experten Report
Versicherungs- und Finanznachrichten

Die DSGVO kommt: Was Makler jetzt tun müssen

23 Apr, 2018

Oliver Petersen Vorstand vom Makler Nachfolger Club e.V.

Unternehmen haben nur noch bis zum 25. Mai 2018 Zeit, die neuen datenschutzrechtlichen Anforderungen nach der europäischen Datenschutz-Grundverordnung (DSGVO) umzusetzen. Denn dann gilt die Verordnung unmittelbar in allen EU-Mitgliedstaaten und löst die bisherigen nationalen Regelungen und EU-weiten Richtlinien ab. Ich habe in diesem Artikel versucht, die wichtigsten Neuerungen und den Umfang der aus meiner Sicht nötigen Maßnahmen zur Umsetzung zu beschreiben.

Bußgelder bereits bei Verstößen gegen die Verordnung – nicht erst bei Datenpannen

Um es vorwegzusagen: Für diejenigen, die sich bisher noch gar nicht mit dem Thema Datenschutz und der DSGVO beschäftigt haben, dürfte es sehr schwer bis unmöglich sein, den Stichtag 25. Mai 2018 für die Umsetzung der neuen Anforderungen an den Datenschutz einzuhalten. Die Zeit wird also knapp.

Es stehen empfindliche Bußgelder im Raum. Der Rahmen bewegt sich bis zu 20 Millionen Euro (oder 4 Prozent des letzten Jahresumsatzes). Dies war vom Gesetzgeber so beabsichtigt: abschreckende Wirkung der drohenden Bußgelder und die Sensibilisierung der Unternehmen für die Wichtigkeit des Datenschutzes.

Es gibt bisher noch keine Praxiserfahrungen, wie sich die Aufsichtsbehörden bei Verstößen verhalten werden und welche Bußgelder wann verhängt werden. Es hängt auch von der Größe des Unternehmens, der Art und dem Umfang des Verstoßes, vom jeweiligen Einzelfall und davon, in welchem Umfang und mit welchen Folgen die Rechte und Freiheiten des Betroffenen eingeschränkt wurden, ab.

Sollte es zu einer Anfrage der Aufsichtsbehörde bei Ihnen kommen, sollten Sie zumindest nachweisen können, dass Sie ein Datenschutz-Management-System in Ihrem Unternehmen eingeführt und dokumentiert haben und für die Aufsichtsbehörde zur Einsicht bereithalten. Wenn Sie das nicht können, ist ein deutliches Bußgeld zu erwarten. Es lohnt sich, trotz der knappen Zeit, proaktiv mit dem Thema Datenschutz umzugehen. Nichts tun ist also keine Option.

Muss ich einen Datenschutzbeauftragten benennen?

In der DSGVO wird in Bezug auf die Benennungspflicht eines Datenschutzbeauftragten im Gegensatz zum BDSG in der Novelle III nicht mehr von einer Mindestanzahl von Mitarbeitern gesprochen. Man könnte also den Eindruck gewinnen, dass nun alle einen DSB benennen müssen. Liest man jedoch ergänzend zu Art. 37 Abs. 1b und c DSGVO den § 38 Abs. 1 DSAnpUG-EU, findet man den Passus „in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigen“. Entwarnung? Leider nicht. Dies gilt nur, wenn der Verantwortliche zum Beispiel keine Datenverarbeitungen vornimmt, die einer Datenschutz-Folgeabschätzung nach Art. 35 der Verordnung (EU) 2016/679 unterliegen.

Eine Datenschutz-Folgenabschätzung ist nach Art. 35 Abs. 3 lit. b) insbesondere dann erforderlich, wenn die Kerntätigkeit in einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO besteht. Dazu gehören unter anderem Gesundheitsdaten. Leider lässt sich der Gesetzgeber nicht darüber aus, was er unter dem Begriff „umfangreiche Bearbeitung“ versteht. Ein Blick auf den Erwägungsgrund 91 könnte einen Hinweis geben.

Dort wird beschrieben, wann eine umfangreiche Bearbeitung nicht vorliegen soll. Zitat: „Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.“

Der einzelne Arzt und der Rechtsanwalt dürfte somit keiner Benennungspflicht unterliegen. Ob sich der Erwägungsgrund 91 auch auf Versicherungsmakler anwenden lässt, die weniger als zehn Mitarbeiter beschäftigen, bleibt zumindest fraglich.

