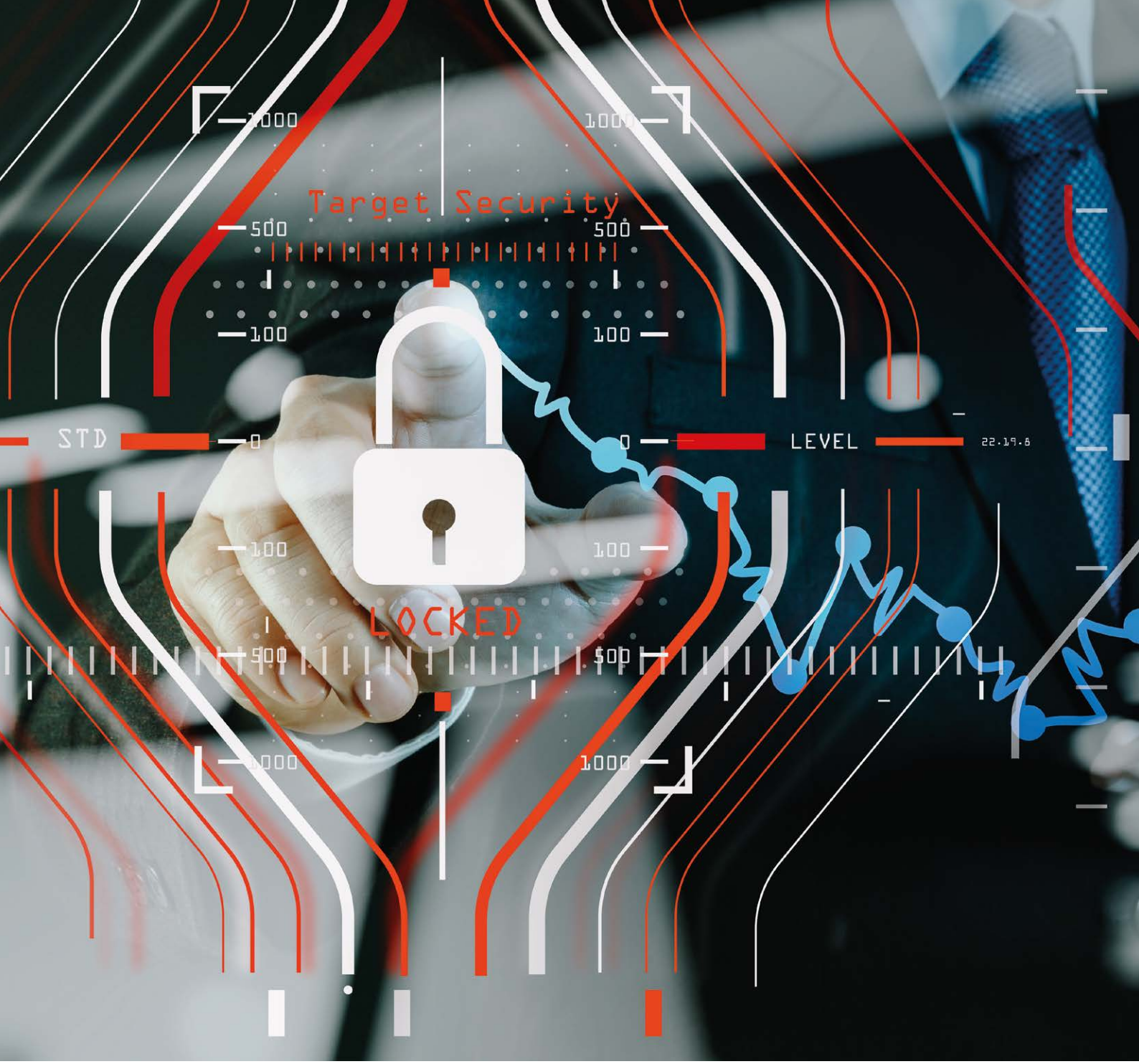

Die neue EU-Datenschutz-Grundverordnung – eine Chance für Unternehmen

Christian Vellmer, PROMATIS Gruppe

Am 25. Mai dieses Jahres beginnt eine neue Zeitrechnung für den Datenschutz in Europa. Die Datenschutz-Grundverordnung (DSGVO) kommt auf alle Unternehmen in Europa zu und wird das wirtschaftliche Handeln miteinander nachhaltig verändern. Personenbezogene Daten werden nicht mehr nur verkauft oder getauscht, sie müssen ab diesem Tag überprüft und hinterfragt werden. Wie wird sich das auf das tägliche Umfeld der Unternehmen auswirken und was ist eigentlich zu tun, um immensen Strafen zu entgehen? Dieser Beitrag beschäftigt sich mit dieser Fragestellung und wird aufzeigen, dass die kommende Datenschutz-Grundverordnung gar nicht so viel verändert, wie bisher kundgetan wird.

