Frankfurter Datenschutz

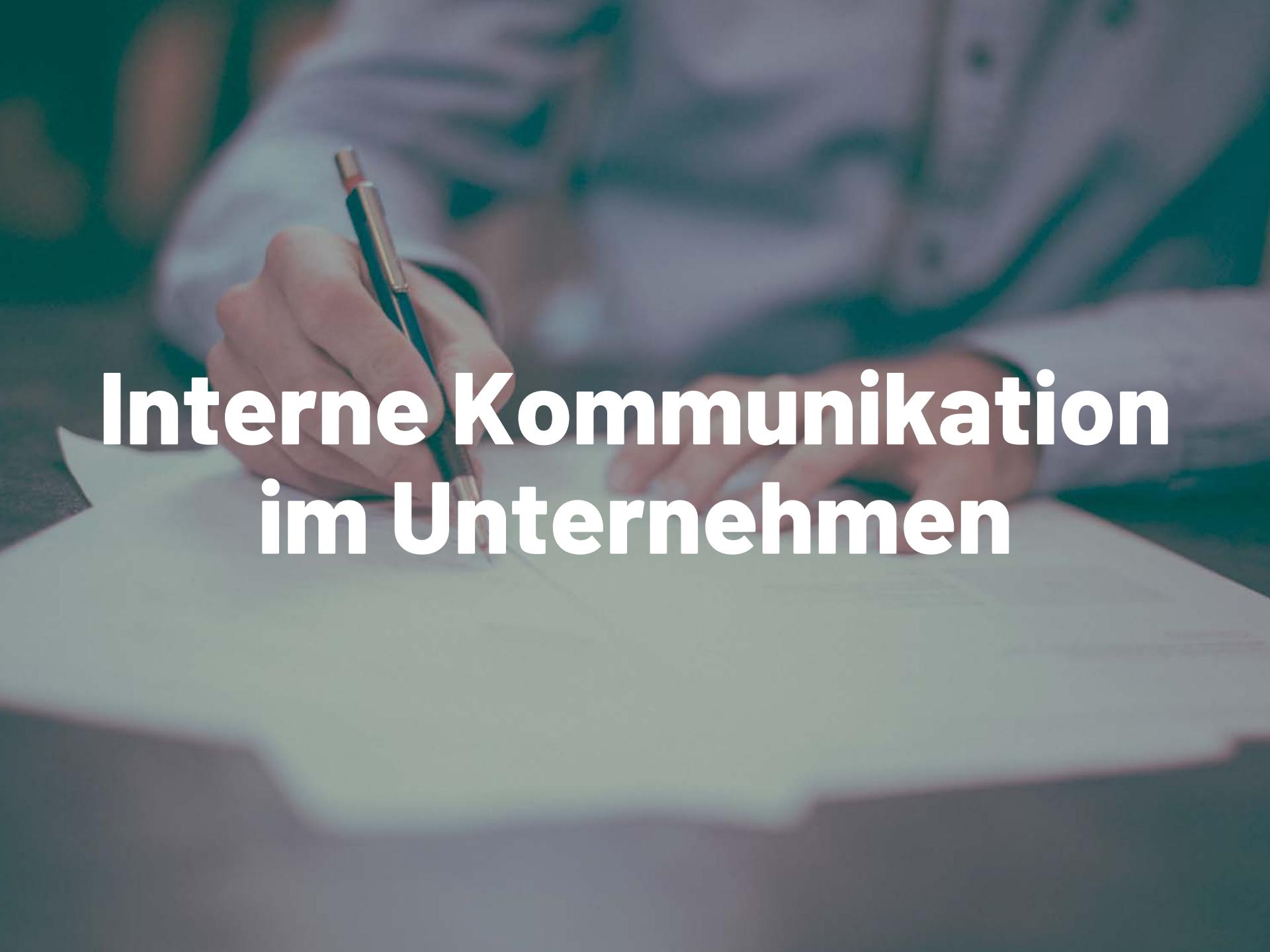
Corona-Krise und Datenschutz

Herausforderung und Lösungsansätze

Die Herausforderungen

Bedingt durch die Corona-Pandemie erfordert die aktuelle Lage, ein besonderes Augenmerk auf den Datenschutz zu werfen. Die augenblicklichen Herausforderungen sowohl für den Arbeitgeber als auch den Arbeitnehmer dürfen nicht in spontanen Lösungen gipfeln, welche den Datenschutz außer Acht lassen.

Im Folgenden zeigen wir zu den Themen „Interne Kommunikation im Unternehmen“, „Homeoffice datenschutzrechtlich sicher“ und „Video-Konferenzen und Datenschutz“ wichtige Punkte zur Bewältigung auftauchender Problemstellungen auf.



Interne Kommunikation im Unternehmen

Interne Kommunikation im Unternehmen

Der Arbeitgeber muss seine Fürsorgepflicht (§ 3 ArbSchG) erfüllen.

