Newsletter Datenschutz

Ausgabe 12 | 2021

Gesichtserkennung, Fingerscan & Co. – nicht ohne Risiko –

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,

in den Medien wird der Datenschutz häufig als Bremser und Verhinderer dargestellt. Diese Einschätzung basiert aber auf Missverständnissen. Denn der Datenschutz verhindert nicht, er ermöglicht vielmehr den Fortschritt der Digitalisierung.
So gibt es gute Gründe dafür, wenn der Datenschutz davor warnt, Passwörter vorschnell durch eine Gesichtserkennung abzulösen. Ihre neue Ausgabe der Datenschutz-Zeitung erklärt Ihnen die Risiken der biometrischen Identifizierung und macht zudem am Beispiel beliebter Cloud-Speicherdienste deutlich, warum Eigeninitiative im Bereich IT nicht immer empfehlenswert ist.
Ebenso erfahren Sie in dieser Ausgabe, was sich hinter dem Begriff „Scoring“ verbirgt und warum Sie vor dem Versand von E-Mails prüfen sollten, ob die Empfänger ungewollt den gesamten Mail-Verteiler sehen können. Auch hier zeigt sich: Wenn der Datenschutz etwas verhindert, dann den Missbrauch von Daten.

Ich wünsche Ihnen viel Spaß beim Lesen!

Ihr Frank Berns, Datenschutzbeauftragter

Dropbox, Google Drive & Co: Darum kann Eigeninitiative gefährlich sein

Legen Sie Daten in einem Cloud-Speicher wie Google Drive ab, können Sie über das Internet von überall darauf zugreifen. Für das flexible Arbeiten im Homeoffice und unterwegs ist das ideal. Für den Datenschutz aber sieht das ganz anders aus.

Das Ziel: Daten speichern, austauschen und sichern

Wer im Homeoffice oder unterwegs arbeitet, muss manchmal kreativ sein, so scheint es. Viele Möglichkeiten, die im Büro bestehen, hat man außerhalb des Unternehmens nicht. Wollen Sie zum Beispiel wichtige Daten speichern, erscheint die Ablage allein auf dem Notebook oder Tablet nicht ausreichend. Was passiert, wenn das Endgerät verloren geht? Dann war alle Arbeit umsonst.

Im Büro können Sie Ihre Daten in einem Verzeichnis im Netzwerk ablegen. Dort können auch Kolleginnen und Kollegen, die mit den Daten arbeiten müssen, bequem darauf zugreifen. Sind Sie aber unterwegs oder im Homeoffice, fehlen mitunter diese Möglichkeiten zur Speicherung im Netzwerk und zum Datenaustausch. Auch die regelmäßigen Backups lassen sich nicht so einfach zentral durchführen, wenn Sie unterwegs oder im heimischen Büro arbeiten.

Bietet das Unternehmen keine entsprechende Unterstützung oder kennt man die vorgesehenen Lösungen zur Datenspeicherung und zum Datentransfer nicht, wird man schnell erfinderisch. Da gibt es doch Lösungen wie Google Drive oder Dropbox, die sich privat bereits bewährt haben. Erkennen Sie sich wieder? Damit sind Sie nicht allein – leider, aus Sicht des Datenschutzes.

Das Problem: Die sogenannte Schatten-IT

Wählen Sie als Nutzer selbst die Lösungen aus, mit denen Sie Daten speichern und austauschen wollen, sorgen Sie für sogenannte Schatten-IT. Gemeint sind damit IT-Lösungen, die die zuständige Stelle im

KONTAKT zu uns MAIL@Konzept17.de

Unternehmen nicht geprüft und genehmigt hat.

Nutzen Sie ungeprüfte und betrieblich nicht freigegebene Lösungen, können damit Risiken für die Daten verbunden sein, die der IT-Abteilung im Unternehmen nicht bekannt sind. Und diese Risiken lassen sich deshalb auch nicht mit den notwendigen IT-Sicherheitslösungen abwenden. Das ist gerade bei den Cloud-Speichern der Fall, die jeder einfach, schnell und meist kostenlos nutzen kann.

Die dringende Empfehlung: Bitte keine Eigeninitiative bei der Datenspeicherung

Normalerweise freut sich jedes Unternehmen über die Eigeninitiative der Mitarbeiterinnen und Mitarbeiter. Doch wenn es um die Sicherheit der Daten und die Einhaltung des Datenschutzes geht, ist es weder gut noch gewünscht, selbst nach Lösungen zu suchen.

Betriebliche Daten dürfen nur in betrieblich genehmigten Lösungen gespeichert und darüber ausgetauscht werden. Andernfalls können die Daten in Gefahr geraten, weil die Sicherheit von Lösungen für private Zwecke nicht den hohen Anforderungen eines Unternehmens entspricht. Zudem kann es gerade bei Cloud-Speichern passieren, dass die personenbezogenen Daten in ein Land übermittelt werden, das nicht ohne Weiteres das notwendige Datenschutzniveau bietet.