Kernpunkte der neuen DSGVO	
Harmonisierung des Datenschutzrechts	Vereinheitlichung von 28 nationalen Rechten
Weltweite Anwendbarkeit	Organisationen innerhalb und außerhalb der EU unter bestimmten Voraussetzungen
Stärkung der Betroffenenrechte	Recht auf Löschung kann vom Nutzer jederzeit verlangt werden
Verbindliche Meldepflicht	Gegenüber Behörden innerhalb von 72 Stunden, Nutzern unverzüglich
Gesamtschuldnerische Haftung	Von verantwortlichen Stellen und Auftragsverarbeitern
Opt-in Einwilligung	Transparenz und Verbindlichkeit für den Nutzer
Datenübermittlung	Datenschutzrechte an Daten gebunden, weltweite Anwendung
Hohe Bußgelder	Bis zu 4% des weltweiten Jahresumsatzes oder 20 Mio. €
Bedürfnis nach Datensicherheit	Forderung nach Datenschutz durch Technikgestaltung und Sicherheit der Verarbeitung

Abbildung 1: Anforderungen der neuen DSGVO

25. Mai 2018 – wie ein Damoklesschwert schwebt dieser Termin über den Unternehmen. Die Datenschutzbeauftragten flattern nervös von einer Abteilung zur nächsten und versuchen in den verbleibenden Wochen, ihr Unternehmen datenschutzkonform zu gestalten. Zwischenzeitlich haben auch die wenig datenschutzinteressierten Mitarbeiter mitbekommen, dass an diesem Stichtag die neue Datenschutz-Grundverordnung in Kraft tritt, ein europaweites Gesetz, das massiv Einfluss auf die gesamten IT-Prozesse nimmt.

Doch woher kommt diese Hektik, obwohl der Beschluss doch schon seit zwei Jahren bekannt ist? Ganz einfach, das ist die Fünf-vor-zwölf-Taktik der Unternehmen, die – bewusst oder unbewusst – das Thema erstmal zur Seite geschoben haben und darauf bauten, nicht beachtet zu werden. Die Umsetzung der neuen Vorgaben ist ein Kostenfaktor für die Unternehmen, der nicht unerheblich ist. Diese Vorgehensweise geht jetzt nicht auf, denn plötzlich ist die DSGVO in aller Munde – quer durch alle Medien. Ein Grund dafür ist, dass wirtschaftliche Faktoren zu berücksichtigen sind und somit die Thematik an Brisanz gewinnt. So müssen die Unternehmen bei Nichteinhaltung der Regularien vier Prozent des weltweiten Jahresumsatzes oder zwanzig Millionen Euro Strafe zahlen – das sind Dimensionen, die aufschrecken lassen!

Eine europaweite Verordnung, die jeden betrifft

Laut einer IDC-Studie im November 2017 sind 44 Prozent der Unternehmen in Deutschland auf die neue Datenschutzverordnung nicht vorbereitet beziehungsweise sehen den Änderungen gelassen entgegen. Doch nun heißt es, sich aktiv mit der Thematik auseinanderzusetzen, denn die neue DSGVO umfasst 99 Artikel, die mit mehr als 170 Anmerkungen ein komplexes und inhaltsreiches Kompendium darstellt, das es in jedem Unternehmen umzusetzen gilt. Ziel dieses Werks ist, für ein einheitliches Datenschutzrecht innerhalb der EU zu sorgen und insbesondere die Rechte und Kontrollmöglichkeiten bei der Erhebung und Verarbeitung personenbezogener Daten zu stärken. Für Unternehmen bedeutet das eine erhöhte Transparenz sowie eine umfassende Informationspflicht in Bezug auf den Umgang mit Daten. Diese Vorgaben sind bindend und die Bußgelder bei Nichteinhaltung erheblich.

