GDPR / DSGVO – neue Chancen nutzen!

Zusammenfassung: Mit der Datenschutzgrundverordnung (DSGVO), die in der EU unmittelbar Gesetz ist, wird der Datenschutz mit Wirksamkeit zum 25. Mai 2018 modernisiert. Das alte Bundesdatenschutzgesetz (BDSG), zum 1. Januar 1978 in Kraft getreten, darf dann nach 40 Jahren, vier Monaten und 24 Tagen aktiver Zeit in den Ruhestand treten. Wie immer wenn der Nachfolger kommt, ergeben sich neue Chancen. Acht davon werden in diesem Praxistipp beschrieben.

Datenschutz modern: Klare Sprache, verständliche Regeln, internationale Ausrichtung, abschreckende Bußgelder, Recht auf Vergessenwerden – die DSGVO bringt eine umfassende Modernisierung des Datenschutzes mit sich. Dabei kümmert sich dieses europaweit gültige Gesetz um das Grundrecht auf informationelle Selbstbestimmung. Dieses ist für Menschen, denen an ihrer persönlichen Freiheit noch etwas liegt, eines der wichtigsten Grundrechte in dieser technikorientierten Zeit. Dass die EU immerhin die Kraft hatte, dieses Grundrecht deutlich zu stärken, ist bemerkenswert.

EU war in der Pflicht Der Österreicher Max Schrems hatte seinen Account bei Facebook gekündigt, über den er einen großen Teil seines Lebens mit anderen geteilt hatte. Obwohl seine Daten nach der Kündigung nach österreichischem Datenschutzrecht eigentlich nicht mehr hätten da sein dürfen, ergab eine Betroffenenanfrage bei Facebook Europe in Irland, dass die gespeicherten Daten, die eigentlich gar nicht mehr hätten da sein dürfen, ausgedruckt immerhin noch 1.800 DIN A4-Seiten ergaben. In zahlreichen Interviews stellte er dann die Frage, wer denn seine Grundrechte schützen könne und ob diese tatsächlich existieren oder nur auf dem Papier stehen. Österreich konnte sie nicht schützen, da Facebook dort keine Niederlassung hat. Irland durfte nicht (selbst wenn man gewollt hätte), weil Schrems kein Ire ist. Blieb nur die EU, die mit der Datenschutz-Richtlinie von 1995 nur einen zahnlosen Tiger im Angebot hatte. Das war letzten Endes der Anstoß für die GDPR oder DSGVO, wie wir sie heute kennen.

Rigoroser und konsequenter Verbraucherschutz: Die GDPR / DSGVO ist gnadenlos am Verbraucherschutz orientiert. Die betroffene Person und deren Rechte und Freiheiten zu schützen ist ein Ziel, das in allen Bereichen dieses modernen Gesetzeswerkes zu spüren ist. Die Betroffenenrechte wurden ausgeweitet, die besonderen Kategorien von Daten wurden ergänzt um genetische und biometrische Daten, das Recht auf Vergessenwerden und damit auf Mitnahme der Daten bei Wechsel des Anbieters kam neu hinzu. Diese Konsequenz hatte das BDSG nicht aufzuweisen. Rigoros sind die Folgen bei Verstößen gegen die Regelungen der DSGVO.

Bußgelder neu geregelt: Betroffene haben ein Recht darauf, dass Verstöße gegen ihre Rechte sanktioniert werden. Die drohenden Bußgelder sind nicht nur deutlich höher als bisher (bis zum 400fachen). Sanktionen müssen darüber hinaus angemessen, wirksam und abschreckend sein. Bei einer Bußgeldhöhe von 20.000.000 Euro oder – falls höher – bis zu 4% des weltweit getätigten Konzern-Jahresumsatzes drohen ernste wirtschaftliche Folgen. Das wir auch außereuropäische Konzerne dazu bringen, sich endlich mit dem Datenschutz europäischer Auslegung zu beschäftigten.

Erste Chance Bußgelder Die drohenden hohen Bußgelder führen dazu, dass Datenschutz auch in deutschen Unternehmen ernster genommen wird als bisher. Ob die hohen Bußgelder in Deutschland jetzt tatsächlich ein reales Risiko darstellen, ob die faktische Gefahr besteht, dass die Höhe auch wirklich ausgeschöpft wird, ist dabei nicht von Bedeutung. Alleine die Tatsache, dass diese Summen im Raum stehen, erfordert eine Reaktion beim Risikomanagement. Dafür werden schon Banken und Wirtschaftsprüfer sorgen. Die Chance, dass Datenschutz künftig auch in den Unternehmen ernst genommen wird, in denen er bisher eher eine Alibi-Rolle gespielt hat, ist deutlich gestiegen.

Zweite Chance Garantien: Verantwortliche müssen „Garantien“ abgeben. Art. 25 DSGVO verpflichtet Verantwortliche, die notwendigen Garantien bei der Verarbeitung abzugeben, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen. Im Art. 28 werden Verantwortliche verpflichtet, nur solche Auftragsverarbeiter zu beauftragen, die ebenfalls entsprechende Garantien abgeben. Diese Garantien sollen durch geeignete Zertifizierungen untermauert werden. Damit betritt deutscher Datenschutz Neuland. Garantien sind eigentlich nur mit Zertifizierung ernst zu nehmen. Zertifizierungen erfordern ein Managementsystem. Das wiederum bedeutet, alle im Unternehmen müssen zum Gelingen beitragen. Datenschutz ist endgültig aus der Exotenecke heraus.

