

Corona und Datenschutz

Lessons learned?!

Tim Hoffmann, UIMC

Corona - Lessons learned? | 11.09.2020 | Fachgruppe SECMGT

Berater

- Wirtschaftswissenschaften an der Universität-GH Essen
- Studien-Schwerpunkte; u. a.
 - » Organisation
 - » Informationsmanagement
- Seit 2002 als Berater bei der UIMC
- mit den Schwerpunkten
 - » Datenschutz und
 - » Informationssicherheit / IT-Sicherheit in KMU

Unternehmensgruppe



akkreditiert durch:



Agenda

- Ausgangssituation
- Datenschutzrechtliche Bewertungen von Datenverarbeitungen
- Innerbetriebliche Maßnahmen
- Fazit

Ausgangssituation

■ Pandemie erfordert

- » Schutzmaßnahmen
- » Distanzregelungen
- » Rückverfolgung

■ Innerbetriebliche Problemstellungen

- » Unvorbereitete Organisation
- » Heterogene Regelungen (Kommune / Länder)
- » Regelmäßige Änderungen bei rechtlichen Vorgaben

Meldung einer Erkrankung (IfSG)

- Zur Meldung verpflichtet nach § 8 – medizinisches Personal
 - » Ein Unternehmen ist nicht meldepflichtig; im Gesundheitswesen jeweils das Personal.
 - » Legitimation durch Art. 9 Abs. 2 lit. i DSGVO
 - » Wird dem Unternehmen eine Erkrankung bekannt, muss der Betroffene einen Arzt aufsuchen, der meldeberechtigt ist.
 - » Eine Meldung durch das Unternehmen an das RKI oder sogar intern (z.B. Rundmail, Intranet) stellt eine Datenpanne dar.

■ Datenerhebung von Besuchern

- » Rückverfolgbarkeit berührt den Datenschutz:
Art. 6 Abs. 1 c DSGVO (keine Gesundheitsdaten)
- » Erhebung von Name, Besuchszeit und Kontaktmöglichkeit
 - › Telefon *oder* E-Mail gemäß Datensparsamkeit (NRW)
- » Aufbewahrungsfrist derzeit vier Wochen
- » Informationspflichten nach Art. 13 DSGVO müssen eingehalten werden

Symptome: Messung

■ Ideen:

- » Fiebermessung bei Mitarbeitern / Besuchern
- » Nutzung von Wärmebildkameras
- » verpflichtende Schnelltests am Werkstor

■ Fieber etc.: Gesundheitsdaten

■ Verarbeitung nur unter hohen Anforderungen

- » für Unternehmen nur in Ausnahmefällen bzw. in engen Grenzen möglich
- » zum Beispiel: keine Zuordnung zu einer Person

Symptome: Befragung

- Mitarbeiter und Besucher dürfen nicht nach Symptomen befragt werden (Gesundheitsdaten); zulässig:
 - » Frage nach Infektion oder
 - » Kontakt mit einer nachweislich infizierten Person
- Die Einholung der Information über Aufenthalte in Risikogebieten (gemäß RKI) ist zulässig
 - » Standortdaten sind nicht besonders schutzbedürftig
 - » eine Verarbeitung aufgrund berechtigtem Interesse ist zulässig (Art. 6 Abs. 1 f DSGVO)

■ Grundsätzlich in der Hoch-Phase:

- » Gewisse Toleranz durch Aufsichtsbehörden

■ Aber:

- » Keine Fristverlängerung für Auskunftersuchen
- » Kein Anspruch auf längere Frist für die Bearbeitung von Datenpannen
- » Nur bei pandemiebedingten Einschränkungen der Arbeitsfähigkeit *denkbar*

Nutzung der Corona-App

■ Im Unternehmen gilt: Freiwilligkeit

- » Installation auf dem Diensthandy kann angeordnet werden, die Nutzung jedoch nicht
- » Installation und Nutzung auf dem Privathandy unterliegen nicht der Einflussnahme des Arbeitgebers
- » Keine Mitteilungspflicht gegenüber dem Arbeitgeber für Warnungen der App
- » Haftungsregelungen noch offen
(z. B. durch Nichtmeldung einer App-Warnung)