Dies bedeutet, dass er seine Beschäftigten vor möglicher Infizierung schützen muss, andererseits aber die Persönlichkeits- und Datenschutzrechte seiner Beschäftigten bei aller wohlgemeinten Aktion nicht verletzen darf.

Kriterium ist hierbei immer die Erforderlichkeit und Zulässigkeit jeglicher Maßnahme.

Interne Kommunikation im Unternehmen

Unzulässig ist

- Die pauschale Befragung der Beschäftigten zu ihren Reisezielen.
- Die pauschale Befragung der Beschäftigten zu ihrem Gesundheitszustand.
- Eine durch die Firmenleitung angeordnete Meldepflicht für die Beschäftigten zur Erkrankung einer Kollegin/eines Kollegen.
- Die angeordnete Fiebermessung vor dem Betreten des Betriebsgeländes.
- Die Nennung des konkreten Namens einer am Virus erkrankten Person gegenüber der Belegschaft.

  (Ausnahme: Sofern die Nennung von Namen Beschäftigter zur Abwendung von Gefahren erforderlich ist – etwa um Mitarbeiter zu identifizieren, die Kontakt mit den Infizierten hatten – ist diese auch aus datenschutzrechtlicher Sicht im nötigen Umfang zulässig (Verarbeitung zum Zwecke der arbeitsmedizinischen Vorsorge gemäß Art. 6 Abs. 1 lit. c D SGVO, Art. 9 lit. i 1, Abs. 4 DSGVO und § 26 Abs. 3 S. 1, § 22 Abs. 1 lit. c BDSG).

Interne Kommunikation im Unternehmen

Zulässig ist (1)

- Die freiwillige Fiebermessung.
- Die freiwillige Selbstauskunft zu Aufenthaltsorten im In- und Ausland und möglichen Symptomen.
- Die Information der Kundschaft ohne Personenbezug, ob es Corona-Fälle gibt oder gegeben hat.
- Die Warnung der MitarbeiterInnen vor direktem Kontakt zu Infizierten (ohne direkte Namensnennung) und vorübergehend Freistellung derselben durch die Team- oder Abteilungsleitung.
- Die Übermittlung von Daten über erkrankte Beschäftigte oder Kontakte zu Infizierten sowie den Aufenthalt von Beschäftigten in Risikogebieten nach Aufforderung durch die Gesundheitsbehörden.

Interne Kommunikation im Unternehmen

Zulässig ist (2)

- Die Befragung, ob sich Urlaubsrückkehrer in einem Risikogebiet aufgehalten haben.
- Die Verarbeitung von Daten der Beschäftigten mit positivem Befund und deren Kontaktpersonen sowie die eingeleiteten Maßnahmen (Verarbeitung zum Zwecke der arbeitsmedizinischen Vorsorge gemäß Art. 6 Abs. 1 lit. c DSGVO i.V.m. Art. 9 Abs. 1, Abs. 4 DSGVO und § 26 Abs. 3 S. 1, § 22 Abs. 1 Nr. 1 lit. b BDSG).
- Die Erhebung von privaten Kontaktdaten mit Einverständnis zu möglichen erforderlichen Informationen der Beschäftigten. Diese Daten sind bei Wegfall des Zweckes direkt zu löschen.

Interne Kommunikation im Unternehmen

Weitere wichtige Hinweise bietet das Handbuch „Betriebliche Pandemieplanung“ des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe:

https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/GesBevS/Handbuch-Betriebl_Pandemieplanung_2_Auflage.pdf

Homeoffice datenschutzrechtlich sicher

Homeoffice datenschutzrechtlich sicher

Erst wenn alle arbeitsorganisatorischen Möglichkeiten, die geeignet sind, die vorgegebenen Gesundheitsziele zu erreichen, ausgeschöpft sind – wie z.B. flexible Verteilung der Arbeitszeit – bleibt das Homeoffice als Mittel der Wahl.

Voraussetzung für das Arbeiten zu Hause ist die Homeoffice-Vereinbarung, die sie mit Ihren MitarbeiterInnen treffen müssen, um das Risiko für die Vertraulichkeit und Integrität zu minimieren – besser auszuschließen. Auch in den Zeiten der Corona-Pandemie hat der Arbeitgeber geeignete technische und organisatorische Maßnahmen entsprechend der DSGVO zu treffen (Art. 32 DSGVO, Art. 24 Abs. 1 DSGVO und Art. 5 Abs. 1 lit. f DSGVO).

Homeoffice datenschutzrechtlich sicher

Der Regelungsbedarf für das Homeoffice (1)

- Vorrangig sollten bereits vorhandene Rechner (z.B. Laptops) genutzt werden, welche schon in das IT-Sicherheitskonzept integriert sind.
- Die zur Verfügung gestellte IT-Ausstattung darf nicht privat genutzt werden.
- Unter Beachtung geeigneter technischer und organisatorischen Maßnahmen ist aber auch der Gebrauch von Privatgeräten zulässig.
- Eingrenzung der Aufgaben, die im Homeoffice erledigt werden können. So ist eine Bearbeitung von sensiblen Daten (z.B. Gesundheitsdaten) nicht zulässig.
- Sichere Passwörter für Laptops, Festplatten sowie externe Speichermedien sind unerlässlich.
- Zugang über privaten Internetanschluss darf nur mit LAN-Kabel oder über ein verschlüsseltes WLAN erfolgen.

