VIEHBÖCK BREITER SCHENK & NAU

RECHTSANWÄLTE

DSGVO – LEITFADEN FÜR VERSICHERUNGSAGENTEN

G. Breiter

1. ANWENDUNGSBEREICH DER DSGVO

Die Datenschutz-Grundverordnung gilt ab 25. 5. 2018. Sie bezieht sich auf jedwede berufliche, d.h. gewerbsmäßige Form der Verarbeitung, Versendung, Vervielfältigung, Speicherung etc. von personenbezogenen Daten natürlicher Personen (Konsumenten oder Einzelunternehmen), die sogenannten „betroffenen Personen".

Sie richtet sich an jeden, der Daten verarbeitet bzw. dem ein eigenständiges Ermessen über die Datenverarbeitung zukommt (datenschutzrechtlich wird dieser als „Verantwortlicher" bezeichnet). Nach herkömmlicher Ansicht fallen darunter auch Vermittler, also auch Versicherungsagenten.

Dabei macht es datenschutzrechtlich keinen Unterschied, ob der Agent als Ausschließlichkeits- oder Mehrfachagent tätig ist. Mit geschützten Daten hat er stets zu tun. So unterliegt er bereits den Anforderungen des Datenschutzes, wenn ein Interessent zu ihm ins Büro kommt und dieser zunächst einmal in eine Kundendatei aufgenommen wird, um ihm später ein Angebot zukommen zu lassen. Dass Interessenten bzw. Kunden bisweilen Daten ohne Aufforderung übermitteln, heißt übrigens nicht, dass sie in jedwede Verwendung eingewilligt hätten (zur Einwilligung unten Punkt 7).

Im Detail sind personenbezogene Daten:

Name, Geburtsdatum, Geburtsort, Anschrift, Beruf, Staatsangehörigkeit, Geschlecht, Größe, Gewicht, Haar- und Augenfarbe, Kleidergröße, Familienstatus, wirtschaftliche Lage, Vorlieben und Freizeitverhalten, Standortdaten, Lebenslauf, Kontaktdaten (wie Telefonnummer, Email),

Online-Kennung, Benutzername, Konto- und Kreditkartennummer, Einkommen, Nummer im Zentralen Melderegister, Video- und Audioaufnahmen, Gesundheitsdaten (vgl. dazu Punkt 7).

Darüber hinaus können auch subjektive Werturteile, die sich auf eine natürliche Person beziehen, personenbezogene Inhalte sein. Es spielt keine Rolle, ob diese Aussagen zutreffen, also z.B. Angaben über Charaktereigenschaften, Arbeitseinstellung, Zuverlässigkeit, Kreditwürdigkeit, Karriereplanung oder Gesundheitsprognosen.

Praxishinweis: Auch Kunden-, Polizzen- und Schadennummern sind personenbezogene Daten.

Die Regelungen des österreichischen Datenschutzgesetzes beziehen sich (weiterhin) auch auf die Daten juristischer Personen. Insofern ist es nicht ratsam, bei solchen Daten eine geringere Sorgfalt an den Tag zu legen. Mit den Daten juristischer Personen werden ohnehin Daten natürlicher Personen mit übermittelt bzw. -verarbeitet (z.B. Name des Ansprechpartners). Zudem wird es im betrieblichen Alltag kaum möglich bzw. sinnvoll sein, zwischen verschiedenen Daten(arten) zu unterscheiden und diese unterschiedlich zu behandeln.

Die DSGVO erfasst lediglich manuelle Dateien nicht, die keiner Ordnung unterliegen. Sind sie aber in einem (wenn auch nicht automatisierten) Dateisystem gespeichert oder sollen sie dort gespeichert werden, unterliegen diese Daten der DSGVO. Ein solches Dateisystem liegt bereits dann vor, wenn diese Sammlung personenbezogener Daten gleichartig aufgebaut ist, nach bestimmten Merkmalen zugänglich ist und daher ausgewertet werden kann (z.B. eine alphabetisch geordnete Kundendatei).

Für sensible Daten (z.B. Gesundheitsdaten/Krankheitsgeschichte) bestehen besondere Anforderungen (dazu noch unten).

Praxistipp: Es sollten im Ergebnis alle elektronisch verarbeiteten Daten (sowie Kundenkarteien in Papierform) nach den strengen Maßstäben der DSGVO behandelt werden.

Sozialversicherungsnummern dürfen übrigens nur im Rahmen der Aufgaben verwendet werden, die der Sozialversicherung gesetzlich übertragen sind. Die Verwendung durch ein Versicherungsunternehmen ist nicht gestattet (also auch nicht durch einen VA). Sie kann auch nicht durch die Zustimmung

der betroffenen Personen gerechtfertigt werden (Empfehlung der Datenschutzbehörde vom 28. 6. 2017).

