Gesetz über den Schutz von Geschäftsgeheimnissen:

Geheimnisschutz und Datenschutz

Das im April in Kraft getretene, neue Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) stellt viele Unternehmen schon kurz nach der aufwendigen Umsetzung der Europäischen Datenschutzgrundverordnung (DS-GVO) vor die nächste Herausforderung.

In manchen Konstellationen können die Regelungen des Datenschutzes mit denen des Geheimnisschutzes konkurrieren – insbesondere, wenn bei Erteilung einer datenschutzrechtlichen Auskunft Informationen an die betroffene Person offengelegt werden sollen und diese Informationen auch Geschäftsgeheimnisse umfassen.

Die gute Nachricht ist aber: Wer sich mit den neuen Regelungen zum Schutz von Geschäftsgeheimnissen auseinandersetzt, findet sehr viele Parallelen zu den Umsetzungsmaßnahmen im neuen Datenschutzrecht. Damit können aus dem zur Erreichung der Datenschutz-Compliance bereits betriebenen Aufwand nachhaltig Synergien geschaffen werden.

Beweislastumkehr im Daten- und Geheimnisschutz

Die DS-GVO normiert die Rechenschaftspflicht der Unternehmen als datenverarbeitende Stellen. Der Verantwortliche muss nachweisen können, dass die Datenverarbeitung gesetzeskonform erfolgt. Es ist also eine teilweise Beweislastumkehr verankert.

Ganz ähnlich sieht es jetzt im Geheimnisschutz aus. Schon die Definition des Geschäftsgeheimnisses setzt voraus, dass der Geheimnisinhaber die für ihn wertvolle Information mit angemessenen Geheimhaltungsmaßnahmen schützt. Fehlt es an solchen Maßnahmen, ist auch keine Geheimnisqualität gegeben: das Gesetz mit seinem vielfältigen Handlungsinstrumentarium findet keine Anwendung. Im Streitfall trägt die Beweislast für den Umstand, dass eine Information dem Geheimnisschutz unterliegt, nicht derjenige, der sie vermeintlich rechtswidrig nutzt oder offenbart, sondern der Geheimnisinhaber muss seine angemessenen Schutzmaßnahmen nachweisen können, um den Anwendungsbereich des GeschGehG zu eröffnen.

Für den Datenschutz wie auch für den Geheimnisschutz gilt somit zwingend eine Pflicht zur fortlaufenden Dokumentation der getroffenen Schutzmaßnahmen zum Schutz der jeweiligen Informationen. Ein schriftliches Konzept über das jeweilige Datenmanagement und die Informationssicherheit ist dabei unerlässlich.

Technische und organisatorische Maßnahmen

Im Mittelpunkt der Dokumentationspflichten stehen die Maßnahmen der IT- bzw. Informationssicherheit – ob als technische und organisatorische Maßnahmen zum Datenschutz (TOM) oder als angemessene Maßnahmen zum Schutz von Geschäftsgeheimnissen. Der größte gemeinsame Nenner wird demnach in einer angemessenen Informationssicherheitsstruktur zu sehen sein, welche allen Anforderungen, allen Chancen und Risiken der Digitalisierung gerecht wird. Wurden im Zuge der DS-GVO-Umsetzung die IT-Sicherheitsinfrastruktur evaluiert und die technischen und organisatorischen Maßnahmen zum Datenschutz dokumentiert, empfiehlt es sich, diese Maßnahmen je nach Grad der Vertraulichkeit auch auf die die jeweilige Schutzklassifizierung von Geschäftsgeheimnissen anzuwenden.

Anknüpfungspunkte für das Geheimnisschutzkonzept können dabei IT-Sicherheitsrichtlinien und TOM-Dokumentationen, Verarbeitungsverzeichnisse, Datenpannen- und Notfallmanagementkonzepte, Arbeitsanweisungen und Richtlinien zum Datenschutz und zur IT-Sicherheit sein.

Was müssen Sie jetzt tun?

Gehen Sie den Geheimnisschutz aktiv an und:

- Definieren Sie Ihre Geschäftsgeheimnisse und evaluieren Sie, wo und wie diese verarbeitet werden.
- Nehmen Sie Ihr Konzept zur Umsetzung der DS-GVO in Revision und suchen Sie nach Synergiepotenzial für den Geheimnisschutz.
- Passen Sie Prozesse und Dokumente an, um den Geheimnisschutz in Ihre bestehende Infrastruktur zum Datenschutz und zur Informationssicherheit zu integrieren und dokumentieren Sie die Änderungen und Erweiterungen.
- Nutzen Sie unsere Kompetenzen, um belastbare Synergien im Daten- und Geheimnisschutz zu finden und effektiv zu nutzen.

KREMER RECHTSANWÄLTE sind überzeugt von den Vorteilen eines konsistenten Gesamtkonzepts für den Schutz von Geschäftsgeheimnissen und personenbezogenen Daten sowie für die Informationssicherheit.

Falls Sie Fragen haben, melden Sie sich gerne.

Ihre Ansprechpartner:

Per Kristian Stöcker, Rechtsanwalt, Data Protection Officer (ECPC, Maastricht University) Datenschutzbeauftragter (TÜV Nord), Mail: per.stoecker@kremer-recht.de

Nadine Schneider, Rechtsanwältin, Datenschutzbeauftragte (TÜV), Mail: nadine.schneider@kremer-recht.de

KREMER RECHTSANWÄLTE, Disch-Haus, Brückenstraße 21, 50667 Köln (Innenstadt), Tel.: +49(221)27141874, Mail: info@kremer-recht.de, www.kremer-rechtsanwaelte.de