Datenschutz in Zeiten von Corona

Aufgrund der Verbreitung des Corona-Virus (SARS-Cov-2) und der Sorge vor einer weiteren Ausbreitung beschäftigen viele Unternehmen aktuell ihre Mitarbeiterinnen und Mitarbeiter als **Notfallmaßnahme** im **Home Office**.

Die Tätigkeit im Home Office weist im Wesentlichen dieselben Herausforderungen auf wie die Arbeit im Unternehmen. Der **Arbeitgeber** bleibt auch im Home Office für die Verarbeitung personenbezogener Daten und deren Sicherheit **verantwortlich**, d.h. er muss die Umsetzung der erforderlichen Sicherheitsmaßnahmen auch dort sicherstellen. Die im Regelfall notwendigen Maßnahmen sind in Notfällen, wie der aktuellen Pandemie, häufig nicht umfänglich zu erfüllen. Ein **Mindestmaß an Datenschutz und Datensicherheit** sollte dennoch gewährleistet werden. Um Sie diesbezüglich zu unterstützen, haben wir hier eine pragmatische Handlungshilfe erstellt.

Technisch-organisatorische Maßnahmen

Zur Zeit bietet das Home Office kurzfristig die Möglichkeit, Mitarbeiter zu schützen, den verordneten Kontaktsperren gerecht zu werden und trotzdem den Betrieb aufrecht zu erhalten. Dennoch ist zunächst in Ruhe zu prüfen, ob die Tätigkeit sinnvollerweise in das Home Office verlagert werden kann. Und auch in einem Notfall sind Mindestvoraussetzungen für technische und organisatorische Maßnahmen einzuhalten.

Im Folgenden finden Sie zwei Check-Listen für eine schnelle Prüfung, ob bzw. wann ein Einsatz im Home Office aus datenschutzrechtlicher Sicht erfolgen darf. Diese Liste kann ebenfalls als Grundlage für die kurzfristige Mitarbeitersensibilisierung bzgl. der Tätigkeit zu Hause dienen.

Check-Liste – Technische Maßnahmen

1. Primärer Einsatz von betrieblichen Endgeräten im Home Office als Grundregel.
    - Nutzung privater Geräte nur, wenn keine anderen Mittel zur Verfügung stehen. Für private Geräte gelten identische Sicherheitsmaßnahmen wie für betriebliche!
2. Zugriff auf betriebsinterne Infrastruktur nur über geeignete Kommunikationswege, z. B. VPN
3. Betriebssysteme befinden sich auf dem aktuellen Stand (Versionen, Updates).
    - KEIN: Windows 7 oder älter, alte Versionen von macOS, iOS oder Android
    - ERLAUBT: z.B. Windows 10, iOS 13, macOS Catalina, Android 9 oder10
4. Router befinden sich auf dem neuesten Stand: Firmware, Software
5. Firewall befindet sich auf dem neuesten Stand: Version
6. Antivirensoftware befindet sich auf dem neuesten Stand: Version, Virendefinition
7. Alle Geräte sind passwortgeschützt

Check-Liste – Organisatorische Maßnahmen

1. Verwendete Geräte (u.a. Laptop, Telefon) sind zu sperren, sobald sie nicht genutzt werden (
2. Kein Zugang Dritter gestattet - z.B. Kinder, Lebenspartner, Haustiere ☺)
3. Benötigte Unterlagen sind möglichst verschlossen aufzubewahren

- Druck und Scans von Dokumenten nur bei Notwendigkeit
- Nicht mehr benötigte Unterlagen sind (datenschutzkonform) zu vernichten

4. Die Installation von Anwendungen auf betrieblichen Endgeräten ist ohne eine ausdrückliche Arbeitgeberanweisung untersagt
5. Ansprechpartner für Datenvorfälle müssen (wie z.B.: Datenpannen, IT-Sicherheit) bekannt sein

Die Prüfung der Sicherheitsmaßnahmen anhand der Checklisten entbindet den Arbeitgeber nicht von seiner Pflicht einer schriftlichen Home Office-Vereinbarung mit den Mitarbeitern.

Sobald der Notfallstatus beendet ist, sind diese gelockerten Maßnahmen entweder zurück zu ziehen oder umfassende Richtlinien für Home Office und IT-Nutzung umzusetzen.