2. CHECKLISTE

Die wichtigsten Fragen, die sich ein Unternehmer angesichts der DSGVO stellen muss, sind:

- Welche personenbezogenen Daten werden wie verarbeitet (vervielfältigt, gespeichert etc)?
- Sind darunter sensible Daten wie Gesundheitsdaten?
- Was sind die Zwecke und die Rechtsgrundlagen?
- Einwilligungserklärungen insb. zur Zusendung von Newslettern sind einzuholen;
- Wie muss das Verzeichnis der Verarbeitungstätigkeiten aussehen und wie bleibt es aktuell?
- werden „Auftragsverarbeiter“ beschäftigt (z.B. externe Buchhalter, Rechenzentrum, Lohnverrechner, Cloud-Anbieter etc); Dienstleistungsverträge sind abzuschließen.
- Welche Datensicherungsmaßnahmen sind vorhanden?
- Gibt es gemeinsame Bereiche mit anderen Datenverantwortlichen? Falls ja, sollte eine Vereinbarung über die Zuständigkeiten abgeschlossen werden.
- Wie werden die Dokumentations- und Informationspflichten gegenüber denjenigen Personen erfüllt, deren Daten verarbeitet werden? (vgl. die Muster-Datenschutzerklärung im Anhang)
- Ist eine Datenschutz-Folgenabschätzung erforderklich?
- Muss ein Datenschutzbeauftragter bestellt werden?
- Erfolgt profiling?
- Und zu „guter“ Letzt: wie kann man nachweisen, dass all dies erfüllt wird?

Sonderregeln bestehen für Dienstanbieter gegenüber Kindern und für den Datenverkehr in das EU-Ausland und in Drittstaaten. Dies wird im vorliegenden Leitfaden nicht behandelt.

Ebenso wenig kann der Leitfaden eine individuelle Bestandsaufnahme und Beratung ersetzen.

3. BEREICHE DER DATENVERARBEITUNG IN EINER VERSICHERUNGSAGENTUR

In einer Versicherungsagentur können verschiedene Vorgänge von Datenverarbeitungen anfallen:

- der Agent verarbeitet Daten entweder unmittelbar selbst (Speicherung in seiner Kundendatei, Weiterleitung an ein Versicherungsunternehmen, Weiterleitung/Einreichung bei Behörden etc.);
- ein Subagent führt u.a. diese Tätigkeiten aus;
- der Versicherungsagent speichert die Daten unmittelbar im System des Versicherungsunternehmens (und bearbeitet sie nur dort);
- dies macht ein Subagent etc.

Wenn der Agent die Daten in seinem eigenen System verarbeitet, hat er (als sog. „Verantwortlicher“) die DSGVO einzuhalten. Die datenschutzrechtlichen Regelungen gelten nach herkömmlicher Ansicht auch für Vertriebspartner, da Ihnen ein gewisses Ermessen über die Datenverwendung zukommt.

Falls der Agent das System des Versicherungsunternehmens zur dortigen Speicherung und Bearbeitung nützt, treffen die Verpflichtungen nach DSGVO das VU. Nur falls der Agent – wenn auch nur in geringem Ausmaß – über den Zweck oder die Mittel der Verarbeitung (mit)entscheidet, dann wäre auch er „Verantwortlicher“. Die Zuständigkeitsbereiche müssten dann in einer Vereinbarung mit dem VU geklärt werden; ansonsten könnte der Agent für Datenschutzverletzungen solidarisch haften. Kommt dem Agenten hingegen keinerlei Ermessen über die (aktuelle und weitere) Datenverwendung zu, sollte hier kein Risiko gegeben sein.

Praxistipp: Der Agent sollte sich diesbezüglich jedenfalls mit dem VU abstimmen und sich zumindest die jeweiligen Datenschutzerklärungen der VU vorlegen lassen. Es sollte insb. sichergestellt sein, dass die datenschutzrechtlichen Informationspflichten gegenüber den Kunden erfüllt werden. Falls es „gemeinsame“ Bereiche der Datenverarbeitung geben sollte, müsste der VA eine Vereinbarung mit dem betreffenden VU über die Verantwortungsbereiche und Zuständigkeiten treffen.

Falls der Agent einen Subagenten heranzieht, ändert dies an den Verpflichtungen des Hauptagenten nichts; er muss diese eben durch den Subagenten sicherstellen, d.h. Vorsorge treffen, dass auch dann alle Verpflichtungen eingehalten werden. Falls der Subagent in einem eigenen

System Daten im Auftrag des Hauptagenten verarbeiten sollte, ist eine spezifisch datenschutzrechtliche Vereinbarung zwischen VA und Subagent erforderlich, die engen Kriterien genügen muss.

