LLR.
Rechtsanwälte
Köln | Brüssel | Helsinki

Informationssicherheit in Zeiten von Corona

Geschäftsgeheimnisschutz und der Einsatz von Video-Chat-Diensten

27. April 2020

Per Kristian Stöcker
Rechtsanwalt
ext. Datenschutzbeauftragter
(TÜV cert.)
per.stoecker@llr.de

Prof. Klaus Gennen
Rechtsanwalt
FA für IT-Recht & Arbeitsrecht
betriebl. Datenschutzbeauftragter
(GDD cert.)
klaus.gennen@llr.de

Zoom und Co. - Immer beliebter

Videokonferenzen erfreuen sich in Zeiten der Pandemie nie dagewesener Beliebtheit. Die Anwendung *Zoom* hat gerade die Marke von 300 Millionen Nutzern erreicht. Mit der gesteigerten Nutzung von Video-Chat-Diensten wie *Zoom*, *Microsoft Teams*, *GoToMeeting, Google Meet, Slack* etc. mehren sich auch die Bedenken zu möglichen Sicherheitsrisiken. Vor allem *Zoom* steht im Zentrum dieser Kritik - Google hat seinen Mitarbeitern bereits verboten, Zoom für Videokonferenzen zu nutzen. Problematisch sind u.a. Lücken in der Verschlüsselung, aber auch der intransparente Datenaustausch mit Dritten wie Facebook.

Schutz von Geschäftsgeheimnissen nach dem GeschGehG

Seit April 2019 gilt in Deutschland das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). Damit hat Deutschland reichlich verspätet die Europäische Richtlinie 2016/943 vom 8. Juni 2016 („Know-How-Richtlinie“) in nationales Recht umgesetzt. Die deutlichste Änderung ist sicher die neue Definition des *Geschäftsgeheimnisses*, der nicht zuletzt die §§ 17-19 des Gesetzes gegen den unlauteren Wettbewerb (UWG) zum Opfer gefallen sind. Demnach zählt nicht mehr der Geheimhaltungswille des rechtmäßigen Inhabers, um eine Information als vertraulich und damit als geschützt zu klassifizieren. Damit eine Information die Qualität eines Geschäftsgeheimnis aufweist – und damit vor ungewollter Nutzung durch ehemalige Beschäftigte oder Wettbewerber geschützt ist – kommt es nunmehr gerade darauf an, dass der rechtmäßige Inhaber der Information angemessene Schutzmaßnahmen nach § 2 Nr. 1 lit. b GeschGehG umgesetzt hat. Solche Maßnahmen sind technisch-organisatorischer oder vertraglicher Natur. Reichen diese objektiv nicht aus, um eine bestimmte Information vor ungewollter Offenlegung oder Nutzung angemessen zu schützen, liegt schon begrifflich kein Geschäftsgeheimnis nach § 2 GeschGehG vor. Zudem trägt der Inhaber der Information die Beweislast dafür, dass angemessene Schutzmaßnahmen implementiert sind. Ohne ein angemessenes Schutzkonzept ist der Inhaber der Information daher im Zweifelsfall völlig schutzlos.

Haben Sie Fragen?
Gerne stehen unsere Experten für IT-Recht und Datenschutz zu Ihrer Verfügung:

Telefon: +49 221 55400-170
Telefax: +49 221 55400-192

LLR Legerlotz Laschet und Partner Rechtsanwälte Partnerschaft mbB
Mevissenstraße 15
50668 Köln
Deutschland
Telefon: +49 221 55400-0
Telefax: +49 221 55400-190
www.llr.de

Sitz: Köln
Registrierung:
AG Essen PR 3609

Anpassung des Geheimnisschutzkonzepts in Krisenzeiten

Hat ein Unternehmen ein entsprechendes Geheimnisschutzkonzept bereits umgesetzt, sollte nun dringend geprüft werden, ob und inwieweit dieses durch etwaige Maßnahmen des Infektionsschutzes – wie insbesondere die Versendung der Beschäftigten ins Homeoffice – angepasst werden muss.

Das betrifft gerade auch den Einsatz von Video-Chat-Diensten:

- Videokonferenzen sollen nicht für die Besprechung besonders sensibler Themen genutzt werden, soweit nicht sicherstellt ist, dass die Übertragung effektiv verschlüsselt ist. Gegebenenfalls sollten bestimmte Abteilungen von der Nutzung von Videokonferenzen ausgenommen werden, so vor allem sensible Bereiche wie vor allem Forschung- und Entwicklung.
- Vorsicht beim Teilen von Dokumenten mit schutzwürdigem Inhalt: Diese sollten im Zweifelsfall verschlüsselt und passwortgeschützt per E-Mail übermittelt werden.
- Kameraeinstellungen verfügen teilweise über eine Weichzeichnerfunktion für den Hintergrund. Diese sollte immer aktiviert werden, um z.B. Flipcharts oder dergleichen nicht ungewollt wiederzugeben.
- Vorsicht bei Gratis-Lizenzen: Hier liegen regelmäßig „Service-gegen-Daten"-Modelle zugrunde.
- Nutzungsbedingungen / AGB, aber auch die Datenschutzerklärungen vor Einführung immer von der Rechtsabteilung geprüft und im Rahmen einer risikoorientierten Dienstleisterauswahl bewertet werden.

Ferner gilt es aber auch sonstige Risiken zu bedenken:

- Homeoffice-Maßnahmen im Allgemeinen (*siehe auch unser Beitrag vom 24.3.2020*) – Gefahren drohen z.B. durch fehlende Zugangssicherungen, die Vermengung von betrieblicher und privater Geräte-Infrastruktur (BYOD u.a.), aber auch in der unsicheren Aktenvernichtung
- Die Nutzung von Sprachassistenten wie Cortana, Alexa, Siri und Co. – diese werden im privaten Alltag immer beliebter, sollten aber gerade im Homeoffice deaktiviert werden angesichts zahlreicher Sicherheitslücken, durch die fremde Nutzer einzelne Dateien, aber auch ganze Rechner übernehmen können (*siehe z.B. https://www.security-insider.de/neue-sicherheitsrisiken-durch-sprachassistenten-a-909854/).*

Fazit

Die Gefahren für den ungewollten Verlust oder Abfluss von sensiblen Geschäftsgeheimnissen sind durch die Beweislastumkehr im GeschGehG seit April 2019 ohnehin gewachsen. Im Zuge der krisenbedingt exponentiell beschleunigten Digitalisierung des Arbeitslebens sind sie größer denn je.

Die Basis für den effektiven Geschäftsgeheimnisschutz ist ein dauerhaft überwachtes und im Bedarfsfall rechtssicher angepasstes Geheimnisschutzkonzept.

Haben Sie Fragen?

Gerne stehen unsere Experten für IT-Recht und Datenschutz zu Ihrer Verfügung:

LLR.

Per Kristian Stöcker
per.stoecker@llr.de

Prof. Klaus Gennen
klaus.gennen@llr.de

T: +49 221 55 400 170
F: +49 221 55 400 192
www.llr.de