Auf telefonische Anfrage hatte sich übrigens die Bundesdatenschutzbehörde für unzuständig erklärt, könne meine Argumentation mit dem Erwägungsgrund 91 zwar nachvollziehen, sei gegenüber den Landesbehörden jedoch nicht weisungsbefugt.

Also hatte man mich an die jeweils zuständigen Landesdatenschutzbehörden verwiesen, die das wiederum ganz anders gesehen haben. Überwiegender Tenor: Bisher hängt alles an Einzelfallentscheidungen der zuständigen Aufsichtsbehörden der Länder. Eine allgemeingültige Aussage kann somit leider nicht getroffen werden.

Wer kommt als Datenschutzbeauftragter infrage?

Wenn Sie als Versicherungsmakler einen Datenschutzbeauftragten (DSB) benennen müssen, haben Sie die Wahl zwischen einem externen oder internen DSB. Sie können also auch einen Ihrer Angestellten als DSB benennen und diesen der Aufsichtsbehörde als Ansprechpartner melden.

Er muss jedoch entsprechende „Fachkunde“ besitzen, sprich sich nachweislich in den Vorschriften der DSGVO und der IT-Systeme auskennen und betriebswirtschaftliche Kenntnisse haben. Sonst kann die Aufsichtsbehörde die Benennung ablehnen.

Außerdem müssen Sie ihn laufend weiterbilden und er genießt einen erweiterten Kündigungsschutz. Interessenkonflikte sind zu vermeiden. So scheiden Sie als Inhaber oder Geschäftsführer ebenso für diese Position aus wie zum Beispiel der IT-Leiter oder der Personalchef. Die Tätigkeit an sich ist umfangreich und es muss Ihnen klar sein, dass der Mitarbeiter weniger Zeit für seine eigentlichen Aufgaben im Unternehmen hat.

Bleibt die Möglichkeit, einen externen Datenschutzbeauftragten zu benennen. Dieser ist in aller Regel auf dem aktuellen Wissensstand und häufig günstiger als ein interner DSB.

Im Idealfall wählen Sie einen externen DSB, der neben den fachlichen Voraussetzungen auch noch einschlägige Branchenkenntnisse hat und weiß, wie zum Beispiel ein Maklerbüro funktioniert und mit welchen Daten ein Versicherungsmakler umgeht.

Was sollten Sie also als Versicherungsmakler tun? Ein Handlungsplan.

1. Status-quo-Analyse erstellen

Als Erstes sollten Sie Ihre Prozesse im Unternehmen überprüfen, bei denen eine Verarbeitung von personenbezogenen Daten (pbD) stattfindet, sprich, Sie sollten alle Prozesse untersuchen, die datenschutzrechtlich relevant sein könnten. Auf Basis dieser Status-quo-Analyse kann identifiziert werden, wo Ihre Prozesse von den Anforderungen der DSGVO abweichen.

2. Datenschutz-Management-System aufbauen

Aus den Art. 5 und 24 DSGVO leiten sich umfangreiche Nachweis- und Rechenschaftspflichten für Unternehmen ab. Unter anderem die Pflicht, ein Datenschutz-Management-System einzuführen! Das ist neu und gab es so im alten BDSG nicht. Künftig müssen Unternehmen nicht nur sicherstellen, dass datenschutzrechtliche Vorgaben eingehalten werden, sondern sie müssen dies auch nachweisen können. Dies betrifft übrigens auch den Bereich Datensicherheit, für den es eine Nachweispflicht, ob „geeignete technische und organisatorische Maßnahmen“, sogenannte TOMs, eingesetzt werden, die dem Schutz der betroffenen Personen dienen, gibt.