Das gilt für alle externen Dienstleister, so auch bei Verwendung von Tarifrechnern, aber auch bei genereller Nutzung externer IT-Dienstleister. Geht es um die Verarbeitung der vom VA erhobenen bzw. die Weiterverarbeitung der vom VA verarbeiteten Daten, darf er nur mit Auftragsverarbeitern zusammen arbeiten, die die Bestimmungen der DSGVO einhalten und nachweisbar Maßnahmen ergreifen, die dem Schutz der personenbezogenen Daten dienen.

Praxistipp: Im Verhältnis zu externen Dienstleistern werden deren vorhandene IT-Zertifikate eine besondere Rolle spielen; im Verhältnis zu Subagenten wird dies praktisch wohl nur so zu bewältigen sein, dass sie ausschließlich im System des Hauptagenten arbeiten (dürfen).

4. GRUNDÄTZE DER DATENVERARBEITUNG

Die Daten dürfen nach der DSGVO nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betreffende Person nachvollziehbaren Weise verarbeitet werden (Transparenz).

Sie dürfen nur für eindeutige Zwecke erhoben werden. Für andere Zwecke dürfen Sie nur weiterverarbeitet werden, wenn diese Zwecke mit den ursprünglichen Zwecken *vereinbar* sind.

Praxistipp: Nachdem dieses Kriterium der Vereinbarkeit äußerst unklar ist, empfiehlt es sich, für jeden Verarbeitungszweck eine gesonderte Einwilligungserklärung einzuholen. Alternative wäre nur, die Daten zu pseudonymisieren (d.h. die persönliche Zuordenbarkeit zu beseitigen).

Es dürfen nicht mehr Daten erhoben bzw. verarbeitet und auch nicht länger gespeichert werden als für den konkreten Zweck erforderlich (Grundsatz der Datenminimierung). Die Daten müssen zudem richtig sein bzw. muss sichergestellt werden, dass unrichtige Daten korrigiert oder gelöscht werden.

Praxistipp: Dies ist durch technische Voreinstellungen bzw. durch Setzen von Fristen für die Löschung oder regelmäßige Überprüfung umzusetzen.

Unbefugte dürfen selbstverständlich keinen Zugang zu den Daten haben.

5. INFORMATIONSPFLICHTEN / „DATENSCHUTZERKLÄRUNG“ (MUSTER IM ANHANG)

Werden Daten erhoben, sind der betroffenen Person im Zeitpunkt der Erhebung, d.h. vorab folgende Informationen zu erteilen:

- **Name und Kontaktdaten** des Verantwortlichen (und ggf seiner Vertreter),
- ggf Kontaktdaten des **Datenschutzbeauftragten**,
- **Verarbeitungszwecke** und **Rechtsgrundlagen** der Verarbeitung,
- im Falle einer Datenverarbeitung aufgrund berechtigter Interessen des Verantwortlichen bzw eines Dritten sind die **berechtigten Interessen**, die vom Verantwortlichen oder einem Dritten verfolgt werden, auszuweisen,
- ggf **Empfänger** der Daten,
- falls die Absicht besteht, die Daten an ein **Drittland** oder an eine **internationale Organisation** zu übermitteln, muss auch darüber informiert werden,
- **Dauer** der Datenspeicherung bzw wenn unmöglich die **Kriterien für die Festlegung** der Dauer,
- **Betroffenenrechte** auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Achtung: über dieses Widerspruchsrecht muss gesondert, d.h. von anderen Infos getrennt, informiert werden),
- die Möglichkeit des **Widerrufs** der Einwilligung,
- das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde,
- ob die Bereitstellung der personenbezogenen Daten **gesetzlich oder vertraglich vorgeschrieben** oder **für einen Vertragsabschluss erforderlich** ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte,
- ggf über das Bestehen **automatisierter Entscheidungsfindung**, inkl aussagekräftiger Informationen über die involvierte Logik und die Tragweite der Entscheidung (zB Profiling)[1].
- Falls die Daten nicht bei der betreffenden Person selbst erhoben werden, aus welcher Quelle die Daten stammen (in diesem Fall sind die Informationen spätestens innerhalb eines Monats nach Erlangung der Daten zu erteilen);
- Sollen die Daten für einen anderen als den ursprünglichen Zweck weiterverarbeitet werden, müssen vor der Weiterverarbeitung auch **Informationen über diesen anderen Zweck** und alle anderen maßgeblichen Informationen erteilt werden.

[1] Das ist die automatisierte Verarbeitung personenbezogener Daten zur Feststellung persönlicher Aspekte wie wirtschaftliche Lage, Interessen etc. Diese unterliegt besonderen Regeln, wenn damit eine automatische Generierung von Einzelentscheidungen verbunden ist. Im Folgenden wird davon ausgegangen, dass ein VA keine solche Verfahren anwendet.

Die Informationen müssen präzise, verständlich und leicht zugänglich sein. Sie können schriftlich, elektronisch oder in einer anderen Form erteilt werden. Sie können auch auf einer Webseite erteilt werden, darauf ist entsprechend hinzuweisen. Der Zugang der Information muss nachweisbar sein.

