeräumt. Wem es gelingt, die Anforderungen der EU-DS-GVO angemessen umzusetzen, der kann Datenschutz langfristig als Qualitätsmerkmal in seinem Unternehmen etablieren und sich so gegenüber seinen Kunden, Partnern und Mitarbeitern als besonders vertrauenswürdig erweisen. Allerdings stellt die Umsetzung der EU-DS-GVO viele Unternehmen vor eine große Herausforderung – auch jetzt noch, kurz vor dem Stichtag. Rainer Seidlitz, Datenschutzexperte von TÜV SÜD, kennt viele dieser Sorgen und weiß, wie ihnen zu begegnen ist. Er erkennt einige Parallelen zu Ansätzen aus dem Qualitäts- und Risikomanagement und ist sich sicher: Eine gute Umsetzung der EU-DS-GVO ist am besten im Rahmen eines systematischen Managementansatzes möglich.

ITS: Die Datenschutz-Grundverordnung bringt viele Änderungen für alle Unternehmen, die mit personenbezogenen Daten arbeiten. Wer ist für die Umsetzung dieser Anforderungen verantwortlich?

Rainer Seidlitz: Die DS-GVO betont das Thema Verantwortung in neuem Ausmaß. Art. 24 EU-DS-GVO regelt die „Verantwortung des für die Verarbeitung Verantwortlichen“. Bei Unternehmen ist somit die Unternehmensleitung dafür verantwortlich, sich systematisch und nachweisbar mit den Risiken der Datenverarbeitung auseinanderzusetzen. Darauf aufbauend müssen angemessene technische und organisatorische Maßnahmen umgesetzt und – wenn erforderlich – überprüft und aktualisiert werden. Diese Verantwortung bedeutet auch, dass ausreichend Ressourcen zur Verfügung gestellt werden, die notwendig sind, um die Umsetzung der EU-DS-GVO erfolgreich zu ermöglichen.

ITS: Wie kann das Management diese Verantwortung wahrnehmen?

Rainer Seidlitz: Die Bereitstellung ausreichender Ressourcen ist auch im Qualitätsmanagement (QM) wesentlicher Erfolgsfaktor. So fordert Kapitel 7.1 der ISO 9001 die Bereitstellung ausreichender Ressourcen für den Aufbau, die Verwirklichung und die fortlaufende Verbesserung des QM-Systems. Der Fokus des Managements hat sich durch die Einführung von QM von der rein betriebswirtschaftlichen Betrachtung deutlich geweitet: Qualität hilft, die Gesamtleistung des Unternehmens zu steigern und gilt als gute Basis für eine nachhaltige Entwicklung. Mit der zunehmenden Verbreitung der ISO/IEC 27007 geraten auch virtuelle Risiken in Bezug auf die Nutzung und Verarbeitung von Informationen in den Blick des Managements. Schließlich wird mit der EU-DS-GVO nun endlich auch der Datenschutz zur

Chefsache. Wenn es die Unternehmensleitung schafft, diesen neuen Aspekt nicht isoliert zu betrachten, sondern Datenschutz als integrales Qualitätsmerkmal versteht, lassen sich bestehende Managementinstrumente nutzen, und es muss nicht von null begonnen werden.

ITS: Wie können Unternehmen fortlaufend sicherstellen, dass sie den Anforderungen der EU-DS-GVO gerecht werden?
Rainer Seidlitz: Für alle Arten von Managementsystemen sind regelmäßige Reviews unabdingbar. Denn damit ein System dauerhaft wirksam ist, sollte es in regelmäßigen Abständen begutachtet und beurteilt sowie gegebenenfalls optimiert werden. Was im QM schon lange vorgeschrieben ist, wird nun mit der EU-DS-GVO auch für den Datenschutz Pflicht. Nach Art. 32 Abs. 1d ist der für die Verarbeitung Verantwortliche dazu veranlasst, die eingerichteten Maßnahmen regelmäßig zu überprüfen, zu bewerten und zu evaluieren. Auf diese Art sind Unternehmen künftig dazu angehalten, die Sicherheit bei der Verarbeitung von personenbezogenen Daten in ihrem Betrieb zu gewährleisten.

