Mai 2019

Die Auswirkungen der Know-How-Richtlinie auf die Softwarebranche

Ihr Nutzen: Sie wissen, wie Sie Ihre Geschäftsgeheimnisse schützen
Ihre Investition: 5 bis 10 Minuten Lesezeit

Am 1.2.2019 ist die europäische Know-How-Richtlinie[1] im Gesetz gegen den unlauteren Wettbewerb („UWG") umgesetzt worden. Unternehmen, die dieses Gesetz übersehen, laufen Gefahr, den Schutz ihrer Geschäftsgeheimnisse zu verlieren. Was das konkret für die Softwarebranche bedeutet, soll in diesem Newsletter thematisiert werden.

1. Was ist ein Geschäftsgeheimnis?

Nach § 26b Abs 1 UWG ist ein Geschäftsgeheimnis definiert als eine Information, die *„Gegenstand von **den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen**…ist"*. Das bedeutet im Umkehrschluss: **Was nicht angemessen geschützt ist, ist kein Geschäftsgeheimnis im Sinne des UWG!** Daher stellt sich die Frage, wie können Informationen *„angemessen"* geschützt werden?[2] Generell können die Schutzmaßnahmen wie folgt gegliedert werden[3]:

- **Vertragliche Maßnahmen**
  - Geheimhaltungsverpflichtungen
  - Verträge mit externen Dienstleistern und Freelancern
- **Organisatorische Maßnahmen**
  - Festlegung von Verantwortlichkeiten
  - Kategorisierung und Kennzeichnung von Geheimissen und Zuordnung von Schutzmaßnahmen
  - Berechtigungskonzept
  - Awarenessschulung
- **Technische Maßnahmen**
  - Zutritts- und Zugriffssteuerungen
  - Umsetzung von Berechtigungskonzepten
  - Firewalls, Trennung von Server-Strukturen

[1] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen.
[2] Vgl *Tretzmüller*, Die Know-How-Richtlinie – und wie der Schutz von Geschäftsgeheimnissen verloren gehen kann, ZIIR 2018, 315 ff.
[3] Vgl *Schirmbacher*, ITRB 5/2019, S 117.

- Verschlüsselung der Kommunikation

2. Zu den Auswirkungen für die Softwarebranche

Die Softwarebranche lebt von ihren Geschäftsgeheimnissen, nämlich ihrem Branchen-Know-How, **Quellcodes**, Algorithmen und Arbeitsprozessen. Gliedert man ein Softwareprojekt in Phasen, können in der jeweiligen Phase folgende Maßnahmen zum Schutz des Know-Hows ergriffen werden:

2.a. Konzeptionsphase

In der Konzeptionsphase werden zwischen dem Auftraggeber und dem Auftraggnehmer (dem Softwareunternehmen) Ideen, Muster, Designs und Konzepte (zusammen „Informationen") ausgetauscht. Daher ist es wichtig, wechselseitig **Geheimhaltungsverpflichtungen** („Non Disclosure Agreements", „NDA") abzuschließen. Zudem sollten geeignete Vereinbarungen mit Beschäftigten, freien Mitarbeitern und Subunternehmern getroffen werden, um die Schutzpflicht an diese weiterzugeben.[4] Wird ein gemeinsamer Share-Point eingerichtet, muss ein **Berechtigungskonzept** erstellt und anschließend technisch umgesetzt werden. Hier ist das „**Need-to-know-Prinzip**" zu beachten. Es dürfen bloß jene Personen auf die Informationen zugreifen bzw diese sehen, die dazu ein legitimes Interesse haben. Die Einhaltung des Berechtigungskonzepts wird durch ein entsprechendes **Passwortmanagement** flankiert. Weiters sollte geklärt werden, dass Pläne eventuell **urheberrechtlich geschützt sind**. Sollten sich beide Vertragsparteien diesbezüglich kreativ verwirklichen, kann auch eine **Miturheberschaft**[5] entstehen. Diesfalls sollte geregelt werden, (i) welche Verwertungsrechte, (ii) welcher Partei (iii) in welchem Ausmaß zustehen. Ein wichtiger Faktor ist zudem, dass sämtliche involvierten Personen eine **Awarenessschulung** erhalten.