Die einmalige Information der betroffenen Person ist hinreichend außer es hätte sich eben der Verarbeitungsvorgang insb. die Verwendungszwecke geändert.

Hat der VA die Daten beim Versicherer angefragt, dann muss der VN nachträglich verständigt und die obigen Informationen erteilt werden.

Praxistipp: Empfehlenswert ist die Verwendung einer standardisierten Datenschutzerklärung **(Muster im Anhang).**

6. RECHTFERTIGUNGSGRUND DER VERTRAGSERFÜLLUNG / BERECHTIGTES INTERESSE DES DATENVERANTWORTLICHEN

Bestimmte Datenverarbeitungsvorgänge sind oftmals zwingende Voraussetzung für die Durchführung und Erfüllung eines Vertrags. So benötigt der Verkäufer die Adressdaten des Käufers, um ihm eine bestellte Ware zu liefern.

Die Datenverarbeitung muss also für die verfolgten, berechtigten Interessen „erforderlich“ sein. Eine bloße Zweckmäßigkeit reicht nicht aus. Generell spielt hier auch die Erwartungshaltung der betroffenen Person eine Rolle, ob sie also nach den Umständen „vernünftigerweise absehen“ konnte, dass eine Verarbeitung zu den in Frage stehenden Zwecken erfolgen werde[2]. Nur wenn die legitimen Interessen des Verantwortlichen überwiegen, darf die Datenverarbeitung auf dessen berechtigtes Interesse gestützt werden. Eine solche Abwägung ist für jeden Verarbeitungsvorgang vorzunehmen. Speicherung und Nutzung können also zulässig sein, die Übermittlung aber nicht.

Für VA bedeutet das: Regelmäßig zulässig wird daher die Verarbeitung der *Kontaktdaten* des VN sein. Soll ein Versicherungsvertrag vermittelt werden,

[2] Damit nähert sich die DSGVO dem US-Recht an. Seit der Entscheidung *Katz vs. US* wendet der Supreme Court in ständiger Rechtsprechung den sog. „reasonable expectations of privacy test“ an, wenn es um die Frage geht, ob ein rechtswidriger Eingriff in die Privatsphäre erfolgt.

wird auch die Erhebung und – notwendige – Verarbeitung aller *Daten* gerechtfertigt sein, die *erforderlich* sind, um einen entsprechenden *Vertrag anzubieten.* Dies gilt freilich auch für Daten, die nach *gesetzlichen Vorschriften* erhoben werden müssen. Auch die Weitergabe dieser Daten an das VU ist vom Vertragszweck umfasst.

Dies gilt auch im vorvertraglichen Stadium, soweit eine Anfrage der betroffenen Person zugrunde liegt.

Ob ein VU einem VA Daten übermittelt, auch wenn dieser den betreffenden Versicherungsvertrag nicht vermittelt hat, liegt zunächst einmal im Verantwortungsbereich des VU. Eine Rechtsgrundlage kann im berechtigten Interesse des VU (Kundenbetreuung bzw. Umsetzung des Kundenwunsches), aber auch des Dritten (VA) gesehen werden.

Ein berechtigtes Interesse ist auch anerkannt, was die spätere Zusendung von Werbung an *bestehende* Kunden für *eigene* Produkte und Dienstleistungen, aber auch für Werbung durch *Dritte* anlangt[3]. Dies umfasst zwar auch die Zusendung von Newslettern[4]; dennoch ist in der beiliegenden Muster-Datenschutzerklärung als Rechtfertigungsrund für die Zusendung von Newslettern die Einwilligung vorgesehen. Das entspricht auch praktischen Erwägungen zumal die Kunden gewohnt sind, Newsletter auch wieder „abbestellen" zu können (die Einwilligung ist ja als Rechtfertigungsgrund widerruflich, ein berechtigtes Interesse – zumindest durch den Kunden – nicht).

Auch der konzerninterne Datenaustausch („interne Verwaltungszwecke") ist als berechtigtes Interesse anerkannt[5]. Das stellt aber kein generelles Konzernprivileg dar; auch hier ist für jeden einzelnen Übertragungsvorgang ein berechtigtes Interesse Voraussetzung.

Sofern effektive Maßnahmen zur Datensicherheit gegeben sind, kann auch die Nutzung von Cloud-Services mit einem berechtigten Interesse gerechtfertigt werden. Dasselbe gilt für Bewertungsportale.

[3] „Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten" gemäß Art 6 Abs. 1 Satz 1 lit f DSGVO.
[4] *Wybitul*, EU-Datenschutz-Grundverordnung Art 6 Rz 37.
[5] Erwägungsgrund 48.

