Newsletter Datenschutz

Ausgabe 08 | 2020

Gute Datenschutzorganisation in Krisenzeiten wichtiger denn je

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,

eine gute Datenschutzorganisation ist gerade in Krisenzeiten wichtig. Andernfalls besteht die Gefahr, dass ungewollt und unbewusst die Privatsphäre vieler in Gefahr gerät.

Diese Ausgabe Ihres Datenschutz-Newsletters will Sie informieren, wie es zum Beispiel um die Weitergabe von Mitarbeiterdaten an Dritte wie das Gesundheitsamt bestellt ist. Eine weitere Frage, die sich häufig stellt, ist die Mitteilung von Arbeitszeiten und Überstunden an Vorgesetzte.

Die vermehrte Nutzung des Homeoffice hat auch die Bedeutung der Videokonferenzen weiter steigen lassen. Erfahren Sie deshalb, wie sich der Datenschutz bei Video-Chats wahren lässt, und bekommen Sie Einblick in eine neue Angriffsform namens Deep Fakes: Selbst Live-Videobilder könnten gefälscht und die Identität des Gegenübers vorgetäuscht sein.

Ich wünsche Ihnen viel Spaß beim Lesen!
Ihr Frank Berns, Datenschutzbeauftragter

Weitergabe von Mitarbeiterdaten wegen Corona

Zumindest die erste Corona-Welle ebbt ab. Umso mehr sind die Gesundheitsbehörden hinter jedem „Verdachtsfall“ her. Schließlich will man alles, bloß keine zweite Krankheitswelle. Welche Auskünfte müssen Arbeitgeber den Gesundheitsbehörden über Mitarbeiter geben?

Infektionsverfolgung und Datenschutz

In der ersten, teils schlimmen Corona-Phase dachten eher wenige über Fragen des Datenschutzes nach. Das ändert sich nun, und das ist gut so. Denn bei der „Infektionsverfolgung“ geht es um viele Daten. Dabei gibt es rechtlich gesehen zwei Aspekte: Welche Fragen darf ein Gesundheitsamt stellen? Und welche Antworten darf ein Unternehmen geben?

Ausgangsfall: ein infizierter Arbeitnehmer

Angenommen, ein Arbeitnehmer ist nachweislich an Covid-19 erkrankt. Das hat sein Arzt dem Gesundheitsamt mitgeteilt. Dazu ist der Arzt gesetzlich verpflichtet. Jetzt will das Gesundheitsamt im Unternehmen nachforschen, wer vielleicht noch infiziert worden ist. Welche Auskünfte darf das Gesundheitsamt verlangen? Die Antwort gibt § 16 Infektionsschutzgesetz, der leicht zu googeln ist: sehr viele! Es darf etwa folgende Fragen stellen:

Typische Fragen des Gesundheitsamts

- Wer hat mit dem Erkrankten in einem Zimmer gearbeitet?
- Wer hatte mit ihm sonst Kontakt, etwa bei Besprechungen?
- Mit welchen Kunden hatte der Erkrankte persönlich zu tun?

Befugnis des Unternehmens für Antworten

Das Gesundheitsamt hat das Recht, solche Fragen zu stellen. Trotzdem könnte einer Antwort durch das Unternehmen der Datenschutz entgegenstehen. Denn vor allem Personaldaten darf ein Unternehmen nicht ohne Weiteres nach außen weitergeben.

DSGVO und lebenswichtige Interessen

Die Datenschutz-Grundverordnung (DSGVO) trifft eine erfreulich konkrete Regelung. Danach ist die Weitergabe von personenbezogenen Daten erlaubt, wenn sie erforderlich ist, um lebenswichtige Interessen zu schützen (siehe Art. 6 Abs. 1 Buchstabe d DSGVO). Dabei kann es ausdrücklich um lebenswichtige Interessen der betroffenen Person selbst gehen, aber auch um die einer anderen Person.

Aussagen der DSGVO zu Epidemien

Ein Blick in Erwägungsgrund 46 zur DSGVO schließt alle Zweifel aus: Die Notwendigkeit, Epidemien zu überwachen, ist dort ausdrücklich als ein Beispiel für lebenswichtige Interessen genannt. Und was für örtlich begrenzte Epidemien gilt, gilt für weltweite Pandemien natürlich erst recht. Das Unternehmen kann und muss die Fragen des Gesundheitsamts daher beantworten.

