Michael Kötting / Dr. Martin Jonas

Umsetzung der Datenschutz-Grundverordnung in Versicherungsunternehmen: Auswirkungen auf Organisation, Prozesse und IT

Sehr geehrte Damen und Herren, ich bin Kunde Ihres Unternehmens und möchte mich mit diesem Schreiben an Ihren Datenschutzbeauftragten richten. Bitte stellen sie mir folgenden Informationen innerhalb der nächsten vier Wochen zur Verfügung: (1) Bitte geben Sie mir Auskunft über alle Informationen, welche Sie über meine Person gespeichert haben. (2) Stellen Sie mir darüber hinaus bitte eine elektronische Kopie aller meiner von Ihnen gespeicherten und verarbeiteten persönlichen Daten bereit. (3) Bitte nennen Sie mir im Detail alle Zwecke, zu welchen Sie meine persönlichen Daten in Vergangenheit, Gegenwart und Zukunft eingesetzte haben bzw. einsetzen werden. (4) Bitte nennen Sie alle anderen Parteien, welche mit meinen Daten in Berührung kommen bzw. kamen. (5) Bitte geben Sie an, über welchen Zeitraum Sie meine persönlichen Daten speichern. Differenzieren Sie dabei bitte anhand der Datenkategorien. (6) Sofern Sie Daten über meine Person aus anderen Quellen beziehen, nennen Sie mir bitte alle Informationen zu dieser Quelle. Vielen Dank und beste Grüße!

Auf ein solches oder ein ähnliches Schreiben müssen sich Versicherungsunternehmen ab dem 25. Mai 2018 einstellen. Zu diesem Zeitpunkt tritt die Datenschutz-Grundverordnung (DSGVO) verbindlich in Kraft und stattet Kunden mit zusätzlichen Datenschutzrechten aus. Versicherungsunternehmen, welche solche einem Schreiben gelassen entgegensehen, sind bereits besser vorbereitet als viele Mitbewerber. Sollten Unternehmen noch Nachholbedarfe sehen, gibt der folgende Artikel wichtige Anhaltspunkte und Impulse zur ordnungsgemäßen Umsetzung der DSGVO.

1. Grundsätzliche Aspekte zur DSGVO

Am 25. Mai 2018 wird die Datenschutz-Grundverordnung (DSGVO) verbindlich in Kraft treten. Die Verordnung der Europäischen Union verfolgt dabei das Ziel, personenbezogene Daten zu schützen und Dateneigentümer durch zusätzliche Rechte zu stärken. Niedergeschrieben sind diese Ziele im ersten Artikel der DSGVO, in dem es heißt, dass die Verordnung die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten wahrt.[1] Um diesem Anspruch gerecht zu werden definiert die DSGVO europaweit gültige Regeln für die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen. Neben dem Schutz personenbezogener Daten, soll die Verordnung darüber hinaus den freien Datenverkehr innerhalb des Europäischen Binnenmarkts gewährleisten.[2]

Nach dem die DSGVO in den vergangenen Jahren das Europäischen Parlament durchlaufen hat, darf sie bereits seit dem 24. Mai 2016 angewendet werden. Die bisher geltende Richtlinie 95/46/EG zum „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ wird dazu durch die DSGVO ersetzt.[3] Da es sich bei der DSGVO um eine europäische Verordnung handelt, wird diese zum Stichtag 25. Mai 2018 direkt in den europäischen Mitgliedsstaaten Gültigkeit besitzen, ohne dass die Richtlinie in nationales Recht überführt werden muss. Gleichwohl gilt es nationale Gesetze unter Berücksichtigung der DSGVO anzupassen, damit die nationale Gesetzgebung dem führenden Europarecht nicht widerspricht. In Deutschland ist die Anpassung in Form des überarbeiteten Bundesdatenschutzgesetzes (BDSG) zum 5. Mai 2017 erfolgt.

Neben der bisher geltenden Gesetzgebung orientiert sich die Mehrheit der deutschen Versicherungsunternehmen zusätzlich am Code of Conduct des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV). So konkretisiert der Code of Conduct bisher Aspekte der Gesetzgebung für die Versicherungswirtschaft. Damit der Code of Conduct auch in Zukunft seiner Funktion als versicherungsspezifisches Verhaltensreglement nachkommen kann und den Grundsätzen der DSGVO und des neuen BDSG entspricht, soll dieser bis 2018 ebenfalls überarbeitet werden. Besonders anzumerken ist, dass sowohl die DSGVO als auch bereits das bis dato geltende BDSG, die Formulierung von Verhaltensregeln, die nach Maßgabe der Besonderheiten einzelner Branchen ausgestaltet sind, explizit befürwortet.

2. Anforderungen der DSGVO

Die DSGVO definiert im Verordnungstext zahlreiche Anforderungen an Unternehmen. Bei genauerer Analyse fällt allerdings auf, dass viele Punkte nicht grundsätzlich neu sind, sondern bereits in den gegenwärtigen Ausführungen des BDSG gefordert werden und sich nun in ähnlicher Art und Weise in der DSGVO wiederfinden. Darüber hinaus profitieren Versicherer, welche sich am Code of Conduct des GDV beteiligen. Der Code of Conduct fordert bereits in seiner bisherigen Version ergänzende Aspekte zum BDSG und verringert somit die Lücke zwischen Status quo und den neuen Anforderungen der DSGVO.

Trotz Ähnlichkeiten sind dennoch bei einigen Anforderungen Verschärfungen der bisherigen Gesetzeslage zu beobachten. Diese Verschärfungen zeigen sich beispielsweise in Beweislastumkehrungen, Verkürzungen von Reaktionszeiten und Ausweitungen von Informationspflichten und Betroffenenrechten. Verweigern sich Unternehmen der DSGVO, müssen sie in der Konsequenz die Verarbeitung personenbezogener Daten einstellen. Verarbei-

Michael Kötting
Senior Consultant der Managementberatung zeb. Seine Tätigkeitsschwerpunkte liegen unter anderem in IT-Strategien und IT-Transformationen von Versicherern.

Dr. Martin Jonas
Manager der Managementberatung zeb. Er befasst sich mit der ganzheitlichen Umsetzung neuer regulatorischer Anforderungen in der Finanzbranche und deren Auswirkung auf Unternehmensstrategie und -steuerung.

ten sie dennoch widerrechtlich personenbezogene Daten, sieht die DSGVO Strafen von bis zu 20 Mio. Euro bzw. bis zu 4% des weltweiten Jahresumsatzes vor.[4]

Abbildung 1

Im Wesentlichen werden sechs zentrale Grundsätze von der DSGVO forciert. Bei den Grundsätzen handelt es sich um die Rechtmäßigkeit der Verarbeitung, die Verarbeitung nach Treu und Glauben, die Transparenz der Verarbeitung, die zweckgebundene Verarbeitung, die Minimierung und die Richtigkeit der Daten, die Speicherbegrenzung sowie die Integrität und Vertraulichkeit.[5] Darüber hinaus muss von den Unternehmen der Nachweis erbracht werden, dass die genannten Grundsätze in ausreichendem Maße eingehalten werden.[6] Die sogenannte Rechenschaftspflicht stellt im Vergleich zu bisherigen Rechtsgrundlagen eine Umkehr der Beweislast dar.

Ausgehend von den aufgeführten Grundsätzen definiert die DSGVO konkrete Anforderungen an die Unternehmen. Diese Anforderungen spiegeln sich zum einen in den Pflichten des Versicherungsunternehmens und zum anderen in einer Stärkung der Betroffenenrechte wider. Im Hinblick auf die Betroffenenrechte erhalten Betroffene das Recht über Auskunft der Datenverarbeitung, die umgehende Korrektur falscher Daten, die Sperrung und Löschung sämtlicher personenbezogenen Daten sowie die Bereitstellung aller personenbezogenen Daten in einem portierbaren Format.[7] Insbesondere das Recht zur Datenportierbarkeit ist dabei im Vergleich zur bisherigen Regelung neu und verlangt vom Unternehmen maximale Transparenz über die gespeicherten Daten.

Eine Ausweitung der Pflichten des Versicherers ist insbesondere im Kontext der Informationspflichten zu sehen. So haben Versicherer bei jeder Erhebung und Dritterhebung personenbezogener Daten den Betroffenen unmittelbar über seine Rechte zu informieren.[8] Damit in Verbindung steht auch das explizite Einholen und Dokumentieren der Einwilligungserklärung für die Verarbeitung personenbezogener Daten. Eine Ausweitung weiterer Maßnahmen ist ebenfalls durch die DSGVO vorgesehen. Während die Nominierung eines Datenschutzbeauftragen schon in bisherigen Gesetzen gefordert ist, sieht die neue Verordnung unter anderem auch eine Ausweitung der Verarbeitungsverzeichnisse sowie die regelmäßige Durchführung von Datenschutz-Folgenabschätzungen vor.[9]

3. Konkrete Auswirkungen auf Organisation, Prozesse und IT

Zur Bestimmung der konkreten Auswirkungen der DSGVO auf die Organisation, die Prozesse und die IT eines Versicherungsunternehmens bietet sich eine Gliederung der wesentlichen DSGVO-Anforderungen in die Themenfelder (1) Rechtmäßige Verarbeitung, (2) Informationspflichten, (3) Betroffenenrechte und (4) Datenschutzmanagement an. Je Themenfeld lassen sich relativ trennscharf die Auswirkungen auf die einzelnen Unternehmensbereiche bestimmen.

Abbildung 2

Im Themenfeld „Rechtmäßige Verarbeitung“ muss unter anderem sichergestellt werden, dass für die Verarbeitung personenbezogener Daten eine explizite Einwilligung des Betroffenen eingeholt wurde und diese dokumentiert vorliegt.[10] Sollen die personenbezogenen Daten für weitere Zwecke genutzt werden (z. B. Werbung), gilt es eine entsprechende Rechtsgrundlage sicherzustellen. Eine Möglichkeit dazu bietet das berechtigte Interesse gem. Art. 6 Abs. 1 (f), wobei Unternehmen in diesem Fall ein Widerspruchsrecht einzuräumen haben. Ebenfalls müssen die Betroffenen über das Widerspruchsrecht explizit informiert werden.[11]

Das Themenfeld „Informationspflichten“ umfasst die Information des Betroffenen über seine Rechte. Diese Information muss der Versicherer unmittelbar bei Datenaufnahme an den Betroffenen entrichten.[12] Dies ist beispielsweise bei neuen Verträgen oder auch Schadenmeldungen der Fall. Versicherer sollten daher prüfen in welchen Geschäftsvorfällen personenbezogene Daten erhoben werden und dann entsprechende Datenschutzhinweistexte in diese Prozesse integrieren. Bestehende Datenschutzhinweistexte gilt es an die DSGVO anzupassen und in den Prozessen und IT-Systemen des Unternehmens umzusetzen. Dies bezieht sich dabei explizit auch auf die Anpassung von Druckmaterialen und ggf. Texten auf der Website des Unternehmens.

Deutlich umfangreicher als die „Informationspflichten“ ist der Anpassungsbedarf im Rahmen des Themenfelds „Betroffenenrechte“. Versicherer haben in diesem Kontext ihre bestehenden Prozesse zum Widerspruchsrecht, zur Auskunft, Berichtigung, Sperrung und Löschung und zur Mitteilungspflicht bei Datenübertragungen an Dritte zu analysieren. In Abhängigkeit des Status quo gilt es daraufhin einerseits die Prozesse anzupassen, als auch andererseits die Betroffenenrechte technisch umzusetzen. Konkret bedeutet dies für die Systeme, dass diese Auskunft über alle gespeicherten personenbezogenen Daten liefern können, personenbezogene Daten verbessert, gesperrt und gelöscht werden können und das ein Datenexport in ein maschinenlesbares Format (Recht auf Datenportierbarkeit) umgesetzt ist.

Das Themenfeld „Datenschutzmanagement“ hat umfassende organisatorische Auswirkungen. Ist zwar zumeist bereits ein Datenschutzbeauftragter im Unternehmen bestellt, gilt es seine Position im Unternehmen durch die Zuweisung zusätzlicher Ressourcen zu stärken, sodass er seinen von der DSGVO geforderten Aufgaben und Pflichten entsprechend nachgehen kann.[13] Weiterhin müssen Versicherer überlegen, ob sie ergänzend zum Datenschutzbeauftragten noch weitere Datenschutzkoordinatoren benennen, um die Fristen der DSGVO einhalten zu können. Die kritische Überprüfung eingerichteter technisch-organisatorischer Maßnahmen (TOM) sollte ebenfalls erfolgen.[14] Auf prozessualer Ebene sind die Prinzipien Privacy by Design und Privacy by Default in den Softwareentwicklungsprozess zu integrieren.[15] Ferner bedarf es Prozessdefinitionen für die regelmäßige Aktualisierung des Verarbeitungsverzeichnisses, die anlassbezogene Durchführung von Datenschutz-Folgenabschätzungen und die Meldung von Datenschutzverstößen an die Unternehmensführung und die Aufsicht.[16] Abschließend müssen die technischen Komponenten der technisch-organisatorischen Maßnahmen wirksam umgesetzt werden.