Praxishinweis: Die Datenverarbeitung kann aber nicht mit dem Vertragszwecke gerechtfertigt werden:

- Im vorvertraglichen Stadium, wenn der VA von sich aus an den Kunden herantritt oder

- wenn sensible Daten (v.a. Gesundheitsdaten) betroffen sind (siehe sogleich).

7. EINWILLIGUNGSERKLÄRUNG

Kann man sich für die Datenverarbeitung nicht auf eine Vertragserfüllung bzw. ein sonstiges berechtigtes Interesse berufen (vgl. die soeben genannten Fälle), ist eine Einwilligungserklärung der betroffenen Person erforderlich.

Achtung: Jede Verarbeitung kann nach Ansicht der Datenschutzgruppe der Kommission nur auf einer einzigen Rechtsgrundlage beruhen.

Praxistipp: Es empfiehlt sich also, klar zwischen den berechtigten Interessen und einer oder mehrerer Einwilligungserklärungen zu unterscheiden.

Eine ausdrückliche Einwilligung ist jedenfalls für die Erhebung bzw. Verarbeitung von sensiblen Daten (insb. Gesundheitsdaten, Krankheitsgeschichte) erforderlich. Im Detail sind darunter folgende Daten zu verstehen:

Daten, die sich auf den Gesundheitszustand einer natürlichen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und/oder zukünftigen körperlichen und/oder geistigen Zustand hervorgehen wie etwa Informationen über

- *Krankheiten*
- *Behinderungen*
- *Krankheitsrisiken*
- *Vorerkrankungen*
- *Behandlungen*

unabhängig von der Herkunft der Daten, ob sie also von einem Arzt oder Krankenhaus stammen, einschließlich von Proben, Röntgen, CT, MR einschließlich genetischer und biometrischer Daten.

Praxishinweis: Für Versicherungsagenten ist dies im Zusammenhang mit Kranken- und Lebensversicherungen von Bedeutung. Hier ist eine ausdrückliche Einwilligungserklärung jedenfalls erforderlich!

Die Einwilligungserklärung muss eindeutig und nachweisbar sein (z.B. durch Anklicken einer vorformulierten Erklärung; nicht ausreichend wäre ein bereits vorab angekreuztes Kästchen).

Die Einwilligungserklärung darf sich auch auf Zwecke erstrecken, die für die Vertragserfüllung nicht erforderlich sind; die Vertragserfüllung darf aber von der Einwilligung in solche (weiteren) Zwecke nicht abhängig gemacht werden (sog. Kopplungsverbot). Soll die Verarbeitung **mehreren Zwecken** dienen, sind stets **gesonderte** Einwilligungserklärungen erforderlich.

Ergebnis: Die Einwilligungserklärungen dürfen sich auf weitere, einzelne Zwecke außerhalb der Vertragserfüllung erstrecken. Die Vertragserfüllung selbst darf davon aber nicht abhängig sein – worüber die betroffene Person auch hinreichend verständlich und präzise zu informieren ist. In der technischen Umsetzung sind separate Checkboxen („Kästchen“) samt entsprechenden Hinweisen vorzusehen.

Ist die Einwilligungserklärung in AGB enthalten, muss sie optisch hervorgehoben werden. Es empfiehlt sich aber ohnehin, eine separate „Datenschutzerklärung“ zu verwenden und nachweislich zur Kenntnis zu bringen (Muster im Anhang); die Einwilligungserklärungen sind separat umzusetzen.

Die Einwilligungserklärung ist widerruflich, worauf vorab hinzuweisen ist. Der Widerruf muss technisch genauso einfach erfolgen können wie die Einwilligung (falls also für die Einwilligung ein Anklicken genügt, muss dies auch für den Widerruf gelten). Aufzuklären ist auch darüber, dass der Widerruf nicht rückwirkend für die Vergangenheit gilt.

Praxishinweis: „Alte“ (d.h. vor dem 25. 5. 2018 vorliegende) Einwilligungen wirken nur fort, wenn sie die (umfassenden) Anforderungen der DSGVO erfüllen. Dies wird in der Praxis kaum der Fall sein.

8. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Statt der Meldung an das Datenverarbeitungsregister und der DVR-Nummer ist ab 25. 5. 2018 ein (internes) Verzeichnis zu führen[6]. Dieses hat zu enthalten:

- Name und Kontaktdaten des bzw. der Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- Zweck der Datenverarbeitung (Versicherungsvermittlung, Schadenbearbeitung, Personalverwaltung, Buchhaltung, Marketing, Email-Newsletter);
- Kategorien betroffener Personen (z.B. Kunden, Mitarbeiter, Interessenten) und
- Kategorien personenbezogener Daten (z.B. Name, Adresse, Geburtsdatum, Polizzennummer, Bankdaten);
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (z.B. Versicherungsunternehmen, Behörden, insb. Zulassungsstellen, Sozialversicherungsträger, Gerichte, Banken, Finanzamt, Rechtsanwalt, Steuerberater).
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien (nach Möglichkeit)[7],
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (nach Möglichkeit); siehe dazu sogleich in Punkt 9.