Strenge Zweckbindung

Beruhigend, dass das Infektionsschutzgesetz auch eine strenge Schutzvorschrift enthält. Das Gesundheitsamt darf alle Daten ausschließlich für die Zwecke dieses Gesetzes verarbeiten. So regelt es dort § 16 Abs. 1 Satz 2. Die Überwachung erfolgt durch die Datenschutzaufsicht.

Mitteilung von Überstunden an Vorgesetzte

Wer darf wissen, wer wie viele Überstunden gemacht hat? Ein Thema voller Facetten, das immer wieder Diskussionen auslöst! Das Bayerische Landesamt für Datenschutzaufsicht schafft Klarheit, was die Mitteilung von Überstunden an Vorgesetzte angeht.

Ein Thema mit vielen Facetten

Überstunden sind in Unternehmen zu allen Zeiten ein Thema. Läuft es wirtschaftlich gut, sind sie oft ein wenig geliebtes Muss. Laufen die Geschäfte schlechter, kann es Differenzen darüber geben, wer sie machen darf. Und bei Kurzarbeit sind sie in der Regel unzulässig. Das sind nur einige Beispiele, die Anlass für Diskussionen sein können.

Umfassender Überblick der Personalabteilung

Klar ist zumindest eines: Die Personalabteilung muss die Überstunden jedes einzelnen Mitarbeiters kennen. Denn bei der monatlichen Lohnzahlung muss sie die Frage beantworten, ob Überstunden bezahlt werden müssen oder nicht. Das hängt vom Arbeitsvertrag ab.

Notwendige Entscheidungen

Je höher es in der Hierarchie „nach oben“ geht, desto eher kommt es vor, dass Überstunden ganz oder teilweise durch das Monatsgehalt abgegolten sind. Beim durchschnittlichen Arbeitnehmer sieht dies durchweg anders aus. Hier stellt sich vor allem die Frage, ob Überstunden „abgefeiert“ werden müssen oder ob sie auszuzahlen sind. Unsicherheiten über den Datenschutz

gibt es in diesem Zusammenhang normalerweise nicht.

Informationsansprüche des Betriebsrats

Das ändert sich, sobald neben der Personalabteilung andere Akteure im Unternehmen ins Spiel kommen. Soweit ein Betriebsrat vorhanden ist, steht ihm bei der Anordnung von Überstunden normalerweise ein Mitbestimmungsrecht zu. Es liegt auf der Hand, dass der Betriebsrat dann wissen muss, welche Arbeitnehmer Überstunden leisten sollen und welchen Umfang diese haben sollen. Die entsprechenden Spielregeln sind Betriebsrat wie Unternehmensleitung vertraut. Im Normalfall läuft deshalb alles routiniert ab.

Informationswünsche unmittelbarer Vorgesetzter

Aber wie sieht es mit den unmittelbaren Vorgesetzten aus? Dürfen sie von der Personalabteilung erfahren, wie viele Überstunden bei den Mitarbeitern aufgelaufen sind, die ihnen unterstehen? Und wie sieht es mit den Überstunden von Mitarbeitern der „Nachbarabteilung“ aus?

Erforderlichkeit als Grenze

Rechtlich geht es dabei letztlich immer um die Frage, was erforderlich ist, um das Beschäftigungsverhältnis durchzuführen. Diesen Maßstab gibt § 26 Bundesdatenschutzgesetz dafür vor, wie der Arbeitgeber mit Mitarbeiterdaten umgehen darf. Nicht erforderlich ist es aus der Sicht des Datenschutzes, dass ein Vorgesetzter Informationen über die „Nachbarabteilung“ erhält. Denn: Für sie ist er schlicht nicht zuständig.

Auf der nächsten Ebene sieht dies jedoch anders aus. Ein Vorgesetzter, dem die Leiter mehrerer Abteilungen berichten, darf über die Überstunden in all diesen Abteilungen Bescheid wissen.

Information an Vorgesetzte über die eigene Einheit

Über die eigene Abteilung, die eigene Arbeitsgruppe oder das eigene Team muss der jeweilige Leiter informiert sein, wenn ihm die Mitarbeiter unterstehen. Dazu gehört es auch, über die aufgelaufenen Überstunden im Bild zu sein. Deshalb darf er diese Information von der Personalabteilung erhalten. Das Bayerische Landesamt für Datenschutzaufsicht führt hierfür gleich mehrere Argumente an:

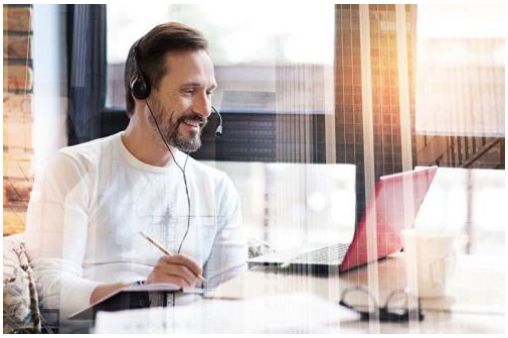
- Der Vorgesetzte muss erkennen können, wie stark die einzelnen Mitarbeiter belastet sind.
- Es muss ihm möglich sein, bei Bedarf Aufgaben umzuverteilen.
- Er muss bei Bedarf Konzepte für den Abbau von Überstunden erstellen können.