Verwenden Sie deshalb nur betrieblich genehmigte Anwendungen, auch im Homeoffice und unterwegs! Kennen Sie die Lösung nicht, fragen Sie bitte nach.

Offene Mailverteiler

Verstärktes Homeoffice hat dazu geführt, dass noch mehr Mails verschickt werden als bisher. Häufig sind das Mails an mehrere Adressaten. Damit taucht das Problem der „offenen Mailverteiler“ auf.

Bei Mails an mehrere Empfänger gibt es drei Adress-Varianten

Wer dieselbe Mail an mehrere Adressaten schicken will, kann dies auf drei Weisen tun:

- Bei Variante 1 kommen die Mail-Adressen aller Adressaten in das „An-Feld“.
- Bei Variante 2 kommt nur die Mail-Adresse eines Adressaten in das „An-Feld“. Die Mail-Adressen aller anderen Adressaten werden in das „Cc-Feld“ eingetragen.
- Bei Variante 3 steht im „An-Feld“ ebenfalls nur die Maildresse eines Adressaten. Die Mail-Adressen aller anderen Adressaten werden in das „Bcc-Feld“ eingetragen

Entscheidend ist: Wer kann was sehen?

Datenschutzrechtlich ist relevant, wer jeweils sehen kann, welche anderen Adressaten die Mail noch erhalten haben. Das macht einen erheblichen Unterschied bei den drei Varianten:

- Bei Variante 1 sehen alle Adressaten gegenseitig, wer die Mail sonst noch bekommen hat.
- Bei Variante 2 ist das im Ergebnis genauso. Sie macht zwar einen Unterschied zwischen dem „unmittelbaren Adressaten“ im „An-Feld“ und den anderen Adressaten im „Cc-Feld“. Diese erhalten nur eine Kopie der Mail an den unmittelbaren Adressaten. Das wirkt sich aber letztlich nicht aus: Jeder kann alle anderen Adressaten sehen.
- Bei Variante 3 ist das ganz anders. Denn „Bcc“ steht für „Blind Carbon Copy“. Das bedeutet, dass diese Empfänger nicht erkennen können, wer diese Mail sonst noch erhalten hat.

Jede Variante hat ihren legitimen Anwendungsbereich

Keine der drei Varianten ist von vornherein etwas Böses. Sie sind für unterschiedliche Situationen gedacht:

- Variante 1 passt beispielsweise, wenn mehrere Kollegen in einem Team gleichberechtigt an einem Projekt arbeiten. Sie kennen einander und jeder soll und muss alles sehen können, was die Teammitglieder einander schreiben.
- Variante 2 eignet sich zum Beispiel dann, wenn zwei Mail-Partner Informationen austauschen und dabei etwas ansprechen, das im konkreten Fall noch jemand wissen muss. Beispiel: Zwei Mitarbeiterinnen des Unternehmens besprechen etwas, das voraussichtlich zu Ausgaben für das Unternehmen führt. Selbst budgetverantwortlich sind sie aber nicht. Dann muss der Budgetverantwortliche wissen, was sie vorhaben. Deshalb erhält er eine „offene Kopie".
- Variante 3 ist das Mittel der Wahl, wenn die Adressaten der Mail nichts miteinander zu tun haben und nichts voneinander wissen sollen. Klassisches Beispiel: Eine Marketing-Mail geht an alle Kunden eines Unternehmens.

Der Unterschied hat auch wirtschaftliche Bedeutung

Besonders dieses Beispiel macht klar, dass es bei der Wahl des richtigen Adressatenfelds nicht um eine datenschutzrechtliche Spitzfindigkeit geht. Wer beispielsweise beim Versand einer Marketing-Mail alle Kunden in das „An-Feld" einträgt, legt den kompletten Kundenverteiler des Unternehmens für alle anderen Kunden sichtbar nach außen offen. Dasselbe gilt, wenn alle Kunden im „Cc-Feld" stehen und im „An-Feld" beispielsweise die eigene Mail-Adresse des Absenders. Das ist dann jeweils auch eine Datenschutzfrage. Unabhängig davon verletzt ein solches Vorgehen aber auch wirtschaftliche Interessen des Unternehmens in massiver Weise.

Mail-Adressen sind in der Regel personenbezogen

Warum ist es aber auch eine Datenschutzfrage? Das liegt daran, dass jedenfalls E-Mail-Adressen, die die Namen von Personen enthalten, personenbezogene Daten darstellen. Das gilt auch dann, wenn es sich um die dienstliche Adresse einer Person handelt, also nicht nur bei privaten Mail-Adressen.

Eine unbefugte Weitergabe verletzt den Datenschutz

Sind solche Mail-Adressen für einen anderen sichtbar, obwohl dies gar nicht notwendig ist, verletzt das den Datenschutz. Die Weitergabe der Mail-Adresse ist dann als unbefugt anzusehen.