Der letzte Punkt ist nicht zu unterschätzen, da alle damit zusammen hängenden Punkte (Vertraulichkeit, Datenverfügbarkeit etc) in das Verzeichnis aufzunehmen sind. Auf der anderen Seite erfüllt man dadurch gleich in einem die Dokumentationspflicht hinsichtlich dieser Datensicherheitsmaßnahmen.

Bei diesem Verzeichnis geht es nicht um die tagesaktuelle Erfassung aller einzelnen Verarbeitungsvorgänge, sondern um einen systematischen Gesamtüberblick, um darstellen zu können, welche Verarbeitungsvorgänge überhaupt stattfinden. Ein Muster finden Sie unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html.

---

[6] Die vorhandenen DVR-Meldungen können in der Internet-Applikation DVR-ONLINE sowohl als PDF-Dokumente als auch als XML-Dateien übernommen werden. Hierfür wurden im DVR-ONLINE-Meldebereich des Auftraggebers entsprechende Funktionen eingefügt (rote Buttons).

[7] Einen Überblick über die in Frage kommenden Fristen und Rechtsgrundlagen finden Sie unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html. .

Praxistipp: Ändern sich die Anforderungen eines VU, was die Datenerfassung bzw. -weiterleitung anlangt, müsste dies im Datenverarbeitungsverzeichnis adaptiert werden (wobei vorab freilich zu prüfen ist, ob die [neu angeforderte] Datenverarbeitung zur Vertragserfüllung erforderlich ist bzw. eine hinreichende Einwilligungserklärung vorliegt bzw. ob auch diese zu aktualisieren, d.h. neu einzuholen ist).

9. DATENSICHERHEITSMASSNAHMEN

Die Datensicherheit muss nach der DSGVO noch stärker als bisher beachtet werden. Je nach Risiko muss ein angemessenes Schutzniveau erreicht werden. Dabei ist der Stand der Technik zu berücksichtigen (*privacy by design*). Datenschutzfreundliche Voreinstellungen (*privacy by default*) sollen sicherstellen, dass nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen Zweck erforderlich sind (dies bezieht sich also vor allem auf internetbasierte Anwendungen wie Online-Portale und -shops, Webformulare, Cookies etc.).

In diesem Zusammenhang nennt die DSGVO einige Maßnahmen (die nicht zwingend sind, aber im Rahmen einer Risikoanalyse geboten sein können):

- Pseudonymisierung (d.h. Daten werden „entpersonalisiert“, so dass sie ohne zusätzliche Informationen einer bestimmten Person nicht mehr zugeordnet werden können; diese zusätzlichen Infos werden gesondert verwahrt);
- Verschlüsselung (Passwortsicherung von Dateien);
- Sonstige Zugriffsbeschränkungen;
- Angestellte dürfen Daten nur nach Anweisung verarbeiten („Auftragsprinzip“)[8];
- Verwendung von Back-up-Programmen;
- Regelmäßige Selbstevaluierungsprozesse

Nicht zu vergessen: Die Datensicherheitsmaßnahmen sind auch in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen (siehe oben Punkt 8.).

[8] Das Datengeheimnis wurde auch durch das Datenschutz-Anpassungsgesetz geschärft: demnach müssen Mitarbeiter verpflichtet werden, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anweisungen zu übermitteln und das Datengeheimnis auch nach dem Ende ihres Arbeitsvertrags zu beachten. Die Mitarbeiter sind über die Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

Praxistipp: Diese Anforderungen sind zu erfüllen durch

- Herstellung und Überwachung des Standes der Technik (also entsprechende Zusammenarbeit mit einem IT-Unternehmen),
- Einschulung/Anweisung/Überwachung der Mitarbeiter (auch durch entsprechende Klauseln in Dienstverträgen und Verschwiegenheits-erklärungen; siehe Fußnote 8) und auch durch
- Beachtung und Umsetzung in der täglichen Praxis (z.B. Passwort-management).

In diesem Zusammenhang stellt sich freilich die Frage, ob denn **Emails** ohne weiteres überhaupt noch versandt werden dürfen oder ob hier besondere Maßnahmen erforderlich sind. Nachdem die DSGVO in diesem Punkt keine spezifischen Vorgaben macht, kann man sich nur am allgemeinen Schutz-standard der Datensicherheit orientieren.

Praxistipp: Zur Umsetzung kann ein VPN (virtual private network) genutzt werden. Dafür gibt es Anbieter, die die Emails gegen ein monatliches Entgelt auf geschütztem Weg versenden. Als (umständliche) Alternative würde sich die Versendung als verschlüsselte Zipp-Datei (samt Übersendung des Passwortes per SMS) anbieten.