All dies geht nicht ohne entsprechende Informationen durch die Personalabteilung. Sie darf deshalb Übersichten mit Überstunden an Teamleiter, Gruppenleiter und Abteilungsleiter geben – immer beschränkt auf die Mitarbeiter, für die der Leiter die Funktion eines Vorgesetzten hat. Diese Beschränkung stellt sicher, dass er wirklich nur das bekommt, was für seine Tätigkeit erforderlich ist.

Besondere Rolle der Geschäftsführung

Die Geschäftsführung ist für das gesamte Unternehmen verantwortlich. Schon deshalb darf sie sich für alle Einheiten des Unternehmens (Teams, Arbeitsgruppen, Abteilungen usw.) Übersichten mit Überstunden vorlegen lassen. Ansonsten könnte sie ihre Aufgaben schlicht nicht erfüllen. So kann sich beispielsweise die Frage stellen, ob sie neue Mitarbeiter einstellen will, um die Überstunden zu verringern. Dies kann im Normalfall nur sie selbst entscheiden.

Videokonferenz im Fokus von Cyberattacken



Die Zahl der beruflichen und privaten Videokonferenzen hat stark zugenommen. Das weckt das Interesse der Datendiebe. Ohne die erforderlichen Sicherheitsmaßnahmen ist die Vertraulichkeit der Gespräche und ausgetauschten Daten in Gefahr.

Der Berufsalltag wandelt sich

Wissenschaftler gehen davon aus, dass die Corona-Pandemie die Arbeitswelt auch längerfristig verändert. Im Arbeitsalltag werden wohl häufiger virtuelle Treffen anstelle von Konferenzen vor Ort stattfinden.

Leider fehlt vielen Berufstätigen noch die Erfahrung, um Videokonferenzen sicher nutzen zu können. Dadurch gerät der Datenschutz in Gefahr.

Videokonferenzen bergen viele Risiken

Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, betont: „Da Videokonferenzen für viele neu sind, haben nicht alle im Blick, welche Risiken damit verbunden sind. Gerade in der Kombination mit Homeoffice ist einiges zu beachten. Um die Teilnehmenden von Videokonferenzen und die besprochenen Inhalte zu schützen, sind technische und organisatorische Sicherheitsmaßnahmen wichtig."

IT-Sicherheitsexperten warnen davor, dass zum Beispiel ein ungebetener Gast an einer Videokonferenzsitzung teilnehmen könnte, um entweder das Gespräch mitzuhören oder die Sitzung durch den Austausch ungeeigneter Medien zu stören. Ebenso könnten Meeting-Links und -Zugänge gestohlen sowie bösartige Links und Schadsoftware verteilt werden.

Im Juni 2020 warnte zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI), dass Angreifer mehrere Schwachstellen in Zoom Video Communications ausnutzen konnten, um Schadcode auszuführen. Unter anderem konnte dies mittels speziell manipulierter animierter Bilddateien geschehen. Für einen Angriff genügte es, die vom Angreifer versendete Datei im Chat empfangen zu haben. Die Datei musste nicht extra geöffnet werden.

Auf eine sichere Lösung kommt es an

Die Aufsichtsbehörden für den Datenschutz warnten in den letzten Monaten vor verschiedenen Lösungen für Videokonferenzen, weil personenbezogene Daten in Gefahr geraten konnten, und empfahlen datenschutzfreundlichere Alternativen.

Die Berliner Beauftragte für den Datenschutz zum Beispiel empfiehlt, zu prüfen,

- ob anstelle von Videokonferenzen auch Telefonkonferenzen ausreichen könnten, um die gewünschte Abstimmung untereinander herbeizuführen,
- ob es mit verhältnismäßigem Aufwand möglich ist, einen eigenen Dienst für Videokonferenzen mit öffentlich verfügbarer oder kommerziell erhältlicher Software bereitzustellen, und
- ob Lösungen eines Anbieters mit Sitz und Verarbeitungsort, insbesondere Server-Standort, im Europäischen Wirtschaftsraum (EWR) oder aus einem Land mit gleichwertigem Datenschutzniveau den Bedürfnissen des jeweiligen Unternehmens entsprechen.