Im Datenschutz-Management-System sollten sich also folgende Punkte wiederfinden:

- Datenschutzorganisation und Verantwortlichkeit für Datenverarbeitungen
- Einbindung des Datenschutzbeauftragten
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung (vgl. Art. 35 DSGVO)
- Vertragsmanagement (welche Dienstleister werden eingesetzt?)
- Datenschutzschulung und Verpflichtung auf das Datengeheimnis
- Prozess zur Wahrnehmung von Betroffenenrechten
- Zulässigkeit der Datenverarbeitung
- Meldung von Datenschutzverstößen
- Nachweis der Datensicherheit (Umsetzung der TOMs)

Das Vorhandensein eines Datenschutz-Management-Systems (DMS) kann sich in Fällen unbeabsichtigter Datenschutzverstöße bußgeldmindernd auswirken (Art. 83 Abs. 2 d DSGVO). Problematisch wird es wie bereits erwähnt dann, wenn es zu einem Datenschutzverstoß kommt und Sie kein DMS nachweisen können.

„Erstellen Sie eine Liste mit allen Auftragsverarbeitern und sonstigen Dienstleistern, die für Sie tätig sind und die mit personenbezogenen Daten umgehen."

3. Verzeichnis von Verarbeitungstätigkeiten aufbauen

Was bisher nach §§ 4g Abs. 2, 4e BDSG Verfahrensverzeichnis hieß, wird in der DSGVO nun Verzeichnis von Verarbeitungstätigkeiten genannt und ist eine Dokumentation und eine Übersicht über alle Verfahren, bei denen pbD verarbeitet werden.

Die Pflicht, ein Verzeichnis für Verarbeitungstätigkeiten zu führen, gilt laut Art. 30 Abs. 5 DSGVO dann nicht, wenn der Verantwortliche oder Auftragsverarbeiter weniger als 250 Beschäftigte hat, es sei denn, die vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder die Verarbeitung betrifft keine besonders sensiblen Datenkategorien oder strafrechtlich relevanten Daten.

Die Verpflichtung für viele Versicherungsmakler, ein Verzeichnis zu führen, dürften die besonders sensiblen Datenkategorien auslösen, da diese zum Beispiel auch Gesundheitsdaten umfassen.

Spätestens bei der Begrifflichkeit „nicht nur gelegentlich" dürfte sich die Pflicht zum Führen des Verzeichnisses für die meisten ergeben, da eine „gelegentliche Verarbeitung" per Definition „nur ab und zu und nicht regelmäßig" erfolgt.

Dies dürfte in einem laufenden Geschäftsbetrieb bei der Verarbeitung von pbD unrealistisch sein. Sie meinen, das wird schon nicht so heiß gegessen? Art. 83 Bas. 4 a DSGVO besagt, dass der Verantwortliche (also Sie als Versicherungsmakler) das Verarbeitungsverzeichnis jederzeit und vollständig für die Aufsichtsbehörden vorhalten muss, ansonsten droht ein Bußgeld.

Auch diese Strafbewehrung durch Bußgeld ist neu und war im BDSG bisher nicht vorhanden, weshalb viele bisher noch kein Verzeichnis erstellt haben, obwohl es bereits Pflicht war.

4. Prüfen, ob Datenschutz-Folgenabschätzungen nötig sind

Die Datenschutz-Folgenabschätzung (DSFA) ist grundsätzlich mit der im deutschen Datenschutzrecht bereits bekannten Vorabkontrolle (§ 4d Abs. 5 BDSG) vergleichbar.

Diese ist immer dann durchzuführen, wenn besonders sensible Daten (zum Beispiel Gesundheitsdaten) verarbeitet werden oder die Datenverarbeitung dazu bestimmt war, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens, zu bewerten.

Die Folgenabschätzung muss zumindest Folgendes enthalten (vgl. Art. 35 DSGVO):

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird

5. Verträge mit Auftragsverarbeitern prüfen und anpassen

Auftragsverarbeiter (bisher Auftragsdatenverarbeiter) ist per Definition eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (vgl. Art. 4 Nr. 8 DSGVO). Auftragsverarbeiter können viele sein.

Vom Pool über den Bürodienstleister, dem Callcenter bis hin zum Betreiber von Serverfarmen, in denen Ihre Daten in der Cloud liegen, und anderen mehr. Prüfen Sie, ob bereits Verträge bestehen, und holen Sie dies im Zweifel nach beziehungsweise passen Sie die bestehenden Verträge an die Anforderungen der DSGVO an. Erstellen Sie eine Liste mit allen Auftragsverarbeitern und sonstigen Dienstleistern, die für Sie tätig sind und die mit personenbezogenen Daten umgehen.

