reuschlaw
Legal Consultants

Mit Sicherheit gut beraten

Die reuschlaw Checkliste für Cybersecurity und Datenschutz im Homeoffice

Unser Maßnahmenplan für Ihre Compliance

Stand: November 2020

Homeoffice – das Gebot der Stunde

Nach einer kurzen Verschnaufpause im Sommer holt die Corona-Pandemie Deutschland derzeit mit voller Wucht ein. Die Fallzahlen steigen, neue Einschränkungen folgen. Ob der jüngst verhängte Teil-Lockdown ausreicht oder die Maßnahmen verschärft und weitere Teile der Wirtschaft heruntergefahren werden müssen, weiß niemand. Gleichzeitig sind Unternehmen dazu angehalten, wo immer es möglich ist, eine Arbeit im Homeoffice zu ermöglichen. Aus der aktuellen Situation ergeben sich einerseits zahlreiche datenschutzrechtliche Fragestellungen, andererseits aber auch neue Bedrohungen für die Cybersecurity von Unternehmen. Die reuschlaw Checkliste für mehr Cybersecurity und Datenschutz im Homeoffice setzt genau an dieser Stelle an und erlaubt Ihnen einen schnellen Überblick über die jetzt notwendigen Maßnahmen. Bei Umsetzung der Maßnahmen unterstützen wir Sie gerne.

Cybersecurity & Datenschutz im Homeoffice

Mitarbeiter ins Homeoffice zu schicken erfordert nicht nur Vertrauen in die Kompetenzen der Mitarbeiter, sondern auch die Berücksichtigung zahlreicher datenschutzrechtlicher Aspekte. Zu denken ist hier etwa an eine Vereinbarung zu Kontrollrechten des Arbeitgebers und der Aufsichtsbehörden oder die Entsorgung von Unterlagen. Wegen der Ausnutzung der Pandemie-Situation durch Cyberkriminelle, die sowohl aktuelle Analysen der Sicherheitsbehörden, aber auch unsere Beratungspraxis bestätigen, werden aber auch Cybersecurity-Maßnahmen immer wichtiger. Um dem pandemiebedingten Zeitdruck Rechnung zu tragen, haben wir in unsere Checkliste in Maßnahmen, die getroffen werden sollten, bevor Homeoffice angeordnet wird und solche, die nachgezogen werden können, unterteilt.

Checkliste: Datenschutzanforderungen an das Homeoffice

Notwendige Maßnahmen, bevor Homeoffice angeordnet wird	- Gewährleistung eines Basisschutzes, insb.
	  - Zutritts- und Zugriffschutz
	  - Grundschutz der eingesetzten Systeme, auch bei Privatgeräten
	  - Sicherer Remote-Zugriff, notfalls über eine Cloud-Lösung
	  - Datensicherung
	  - Festlegung von Kommunikationsprotokollen
	  - Dokumentation der Maßnahmen im Rahmen einer IT-Sicherheitsrichtlinie

	- Sensibilisierung bzw. Dienstanweisung zur IT-Sicherheit im Homeoffice an die Mitarbeiter - Homeoffice-Vereinbarung mit den Mitarbeitern

Maßnahmen, die tendenziell fortlaufend ergänzt werden können	- Verbesserung des Basisschutzes, insb.
	  - Zurverfügungstellung von abschließbaren Behältnissen statt Anweisung zur sicheren Aufbewahrung
	  - bei Privatnutzung: Zurverfügungstellung von Dienstgeräten
	  - Remote-Zugriff über VPN
	  - Etablierung einer Datenträgerverschlüsselung
	  - Support für Telearbeitsplätze
	- Schaffung von Möglichkeiten zur Entsorgung von vertraulichen Informationen (vorher Anweisung, diese sicher aufzubewahren)
	- Verbesserung der Dokumentation und Etablierung eines auf die Corona-Krise angepassten IT-Sicherheitsmanagements
	- Fortlaufende Sensibilisierung der Mitarbeiter bzgl. aktueller Bedrohungen

Videokonferenzdienste & Co

Die Notwendigkeit von Homeoffice ist eng verknüpft mit dem Einsatz von Videokonferenzdiensten und anderen Kollaborationslösungen. Sie dienen sowohl dem Austausch der Mitarbeiter untereinander als auch der Kommunikation mit Externen. Herausforderungen in diesem Bereich sind vor allem die Auswahl einer datenschutzkonformen Lösung sowie eine entsprechende Konfiguration. Nicht übersehen werden sollte auch die Notwendigkeit einer Schulung der Mitarbeiter im Umgang mit der neuen Software und passende Dienstanweisungen. Weil auch hier die Zeit drängen kann, haben wir auch diese Checkliste in notwendige Maßnahmen und Nachfolgemaßnahmen unterteilt.

