Fragen und Antworten zur

EU-Datenschutzgrundverordnung (EU-DSGVO)

Stand 18.02.2020

Hinweis:

Für das neue Datenschutzrecht stellen die nachfolgenden Antworten lediglich einen Ausschnitt der wesentlichen Änderungen dar. Sie ersetzen keine qualifizierte Beratung, insbesondere keine Rechtsberatung. Sie erheben keinen Anspruch auf Vollständigkeit. Für die Richtigkeit der Angaben wird keine Haftung übernommen.

1. Was ist die DSGVO (Datenschutzgrundverordnung)?

Die europäische Datenschutzgrundverordnung – abgekürzt EU-DSGVO - ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Ziel ist eine Erhöhung des Datenschutzniveaus. Man möchte gleiche Standards und Informationspflichten gegenüber Betroffenen für alle in der EU tätigen Unternehmen einführen und Wettbewerbsverzerrungen infolge unterschiedlicher nationaler Datenschutzbestimmungen beseitigen. Der EU-weite Stichtag für die Einführung war der 25.05.2018. Mit der DSGVO einher geht eine erhebliche Erhöhung der Bußgelder auf bis zu 20 Mio. Euro oder 4% des weltweiten Jahresumsatzes (jeweils der höhere Betrag).

2. Falle ich als Makler unter die Regelungen der DSGVO?

Ja, der Makler fällt unter den Anwendungsbereich der DSGVO. Er ist nach Artikel 4 Nr. 7 ein sogenannter Verantwortlicher, d.h. eine natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

3. Welche Bereiche meiner Tätigkeit sind besonders sensibel?

Die DSGVO schützt sämtliche Daten natürlicher Personen (inkl. Mitarbeiter, Vertriebspartner etc.). Personenbezogene Daten (pbD) sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Dabei wird unterschieden nach einfachen pbD (Name, Adresse, VS-Nummer, Standortdaten u.ä.) und besonderen Kategorien von pbD. Diese sind besonders schützenswert. Darunter fallen beispielsweise die ethnische Herkunft, Gesundheitsdaten, biometrische Daten oder auch genetische Daten. Vermittlern ist die Verarbeitung/Erfassung dieser Daten bei Vorliegen einer entsprechenden Einwilligung gestattet, wenn dies (wie beispielsweise die Erfassung von Gesundheitsdaten bei Biometrieprodukten) zum Abschluss eines Vertrages unerlässlich ist. Eine Verarbeitung dieser Daten über diesen Zweck hinaus ist nicht zulässig. Auch die Weitergabe ist nur mit Einwilligung gestattet.

4. Benötige ich einen betrieblichen Datenschutzbeauftragten? Welche Anforderungen werden an diesen gestellt und kann ich mich dazu schulen lassen?

Hierzu gibt es keine konkrete Vorgabe, so dass diese Thematik individuell zu betrachten ist. Grundsätzlich gilt jedoch:

- Wenn **mehr als 19 Personen** im Unternehmen – dazu zählen auch freie Mitarbeiter, Auszubildende und Praktikanten – mit automatisierter Datenverarbeitung beschäftigt sind, ist ein Datenschutzbeauftragter zu bestellen. Jede Eingabe von Kundendaten in ein EDV-System gilt dabei als automatisierte Datenverarbeitung.

7000000000

- Die Pflicht zur Bestellung eines Datenschutzbeauftragten besteht unabhängig von der Mitarbeiterzahl, wenn das betreffende Unternehmen **regelmäßig besonders geschützte Daten** (z.B. Gesundheitsdaten) verarbeitet.

Der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen ist zu der Einschätzung gekommen, dass bei einem einzelnen Makler, der seine Tätigkeiten im Rahmen des üblichen Standardgeschäftes ausübt, keine umfangreiche Datenverarbeitung stattfindet, so dass dieser keinen betrieblichen Datenschutzbeauftragten stellen muss.

Sofern Sie nach eingehender Prüfung zu der Einschätzung gelangen, keine Pflicht zur Ernennung eines Datenschutzbeauftragten zu haben, sollten die Grundlagen dieser Entscheidung genau dokumentiert werden. Alternativ ist die freiwillige Ernennung eines Datenschutzbeauftragten möglich. Die DSGVO erlaubt außerdem ausdrücklich Interessenverbänden einen Datenschutzbeauftragten zu ernennen, der dann in deren Auftrag handelt.