ITS: Die systematische Auseinandersetzung mit Risiken ist längst fester Bestandteil des Qualitätsmanagements. Wie geht die EU-DS-GVO mit dem Thema um?
Rainer Seidlitz: Die EU-DS-GVO bringt das Thema „Risiken identifizieren und bewerten" nun auch für den Datenschutz auf den Tisch. Sie fordert eine Datenschutz-Folgenabschätzung (DSFA), wenn für die Rechte und Freiheiten der betroffenen Person voraussichtlich ein hohes Risiko besteht. Auch im QM wird die Beschäftigung mit potenziellen Risiken schon lange eingefordert. Da die Erhebung und Verarbeitung personenbezogener Daten bei vielen Unternehmensprozessen integraler Bestandteil ist, können auch diese Auswirkung auf die Qualität haben und müssten daher ebenfalls betrachtet werden, was aber noch nicht regelmäßig der Fall ist. Für die Einführung eines Informationssicherheitsmanagementsystems nach ISO/IEC 27001 ist die Einführung eines Prozesses für die kontinuierliche Ermittlung und Behandlung von Risiken schon lange Standard. Solche Vorgehensweisen können leicht auf die Anforderungen der EU-DS-GVO ausgeweitet beziehungsweise angepasst werden.

ITS: Mit der EU-DS-GVO wird auch das Thema „Dokumentationspflicht" für den Datenschutz wesentlich. Inwiefern ist ein Managementsystem hierbei hilfreich?
Rainer Seidlitz: Die verantwortliche Stelle muss die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen können. Um dieser „Rechenschaftspflicht" (Art. 5 Abs. 2 EU-DS-GVO) nachkommen zu können, ist neben der Umsetzung der entsprechenden technischen und organisatorischen Maßnahmen ein guter Dokumentenmanagementprozess wichtige Basis. Solche Prozesse zur Lenkung dokumentierter Informationen sind im QM längst Standard und sollten – wo vorhanden – auf die Datenschutzdokumentation übertragen werden.

ITS: Im Qualitätsmanagement gilt schon länger eine klare Prozessorientierung. Inwiefern sieht die EU-DS-GVO so einen Ansatz nun auch für den Datenschutz vor?
Rainer Seidlitz: Ein zentraler Aspekt der EU-DS-GVO sind die mit der Datenverarbeitung einhergehenden Verfahren. So fordert die EU-DS-GVO in Art. 30, dass die Verantwortlichen ein Verzeichnis über alle Verarbeitungstätigkeiten führen. In diesem Zuge muss beschrieben werden, in welchen Zusammenhängen die Verarbeitung personenbezogener Daten erfolgt. Grundlage dafür sind die entsprechenden Datenerhebungs- und Verarbeitungsprozesse. Auch die Forderung, dass Datenschutz durch Technik gestaltet wird, setzt voraus, dass die entsprechenden Anforderungen in die Produktentwicklungsprozesse integriert werden (Privacy-by-Design). Unternehmen, die diese Designprozesse bereits klar definiert und transparent gemacht haben, tun sich jetzt entsprechend leichter, die Datenschutzanforderungen ergänzend zu berücksichtigen. Gleiches gilt auch für die Umsetzung der „Rechte der Betroffenen", wie zum Beispiel Auskunftsrechte oder das „Recht auf Vergessenwerden", welche ohne wirksame Prozesse nicht oder zumindest nicht effizient umgesetzt werden können.

ITS: Im Zusammenhang mit der EU-DS-GVO hört man vor allem das Wort „Herausforderung" besonders oft. Inwiefern können Unternehmen und auch Betroffene aber letztlich von ihr profitieren?
Rainer Seidlitz: Die Umsetzung der EU-DS-GVO fördert durch Minimierung der Risiken der Datenverarbeitung und durch Transparenz das Vertrauen von Kunden, Partnern und den eigenen Mitarbeitern. Das kommt den Unternehmen langfristig zugute. Die EU-DS-GVO rückt die Betroffenen mit ihren Rechten in den Fokus des unternehmerischen Handelns und macht sich quasi zu deren Anwalt. So gibt es etwa Rechte auf Auskunft, Berichtigung und Löschung.

ITS: Während sich die großen Unternehmen Sorgen um die fristgerechte Umsetzung der EU-DS-GVO machen, sind die kleinen und mittelständischen Unternehmen (KMU) bislang eher wenig für das Thema sensibilisiert. Was ist Ihr Rat, wie sich besonders KMUs für die EU-DS-GVO wappnen können?
Rainer Seidlitz: Für KMUs gelten grundsätzlich die gleichen Vorgaben wie für große Unternehmen. Es gibt bereits umfangreiche Informationen und Arbeitshilfen, zum Beispiel von Verbänden oder Aufsichtsbehörden, die als Handreichungen zur Umsetzung der EU-DS-GVO verstanden werden können. Aber auch diese müssen unternehmensspezifisch angepasst werden und ersparen keinesfalls eine umfassende Auseinandersetzung mit dem Thema. Wichtig ist in jedem Fall, dass auch KMUs die Umsetzung der EU-DS-GVO als Managementaufgabe verstehen.

ITS: Vielen Dank für das Gespräch!

Das Interview führte Stefan Mutschler,
Chefredakteur IT-SICHERHEIT