„Sensibilisieren Sie Ihre Mitarbeiter für das Thema Datenschutz und geben Sie einen Überblick über die neuen Bestimmungen der Verordnung und deren Rechtsfolgen.“

6. Führen Sie Datenschutzschulungen durch

Im Rahmen der Schulung und Beratung sämtlicher Mitarbeiter im Sinne von Art. 39 Abs. 1 lit. a) DSGVO ist es sinnvoll, auf die Änderungen im Datenschutzrecht in geeigneter Form, gegebenenfalls per Rundschreiben, hinzuweisen.

Sensibilisieren Sie Ihre Mitarbeiter für das Thema Datenschutz und geben Sie einen Überblick über die neuen Bestimmungen der Verordnung und deren Rechtsfolgen. Die Mitarbeiter sollten auch weiterhin auf das Datengeheimnis verpflichtet werden, auch wenn dies in der Datenschutz-Grundverordnung nicht mehr ausdrücklich geregelt ist.

7. Beginnen Sie einen Prozess zur Wahrnehmung von Betroffenenrechten

Pflichten zur Information von betroffenen Personen gab es bisher bereits, nur werden diese Pflichten deutlich erweitert. Geregelt sind diese in den Art. 13 und 14 DSGVO. Demnach sind den betroffenen Personen besonders folgende Informationen mitzuteilen (und zwar in präziser, transparenter, verständlicher und leicht zugänglicher Form):

- Identität des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Verarbeitungszwecke und Rechtsgrundlagen
- Berechtigtes Interesse
- Empfänger
- Übermittlung der Daten in Drittstaaten
- Dauer der Speicherung
- Betroffenenrechte
- Widerrufbarkeit von Einwilligungen
- Beschwerderecht bei der Aufsichtsbehörde
- Verpflichtung zur Bereitstellung personenbezogener Daten
- Automatisierte Entscheidungsfindung und Profiling

Aus Art. 14 DSGVO ergibt sich, dass nahezu dieselben Informationspflichten bestehen, wenn die Daten nicht beim Betroffenen selbst erhoben werden.

8. Prüfung der Zulässigkeit der Datenverarbeitung

Nach DSGVO ist die Verarbeitung personenbezogener Daten verboten – mit Erlaubnisvorbehalt. Sie brauchen also immer eine Rechtsgrundlage, auf der die Verarbeitung erfolgt, sonst handeln Sie illegal. Sie sollten also alle Einwilligungen und die Rechtsgrundlagen überprüfen.

Die gute Nachricht ist, dass die bisher erfolgten Einwilligungen Gültigkeit behalten (sofern sie den Bestimmungen der DSGVO entsprechen). Einwilligungen zur Datenverarbeitung, die rechtskonform sind, ergeben sich aus den Art. 6 bis 11 DSGVO.

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten besteht …

- wenn eine Einwilligung der betroffenen Person vorliegt,
- zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen,
- zur Erfüllung einer rechtlichen Verpflichtung,
- zum Schutze lebenswichtiger Interessen,
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder
- aufgrund einer Interessenabwägung erforderlich ist.

„Die Mitarbeiter sollten auch weiterhin auf das Datengeheimnis verpflichtet werden, auch wenn dies in der Datenschutz- Grundverordnung nicht mehr ausdrücklich geregelt ist.

Die Datenverarbeitung ist bereits dann rechtmäßig, wenn einer der genannten Tatbestände vorliegt. Für Minderjährige unter 16 Jahren sind Einwilligungen nur wirksam, wenn die Eltern (beziehungsweise Personen mit elterlicher Verantwortung) diese erteilt oder dieser zugestimmt haben (vgl. Art. 8 DSGVO).