Homeoffice datenschutzrechtlich sicher

Der Regelungsbedarf für das Homeoffice (2)

- Zugriff auf das Unternehmensnetzwerk nur über eine sichere VPN-Verbindung zulassen.
- Virenschutz und Firewall müssen technisch immer auf dem neuesten Stand sein.
- Bei der Verarbeitung von personenbezogenen Daten ist auch im Homeoffice die Vertraulichkeit zu gewährleisten.
- In Arbeitspausen ist der genutzte Rechner grundsätzlich zu sperren.
- Berufliche E-Mails dürfen nicht an private E-Mail-Postfächer weitergeleitet werden.
- Daten dürfen nicht auf private Speichermedien (z.B. USB-Sticks) gespeichert werden.

Homeoffice datenschutzrechtlich sicher

Achtung:

Auch im Homeoffice verbleibt die Verantwortung für die Verarbeitung der Daten beim Arbeitgeber!

Video-Konferenzen und Datenschutz

Video-Konferenzen und Datenschutz

Kommunikation ist das A und O eines funktionierenden Unternehmens. Und gerade in unserer Zeit der Corona-Pandemie erscheint sie plötzlich noch mehr in den Vordergrund zu treten. Wenn der persönliche Kontakt nicht mehr gegeben ist, wünschen wir zumindest eine Face-to-Face Kommunikation.

Vor einer Nutzung von Tools für Video-Konferenzen sollte jedoch aus Sicherheits-aspekten die Nutzung von Alternativen geprüft werden, z.B.:

- Datenschutzfreundliche und sichere Messenger (kein WhatsApp!)
- Telefonkonferenzen
- Text-Chats über datenschutzfreundliche und Ende-zu-Ende-verschlüsselte Plattformen
- E-Mails, möglichst gesichert durch Ende-Zu-Ende-Verschlüsselung

Video-Konferenzen und Datenschutz

Sollten diese Alternativen verworfen werden, stehen wir vor der Wahl eines aus datenschutzrechtlicher Sicht geeigneten Tools für Video-Konferenzen. Der Markt ist hier sehr groß, weswegen der Frankfurter Datenschutz aus Wettbewerbsgründen keine Empfehlung abgibt – aber das bekannteste Tool muss nicht das Beste sein.

Zu beachten bei der Auswahl einer Video-Konferenz-Software (1)

- Gibt es eine Business-Variante der Software, da diese öfters einen höheren Sicherheitsstandard bietet?
- Ist das Tool in der Lage die gesendeten Daten verschlüsselt zu übertragen?
- Tools aus Deutschland oder der EU sind zu bevorzugen, da diese der DSGVO unterliegen.

Video-Konferenzen und Datenschutz

Zu beachten bei der Auswahl einer Video-Konferenz-Software (2)

- Video-Konferenz-Tools, deren Anbieter außerhalb der EU niedergelassen sind, bei deren Nutzung Daten in diese sogenannten „Drittländer“ übermittelt werden, sind kritisch zu betrachten.
- Für Software aus z.B. der Schweiz, Neuseeland, Andorra, Argentinien, den Faröer Inseln, Guernsey, Japan, Kanada und Israel ist laut der EU-Kommission ein angemessenes Datenschutzniveau festgestellt.
- Ein angemessenes Datenschutzniveau ist auch bei US-Anbietern mit einem Privacy-Shield-Zertifikat anzunehmen.
- Grundsätzlich ist mit dem Software-Anbieter ein Auftragsverarbeitungsvertrag abzuschließen.

Video-Konferenzen und Datenschutz

Zu beachten bei der Anwendung des ausgewählten Video-Tools

- Die Konfiguration des Tools ist so vorzunehmen, dass eine gemäß Datenschutz unzulässige Verarbeitung der Daten verhindert wird.
- Bei Mitschnitten der Video-Konferenz sind alle Beteiligten vorher zu informieren, um deren Einverständnis einzuholen.
- Eventuelle Mitschnitte müssen nach einem festgelegten Zeitraum gelöscht werden können. Dieser Zeitraum wird allein durch den Zweck bestimmt.
- Einladungen zur Video-Konferenz dürfen nur an Personen gehen, die auch eine Freigabe zu den behandelten Themen haben.
- Logins sind keinesfalls weiterzugeben.
- Der Hintergrund der Teilnehmer darf keinerlei Informationsgehalt aufweisen.

Herzlichen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen nehmen Sie einfach Kontakt zu uns auf:

Frankfurter Datenschutz
Martin Hanf-Dressler
E-Mail: info@frankfurter-datenschutz.de
Telefon: 069 – 27279049
Mobil: 0178 – 8166312
www.frankfurter-datenschutz.de