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat eine Praxishilfe zum Thema Datenschutzbeauftragte veröffentlicht, die Sie hier herunterladen können.

5. Was ist ein Verarbeitungsverzeichnis und benötige ich als Makler ein solches?

Neben der Information der Betroffenen müssen Unternehmen bei Datenverarbeitungen zusätzlich in einem „Verzeichnis von Verarbeitungstätigkeiten“ eine Reihe von Informationen dokumentieren (Art. 30 DSGVO). Aufsichtsbehörden soll es auf diese Weise erleichtert werden, die Erfüllung sämtlicher Pflichten der DSGVO rückblickend zu kontrollieren. Das Verzeichnis sollte aber auch deshalb sorgfältig geführt werden, weil es bei Beschwerden Vorgänge lückenlos darlegen kann.

Das Verzeichnis ist durch den Verantwortlichen selbst zu führen. Für den Makler bedeutet dies, dass er in aller Regel auch ein eigenes Verfahrensverzeichnis erstellen muss. Es gibt eine Ausnahme für kleine und mittlere Unternehmen und Einrichtungen mit weniger als 250 Beschäftigen. In der Praxis wird diese Ausnahme aber nur sehr selten greifen. Sie gilt nämlich lediglich, wenn ein Unternehmen „nur gelegentlich“ Daten verarbeitet und die vorgenommene Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt (also z.B. keine Verarbeitung von Gesundheitsdaten). Da bereits die Existenz einer Kundendatenbank oder die Verwaltung von Mitarbeiterdaten dazu führt, dass nicht mehr „nur gelegentlich“ Daten verarbeitet werden, ist diese Ausnahme für die meisten Unternehmen bedeutungslos.
Für die durch HDI zur Verfügung gestellten Systeme übernimmt der Konzern die durch die DSGVO nötigen Anpassungen. Für die in Eigenregie verarbeiteten und in eigenen Systemen gespeicherten Daten bietet sich ein Muster an, das die Landesdatenschutzbeauftragte Niedersachsen in Abstimmung mit allen deutschen Aufsichtsbehörden erstellt hat und das Sie hier finden. Eine Praxishilfe der Gesellschaft für Datenschutz und Datensicherheit (GDD) zur Erstellung eines Verarbeitungsverzeichnisses können Sie hier herunterladen.

6. Wer kann mich kontrollieren bzw. wie läuft so ein Vorgang ab?

In Deutschland sind die Landesdatenschutzbeauftragen die zuständigen Aufsichtsbehörden. Sie können Informationen anfordern, Datenschutzüberprüfungen durchführen und auf Verstöße hinweisen. Auf Verlangen müssen ihnen die erforderlichen Auskünfte erteilt werden. Sie sind berechtigt, zur Erfüllung ihrer Aufgaben Grundstücke und Geschäftsräume zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten.

Bei evtl. Verstößen steht ein Bußgeld erst am Ende vieler Sanktionsmöglichkeiten. Bevor ein Unternehmer zahlen muss, wird es von den Aufsichtsbehörden gewarnt oder abgemahnt. Es wird dann ein Zeitraum eingeräumt, in dem die festgestellten Mängel behoben werden müssen.

7. Welche Daten darf man erfassen und für welche braucht man ein gesondertes Einverständnis?

Für die Verarbeitung personenbezogener Daten gilt ein sogenanntes „Verbot mit Erlaubnisvorbehalt“. Das heißt die Verarbeitung ist grundsätzlich verboten. Es gibt aber bestimmte Voraussetzungen, unter denen sie erlaubt ist. Für Makler relevant sind vor allem die Einwilligung sowie die Erfüllung eines Vertrages bzw. vorvertragliche Maßnahmen.

Wenn die betroffene Person ihre Einwilligung zur Verarbeitung ihrer Daten für einen oder mehrere bestimmte Zwecke gegeben hat, ist diese immer zulässig. Für die Einwilligung gelten bestimmte formale Voraussetzungen. Daten, die für die Erfüllung eines Vertrags mit der betroffenen Person notwendig sind, dürfen grundsätzlich ohne Einwilligung verarbeitet werden. Darunter fällt auch die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, also zum Beispiel das Einholen von Versicherungsangeboten.