Bestehen bereits interne Regelungen für Home Office in Ihrem Unternehmen (z.B. Richtlinien, Betriebsvereinbarungen), so sind die Mitarbeiter über das Ergreifen der erforderlichen Maßnahmen im Home Office bereits informiert und Sicherheitsmaßnahmen festgelegt worden. Dessen ungeachtet sind die Mitarbeiter weiter regelmäßig zu sensibilisieren und die Sicherheitsmaßnahmen in regelmäßigen Abständen hinsichtlich des Stands der Technik zu prüfen.

Umgang mit Beschäftigtendaten

Aufgrund der aktuellen Situation beschäftigen sich sowohl Arbeitgeber als auch Arbeitnehmer intensiv mit Gesundheitsdaten (d.h. hochsensible personenbezogene Daten) der Beschäftigten bzw. der Arbeitskollegen. Das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder - die Datenschutzkonferenz - hat aus diesem Anlass konkrete Hinweise zu Datenschutz und Corona veröffentlicht. Weitere Fragen zu dem vorliegenden Thema wurden von dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg in einer FAQ Liste zum Thema Corona behandelt.

Phishing-Mails

Die Ausnahmesituation aufgrund der Corona-Pandemie wird leider vermehrt von Cyber-Kriminellen u. a. für Phishing-Attacken ausgenutzt. Sind diese bereits in der betrieblichen IT-Infrastruktur schwer abzuwehren, stellt ein neues oder wachsendes Home Office-Umfeld IT-Verantwortliche vor weitere Herausforderungen. Auch die aktuell sehr kurzfristige Umstellung der Infrastruktur erschwert die Bedingungen zusätzlich. Einerseits ist die Technik oftmals nicht für die Arbeit von zu Hause bereit, andererseits sind die Mitarbeiter weder auf das besondere Arbeitsumfeld noch auf die gegebenenfalls auftretenden technischen Probleme ausreichend vorbereitet.

Gerade dieser Tage werden Angst, Informationsbedürfnis oder einfach nur die Neugier der Menschen von Cyber-Kriminellen ausgenutzt. Phishing-Mails sind inzwischen so intelligent verfasst, dass diese personalisiert erscheinen können. Öffnen Sie keine E-Mails von unbekannten / fragwürdigen Absendern. Öffnen Sie keinesfalls Anhänge aus solchen E-Mails und folgen Sie bitte nicht den Links. Lassen Sie sich auch nicht von gegebenenfalls sogar personalisierten Betreff- und Nachrichtentexten täuschen. Möchten Sie sich über die Corona-Pandemie informieren, nutzen Sie z.B. das Angebot der Bundeszentrale für gesundheitliche Aufklärung, des Robert-Koch-Instituts oder anderer verlässlicher Quellen.

Trennen Sie im Home Office ganz bewusst Arbeit von Privatem. Dies ist insbesondere bei der beruflichen Nutzung von privaten Endgeräten zu beachten.

In der Regel verbinden Sie sich per VPN mit dem Unternehmensnetzwerk. Greifen Sie parallel auf Ihr privates Postfach (auch FreeMail-Webseiten) zu und öffnen eine Phishing-E-Mail, können Cyber-Kriminelle über eine Hintertür in das Unternehmensnetzwerk eindringen und dort schwerwiegende Schäden verursachen.

Auch wenn uns alle zurzeit andere Gedanken beschäftigen, seien Sie besonders aufmerksam. Teilen Sie diese Nachricht bitte mit allen Kolleginnen und Kollegen, unabhängig vom derzeitigen Arbeitsplatz.

Haben Sie Fragen zum Thema Datenschutz? Kontaktieren Sie uns! Zwar befindet sich auch das GfP-Datenschutz Team im Home Office, trotzdem stehen wir Ihnen ohne Einschränkungen unter den üblichen Kontaktdaten zur Verfügung. Wir sind gerne für Sie da.

Viele Grüße

Ihr Datenschutzteam

E-Mail: datenschutz@gfp24.de

Die direkte Durchwahl Ihrer Ansprechpartner finden Sie hier.

Gesellschaft für Personaldienstleistungen mbH
- Einrichtung der Handels- und Dienstleistungsverbände

Pestalozzistraße 27, 34119 Kassel
Telefon: +49 561 78968-93 /-99, Fax: -61
Web: www.gfp24.de, E-Mail: datenschutz@gfp24.de

GF: Dirk Schöttelndreier, Sitz der Gesellschaft: Marburg
Amtsgericht Marburg HR B 2038, Steuer-Nr. 020 225 130 17

Eine ausführliche Belehrung über Ihre Rechte nach Art. 13 DSGVO finden Sie in der Datenschutzerklärung und den Betroffenenrechten auf unserer Webseite.