

## Schutz von betrieblichem Know-how

### Die Umsetzung der EU-Richtlinie über den Schutz vertraulichen Know-hows aus arbeitsrechtlicher Sicht

Nach der DSGVO im vergangenen Jahr wurde vom Gesetzgeber 2019 die EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung durch eine UWG-Novelle umgesetzt.

Es kann eine Überlebensfrage für das Unternehmen sein, das betriebliche Know-how zu schützen. Nach den neuen Bestimmungen betrifft betriebliches Know-how Informationen, die geheim, von wirtschaftlichem/kommerziellem Wert sowie Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen sind. Diese Maßnahmen beziehen sich auf jene Person, welche die rechtmäßige Verfügungsgewalt über diese Informationen ausübt.

**Welche Informationen betroffen sind, kann man durch einfache Fragen erkennen:**

- Welche Informationen wären für meine Konkurrenten besonders wertvoll?
- Welche Informationen sollten nicht offengelegt werden, weil diese meinem Unternehmen besonders schaden würden?

Vom Schutz erfasst sind vor allem Know-how, Geschäftsinformationen sowie technologische und kaufmännische Informationen, bei denen sowohl ein legitimes Interesse an ihrer Geheimhaltung besteht als auch die legitime Erwartung, dass diese Vertraulichkeit gewahrt wird. Beispiele sind etwa Kundenlisten, Musterkollektionen, Lieferangebote, Einkaufskonditionen, nicht allgemein bekannte Rezepturen etc. Ausgenommen sind: belanglose Informationen und allgemeine Erfahrungen, Wissen, Fähigkeiten und Qualifikationen, die Beschäftigte im Zuge der Ausübung ihrer üblichen Tätigkeiten erwerben, sowie Informationen, die den Personenkreisen, die üblicherweise mit derartigen Informationen umgehen, generell bekannt sind bzw. für sie leicht zugänglich sind.

#### Angemessene Geheimhaltungsmaßnahmen

Neu ist, dass vertrauliche Information erst durch angemessene Geheimhaltungsmaßnahmen zum Geheimnis werden. Das lässt sich durchaus mit der im Datenschutzrecht verankerten Bestimmung vergleichen, wonach angemessene geeignete technische und organisatorische Maßnahmen (TOMs) zur Gewährleistung der Datensicherheit getroffen werden müssen. Im Datenschutzrecht geht es freilich um den Schutz der Betroffenen und es wird aus der Sicht des Betroffenen agiert. So macht sich ein Unternehmer unter Umständen strafbar, wenn die implementierten Datensicherheitsmaßnahmen nicht angemessen und geeignet sind. Im Bereich der Know-how-Richtlinie geht es um den Schutz des Unternehmens. Unangemessene (oder keine) Geheimhaltungsmaßnahmen zu treffen, ist mit keiner Strafe bedroht, führt aber zum Verlust des Schutzes. Datensicherheit und Schutz von Betriebs- und Geschäftsgeheimnissen sind aber jedenfalls zwei Themen, die sich weitläufig überschneiden, vor allem, wenn Geschäftsgeheimnisse personenbezogene Daten beinhalten. Ein sauber umgesetztes Datensicherheitskonzept dient daher ebenso dem Schutz der Geschäftsgeheimnisse.

#### Was ist zu tun?

Definitionsgemäß sind Geschäftsgeheimnisse solche, die nicht ohne weiteres für jedermann zugänglich sind. Inwieweit aktive Vorkehrungen erforderlich sind oder ob sich die Geheimhaltungsmaßnahmen passiv aus den jeweiligen Umständen ergeben, ist im Einzelfall zu entscheiden. Die Angemessenheit wird von der Art des Geschäftsgeheimnisses und der Branche und Größe des Unternehmens abhängig sein. Beispiele für Maßnahmen sind:

- Weitergabe der Geschäftsgeheimnisse nur an ausgewählte vertrauenswürdige Personen;
- Richtlinien betreffende Geschäftsgeheimnisse und ihre nachvollziehbare Dokumentation;
- IT-Sicherheitsmaßnahmen;
- Mitarbeitergespräche;
- Durchführung bestimmter Arbeitsschritte nur von bestimmten Personen;

Auf Geschäftsgeheimnisse sollten nur diejenigen Mitarbeiter zugreifen können, die zur Erbringung ihrer Arbeitsleistung auch darauf zugreifen müssen. Mitarbeiter, die keine Kenntnis von Geheimnissen zu Ihrer Arbeit benötigen, sollten keine Zugriffsberechtigung erhalten. Das kann durch Vergabe

persönlicher Benutzer-Accounts geschehen.

Auch die Einrichtung einer Zugangskontrolle zu versperrbaren Türen usw. sollte derart geregelt werden, dass nur jene Mitarbeiter einen Schlüssel erhalten, denen auch tatsächlich Zugang gewährt werden soll.

**Expertentipp von Mag. Florian Brutter,  
Abteilung Arbeits- und Sozialrecht in der Tiroler Wirtschaftskammer**

Es empfiehlt sich, mit den Mitarbeitern eine Verschwiegenheitsvereinbarung abzuschließen, worin sich diese zur Geheimhaltung – auch nach ihrem Ausscheiden aus dem Unternehmen – verpflichten. Dies kann durch eine Konventionalstrafe abgesichert werden. Sie finden eine Mustervereinbarung auf unserer Website [www.WKO.at/tirol/arbeitsrecht](http://www.WKO.at/tirol/arbeitsrecht).

Eine regelmäßige Sensibilisierung der Mitarbeiter und das Aufstellen von Verhaltensregeln sind zweckmäßig. Sensible Dokumente sollten im Shredder und nicht im Ganzen im Papierkorb landen, eventuell sollten keine Fotos aus dem Unternehmen gemacht und veröffentlicht werden.

Stand: 28.03.2022