Innerbetriebliche Maßnahmen

- Umsetzung von Distanzregelungen
 - » Home Office
 - » Videokonferenz
- Problem:
 - » Sehr schnelle Umsetzungsnotwendigkeit
 - » Oftmals fehlende Infrastruktur
 - » Zum Teil keine Erfahrungswerte
 - » Beschaffungsengpässe

■ Erreichbarkeit

- » Nutzung von privater Telefonnummer in der Regel nur mit **Einwilligung** und ausschließlich zweckgebundene Nutzung
- » Unerheblich, ob für eine Telefonliste, Einbindung in die Telefonanlage, Nutzung von Soft-Token auf Privathandy etc.
- » Unerheblich, ob Daten erhoben werden müssen oder schon vorliegen
- » Beachtung des Spannungsfelds der Freiwilligkeit im Arbeitsverhältnis

■ Gleiches gilt für laufende Informationen („Newsletter“)

Home Office: Empfehlungen

- Erarbeitung von Richtlinien und Vorgaben
 - » Gilt auch für private Arbeitsumgebung, Umgang mit zu vernichtenden Unterlagen etc.
 - » Sensibilisierung bzgl. der besonderen Risiken
- Keine Nutzung von privater Hardware und Dienste
- Ausreichende Sicherheitsmaßnahmen
 - » in Abhängigkeit zur Risiko-Situation
 - » inkl. Vorgaben für das Heimnetzwerk

Videokonferenzsysteme

- Oftmals SaaS:
 - » Daher liegt eine Auftragsverarbeitung vor.
- Oftmals Nicht-EU-Anbieter:
 - » Daher liegt ein Drittlandtransfer vor.
 - » beachte: EuGH-Urteil zum Privacy Shield und SCC
- Informationspflichten nicht vergessen

Revision der Maßnahmen

- Viele Maßnahmen mussten schnell umgesetzt werden
 - » Sorgfalt im Datenschutz nicht immer „100%ig“
- Daher: Neu-Bewertung der Risikosituation
- Überprüfung der getroffenen Maßnahmen und ggf. Nachbesserung
 - » Einwilligungen
 - » Anbieter von Systemen
 - » Vorgaben / Richtlinien

- Corona hatte/hat Auswirkungen auf den innerbetrieblichen Datenschutz
 - » Datenerhebung und -verarbeitung
 - » Einsatz von (neuen) Systemen
 - » Dezentralisierung der Arbeiten (Home Office / Mobile Computing)
- Akut-Maßnahmen sollten auf den Prüfstand
- Chancen und Risiken ebenbürtig abwägen
- Mitarbeiter-Sensibilisierung wichtig

An illustration of a meeting room with several people sitting around a large wooden table. The room has large windows in the background showing a cityscape. Two blue banners with white text are overlaid on the top half of the image. The text on the banners is: www.uimc.de/kommunikation/corona/ and www.uimc.de/kommunikation/uimcommunication/.

www.uimc.de/kommunikation/corona/

www.uimc.de/kommunikation/uimcommunication/

Fragen?? Diskussion??

thoffmann[at]uimc.de
+49 202 946 7726 200

Haben Sie noch Fragen?



UIMC DR. VOSSBEIN GMBH & Co. KG
Otto-Hausmann-Ring 113
42115 Wuppertal
Telefon: +49 202 946 7726 200
Telefax: +49 202 946 7726 9200
E-Mail: consultants@uimc.de
Internet: www.UIMC.de



UIMCert GmbH
Otto-Hausmann-Ring 113
42115 Wuppertal
Telefon: +49 202 946 7726 300
Telefax: +49 202 946 7726 9300
E-Mail: certification@uimcert.de
Internet: www.UIMCert.de

akkreditiert durch:

