Know-how Richtlinie

NEUE ANFORDERUNGEN AN DEN SCHUTZ VON GESCHÄFTSGEHEIMNISSEN

Warum?

Die neue EU-Richtlinie zum Schutz von Geschäftsgeheimnissen und Know-how zielt darauf ab, Unternehmen vor Geheimnisverrat und Wirtschaftsspionage zu schützen und grenzüberschreitende Innovationen im europäischen Binnenmarkt zu fördern. Gleichzeitig stellt die Richtlinie neue Anforderungen an den Schutz von Geschäftsgeheimnissen.

Es gilt: Die Richtlinie schützt nur den, der die Anforderungen erfüllt. Geschützt werden nur Informationen, die Gegenstand angemessener Geheimhaltungsmaßnahmen sind. Unternehmen müssen deshalb zukünftig beweisbare Geheimhaltungsmaßnahmen treffen, um Rechtsschutz zu erlangen.

Worum geht es?

Im April 2016 hat das europäische Parlament die Richtlinie 2016/943 über den Schutz von Geschäftsgeheimnissen verabschiedet. Sie ist von den nationalen Gesetzgebern bis zum 9. Juni 2018 umzusetzen. Zweck der Richtlinie ist ein wirkungsvoller und europaweit einheitlicher Schutz vor Geheimnisverrat und Wirtschaftsspionage.

Hintergrund der Richtlinie ist folgender:

Zentrale Bedeutung von Geschäftsgeheimnissen: Für Unternehmen ist der Schutz von Geschäftsgeheimnissen von zentraler Bedeutung. Dies betrifft zum einen technische Innovationen und Know-how als entscheidende Faktoren für die Wettbewerbsfähigkeit und den Markterfolg von Unternehmen. Zum anderen besteht großes Interesse daran, vertrauliche kaufmännische Information, wie Kunden- und Lieferantendaten, Businesspläne, Bilanzen und Marktstrategien von der Öffentlichkeit und der Konkurrenz abzuschirmen.

Verschärfte Bedrohungslage: Der zentralen Bedeutung der Geschäftsgeheimnisse steht eine verschärfte Bedrohungslage gegenüber: Faktoren wie Globalisierung, Digitalisierung, Outsourcing, komplexere Geschäftsmodelle und längere Lieferketten erhöhen das Risiko, dass Dritte unbefugt Zugriff auf Geschäftsgeheimnisse erlangen.

Bisherige Situation: Geschäftsgeheimnisse sind bislang europaweit nicht einheitlich geschützt. Die nationalen Regelungen in den EU-Mitgliedsstaaten weisen erhebliche Unterschiede auf. Die Regelungen sind über mehrere Gesetze verstreut. Nur in den Fällen, in denen Geschäftsgeheimisse als geistiges Eigentum geschützt sind, zB als Patente, Geschmacksmuster, Gebrauchsmuster oder urheberrechtliche Werke, besteht ein ausreichendes Maß an Rechtssicherheit. Mit der Richtlinie soll europaweit ein einheitlicher Rechtsschutz auf hohem Niveau gewährleistet werden.

Inhalt der Richtlinie

Der Begriff des Geschäftsgeheimnisses wird neu definiert. Geschäftsgeheimnisse sind alle Informationen,

- die nicht allgemein bekannt oder ohne Weiteres zugänglich, also geheim sind, und
- von kommerziellem Wert, weil sie geheim sind, und
- Gegenstand angemessener Geheimhaltungsmaßnahmen des Geheimnisträgers sind.

Zudem legt die Richtlinie fest, wann Erwerb, Nutzung und Offenlegung von Geschäftsgeheimnissen rechtmäßig und wann diese rechtswidrig sind. Wichtig für Unternehmen ist in diesem Zusammenhang, dass das Reverse Engineering, also die Untersuchung, Entschlüsselung oder der Rückbau eines öffentlich verfügbar gemachten oder rechtmäßig erworbenen Produkts, nun ausdrücklich als rechtmäßig erachtet wird. Weiterhin regelt die Richtlinie, welche Rechtsschutzmöglichkeiten für Inhaber von Geschäftsgeheimnissen bei rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung bestehen. Neben Unterlassung und Schadensersatz sollen weitere Maßnahmen wie Vernichtung, Rückruf, Beseitigung und Beschlagnahme gerichtlich durchgesetzt werden können.

Schließlich wird der Umgang mit Geschäftsgeheimnissen in gerichtlichen Verfahren geregelt. Um zu verhindern, dass Geschäftsgeheimnisse im gerichtlichen Verfahren an die Öffentlichkeit gelangen, soll der Kreis derjenigen beschränkt werden, die Zugang zu solchen Verfahrensdokumenten oder Anhörungen haben, die Geschäftsgeheimnisse beinhalten.