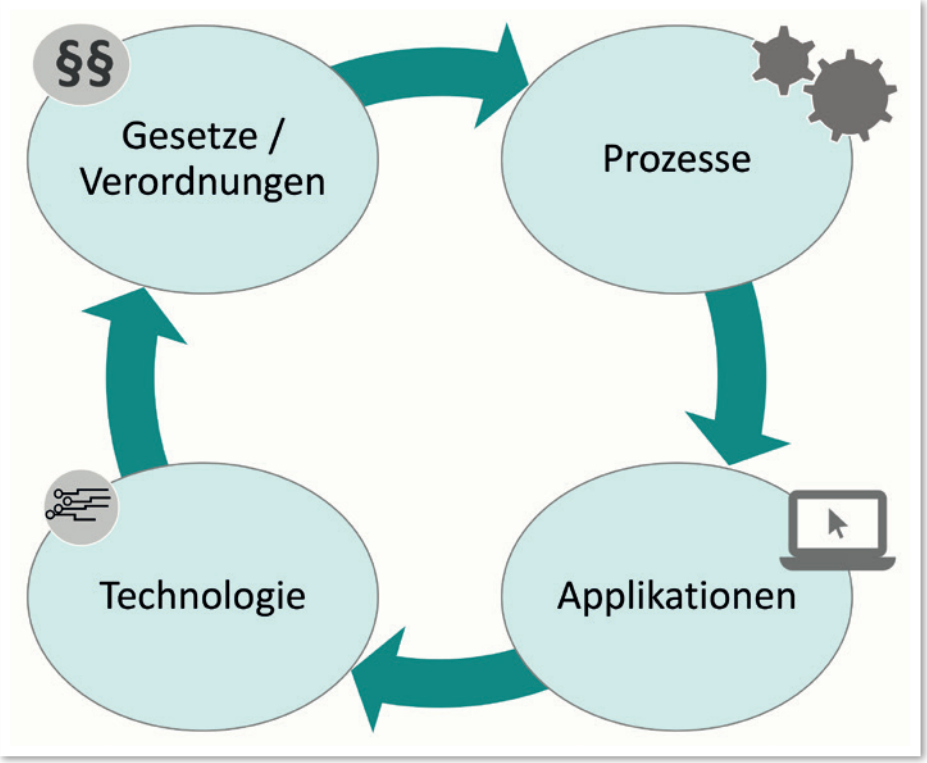

Abbildung 2: Erfolgsfaktoren im Zusammenspiel

Rechtliche Anforderungen und Grundsätze der DSGVO

Die DSGVO sieht in Artikel 5 eine Vielzahl von allgemeinen Grundsätzen vor. Sie stellen so etwas wie die Grundregeln für die Verarbeitung von personenbezogenen Daten dar und helfen insbesondere bei der Auslegung von Regelungen der DSGVO. Normiert sind die Themen „Rechtmäßigkeit, Verarbeitung

nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit". So müssen personenbezogene Daten folgende Kriterien erfüllen:

- Auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
- Für festgelegte, eindeutige und legitime Zwecke erhoben sein und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
- Auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
- Sachlich richtig und auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.
- In einer Form gespeichert sein, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- In einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Verstöße gegen die in Artikel 5 der DSGVO normierten Grundsätze können Maßnahmen der Aufsichtsbehörden nach sich ziehen. Die Anforderungen und Auswirkungen für Unternehmen sind insbesondere vor dem Hintergrund dieser Sanktionen erheblich *(siehe Abbildung 1)*.

Auswirkungen auf die Unternehmen

Unternehmen, die mit personenbezogenen Daten arbeiten, was praktisch in jedem Betrieb der Fall ist, müssen also sehr genau darauf achten, die genannten Vorgaben einzuhalten. Geeignete technische und organisatorische Maßnahmen sind zu treffen, um die Rechte der Betroffenen zu bewahren. Dies betrifft nicht nur organisatorische Schritte wie beispielsweise die Datenerhebung, sondern es wird auch eine transparente Darstellung aller relevanten Prozesse sowie die Anpassung aller technischen Geräte und Software gefordert. Die betrieblichen, technischen, organisatorischen und rechtlichen Anforderungen der neuen DSGVO fordern von den Unternehmen sichere Konzepte.