Im Zusammenhang mit der Datensicherheit ist zu berücksichtigen, dass eine Datenübermittlung in ein Drittland (außerhalb der EU) zusätzlichen Anforderungen bzw. Einschränkungen unterliegt, was bei **Cloud**-Lösungen eine Rolle spielt. So müssten Standarddatenschutzklauseln abgeschlossen werden oder verbindliche, von der Aufsichtsbehörde genehmigte Datenschutzvorschriften bestehen. Zudem wäre die Datenübermittlung in ein Drittland zulässig, wenn die betroffene Person ausdrücklich eingewilligt hat, was eine entsprechende Information bzw. Aufklärung voraussetzt.

Praxistipp: Wenn ein Cloud-Anbieter mit Sitz in einem EU-Land ausgewählt wird, bestehen diesbezüglich keine zusätzlichen Anforderungen.

10. DATENÜBERTRAGBARKEIT

Jeder Datenverantwortliche muss der betroffenen Person auf Antrag sämtliche, sie betreffende gespeicherte bzw. sonst wie verarbeitete Daten in einem strukturierten und maschinenlesbaren Format übermitteln (können). Sie hat auch den Anspruch, dass die Übermittlung an einen von ihr

benannten Dritten erfolgt (z.B. an einen anderen VA, einen Makler oder an ein VU).

Dies muss nach Aufforderung unverzüglich und kostenfrei erfolgen.

11. DATENSCHUTZBEAUFTRAGTER

Besteht die Kerntätigkeit eines Unternehmens (auch) in einer regelmäßigen und systematischen Überwachung der Personen, deren Daten verarbeitet werden, ist ein Datenschutzbeauftragter zu bestellen. Dies trifft auf Versicherungsunternehmen zu (Zahlungsverhalten der Kunden), aber wohl nicht auf VA.

Für VA könnte der zweite Anwendungsfall maßgebend sein: wenn nämlich die *Kerntätigkeit* in der *umfangreichen* Verarbeitung *sensibler* Daten (z. B. Gesundheitsdaten) besteht, wäre ein Datenschutzbeauftragter zu bestellen. Die Datenschutzgruppe der EU-Kommission nennt diesbezüglich als Beispiel eine Krankenanstalt, die einen Datenschutzbeauftragten bestellen muss, nicht aber der einzelne Arzt. Dasselbe muss für einen VA gelten.

Ein VA sollte daher i.d.R. nicht verpflichtet sein, einen Datenschutz-beauftragten zu bestellen.

12. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Nach dem Text der DSGVO klingt es (zunächst) eher nicht so, als müsste ein VA eine Folgenabschätzung durchführen. Diese ist vorzunehmen, wenn *voraussichtlich* ein *hohes* Risiko für die betroffenen Personen entsteht, insb. wenn *neue Technologien* zum Einsatz kommen. Zwingend erforderlich ist eine solche Abschätzung nur, falls *umfangreich* sensible Daten verarbeitet werden.

Das scheint bei einem Agenten nicht der Fall zu sein. Aber: In der juristischen Kommentarliteratur wird auf die englische Fassung der DSGVO verwiesen, wonach der leise Anschein eines hohen Risikos maßgebend sein soll; neue Technologien sollen übrigens auch neue Algorithmen sein.

Die Datenschutzgruppe der EU-Kommission legt die DSGVO in ihren Leitlinien so aus, dass eine Folgenabschätzung nur dann nicht erforderlich ist,

*wenn die Verarbeitung „**wahrscheinlich kein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen mit sich bringt“.*

Im Ergebnis wird auch ein VA sicherheitshalber, um allen Eventualitäten vorzubeugen, eine solche Datenschutz-Folgenabschätzung vornehmen (müssen). Neben der unklaren rechtlichen Situation ist auch auf einen rein praktischen Aspekt zu verweisen: sollte es tatsächlich einmal ein Problem mit der Datensicherheit geben, kann der Datenschutzbehörde sogar eine Folgenabschätzung vorgelegt werden.

Die Datenschutz-Folgenabschätzung besteht insb. aus folgenden Prüfschritten[9]:

Werden die datenschutzrechtlichen Prinzipien eingehalten?
Warum ist eine Folgenabschätzung erforderlich?
Beschreibung der Datenverarbeitungsvorgänge
Welche möglichen Risiken bestehen betreffend
- Datenverfügbarkeit
- Vertraulichkeit
- Zweckbindung
- Datenminimierung, Speicherbegrenzung etc.
- Risikoanalyse: von wem kann mit welchen Motiven eine Gefahr ausgehen? Eintrittswahrscheinlichkeit? Folgen für die betroffenen Personen?