Strengere Anforderungen an Geheimhaltungsmaßnahmen

Nach dem neuen Recht liegt nur dann ein Geschäftsgeheimnis vor, wenn die betreffende Information Gegenstand angemessener Geheimhaltungsmaßnahmen des Geheimnisträgers ist. Dies hat zur Folge, dass Unternehmen in einem gerichtlichen Verfahren konkret vortragen und beweisen müssen, welche Geheimhaltungsmaßnahmen zum Schutz der jeweiligen Information getroffen wurden. In welchem Fall welche Geheimhaltungsmaßnahmen angemessen sind, ergibt sich indes weder aus der Richtlinie, noch aus ihrer Begründung. Die konkrete Umsetzung der Richtlinie unterliegt daher einiger Rechtsunsicherheit.

Es kann davon ausgegangen werden, dass der nationale Gesetzgeber sich bei der Konkretisierung an Maßnahmen orientiert, die bereits aus dem IT- und Datenschutzbereich bekannt sind. Bei der Beurteilung der Frage, ob sie auch angemessen sind, ist im konkreten Einzelfall unter anderem auf die Schutzbedürftigkeit der vertraulichen Information und die drohenden Risiken abzustellen.

Konkrete Maßnahmen

Folgende Maßnahmen werden von uns für unsere Unternehmen innerhalb der Unternehmensfamilie getroffen:

- **Umsetzung von "Wechselmedien (USB-Sticks)" lt Internet- und IT-Sicherheitsrichtlinie 2018**
  - Verschlüsselung mittels VeraCrypt (https://www.chip.de/news/Daten-auf-USB-Stick-verschluesseln-So-klappt-es-ganz-einfach-mit-VeraCrypt_145746855.html)
- **NDA's**
  - mit Mitarbeitern vorhanden bzw im Anlassfall laufend umgesetzt
  - mit Geschäftspartnern vorhanden bzw im Anlassfall laufend umgesetzt
- **Vertraulichkeits-Footer in Email-Kommunikation**
- **Festsetzen einer Unternehmenspolitik hinsichtlich des Umgangs mit Geschäftsgeheimnissen**
  - Dies wird alsbald in einer unserer internen Richtlinien festgehalten
- **Regelmäßige Gespräche (im Verlauf der Mitarbeitergespräche) zur Sensibilisierung für die Vertraulichkeit**

Konkrete Maßnahmen

- Protokollierung von Zugriffsberechtigungen
  - laufende und regelmäßige Überwachung
  - Protokollierung von Zugriffen: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
  - Regelung intern mittels unterschiedlichen Zugriffsrechten: unternehmensspezifische Zugriffsmatrix: daraus ergibt sich die strikte Trennung der Zugriffsberechtigungen auf den Server und darauf abgelegte Dokumente je Position/Aufgabenbereich der Mitarbeiter im Unternehmen
  - Der Zugriff auf alle Daten ist per Zertifikat verschlüsselt
  - Die Kommunikation zwischen den E-Mail-Servern ist bei unserem E-Mail-Gateway standardmäßig verschlüsselt
- Räumlichkeiten: Zugangskontrollen
  - Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, mittels Magnet- bzw Chipkarten und elektrischer Türöffner
  - Zutritt nur mittels persönlicher BOKUCard möglich
  - Verlust einer BOKUCard: beim Verlust der eignen Karte ist diese sofort direkt zu sperren!
- Mitarbeiter-Awareness schaffen
  - Diese Aussendung via Email inkl dieser Präsentation

Konkrete Maßnahmen

- **Server-Web-Einstieg mittels Passwort geschützt**
  - Datenschutzfreundliche Voreinstellungen: User bekommen anhand vorgegebener Active Directory Berechtigungsgruppen entsprechende Berechtigungen auf Dateien, Ordner, Programme und Zugriffe.
  - Schutz vor unbefugter Systembenutzung, mittels Kennwörter (einschließlich entsprechender Richtlinien), automatische Sperrmechanismen, Verschlüsselung von Datenträgern
- **Need-to-Know Personenkreis**
  - Identifizierung von
    - Geschäftsgeheimnissen (zu strukturieren nach ihrer Schutzbedürftigkeit, Risiken evaluieren und überlegen, mit welchen Maßnahmen den Risiken begegnet werden kann)
    - Know-How Trägern
  - → bestimmte Arbeitsschritte werden nur von bestimmen Personen durchgeführt
  - → Zugriff zu vertrauenswürdigen Programmsystemen nur von berechtigten Benutzern

Fazit

Die EU-Richtlinie zum Schutz von Geschäftsgeheimnissen und Know-how öffnet Raum für einen vereinfachten und verbesserten Schutz von Geschäftsgeheimnissen. Der damit einhergehenden Pflicht zum Einsatz angemessener Geheimhaltungsmaßnahmen können Unternehmen mit vertraglichen sowie technischen und organisatorischen Maßnahmen begegnen. Hierbei ist darauf zu achten, dass die Maßnahmen ausreichend dokumentiert werden, um Beweisschwierigkeiten zu vermeiden.

→ dies haben wir intern anhand der vorhin aufgezeigten konkreten Maßnahmen unseres Erachtens ausreichend und umfangreich umgesetzt