Der gewählte Anbieter sollte die Daten nur im zulässigen Rahmen verarbeiten und insbesondere nicht entgegen europäischem Datenschutzrecht an Dritte – einschließlich ausländischer Behörden – weitergeben, ausreichende Datensicherheit (zum Beispiel durch Zertifizierung) nachweisen können, die Verschlüsselung der Datenübertragung garantieren und einen ordnungsgemäßen Auftragsverarbeitungsvertrag anbieten.

Auch wichtig: das richtige Verhalten der Teilnehmerinnen und Teilnehmer

Allein die Wahl einer datenschutzgerechten Lösung reicht aber nicht, sie muss auch genutzt werden: Laut einer Kaspersky-Studie verwenden 26 Prozent der deutschen Mitarbeiter nicht genehmigte Videokonferenz-Tools und setzen die eigenen Daten und die Daten des Arbeitgebers möglichen Angriffen aus. Security-Experten beobachten den Trend, der BYOM (Bring Your own Meeting) genannt wird, also die Verwendung privater Videokonferenz-Lösungen zu betrieblichen Zwecken. Das kann gerade im Home-Office leicht passieren.

Bei den „kostenfreien" Diensten sollte man ganz genau in die Datenschutzbestimmungen schauen. Oftmals zahlen die Nutzer hier mit ihren Daten. Das kann nicht im Sinne von Unternehmen sein und auch nicht im Sinne des Nutzers selbst.

Für den Datenschutz kommt es deshalb auch auf das Verhalten der Teilnehmer an. Die Datenschutzaufsicht von Schleswig-Holstein rät den Teilnehmern an Videokonferenzen insbesondere:

- Informieren Sie sich bei der organisierenden Person, ob im Zusammenhang mit der Videokonferenz eine Datenschutzerklärung oder eine Datenschutz-Kurzinformation bereitgestellt wird.
- Testen Sie die Funktionen, mit denen Sie Ihre Privatsphäre schützen können, um sie während der Videokonferenz sicher verwenden zu können, zum Beispiel Ton und/oder Bild deaktivieren.
- Seien Sie sich bewusst, dass in einer Videokonferenz alle anderen Teilnehmenden zuhören, und geben Sie keine sensiblen Informationen weiter.

- Schalten Sie Ihr Mikrofon stumm und ggf. die Kamera aus, etwa wenn im Homeoffice andere Personen aus Ihrem Haushalt in den Aufnahmebereich des Mikrofons oder in das Sichtfeld der Kamera kommen.
- Seien Sie in der Videokonferenz aufmerksam und informieren Sie die organisierende Person bzw. die anderen Teilnehmenden, wenn beispielsweise eine fremde Person den Konferenzraum betritt.

Deep Fakes: Das gefälschte Gegenüber

Nicht nur Fotos können gefälscht sein, sondern sogar der Gesprächspartner in der Videokonferenz. Sogenannte Deep Fakes helfen Internetkriminellen dabei, falsche Identitäten vorzutäuschen. Trauen Sie also nicht nur Ihren Augen!

Gefälschte Bilder werden beweglich

Die Zeiten sind lange vorbei, in denen man glaubte, ein Foto könnte ein sicheres Beweismittel sein. Seit es digitale Fotos und Bildbearbeitungsprogramme gibt, besteht das Risiko, dass ein Foto, das man sich anschaut, nicht echt, sondern manipuliert ist.

Bei Videos hat man dagegen ein besseres Gefühl. Denn die Fälschung eines Videos erscheint doch wesentlich komplizierter. Wenn es sich dann noch um ein Live-Video handelt, zum Beispiel bei einer Videokonferenz, ist man geneigt, alle Vorsicht fallen zu lassen. Die Live-Bilder, die die Webcam überträgt, müssen echt sein, oder etwa nicht?

Leider lassen sich nicht nur Videos inzwischen mit vergleichsweise geringem Aufwand verändern. Selbst Live-Videos, die man sich ansieht, müssen nicht mehr echt sein. Für den Datenschutz ist dies ein großes Problem: Wenn man in der Videokonferenz scheinbar seine Chefin sieht, dann spricht man offen über vertrauliche Dinge. Es kann aber sein, dass es nicht die Chefin ist, sondern ein Datenspion.