4. Vorgehen zur Umsetzung

Das Vorgehen zur Umsetzung der Anforderungen ist stark vom Ambitionsniveau es Versicherungsunternehmens abhängig. Das Ambitionsniveau sollte dabei zu Beginn der Umsetzung vom Unternehmen festgelegt werden, um die konkreten prozessualen, organisatorischen und technischen Umsetzungsaktivitäten konkretisieren zu können:

Für Versicherer, die Datenschutz als reine Pflichtaufgabe begreifen, empfiehlt sich beispielsweise ein sehr pragmatisches Umsetzungsvorgehen. Unternehmen können in diesem Fall die Anforderungen der DSGVO inhaltlich würdigen und mit dem bisherigen Datenschutzniveau des Unternehmens abgleichen. Da durch die Umsetzung des BDSG (alt) und des Code of Conducts bereits eine datenschutzrechtliche Ausgangsbasis existiert, kann bei einigen Unternehmen auf diesem Stand aufgesetzt werden. Lücken zwischen Status quo und DSGVO können daraufhin zielgerichtet geschlossen werden. Dennoch ergeben sich trotz des Minimalansatzes neue Anforderungen aus der DSGVO, welche zwingend umzusetzen sind.

Ferner lassen sich in der Praxis Unternehmen finden, welche Datenschutz weniger als lästige Pflicht, sondern mehr als Wettbewerbsvorteil und Differenzierungsmerkmal begreifen. Sofern diese Unternehmen noch nicht den Anforderungen der DSGVO genügen, empfiehlt sich ein ganzheitlicher Ansatz zur Umsetzung der Anforderungen. So kann beispielsweise auf Basis der Norm ISO/IEC 27001 ein umfassendes Datenschutzmanagementsystem aufgebaut werden. Zentrales Element des Systems ist dabei ein regelmäßiger Verbesserungsprozess, welcher die kontinuierliche Optimierung des Datenschutzes zum Ziel hat. Insbesondere unter Berücksichtigung des Artikels 42 der DSGVO, welcher explizit Datenschutz-Zertifizierungen vorsieht, kann sich die frühzeitige Nutzung eines anerkannten Standards als vorteilhaft erweisen.

Abbildung 3

Haben beide Vorgehensweise individuelle Vor- und Nachteile, entscheidet letztlich die Datenschutzphilosophie des Versicherungsunternehmens über den einzuschlagenden Weg. Die Versicherer sollten dabei jedoch berücksichtigen, dass ein sehr pragmatisches Vorgehen durchaus höhere Nachbesserungsmaßnahmen in 2018 nach sich ziehen kann. Dies gilt vor allem, wenn die Versicherungskunden umfassenden Gebrauch von Ihren neuen Rechten machen. Es ist daher davon auszugehen, dass eine umfassende und ganzheitliche Umsetzung lediglich verschoben ist, perspektivisch aber dennoch an Relevanz gewinnen wird.

5. Zeitnahe Umsetzung gefordert

Während sich der Bankensektor bereits intensiv mit der Umsetzung der DSGVO befasst, agiert die Versicherungswirtschaft noch zaghaft. Sind zwar erste Unternehmen bereits dabei in die konkrete Umsetzung der Anforderungen einzusteigen, zeigen sich zahlreiche andere Unternehmen noch zurückhaltender. Die Zurückhaltung ist dabei nicht nachvollziehbar, da erfahrungsgemäß insbesondere die technische Umsetzung vereinzelter Anforderungen mit hohen zeitlichen Aufwänden verbunden ist. Es muss daher davon ausgegangen werden, dass zahlreiche Unternehmen, welche die Umsetzung weiter aufschieben zum Stichtag am 25. Mai 2018 nicht konform mit der DSGVO agieren können.

Die Auswirkungen der DSGVO sollten dabei von den Versicherern nicht unterschätzt werden. Insbesondere durch die Ausweitung der Informationspflichten ist mit einer Zunahme der Betroffenenanfragen zu rechnen. Sind die Betroffenenrechte daher bis Mai 2018 nicht adäquat im Unternehmen umgesetzt, sehen sich vor allem die Datenschutzbeauftragten mit hohen manuellen Aufwänden konfrontiert. Da in Verbindung mit den Betroffenenrechten auch zeitliche Fristen in der DSGVO verankert sind, kann eine unzureichende Umsetzung der entsprechenden Prozesse ebenfalls schnell zu einem Verstoß gegen die DSGVO führen.[17]

Verstärkt wird die Problematik durch das Klagerecht der Verbraucherschutzverbände. So besitzen die Verbraucherschutzverbände seit Anfang 2016 ein Klagerecht für die Einhaltung des Datenschutzes.[18] Die Verbände können somit Unternehmen auf Unterlassung verklagen. Sollten Versicherungsunternehmen die DSGVO daher nicht hinreichend genug umsetzen, drohen neben Verbraucherklagen auch Klagen der Verbraucherschutzverbände. Durch die Höhe der Strafen von bis zu 20 Mio. Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes haben erfolgreiche Klagen umfangreiche Auswirkungen.

