
Datenerhebung sowie Datenübermittlung vom Gruppenvertragspartner an die HALLESCHE

- **Welche datenschutzrechtlichen Bestimmungen muss der Gruppenvertragspartner beachten, wenn er die Daten seiner Mitarbeiter erhebt und dann an uns weitergibt/übermittelt?**
 - Der Gruppenvertragspartner/Arbeitgeber (GVP/AG) muss in erster Linie nach den Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) vorgehen. Zu beachten sind für den Arbeitgeber ggf. aber auch noch Bestimmungen aus dem Bundesdatenschutzgesetz (BDSG n. F.), wie etwa der § 26, der Näheres zur „Datenverarbeitung für Zwecke des Beschäftigtenverhältnisses“ beinhaltet.
 - Grundsätzlich muss der GVP/AG erst einmal Art. 6 „Rechtmäßigkeit der Verarbeitung“ DSGVO beachten: Danach ist die Verarbeitung (v. a. die Erhebung, die Speicherung, die Übermittlung sowie die Nutzung) durch den GVP/AG erst dann rechtmäßig, wenn
 1. die betroffene Person (Versicherte Person/Mitarbeiter – VP/MA) ihre Einwilligung dazu gegeben hat oder sie den GVP/AG dazu bevollmächtigt hat, oder
 2. die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Gruppenvertragspartner unterliegt, oder
 3. die Verarbeitung zur Wahrung der berechtigten Interessen des Gruppenvertragspartners erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der versicherten Personen überwiegen.
 - Neben diesen Erlaubnistatbeständen ist es wichtig, dass der GVP/AG den Art. 13 DSGVO berücksichtigt. Danach hat der VP/MA vor allem das Recht zu erfahren, für welchen Zweck die Mitarbeiterdaten erhoben werden (für den privaten Krankenversicherungsschutz), an welchen Empfänger sie übermittelt werden und wo die Daten gespeichert werden (HALLESCHE Krankenversicherung), Dauer der Verarbeitung und ggf. auch über seine Widerrufsmöglichkeit.
- **Was sind spezielle rechtliche Verpflichtungen?**
 - Eine spezielle rechtliche Verpflichtung liegt mit § 17 SGB V vor, wenn der GVP/AG seine Mitarbeiter ins Ausland entsendet und für einen Versicherungsschutz zu sorgen hat. Folglich sind auch Datenverarbeitungsvorgänge notwendig.
 - Als spezielle rechtliche Regelungen werden auch betriebsverfassungsrechtliche Kollektivvereinbarungen (gem. § 26 Abs. 4 BDSG n. F.) oder arbeitsvertragliche Vereinbarungen angesehen (beide vereinbarungsarten müssen sich allerdings an den datenschutzrechtlichen Maßgaben der DSGVO messen lassen).
 - Der GVP/AG sollte prüfen, ob hausinterne Regelungen bestehen. Auch bietet sich die Einbeziehung des eigenen betrieblichen Datenschutzbeauftragten an.
- **Und wenn der Mitarbeiter ausdrücklich und vorab einwilligt?**
 - Holt der GVP/AG bei seinen MA die Einwilligung ein, dass bestimmte Mitarbeiterdaten zum Zwecke des Versicherungsschutzes an den Versicherer übermittelt werden, so besteht größtmögliche Transparenz und auch allseitige Akzeptanz (auch die explizite Einwilligung ist verbunden mit der Mitteilung diverser Informationen (gem. Art. 13 DSGVO).
- **Und wenn keine speziellen Regelungen bestehen und auch keine Einwilligungseinholung möglich ist?**
 - Liegen weder spezielle hausinterne Regelungen noch können explizite Einwilligungen eingeholt werden noch besteht die gesetzliche Verpflichtung zum Versicherungsschutz, so kann der GVP/AG die Rechtmäßigkeit

seiner Verarbeitung (Erhebung, Speicherung und Übermittlung) auf eine Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO stützen. Dabei gilt jedoch immer, dass die Verarbeitung zur Wahrung der berechtigten Interessen des Gruppenvertragspartners erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der versicherten Personen überwiegen.

- Erhebt der GVP/AG Gesundheitsdaten bei seinem MA, so ist auf jeden Fall die ausdrückliche Einwilligung des betroffenen MA erforderlich.
- Zwischen GVP/AG und Versicherer besteht keine Auftragsverarbeitung gemäß Art. 28 DSGVO. Somit ist die Legitimation zur Übermittlung an die HALLESCHE Krankenversicherung immer unter den Maßgaben des Art. 6 DSGVO sowie § 26 BDSG n. F. zu prüfen.

Die HALLESCHE beachtet die datenschutzrechtlichen Maßgaben

■ Was muss die HALLESCHE beachten, wenn externe Dienstleister beauftragt werden?