Wie die betroffene Person ihre Einwilligung zu erteilen hat, ist in Art. 7 DSGVO geregelt:

- Freie Entscheidung des Betroffenen
- Ausführliche, erkennbare und bestimmte Information des Betroffenen
- Schriftform der Einwilligungserklärung
- Widerruflichkeit der Einwilligungserklärung
- Informationspflichten beachten

Gemäß Art. 17 DSGVO sind personenbezogene Daten immer dann unverzüglich zu löschen, wenn einer der folgenden Fälle gegeben ist:

- Der Zweck der Verarbeitung ist erreicht und eine Kenntnisnahme ist nicht mehr erforderlich.
- Eine gegebene Einwilligung wird widerrufen und es fehlt an einer anderen Rechtsgrundlage.
- Die betroffene Person widerspricht der Verarbeitung und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die personenbezogenen Daten müssen zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten gelöscht werden.
- Es wurden personenbezogene Daten eines Kindes bezüglich der angebotenen Dienste der Informationsgesellschaft (zum Beispiel soziales Netzwerk, Online-Spiele) erhoben.

Das heißt nicht, dass alles sofort gelöscht werden muss. Es gibt Ausnahmen, wenn zum Beispiel Aufbewahrungsfristen der Steuerbehörden entgegensprechen.

In solchen Fällen müssen Sie aber gewährleisten, dass der Zugriff auf die Daten eingeschränkt ist beziehungsweise die Daten gesperrt sind. Diese Funktionen sollte Ihr MVP besitzen.

9. Prozess für die Erfüllung der Meldepflicht erstellen

Gemäß Art. 33 Abs. 1 DSGVO hat der Verantwortliche die zuständige Aufsichtsbehörde bei Datenpannen, also bei jeder „Verletzung des Schutzes personenbezogener Daten“, unverzüglich zu benachrichtigen.

Die Meldepflicht gilt damit für jeden Fall der rechtswidrigen Datenverarbeitung, also auch bei jeder rechtswidrigen Zerstörung, Veränderung oder dem rechtswidrigen Verlust von Daten, auch bei versehentlicher Verletzung und nicht nur dann, wenn Dritte unbefugt Zugriff auf Daten erlangen. Das ist neu in der DSGVO. Unverzüglich bedeutet in diesem Zusammenhang innerhalb von 72 Stunden, nachdem dem Verantwortlichen die Verletzung bekannt geworden ist. Wird diese Frist nicht eingehalten, ist der Meldung an die Aufsichtsbehörde eine Begründung für die Verzögerung beizufügen.

Einer Meldung bedarf es laut DSGVO jedoch nicht, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.“

Ob Risiken für natürliche Personen wahrscheinlich sind, ist unter Berücksichtigung des Risikokatalogs in Erwägungsgrund 75 DSGVO abzuwägen. Diese Risikoabschätzung sollte

unbedingt dokumentiert werden. Die Meldepflicht gilt nach DSGVO übrigens für alle Arten personenbezogener Daten und nicht mehr nur für besonders sensible Daten.

10. Nachweis der Datensicherheit (technische und organisatorische Maßnahmen)

Nach Art. 32 DSGVO müssen Sie geeignete technische und organisatorische Maßnahmen (TOM) ergreifen, um Ihre Daten zu schützen. Für die Form gibt es bisher wenige Anforderungen, die folgenden Punkte sollten aber in den TOMs beschrieben werden:

- Pseudonymisierung
- Verschlüsselung
- Gewährleistung der Vertraulichkeit
- Gewährleistung der Integrität
- Gewährleistung der Verfügbarkeit
- Gewährleistung der Belastbarkeit der Systeme
- Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall erfahren regelmäßiger Überprüfung, Bewertung und
- Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Fazit

Auch wenn es schon eher fünf nach zwölf als fünf vor zwölf ist – bleiben Sie ruhig und beginnen Sie mit der Umsetzung der DSGVO. Es ist ein langwieriger Prozess und das Thema Datenschutz sollte in die Datenverarbeitungsprozesse fest implementiert und nicht nur aufgesetzt werden.

Über den Autor:

Oliver Petersen ist Versicherungsfachwirt, geprüfter betrieblicher & behördlicher Datenschutzbeauftragter und Unternehmensberater. Er beschäftigt sich mit der Nachfolge- und Notfallplanung von Unternehmern und mit der Umsetzung der EU-DSGVO im Betrieb. Von Datenschutz-Status-Analysen (Audits), Datenschutzberatungen, Seminaren, Schulungen und Workshops bis hin zur Stellung des externen Datenschutzbeauftragten ist er für verschiedene Unternehmen beratend tätig https://www.petersen-consulting.eu/ Mail: info@petersen-consulting.eu