Zusammenspiel von DSGVO und Cyber-Versicherung.

Am 25. Mai 2018 endet für Unternehmen die Übergangsfrist für die Umsetzung der geforderten Maßnahmen zur Einhaltung der neuen Datenschutz-Grundverordnung. Insbesondere für kleine und mittelständische Unternehmen stellt diese Verordnung eine große Herausforderung in Bezug auf die IT-Sicherheit und die damit verbundenen Prozessen dar.

Die DSGVO-Konformität kann durch eine Cyber-Versicherung nicht hergestellt werden. Die Cyber-Versicherung kann insbesondere keine der geforderten Sicherheitsmaßnahmen ersetzen.

Die Anstrengungen der Unternehmen liegen bisher darin, den Datenschutzanforderungen spätestens zum Fristende am 25. Mai 2018 zu entsprechen. Jedoch muss auch das Szenario betrachtet werden, wenn trotz aller getroffenen Maßnahmen ein Sicherheitsvorfall, bspw. durch einen Hackerangriff, Ransomware oder unzufriedenen Mitarbeiter eintritt.

Schutz durch die Cyber-Versicherung

Meldepflicht ggü. Aufsichtsbehörde bei einer Verletzung personenbezogener Daten (Art. 33 DSGVO)

Die Verordnung fordert die Unternehmen im Falle einer Verletzung des Schutzes personenbezogener Daten dazu auf, unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde zu melden. Eine Ausnahme von dieser Regel gibt es dann, wenn die Verletzung „voraussichtlich“ nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Meldung selbst muss lt. Abs. 3 des Artikels 33 DSGVO bestimmte Mindestinformationen enthalten.

Die Cyber-Versicherung kann die Organisation sowie die Kosten zur Erfüllung der gesetzlichen Vorschriften einer korrekten Meldung im Rahmen der Assistance-Dienstleistung bei einem versicherten Schadensfall übernehmen.

Die Cyber-Versicherung kann die forensische Analyse und Ermittlung der betroffenen Daten sowie deren Eigenschaften (Risiko-Daten) im Rahmen der Assistance-Dienstleistung bei einem versicherten Schadensfall übernehmen.

Meldepflicht ggü. betroffenen Personen bei einer Verletzung personenbezogener Daten (Art. 34 DSGVO)

Die Verordnung fordert die Unternehmen im Falle einer Verletzung des Schutzes personenbezogener Daten dazu auf, unverzüglich nachdem die Verletzung bekannt wurde, die betroffenen Personen zu benachrichtigen, sofern voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der natürlichen Person vorliegt. Die Benachrichtigung selbst muss in klarer und einfacher Sprache die Verletzung beschreiben und lt. Abs. 3 des Artikels 33 DSGVO bestimmte Mindestinformationen enthalten.

Die Cyber-Versicherung kann die Organisation sowie die Kosten eins ausreichenden Benachrichtigungs-Managements im Rahmen der Assistance-Dienstleistung der zugrundeliegenden Bedingungen bei einem versicherten Schadensfall übernehmen.

Die Cyber-Versicherung kann die forensische Analyse und Ermittlung der betroffenen Daten (welche natürlichen Personen sind betroffen) sowie deren Eigenschaften (Risiko-Daten) im Rahmen der Assistance-Dienstleistung der zugrundeliegenden Bedingungen bei einem versicherten Schadensfall übernehmen.

Aufrechterhaltung der DSGVO-Konformität

Die Einhaltung der Verordnung kann durch Unternehmen nur über eine ständige Einhaltung des geforderten Sicherheitsniveaus sichergestellt sein. Dieses Niveau kann als Folge eines Hackerangriffs, einer Ransomware-Attacke oder einer Manipulation eines unzufriedenen Mitarbeiters beeinträchtigt werden. Eine Wiederherstellung des geforderten Niveaus ist für ein Unternehmen unerlässlich um ggü. dem Gesetzgeber keinen Fehltritt darzustellen.

Die Cyber-Versicherung kann neben der forensischen Analyse und Ermittlung von betroffenen Daten auch die Kosten für die Wiederherstellung der Systeme im Rahmen der Assistance-Dienstleistung bei einem versicherten Schadensfall übernehmen.

Kein bzw. eingeschränkter Schutz durch die Cyber-Versicherung

Bußgelder bei Verstößen gegen die DSGVO (Art. 83 DSGVO)

Die Versicherer haben im Rahmen ihrer Bedingungen unterschiedliche Formulierungen zu der Versicherbarkeit behördlich verhängter Bußgeldern gewählt. Die DSGVO sieht Bußgelder bis zu 20 Mio. € oder 4 % des weltweit erzielten Jahresumsatzes vor.

Im Grundtenor ist die Versicherung von Bußgeldern in Deutschland- auch in anderen Versicherungssparten – möglicherweise nicht zulässig. Einige Versicherer haben daher die Regelung aufgenommen, dass Bußgelder als versichert gelten, sofern national kein gesetzliches Versicherungsverbot dagegensteht. Diese Regelung ermöglicht international aufgestellten Unternehmen eine Absicherung des Bausteins.

Betriebsunterbrechung aufgrund behördlicher Auflagen

Die Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten (Art. 1 DSGVO). Bei einer Gefährdung dieses Schutzziels kann die zuständige Aufsichtsbehörde einen Betriebsstop des betroffenen Unternehmens mit der Folge eines Betriebsunterbrechungsschadens anordnen. Die Cyber-Versicherer haben Betriebsunterbrechungsschäden aufgrund behördlich angeordneter Beschränkungen teilweise ausgeschlossen.