Entscheide und Fragen zum Datenschutz, insbesondere im Versicherungsbereich

Nando Stauffer von May* / Sonia Lehner**

Das Schweizer Datenschutzrecht orientiert sich stark an der europäischen Datenschutz-Grundverordnung. In der EU werden beinahe täglich neue Entscheide gefällt sowie Merkblätter veröffentlicht. Auch in der Schweiz liegen erste Entscheide zum revidierten Datenschutzgesetz vor und der Tätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wird vermehrt Beachtung geschenkt. Der vorliegende Beitrag geht auf neueste Entwicklungen und Praxisfragen in den Bereichen Datensicherheit, Bekanntgabe von besonders schützenswerten Personendaten an Dritte, Informationspflicht, Auskunftsbegehren, Bussen und Auftragsbearbeitung ein, jeweils mit einem Fokus auf die Versicherungsbranche.

Le droit de la protection des données suisse s'inspire fortement du règlement européen sur la protection des données (RGPD). Au sein de l'Union européenne, de nouvelles décisions sont rendues et des fiches informatives sont publiées presque quotidiennement en la matière. En Suisse, l'on dispose également des premières décisions prises en application de la nouvelle loi fédérale sur la protection des données (LPD) et l'activité du préposé fédéral à la protection des données et à la transparence suscite de plus en plus d'intérêt. La présente contribution s'intéresse aux développements récents et aux questions pratiques dans les domaines de la sécurité des données, de la communication de données sensibles à des tiers, du devoir d'information, des demandes d'accès, des amendes ainsi que de la sous-traitance en mettant l'accent sur le secteur de l'assurance.

I. Einleitung

Nahezu jeder Versicherer kennt die nachfolgenden Situationen: Nachdem die Leistungspflicht abgelehnt wird, fliegt ein Auskunftsbegehren ins Haus. Oder mit Geschäftspartnern diskutiert «Legal» oder «Compliance», ob der Partner nun Auftragsbearbeiter, gemeinsam Verantwortlicher oder eigenständiger Verantwortlicher ist und ob man diesem Personendaten bekanntgeben darf. Bei der Datensicherheit verlässt sich der Versicherer auf seine IT-Abteilung und wenn etwas schiefläuft, kommt die Frage, ob die Verletzung der Datensicherheit (sog. *Data Breach*) gemeldet werden muss. Versicherungsnehmer wünschen entsprechenden Cyber-Schutz und hätten am liebsten auch Bussen für Datenschutzverletzungen versichert. Der vorliegende Beitrag will auf einige der sich für Versicherer stellenden Fragen Antworten geben und erste Entscheide präsentieren.

II. Datensicherheit und *Data Breach*

A. Gesetzliche Regelung

Das Schweizer Datenschutzgesetz (DSG) verpflichtet den Verantwortlichen und die Auftragsbearbeiter, durch technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten.[1] Die europäische Datenschutz-Grundverordnung (DSGVO) enthält eine ähnliche Bestimmung,[2] die den Verantwortlichen und den Auftragsverarbeiter anweist, geeignete technische und organisatorische Massnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu erreichen. Diese Bestimmung beinhaltet darüber hinaus eine exemplarische Liste von Massnahmen. In der Schweiz hat der Bundesrat die notwendigen Massnahmen in der Datenschutzverordnung präzisiert.[3] Diese Anforderungen gehen teilweise sehr weit und es ist fraglich, inwiefern diese noch durch die Delegationsnorm im DSG gedeckt sind.[4] Die Frage ist indes eher akademischer Natur, da den meisten Artikeln nur programmatischer Charakter zukom-

* Dr. iur., Rechtsanwalt, Partner bei gbf Rechtsanwälte AG, von 2016 bis 2019 Datenschutzbeauftragter eines Erst- und eines Rückversicherers.
** MLaw, *Greffière* bei der Staatsanwaltschaft des Kantons Waadt.

1 Art. 8 Abs. 1 DSG.
2 Art. 32 DSGVO.
3 Art. 1 ff. DSV.
4 Nach Art. 164 und Art. 182 BV sind alle wichtigen Rechtssätze in Form des Bundesgesetzes, d.h. durch das Parlament unter Referendumsvorbehalt, zu erlassen (formelles Legalitätsprinzip; Gesetzesvorbehalt im Sinne eines Vorbehalts des formellen Gesetzes). In diesem Sinne muss der Gesetzgeber nach der sog. Wesentlichkeitstheorie das Wichtige selber festlegen. Namentlich die Auferlegung von Leistungspflichten, wie auch die Festlegung der Rechte und Pflichten unter Privaten, bedürfen eines Entscheides durch den Gesetzgeber. Die Verordnungsstufe genügt hierfür nicht (vgl. Nando Stauffer von May, Regionale Aufgabenerfüllung und demokratische Rechte, Diss. Bern 2018, N 182–192).