- **Auftragsverarbeitung (Art. 28 DSGVO):** Die HALLESCHE schließt mit dem externen Dienstleister ein Auftragsverarbeitungsverhältnis ab (derartige Auftragsvertragsverträge bestehen bereits mit Dienstleistern, mit denen wir regelmäßig zusammenarbeiten; die bisher nach § 11 BDSG a. F. abgeschlossenen Verträge wurden allesamt DSGVO-konform umgestellt).
- **Verletzung von Privatgeheimnissen (§ 203 StGB):** Als privates Krankenversicherungsunternehmen unterliegen wir – wie auch Ärzte, Rechtsanwälte und Steuerberater etc. – einer speziellen Schweigepflicht, so dass es für die Datenübermittlung/-offenbarung eines Erlaubnistatbestandes bedarf. Mit § 203 StGB n. F. sind auch die Dienstleister auf diesen Geheimnisschutz zu verpflichten und sind dann mithin dem genannten Personenkreis gleichgestellt.
- **Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft – Code of Conduct (CoC):** Mit dem CoC a. F. hatten die Datenschutzaufsichtsbehörden der Bundesländer in Abstimmung mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) und dem Verbraucherzentrale Bundesverband (vzbv) die Regelungen des BDSG, des (VVG) und des (StGB) in Einklang gebracht. Mit Einführung der DSGVO und dem BDSG n. F. wird auch eine neue Fassung des CoC für die HALLESCHE Anwendung finden.
- **Datenschutzerklärung:** Im Antragsformular stehen unter der „Datenschutzerklärung“ die Einwilligungsklauseln nach den Maßgaben der DSGVO sowie die Schweigepflichtentbindungsklauseln nach § 203 StGB. Darin enthalten sind auch die Regelungen hinsichtlich der „Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)“ zusammen mit dem Verweis auf die „Dienstleisterliste“.
 - Liegt dem Versicherungskunden ein Antrag bzw. eine Anmeldung vor, so unterschreibt er diese vom GDV zusammen mit den Datenschutzaufsichtsbehörden vorgegebenen Passagen. (Die HALLESCHE wird auch künftig nur „Datenschutzerklärungen“ verwenden, die der GDV nach Abstimmung mit den Datenschutzaufsichtsbehörden zur Verfügung stellt.)
 - Spezielle Informationen zur DSGVO und zu den Betroffenenrechten haben wir im Anschluss an die „Datenschutzerklärungen“ aufgeführt (auch diese Ausführungen basieren auf einem Muster des GDV).
 - Die „Datenschutzerklärungen“ zielen vornehmlich auf die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten ab, während der CoC den Umgang mit den ‚Nicht-Gesundheitsdaten‘ bzw. den übrigen Daten regelt. Beide Regelwerke stehen nebeneinander mit dem Ziel, das gesamte Spektrum der Versicherungskundendaten im Sinne der DSGVO, des BDSG n. F., des StGB und des VVG transparent und vollumfänglich zusammenzufassen.

■ **Was müssen wir auf jeden Fall gegenüber dem Versicherungskunden beachten?**

- Wir beachten auf jeden Fall
 - die DSGVO-Bestimmungen,
 - die Verschwiegenheitspflicht des Versicherers (§ 203 StGB),
 - den Code of Conduct,
 - und die Datenschutzerklärung in der Anmeldung (mit den darin enthaltenen Einwilligungen),
 - sowie auch alle übrigen Maßgaben, die den Datenschutz betreffen.

■ **Muss der Versicherungskunde unbedingt einwilligen oder genügt auch eine umfangreiche Information?**

- Die DSGVO verlangt keine schriftliche Einwilligung mehr.
- Die Erlaubnistatbestände nach Art. 6 DSGVO sind einfacher anzuwenden.
- Die Informationspflichten nach Art. 12 DSGVO (und ggf. 13 DSGVO „Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden“) sind dagegen strenger geworden, insofern, als dass im Zuge der Datenerhebung zeitnahe und umfangreiche Informationen dem Mitarbeiter bzw. der versicherten Person zur Verfügung zu stellen sind.
- Mit den Informationen zur DSGVO ist der Versicherungskunde vorab, zeitnah und vollumfänglich in Kenntnis gesetzt, was mit seinen Daten passiert, welche Rechte er hat und welche Pflichten wir haben. Dies entspricht auch der Intention des CoC.

■ **Und wie verhält es sich mit der Verarbeitung eingereichter Rechnungen/Gesundheitsdaten?**

- Wenn der Versicherungskunde uns Rechnungen einreicht, ist die Verarbeitung durch die DSGVO gedeckt.

■ **Ist die Vorgehensweise der Datenschutzzinformation anstelle der Einwilligungseinholung rechtskonform?**

- Hat der VP/MA nicht die Möglichkeit das Antrags- bzw. Anmeldeformular zu unterschreiben, so bietet das Formular „Datenschutzzinformation – für unsere Versicherungskunden in der Gruppenversicherung“ eine Form der informierten Einwilligung.
- Explizite, schriftliche Einwilligungserklärungen werden dann noch zusätzlich eingeholt, wenn wir Anfragen bei Krankenhäusern oder Ärzten halten, medizinische Gutachter oder nachuntersuchende Ärzte einschalten müssen und hierzu gesundheitsbezogene Daten mitgeben.