Für die besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) gelten strengere Anforderungen. Hier wird eine ausdrückliche Einwilligung des Betroffenen verlangt. Auch diese muss bestimmte for-

male Voraussetzungen erfüllen.

8. Muss ich mir bei jeder einzelnen bAV-Beratung vom AN eine Einwilligungserklärung unterzeichnen lassen, wenn die Firma als VN den Maklerauftrag unterzeichnet hat?

In einem solchen Fall dürfte der Erlaubnistatbestand „vorvertragliche Maßnahmen" zur Anwendung kommen. Sobald jedoch Gesundheitsdaten oder sonstige besonders schützenswerte Daten erhoben werden, ist eine ausdrückliche Einwilligung des Betroffenen nötig.

9. Was gilt für meinen Bestand? Muss ich von allen Mandanten, von welchen ich Daten gespeichert habe, aber keinen Maklerauftrag besitze eine Datenschutzerklärung einholen?

Diese Frage lässt sich nicht eindeutig beantworten. Es ist im Einzelfall zu prüfen, auf welcher Grundlage die Daten gespeichert werden und ob die Regelungen der DSGVO eingehalten werden. Die Ergebnisse der Prüfung sollten in einem Verarbeitungsverzeichnis dokumentiert werden. Für eine rechtssichere Einschätzung sollte ein Rechtsanwalt oder ein zertifizierter Datenschützer konsultiert werden.

10. Was muss ich tun, wenn ich einen Dienstleister einsetzen möchte?

Wenn Sie einen Dienstleister einsetzen, der in irgendeiner Form eine Datenverarbeitung in Ihrem Auftrag durchführt, so handelt es sich datenschutzrechtlich um einen Auftragsverarbeiter. Mit diesem müssen Sie einen schriftlichen Vertrag abschließen. Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat einen Mustervertrag zur Auftragsverarbeitung entworfen, den Sie hier herunterladen können. Die Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder hat ein Kurzpapier zum Thema veröffentlicht, das Sie hier finden.

11. Muss ich mit Versicherern Aufträge zur Auftragsvereinbarung abschließen?

Nein. Als Versicherer treten wir Maklern gegenüber in ihrer Funktion als Vermittler nicht als Auftragsverarbeiter im Sinne des Art. 28 DSGVO auf. Vielmehr ergibt sich die Grundlage für die rechtmäßige Datenverarbeitung zukünftig aus Art 6 Abs. 1 lit. b) DSGVO, da wir die Kundendaten zur Erfüllung des Maklervertrages als Verantwortliche und nicht im Auftrag des Maklers verarbeiten. Auch nach Inkrafttreten der DSGVO ist somit der Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO sowie die Durchführung der von Art 28 DSGVO geforderten Kontrollen in der vorliegenden Sachverhaltskonstellation nicht notwendig.

Mit dem Beitritt zum Code of Conduct für die Versicherungswirtschaft bekennt sich der HDI zur Einhaltung der datenschutzrechtlichen Bestimmungen im Sinne des Bundesdatenschutzgesetzes sowie der DSGVO. Darüber hinaus beachten wir die hierfür erforderlichen technischen und organisatorischen Maßnahmen, die wir mittels einer ISO Zertifizierung ISO/IEC 27001:2013 nachweisen können.

12. Muss ich meine bestehenden Vereinbarungen mit Versicherern ersetzen, aktualisieren oder ergänzen?

Die EU-DSGVO trat am 25. Mai 2018 in Kraft. Rein formal müssen Alt-Verträge nicht angepasst werden. Es empfiehlt sich dennoch eine Aktualisierung, um die vollständige Einhaltung der DSGVO-Anforderungen zu gewährleisten.

13. Welche Auskunftspflichten haben wir als selbständige Unternehmer generell? Wann müssen wir Kunden beauskunften?

Grundsätzlich sind Sie als Unternehmer verpflichtet, den Kunden auf Verlangen über die zu ihm gespeicherten Daten zu informieren. Dabei gelten folgende Voraussetzungen:

- Die Auskunft muss grundsätzlich unentgeltlich erfolgen.
- Das Auskunftsersuchen kann schriftlich, per Email oder telefonisch gestellt werden. Grundsätzlich hat die Beauskunftung in der gleichen Form zu erfolgen. Aus Gründen der Datensicherheit ist eine schriftliche Antwort per Brief zu bevorzugen.