2.b. Implementierungsphase

In der Implementierungsphase muss der Fokus darauf gerichtet werden, den Quellcode zu schützen. Gerade bei einer Individualsoftware wird dessen Austausch mit dem Auftraggeber oft unvermeidbar sein. Umso mehr ist darauf zu achten, dass **Geheimhaltungsverpflichtungen** abgeschlossen und **Berechtigungskonzepte** umgesetzt werden. Zudem ist es regelmäßig sinnvoll, ein **Escrow-Agreement** abzuschließen. Der Zweck eines Escrow-Agreements ist, den Quellcode bei einer neutralen Person (oft ein Notar oder ein Rechtsanwalt) zu hinterlegen. Die Person darf den Quellcode

[4] Vgl *Schirmbacher*, ITRB 5/2019, S 118.
[5] § 11 UrhG.

nur in speziell vertraglich definierten Fällen an den Auftraggeber aushändigen (z.B.: Insolvenz des Auftragnehmers). **Veränderungen des Quellcode** sollten **mitprotokolliert** und dokumentiert werden. **Container-Verfahren und das Arbeiten in Testumgebungen** können ebenfalls zur Informationssicherheit[6] beitragen. Sollten Freelancer eingesetzt werden, sollte ein **Audit-Recht vor Ort** vereinbart werden. Schließlich können Softwareunternehmen **spezielle technische Schutzmaßnahmen[7]** (z.B.: Kopierschutz, Freischaltung über einen Registrierungscode, Passwortabfragen, Verschlüsselungen, Einsatz von Dongles, Implementierung von Identifizierungsmerkmalen [z.B.: Wasserzeichen]) zum Schutz ihres Know-Hows einsetzen.

2.c. Abschlussphase

Gerade in der Softwarebranche besteht die Gefahr, dass in der Implementierungsphase involvierte Mitarbeiter des Softwareunternehmens vom Auftraggeber abgeworben werden. Daher ist empfehlenswert, frühzeitig ein – zeitlich befristetes – **Abwerbungsverbot** zu vereinbaren. Zudem sollte bei der Konzipierung der Geheimhaltungsverpflichtungen darauf geachtet werden, dass diese NDA auch über das Vertragsverhältnis hinaus respektiert werden muss („***survival clause***"). Nicht mehr erforderliche Informationen sollten **gelöscht** werden.

3. Zusammenfassung und Handlungsempfehlung

Voraussetzung für den Schutz eines Quellcodes[8] als Geschäftsgeheimnis im Sinne des UWG ist das Bestehen und die Umsetzung angemessener Schutzmaßnahmen. **Gerade in der Softwarebranche besteht daher ein unmittelbarer Handlungsbedarf**.[9] Bei der Umsetzung von Softwareprojekten müssen vor allem Geheimhaltungsverpflichtungen abgeschlossen werden und das Berechtigungskonzept im Sinne des „Need-to-know-Prinzips" umgesetzt werden. **Sollten die in diesem Artikel genannten *„Geheimhaltungsmaßnahmen"* sorgfältig umgesetzt werden, wird das Wissen des Softwareunternehmens als Geschäftsgeheimnis im Sinne des UWG geschützt sein und auch bleiben**.

---

[6] Vgl Control A.14.2.7. ISO 27001.
[7] Vgl § 90b UrhG.
[8] Unabhängig davon, kann ein Quellcode nach dem Urheberrechtsgesetz geschützt sein; vgl *Tretzmüller*, Rechtsleitfaden für Software-Programmierer: https://www.kt.at/wp-content/uploads/2019/01/Ein-Rechtsleitfaden-für-Softwareprogrammierer_03012019.pdf
[9] Vgl *Schirmbacher*, ITRB 5/2019, S 118.

Mai 2019

Zur Kanzlei

Wir sind seit 1.1.2017 Ihre Experten für die Themen, die Unternehmen im 21. Jahrhundert bewegen: Datenschutzrecht, IT-Softwarevertragsrecht, Urheberrecht, Arbeitsverfassungsrecht und Vertragsrecht

Zum Autor:

Dr. Tobias Tretzmüller, LL.M. ist Rechtsanwalt in ständiger Kooperation mit der Knyrim Trieb Rechtsanwälte OG, Wien. E-Mail: tt@kt.at. Er berät und vertritt Unternehmen in den Bereichen des IT-Softwarevertragsrechts, Datenschutzrechts, Urheberrechts, und streitigen Behörden- und Zivilverfahren. Regelmäßige Vortrags- und Veröffentlichungstätigkeit (ua imh trainer of the year 2017 und 2018; Jahrbuch Datenschutzrecht 2017, ZIIR, Dako). Er ist zertifizierter Datenschutzbeauftragter und TÜV geprüfter ISO 27001-Auditor.