Intelligente Lösungen statt operativer Hektik

Statt in blinden Aktionismus zu verfallen, ist es erforderlich, die verbleibende Zeit gut zu planen, denn im Grunde befasst sich die DSGVO ja nur mit der Verarbeitung von personenbezogenen Daten. Das hört sich nicht so gewaltig an – kratzt man jedoch ein wenig an der Oberfläche, zeigt sich, wo überall in dem enormen und verzweigten Netzwerk der Unternehmens-IT diese Daten zu finden sind.

Um die Anforderungen gesetzeskonform umzusetzen, gibt es nun zwei Möglichkeiten: entweder selbst die unzähligen Stellen in der umfassenden digitalen Unternehmenswelt mühsam zu suchen, um danach die Änderungen individuell zu realisieren, oder die Aufgabe an einen Experten zu übertragen. Dabei müssen bestimmte Voraussetzungen erfüllt sein: ein tiefes Verständnis der Gesetze sowie der Anwendungsbereiche gepaart mit fundiertem Know-how der gesamten Unternehmensprozesse und Datenstrukturen.

Die Vorgehensweise der externen Spezialisten orientiert sich meistens an der klassischen Handhabung: Analyse, Konzeption, Umsetzung. Auch hier nichts Neues, wenn der Fokus des Verfahrens auf der Analyse liegt, denn je detaillierter und systematischer die Untersuchungen der Systeme durchgeführt werden, desto schneller und somit auch effizienter kann die Umsetzung erfolgen *(siehe Abbildung 2)*.

Optimierung der Prozesse

Ein weiterer Vorteil einer umfassenden Analyse liegt in dem Erkennen von Schwachstellen, unnötigen Prozessen und Daten, redundanten Vorgängen und vielen weiteren Punkten, die eine IT-Landschaft belasten. Um für Unternehmen pragmatische und valide Konzepte erstellen zu können, ist eine systematische Intelligenz erforderlich, die sowohl die Gesetzesvorgaben als auch die Prozessstrukturen innerhalb des Unternehmens kennt. Diese Methodik spiegelt sich auch in der Umsetzung wider, praxisorientierte Lösungen mit minimalem Aufwand zu implementieren. Das ist die große Chance, die durch die Einführung der DSGVO für die Unternehmen besteht. Aufgrund der detaillierten und vor allem systematischen Betrachtung können Prozesse optimiert, Daten minimiert und die Transparenz erhöht werden. Mit diesem Vorgehen können Unternehmen ihr jahrelanges Ignorieren der DSGVO in einen einmaligen Vorteil wandeln und die gesamte IT-Landschaft innerhalb kürzester Zeit gesetzeskonform, valide, schlank und bereinigt gestalten.

Christian Vellmer
Christian.vellmer@promatis.de

Der DOAG Jahresbericht 2017 ist online

Highlights, Neuigkeiten, Herausforderungen: Der Jahresbericht 2017 gibt dazu Auskunft. Auf 32 Seiten lassen die DOAG-Verantwortlichen das vergangene Jahr Revue passieren. Vorstandsvorsitzender Stefan Kinnen sieht den Verein auf einem sehr guten Weg, wie er in seinem Vorwort im Jahresbericht betont. Im Hinblick auf die Cloud richteten Mitglieder jetzt auch andere Fragen und Erwartungen an den Verein: „Neben technischen und methodischen Themen sind nun auch rechtliche sowie wirtschaftliche Aspekte relevant." Bei Themen wie IT-Sicherheit, Datenschutz und notwendige Zertifizierungen bleibe die DOAG „nachhaltig am Ball, um unseren Mitgliedern beim schrittweisen Weg in die Cloud wertvolle Hilfestellungen geben zu können." Auch wiederkehrende Fragestellungen aus dem Alltag – wie die Qualität des Oracle Supports oder Lizenzfragen in virtuellen Umgebungen – wird die DOAG laut Kinnen im Blick behalten.

Der DOAG Jahresbericht 2017 ist ab sofort hier verfügbar: *„https://www.doag.org/formes/pubfiles/10046451/docs/DOAG/Delegiertenversammlungen/2018/2017-DOAG-Jahresbericht-Web.pdf"*.