Bisher getroffene Abwehrmaßnahmen
Maßnahmenplan (allfällige weitere Maßnahmen)
Prioritätensetzung

Praxistipp: Die Folgenabschätzung kann am besten und einfachsten in enger Zusammenarbeit mit dem beauftragten IT-Unternehmen durchgeführt werden. Letztlich geht es darum, Datenschutz ernst zu nehmen, sich (intensiv) damit zu beschäftigen und dies – auch im Nachhinein – dokumentieren zu können.

[9] Eine detaillierte Aufstellung finden Sie unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html.

13. BETROFFENENRECHTE

Die DSGVO sieht – da es um den Schutz personenbezogener Daten geht – naheliegender Weise auch (formale) Rechte der betroffenen Personen vor. Diese Rechte sind teilweise nicht neu, auch das bisherige Datenschutzrecht hatte ähnliche Instrumente vorgesehen. Es geht dabei um:

- die (bereits erörterte) Informationspflicht (siehe oben Punkt 5);
- Auskunftsrecht (im Wesentlichen über die Daten und den Umfang der Verarbeitung)
- Recht auf Berichtigung (unrichtiger Daten);
- Recht auf Löschung („Recht auf Vergessenwerden“);
- Recht auf Einschränkung (dazu noch unten);
- Recht auf Datenübertragbarkeit (dazu schon oben Punkt 10);
- Widerspruchsrecht

Ein Recht auf Löschung besteht nicht, soweit die Verarbeitung (damit auch die Speicherung) zur Erfüllung einer rechtlichen Verpflichtung notwendig ist (also etwa für die Betreuung in Schadensfällen [sofern in diesen Fällen noch erwünscht], die Erfüllung von Aufbewahrungs- und Dokumentations-pflichten etc.).

Das Widerspruchsrecht spielt insb. eine Rolle, wenn die Rechtsgrundlage der Verarbeitung in der Vertragserfüllung (und nicht in einer Einwilligung) besteht (ansonsten ja der richtige Rechtsbehelf der Widerruf wäre). Damit im Zusammenhang steht das Recht auf Einschränkung. Widerspricht der Betroffene einer weiteren Datenverarbeitung und ist der Verantwortliche der Ansicht, dass seine Interessen überwiegen, dann steht dem Betroffenen bis zur Klärung der Angelegenheit das Recht auf Einschränkung zu. Die Daten dürfen dann weiterhin gespeichert, aber ansonsten nicht verarbeitet werden.

Die „Hürde“ für einen solchen Widerspruch ist aber durchaus hoch. Dafür müssen Gründe vorliegen, die sich aus der **besonderen Situation** der betroffenen Person ergeben. Nicht ausreichend wäre es, wenn sie generell keine Speicherung und sonstige Verarbeitung wünscht. Vielmehr muss sie persönliche Gründe darlegen, weshalb ihr, anders als anderen Kunden und Nutzern, die (weitere) Verarbeitung von Daten über ihre Person unzumutbar ist. Wird dies dargelegt, ist eine weitere Verarbeitung der personen-bezogenen Daten nur in zwei Fällen zulässig:

- das Unternehmen weist zwingende schutzwürdige Gründe für die Verarbeitung nach, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder
- die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Wichtig; nach einem Widerspruch ist die Zusendung von Werbung an die betreffende Person jedenfalls untersagt. Über das Recht auf Widerspruch muss gesondert, d.h. von anderen Informationen getrennt, informiert werden.

Praxishinweis: Werden Betroffenenrechte ausgeübt, muss der VA auch das VU verständigen, an das die Daten weitergeleitet wurden.

In diesen Fällen hat der VA – mangels Kontrollmöglichkeit – freilich keine abschließende Sicherheit, ob das VU z.B. eine begehrte Löschung der Daten korrekt umsetzt. Dies ist dann aber nicht (mehr) seine Verantwortung.

14. MELDUNG VON DATENSCHUTZVERLETZUNGEN

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, ist dies zu melden („*data breach notification*“).

Die Datenverletzung ist an die Aufsichtsbehörden zu melden, wenn die Verletzung zu einem Risiko für die Rechte der betreffenden Personen führt. Diese sind ebenso zu informieren. Geht es um Passwörter, ist bei der Risikobewertung zu berücksichtigen, dass Kunden ihre Passwörter erfahrungsgemäß durchaus mehrfach verwenden.

Praxistipp: Kommt es zu (möglichen) Datenverletzungen, sollten jedenfalls die Aufsichtsbehörde, die betreffenden Personen und das VU, an das die Daten weiter geleitet wurden, verständigt werden.

15. STRAFEN; VERTRAGLICHE VEREINBARUNGEN

Die DSGVO sieht für Verstöße bekanntlich sehr hohe Strafen vor (Geldbuße bis € 20 Mio oder 4% des weltweiten Jahresumsatzes).

Sind nun mehrere Verantwortliche oder Auftragsverarbeiter an einer Datenverarbeitung beteiligt (vgl. die Darstellung in Punkt 3), haftet jeder einzelne für den gesamten Schaden.