Wie sich Videos fälschen lassen

Das Wort Deep Fake ist eine Wortkombination aus Deep Learning und Fake. Es beschreibt die Technik der digitalen Manipulation von Ton-, Bild- und Videomaterialien mithilfe von Deep Learning. Das ist ein Verfahren des maschinellen Lernens, das in Systemen mit Künstlicher Intelligenz (KI) eingesetzt wird, berichtet das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. Zentrales Merkmal ist die (foto)realistische Erzeugung fiktiver Medieninhalte oder die Manipulation bereits existierender Filmsequenzen.

KI-Systeme sind inzwischen so gut, dass sie die Aufnahmen einer Webcam in nahezu Echtzeit in andere Bilder verwandeln können. Eine Video-Identifizierung könnte dadurch erschwert oder untergraben werden, Videobeweise könnten ihren Wert

verlieren.

Die Fortschritte der KI-Technologie haben die Erstellung gefälschter Videos auf eine Weise ermöglicht, die zuvor nicht möglich war, berichtet zum Beispiel die Universität von Albany. Solche gefälschten Videos erschweren das gesellschaftliche Vertrauen in die Authentizität digitaler Medien und verursachen schwerwiegende ethische, rechtliche, soziale und finanzielle Konsequenzen, wie die Wissenschaftler erklären.

Was man gegen Deep Fakes tun kann

Auch die Bundesregierung hat sich bereits ausführlich mit den Risiken durch Deep Fakes befasst. Dabei kommen die Experten des Bundes zu der Auffassung: Mit fortschreitender Entwicklung der Technik verbessern sich gleichzeitig auch die Mechanismen zur Erkennung von Fälschungen und Fälschungsversuchen, wenngleich kaum eine 100%-ige Verifizierung möglich sein wird.

Schutzmechanismen zur Erkennung von Deep Fakes suchen nach winzigen Fehlern, die die Fälscher machen. Zum Beispiel beim Blinzeln der Augen, bei der Ausleuchtung des Gesichts oder bei dessen Proportionen. Leider werden die Angreifer dank KI immer besser.

Als Nutzer von Videokonferenzen werden einem kaum solche Details auffallen. Sicherheitsexperten raten deshalb Anwendern dazu, was Datenschützer ebenfalls schon lange empfehlen: Man sollte so sparsam wie möglich mit eigenen Bildern und Videos sein, die man für die Öffentlichkeit ins Internet stellt. Dadurch kann man es zumindest schwieriger machen, selbst einmal als Deep Fake zu erscheinen. Denn die KI der Angreifer braucht Futter, also Bilder und Videos, um für die Täuschung zu lernen.

Kennen Sie die Risiken durch Deep Fakes? Machen Sie den Test!

Frage: Bilder lassen sich fälschen, Videos dagegen nicht. Stimmt das?

1. Nein, inzwischen lassen sich sogar Live-Videos manipulieren.
2. Ja, das wäre viel zu kompliziert. Videobeweisen kann man vertrauen.

Lösung: Die Antwort 1. ist richtig. Spezielle Verfahren des maschinellen Lernens machen es möglich, dass zum Beispiel über das Gesicht einer Person in einem Video ein anderes Gesicht gelegt wird, das Mimik zeigt und passend zum gehörten Ton spricht. Die. Verfahren der Angreifer werden immer besser, sodass sich sogar Video-Identifizierungen, wie sie gegenwärtig genutzt werden, in Zukunft austricken lassen könnten.

Frage: Als Internetnutzer kann man nichts gegen Deep Fakes unternehmen. Stimmt das?

1. Ja, da ist man machtlos. Man muss mit diesem Risiko leben.
2. Nein. Zum einen werden Verfahren zur Aufdeckung der Fälschungen entwickelt, zum anderen kann man versuchen, solche Fälschungen für die eigene Personen zu erschweren.

Lösung: Die Antwort 2. ist richtig. In Zukunft wird es Sicherheitslösungen geben, die vor Deep Fakes warnen, genauso wie sie heute vor verseuchten Dateien warnen können. Man selbst sollte aber Datenminimierung ernst nehmen, also Fotos und Videos der eigenen Person nicht unüberlegt ins Internet stellen. Dann hat es die KI der Datendiebe schwerer, die eigene Person zu simulieren

Impressum

Redaktion: Frank Berns, Datenschutzbeauftragter

Anschrift:

Konzept 17 GmbH, Westring 3, 24850 Schuby

Telefon: 0049 4621 5 30 40 50

E-Mail: mail@konzept17.de