Checkliste zur Prüfung neuer Software

Notwendige Maßnahmen vor dem Einsatz der Software	- Basisprüfung im Hinblick auf eindeutige Verstöße gegen die DSGVO, insb. - Grundsätzliche Wahrung von Betroffenenrechten

	- Keine gravierenden Mängel bzgl. der IT-Sicherheit sowie data protection by design und by default - Bei Drittlandsbezug: Prüfung des angemessenen Datenschutzniveaus - Notwendigkeit einer Datenschutz-Folgeabschätzung - Klärung der Rolle des Softwareanbieters: Verantwortlicher oder Auftragsverarbeiter (ggf. Abschluss eines entsprechenden Vertrages) - Rudimentäre Eintragung in das Verarbeitungsverzeichnis - Wahrung der Informationspflichten nach Art. 13 DSGVO
Maßnahmen, die tendenziell fortlaufend ergänzt werden können	- Verbesserung der Basisprüfung, insb. - Umfassende Prüfung zur Wahrung von Betroffenenrechten - Umfassende Prüfung der IT-Sicherheit sowie data protection by design und by default, hierzu auch intensive Evaluierung von Einstellungsmöglichkeiten und Zusatzdiensten - Umfassende Prüfung des Datenschutzniveaus - Durchführung einer Datenschutz-Folgeabschätzung, sofern notwendig - Sofern abzuschließen: genaue Prüfung des Vertrages zur Auftragsverarbeitung sowie der Anlagen - Ergänzung des Verarbeitungsverzeichnisses

Voller Einsatz für den Mandanten – Unser Cybersecurity & Datenschutz Team

Das reuschlaw Cybersecurity & Datenschutz Team wird von Dr. Carlo Piltz geleitet und besteht aus drei Rechtsanwälten, zwei Wirtschaftsjuristen und einer wissenschaftlichen Mitarbeiterin. Wir haben ein großes Erfahrungsrepertoire an datenschutzrechtlicher Beratung und Implementierungsprojekten in öffentlichen Stellen, Unternehmen sowie Konzernverbünden diverser Größenordnungen. reuschlaw Legal Consultants wurde im „Kanzleimonitor 2020/2021“ in der Top 10 der „Führenden Kanzleien Datenschutz“ und Dr. Carlo Piltz in der Top 10 der „Führenden Anwälte Datenschutz“ empfohlen.

Dr. Carlo Piltz

Rechtsanwalt |Salary Partner, Teamleader Cybersecurity & Datenschutz

Sandra Häntschel

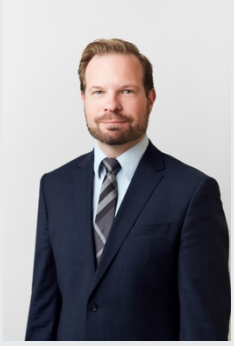
Wissenschaftliche Mitarbeiterin

Stefan Hessel

Rechtsanwalt | Associate

Philipp Quiel

Wirtschaftsjurist | Senior Associate



Moritz zur Weihen

Wirtschaftsjurist | Associate

Johannes Zwerschke

Rechtsanwalt | Associate

Zudem erhielten wir 2019 und 2020 durch die WirtschaftsWoche die Auszeichnungen als „TOP Kanzlei 2019“ und „TOP Kanzlei 2020“ im Bereich Datenschutzrecht. Im gleichen Bereich wurde Dr. Carlo Piltz 2019 und 2020 als „TOP Anwalt“ ausgezeichnet. reuschlaw Legal Consultants wird darüber hinaus seit 2009 jedes Jahr von Best Lawyers® ausgezeichnet und erhielt 2020 erstmalig die Auszeichnung "Best Lawyers® Data Security and Privacy Law" in Deutschland. Im Handelsblatt-Ranking „Deutschlands Beste Anwälte“ wird die Kanzlei seit 2016 jedes Jahr im Bereich Produkthaftung ausgezeichnet. 2020 erfolgte zusätzlich die Auszeichnung "Deutschlands beste Anwälte" im Bereich Datenschutzrecht.

Über reuschlaw Legal Consultants
reuschlaw Legal Consultants gehört zu den führenden wirtschaftsberatenden Kanzleien im Produkthaftungsrecht und berät seit 2004 national und international tätige Unternehmen mit Schwerpunkt Produktsicherheitsrecht, Produkthaftungsrecht, Datenschutz & Cybersecurity, Rückrufmanagement, Versicherungsrecht, Compliance Management und Vertragsrecht.

Unternehmenskontakt
Dr. Carlo Piltz
Teamleader Cybersecurity & Datenschutz

T > +49 30 / 2332895 0
E > carlo.piltz@reuschlaw.de

Büro Berlin
Joachimsthaler Str. 34
10719 Berlin

T > + 49 30 / 2332 895 0
F > + 49 30 / 2332 895 11
E > info@reuschlaw.de

Büro Saarbrücken
Stengelstr. 1
66117 Saarbrücken

T > + 49 681 / 859 160 0
F > + 49 681 / 859 160 11
E > info@reuschlaw.de