Dritte Chance Gestaltungsdatenschutz: Bisher war Kontrolldatenschutz, jetzt ist Gestaltungsdatenschutz. Die Anlage zu § 9 BDSG bestand aus Kontrollanordnungen, von der Zu-

trittskontrolle zur Trennungskontrolle. Dieses für preußisches Recht typische Anordnen ist einem deutlich flexibleren Gestaltungsdatenschutz gewichen. Die eher von angelsächsischer Rechtsgestaltung geprägte DSGVO kennt stattdessen die in der Informationstechnik heute gebräuchlichen Begriffe Integrität, Vertraulichkeit und Verfügbarkeit. Daneben spielen Verschlüsselung und Pseudonymisierung eine große Rolle (Art. 32 DSGVO). Außerdem ist ein Business Continuity Management (BCM) gefordert. Kurz gesagt, ist es den Verantwortlichen weitgehend selbst überlassen, wie sie den Datenschutz gestalten, wenn sie nur die Einhaltung der genannten Anforderungen garantieren.

Vierte Chance Internationalität: Die EU mit ihren 800.000.000 Verbrauchern ist für amerikanische und asiatische Unternehmen ein sehr wichtiger Markt. Diesen wollen sie nicht verlieren. Aber bislang war für diese Unternehmen Datenschutz in der EU in seiner ganzen Zerrissenheit schlicht nicht erkennbar. Erst jetzt, wo EU-weit geltende Standards definiert sind und die drohenden Bußgelder auch diesen Unternehmen richtig wehtun können, wird das Thema dort ernst genommen. Versuchte man bisher, einen außereuropäischen Auftragsverarbeiter zur Unterzeichnung eines Vertrags mit EU-Standardvertragsklauseln zu bewegen, erntete man nicht selten Unverständnis. Das hat sich schon jetzt spürbar geändert. Vor allem für die angebotsorientierten US-amerikanischen Rechtsanwälte ist das Thema, so paradox das klingt, erst durch die drohenden hohen Bußgelder attraktiv geworden. Datenschützer werden plötzlich verstanden und ernst genommen.

Fünfte Chance betroffene Person: Die konsequente Ausrichtung des Datenschutzes an den Rechten und Freiheiten der betroffenen Person verändert auch die Risikobeurteilung. Auch wenn das nach dem alten Datenschutzrecht eigentlich schon immer so war, hatten etliche Unternehmen den Datenschutz weniger wegen der Betroffenenrechte, als mehr zur Vermeidung oder Minimierung eigener Risiken betrachtet. Die jetzt zwingend geforderte Risikobetrachtung des Art. 32 DSGVO stellt eindeutig die betroffene Person und deren Rechte und Freiheiten in den Vordergrund, und zwar ganz formell. Sowohl bei den Verarbeitungstätigkeiten als auch bei den damit zusammenhängenden technischen und organisatorischen Maßnahmen müssen die Risiken aus Sicht der betroffenen Personen ermittelt, beschrieben und mit geeigneten Maßnahmen minimiert werden. Diese neue Sicht erfordert neue Methoden, was dem Datenschutz nur gut tun kann.

Sechste Chance Managementsystem: Um der besonderen neuen Rolle des Verantwortlichen gerecht werden zu können, kann Datenschutz künftig nur noch als Managementsystem ausgeführt werden. Ob sie wollen oder nicht, müssen sich jetzt Geschäftsführer mit dem Thema beschäftigten. Auch wenn Datenschutzbeauftragte schon bisher eine Stabsstelle innehatten und direkt der Geschäftsführung zu berichten hatten, so ist Datenschutz als Managementsystem mit verbindlichen Vorgaben, Freigabe von Dokumenten und systematischen Überprüfungen doch noch einmal eine ganz andere Hausnummer als bisher. Das wird Auswirkungen auf die Budgets des Datenschutzes haben und stärkt die Position von Datenschutzbeauftragten.

Siebte Chance Informationssicherheit: Durch die geforderten Garantien im Zusammenhang mit den technischen und organisatorischen Maßnahmen wachsen die Aufgaben des Datenschutzbeauftragten und Informationssicherheitsbeauftragten immer mehr zusammen. Statt zweimal ein eigenes System vorzuhalten bringen die Gemeinsamkeiten von Datenschutz und Informationssicherheit deutliche weniger Aufwand als wenn beide Systeme jeweils voll eigenständig wären. Gleichzeitig bekommen Datenschutzbeauftragte durch die enge Zusammenarbeit deutlich mehr Einblicke in die Abläufe der IT als das vorher der Fall war.

Achte Chance veränderte Verantwortung: Datenschutzbeauftragte sind, anders als bisher, mit deutlich weniger persönlicher Verantwortung belegt. Diese verschiebt sich hin zum Verantwortlichen, also zur Geschäftsführung. Damit kann man die Funktion des DSB mehr mit der des Steuerberaters vergleichen – dieser bereitet die Bilanzen vor, die Steuerpflichtigen unterschreiben sie und haften. So ist das auch beim Datenschutzbeauftragten. Der Verantwortliche muss handeln und sollte sich dazu der Kenntnisse und Fertigkeiten des Datenschutzbeauftragten bedienen. Eine neue Rolle, an die sich Datenschutzbeauftragte erst einmal gewöhnen müssen.

Ein großer Wurf: Die DSGVO ist für die Rechte der betroffenen Personen, aber auch für die Erleichterung der Arbeit der Datenschutzbeauftragten ein großer Wurf, den viele der EU nicht mehr zugetraut hätten. Werden die Chancen in den deutschen Unternehmen jetzt genutzt, werden ganz nebenbei auch die Chancen für datenschutzkonformes Datamining (und damit einer besseren wirtschaftlichen Verwertbarkeit der eigenen Datenbestände) deutlich größer. Doch dazu folgt noch ein eigener Praxistipp.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de.