[1] *vgl. Art. 1 (2) DSGVO*
[2] *vgl. Art. 1 (3) DSGVO*
[3] *vgl. Art. 94 (1) DSGVO*
[4] *vgl. Art. 83 (5) DSGVO*
[5] *vgl. Art. 5 (1) DSGVO*
[6] *vgl. Art. 5 (2) DSGVO*
[7] *vgl. Art. 15 - 20 DSGVO*
[8] *vgl. Art. 13, 14 DSGVO*
[9] *vgl. Art. 30, 35 DSGVO*
[10] *vgl. Art. 6, 7 DSGVO*
[11] *vgl. Art. 13 (2) b) DSGVO*
[12] *vgl. Art. 13 (1) DSGVO*
[13] *vgl. Art. 38 (2) DSGVO*
[14] *vgl. Art. 32 DSGVO*
[15] *vgl. Art. 25 DSGVO*
[16] *vgl. Art. 33, 34 DSGVO*
[17] *vgl. Art. 12 (3) DSGVO*
[18] *vgl. §2 (2) 11) UKlaG*

Abbildung 1: Umfang umzusetzender Anforderungen

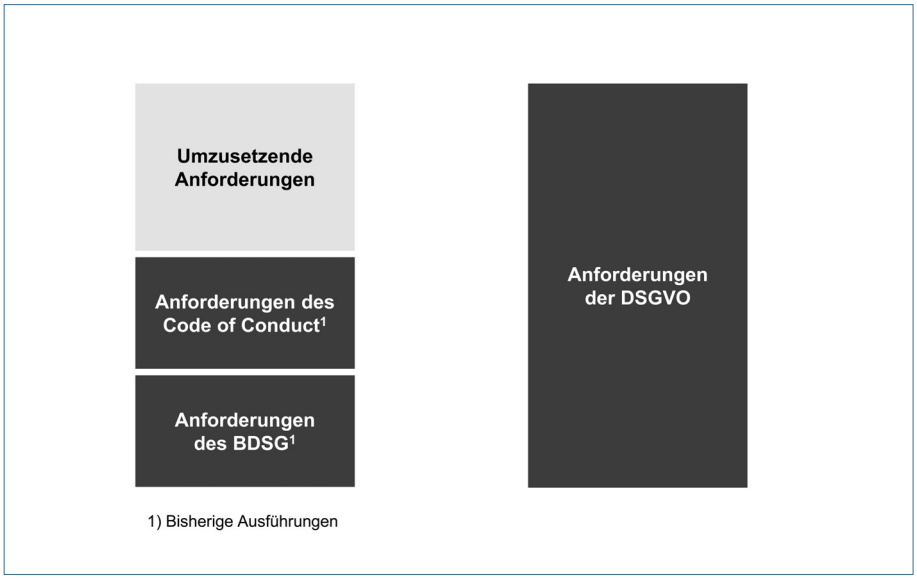

Abbildung 2: Wesentliche Handlungsfelder der DSGVO

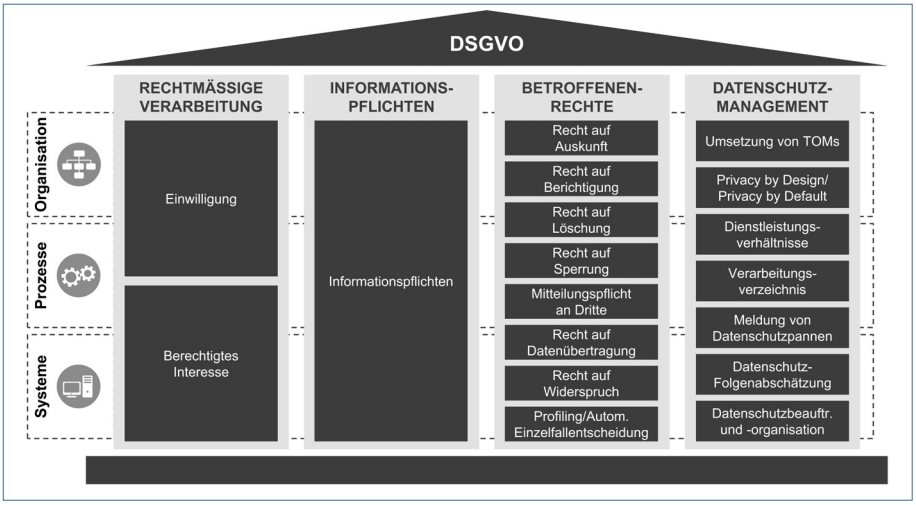

Abbildung 3: Verschiedene Reifegrade der DSGVO-Umsetzung