7000000000

- Es werden nur die Daten zur betroffenen Person (Antragsteller) beauskunftet.
- Die Pflicht gilt nur insoweit, als keine Rechte und Freiheiten Dritter beeinträchtigt werden (etwa bei einer Offenlegung von Geschäftsgeheimnissen). In Zweifelsfällen sollte zunächst der Datenschutzbeauftragte bzw. die Aufsichtsbehörde konsultiert werden.
- Sofern der Betroffene nicht identifiziert werden kann, darf die Auskunft verweigert werden. Hat der Verantwortliche begründete Zweifel an der Identität des Anfragenden können zusätzliche Informationen angefordert werden (z.B. Nachweise).
- Informationen müssen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt werden. Bei Komplexität und hoher Anzahl kann die Frist um weitere zwei Monate verlängert werden.

14. Kann der Kunde widersprechen und muss ich diese Daten irgendwann löschen?

Der Kunde kann jederzeit ganz oder in Teilen die gegebenen Einwilligungen widerrufen. Neben dem Widerruf kann er auch einer Datenverarbeitung widersprechen. In der Praxis greift das, wenn man die Verarbeitung nur aufgrund eines berechtigten Interesses vornimmt (z.B. als Werbewiderspruch). Auch kann der Kunde verlangen, dass über Ihn gespeicherte Daten zu löschen sind. Dabei sind jedoch etwaige gesetzliche Aufbewahrungsfristen z.B. aus dem Steuer- oder Handelsrecht zu berücksichtigen. Generell setzen die HDI-Systeme (auch ohne aktive Forderung zur Löschung durch den Kunden) eine Sperr- und Löschsystematik gemäß des Code of Conduct um.

15. Sind die Angebots- und Auskunftssysteme des HDI DSGVO-konform?

Ja, das Unternehmen hat alle Dokumente sowie Angebots- und Beratungssysteme, die den Maklern zur Verfügung gestellt werden, auf einen DSGVO-konformen Stand gebracht.

16. Muss ich eine Datenschutzfolgeabschätzung machen?

Die Datenschutzfolgenabschätzung ist immer dann erforderlich, wenn ein hohes Risiko für die Rechte und Freiheiten der Betroffenen vorliegen kann. Bei bestimmten Formen der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, muss sie vorgenommen werden. In der Praxis wird das zum Beispiel notwendig, wenn eine Videoüberwachung öffentlich zugänglicher Räume geplant ist. In diesen Fällen ist ein Datenschutzbeauftragter einzubeziehen.

Die Datenschutzkonferenz hat eine Liste mit Verarbeitungsvorgängen veröffentlicht, die stets eine Datenschutzfolgenabschätzung erfordern, sowie ein Informationsblatt zu diesem Thema veröffentlicht. Diese Dokumente finden Sie hier und hier.

Eine Praxishilfe der Gesellschaft für Datenschutz und Datensicherheit (GDD) ist hier zu finden.

17. Wo finde ich weitere Informationen und Hilfen für meine betriebliche Praxis?

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat eine Reihe von Praxishilfen im PDF-Format veröffentlicht, die Sie hier finden.

Die Aufsichtsbehörden des Bundes und der Länder haben gemeinsame Kurzpapiere zur DSGVO herausgegeben, die jeweils eine Einführung in einzelne Themenkomplexe des neuen Datenschutzrechts enthalten. Sie dienen als erste Orientierung, wie nach Auffassung der Datenschutzkonferenz die Datenschutzgrundverordnung im praktischen Vollzug angewendet werden sollte. Die Kurzpapiere finden Sie hier.

Die Stiftung Datenschutz hat die Broschüre “Datenschutz im Betrieb – Eine Handreichung für Beschäftigte” erstellt, die Mitarbeitern die notwendigen Hintergründe vermittelt und praxisnah die gesetzlich vorgeschriebenen Grundinformationen darstellt. Diese sowie weitere Broschüren finden Sie hier.

Viele Rechtsanwälte und externe Datenschutzbeauftragte bieten speziell auf Versicherungsmakler zugeschnittene Schulungen und Informationen an. Diese finden Sie über Internet-Suchmaschinen. Dort können Sie auch nach Checklisten für Makler suchen.