reuschlaw Whitepaper: Datenschutz im Homeoffice und beim Einsatz neuer Software – mit Checklisten zur Umsetzung

Ein Whitepaper von Dr. Carlo Piltz und Stefan Hessel

reuschlaw
Legal Consultants

Inhalt

Ausgangssituation

Wegen der seit einigen Wochen andauernden Corona-Krise geben viele Unternehmen ihren Mitarbeitern die Möglichkeit, aus dem Homeoffice zu arbeiten. Gleichzeitig greifen Unternehmen verstärkt auch auf Videokonferenzlösungen und Kollaborationsplattformen zurück. Hieraus ergeben sich zahlreiche datenschutzrechtliche Fragestellungen, bei deren Lösung dieses Whitepaper helfen soll.

Datenschutzanforderungen an das Homeoffice

Wesentlicher Anknüpfungspunkt für den Datenschutz im Homeoffice ist Art. 32 Abs. 1 DSGVO. Dieser verlangt vom Verantwortlichen und auch von Auftragsverarbeitern, angemessene IT-Sicherheitsmaßnahmen nach dem Stand der Technik umzusetzen. Die Anforderungen dafür waren, wie z. B. das Faltblatt „Telearbeit und Mobiles Arbeiten“ des BfDI von Januar 2019 zeigt, sehr hoch. Aufgrund der aktuellen Situation sind sie jedoch von Aufsichtsbehörden, dies belegen exemplarisch die „Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie“ des BayLfD, abgesenkt worden. Doch auch die aktuell geltenden Anforderungen erfordern strenge Maßnahmen zur IT-Sicherheit. Zur Umsetzung empfiehlt sich für deutsche Unternehmen sicherlich ein Rückgriff auf die aktuellen Empfehlungen des BSI, welche mit den Stellungnahmen der Datenschutzaufsicht ergänzt werden sollten. Besonders wichtig ist die Erstellung einer IT-Sicherheitsrichtlinie für das Homeoffice und die Sensibilisierung der Mitarbeiter. Sind Unternehmen derzeit nicht der Lage, alle Anforderungen direkt zu erfüllen, sollten zwingend erforderliche Basismaßnahmen festgelegt und dokumentiert werden. Diese können dann fortlaufend im Rahmen eines angepassten IT-Sicherheitsmanagements, welches auch die derzeitigen Risiken gesondert adressiert, ergänzt werden.

Datenschutzanforderungen an den Einsatz neuer Software

Für den Einsatz neuer Software gelten in der derzeitigen Situation keine veränderten Anforderungen. Bei der notwendigen Prüfung der Software kann jedoch ein abgestufter Prozess gewählt werden. Nach der Prüfung, welche Software geeignet ist, die benötigten Anforderungen zu erfüllen, sollte im Rahmen einer Basisprüfung festgestellt werden, ob ernste Gründe gegen den datenschutzkonformen Einsatz der Software sprechen. Dieser Prozess sollte dokumentiert werden im Sinne einer ersten Auswahlschwelle. Produkte, die diese Hürde nicht nehmen, sollten auch nicht zum Einsatz kommen. Hält die Software dieser Prüfung stand, ist zwingend zu klären, ob der Softwareanbieter selbst Verantwortlicher ist oder ein Fall der Auftragsverarbeitung vorliegt. In letzterem Fall muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden. Außerdem müssen die Informationspflichten gewahrt werden und zumindest ein rudimentärer Eintrag in das Verarbeitungsverzeichnis erfolgen. Die detaillierte Prüfung der Software kann in einem zweiten Schritt parallel zum Einsatz erfolgen.

Fazit

Das Datenschutzrecht gilt auch in der Corona-Krise. Unternehmen sollten daher nicht nur bei Homeoffice und beim Einsatz neuer Software, sondern auch insgesamt weiterhin das Datenschutzrecht beachten. Wenn wir Sie

bei der Umsetzung unterstützen können, melden Sie sich gerne. Weitere Informationen finden Sie auch unter https://www.reuschlaw.de/news/dossier/covid-19/.

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

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

Checkliste: Datenschutzanforderungen an den Einsatz 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

Unternehmenskontakt: Dr. Carlo Piltz I Teamleader Cybersecurity & DatenschutzI T > +49 30 / 2332895 0 I E carlo.piltz@reuschlaw.de