Verstöße müssen der Datenschutzaufsicht gemeldet werden

Die Folgen für das betroffene Unternehmen sind ausgesprochen unangenehm. Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass Datenschutzverstöße grundsätzlich der Datenschutzaufsicht zu melden sind. Dafür gibt es auf den Internetseiten der Aufsichtsbehörden sogar eigene Meldeformulare.

Ausnahmen von dieser Meldepflicht gibt es nur dann, wenn nicht mit einer Beeinträchtigung berechtigter Interessen zu rechnen ist. Diese Ausnahmen greifen hier aber nicht. Denn niemand kann ausschließen, dass offene Mail-Adressen missbraucht werden, für was auch immer. Ein Beispiel hierfür wäre die Zusendung unerwünschter Werbung. Alle im Unternehmen sollten deshalb genau beachten, wie sie mit Mailverteilern korrekt umgehen.

Was ist Scoring?

„Scoring-Verfahren" und „Score-Werte" sind aus der Wirtschaft nicht mehr wegzudenken. Meist geht es dabei um die Einschätzung der Kreditwürdigkeit. Und Kredit nimmt man viel häufiger in Anspruch, als vielen bewusst ist.

Kredit ist häufiger als zunächst vermutet

Wer bei einer Bank einen Ratenkredit aufnimmt, ist sich darüber klar: Den Kredit bekommt er von der Bank nur, wenn er auch kreditwürdig ist. Aber wenn er mit einem Händler eine Ratenzahlung vereinbart, gilt das genauso. Und wer einen Handyvertrag abschließt, nimmt ebenfalls Kredit in Anspruch. Schließlich zahlt er die Rechnung immer erst im Nachhinein.

Die Kreditwürdigkeit ist ein wichtiger Aspekt

Wer Kredit gewährt, steht vor dem Problem, die Kreditwürdigkeit seines Vertragspartners zuverlässig einzuschätzen. Das bloße Bauchgefühl ist dabei ein schlechter Ratgeber. Nötig sind rationale Kriterien, die sich objektiv nachvollziehen lassen.

Score-Werte ermöglichen objektive Aussagen

An dieser Stelle kommen Score-Werte ins Spiel. Sie knüpfen an Tatsachen an, die Rückschlüsse auf die Kreditwürdigkeit erlauben. Hierzu ein Beispiel: Wer in einem unbefristeten Arbeitsverhältnis steht, wird seltener zahlungsunfähig als jemand, dessen Arbeitsverhältnis befristet ist. Ob diese Aussage stimmt, muss der Kreditgeber im Ernstfall mit statistischen Methoden nachweisen.

Sie müssen auf aussagekräftigen Tatsachen beruhen

Aus der Sicht des Datenschutzes ist zunächst wichtig, welche Tatsachen in einen Score-Wert einfließen dürfen. Stets muss es sich um Faktoren handeln, deren Eignung sich nachprüfen lässt. Praktisches Beispiel: frühere Kredite, die der Kreditnehmer ordnungsgemäß zurückgezahlt hat.

Es dürfen aber auch allgemeine Erfahrungen einfließen. So wäre es etwa denkbar, dass Hauseigentümer Kredite zuverlässiger zurückzahlen als Personen, die keine Hauseigentümer sind. Genausogut könnte es aber umgekehrt sein. Grund hierfür könnte sein, dass Hauseigentümer wegen der Belastungen durch das Haus über weniger Geld verfügen. Wie auch immer: Solche Aussagen müssen sich mit statistischen Mitteln begründen lassen.

Diskriminierungen sind verboten

Äußerst umstritten ist es, ob berücksichtigt werden darf, in welchem Stadtviertel oder in welcher Straße jemand wohnt. Ein solcher Ansatz kann schnell zu einer unzulässigen Diskriminierung führen.

Besonders deutlich wird dies an folgendem Beispiel: In einem bestimmten Haus wohnen mehrere Personen, die in der Vergangenheit Kredite nicht ordnungsgemäß zurückgezahlt haben. Jemand zieht neu in dieses Haus. Der Rückschluss, dass auch diese Person Kredite nicht ordnungsgemäß zurückzahlen wird, würde sie unzulässig diskriminieren

Ein Score-Wert ist ein Punktwert

Für jedes einzelne Merkmal der Kreditwürdigkeit werden Bewertungspunkte vergeben. Die Summe dieser Bewertungspunkte ist der Score-Wert. Der Kreditgeber entscheidet, wie hoch der Wert sein muss, damit er noch einen Kredit gewährt. Hier darf jeder Kreditgeber seine eigenen Maßstäbe anlegen. Welches Risiko er noch eingehen will und welches nicht mehr, ist Teil seiner Geschäftspolitik.

Auskunfteien berechnen ihn als Dienstleister

Die wenigsten Kreditgeber berechnen Score-Werte selbst. Dazu fehlt ihnen in aller Regel das Know-how. Sie schalten deshalb Auskunfteien als Dienstleister ein. Sehr bekannt ist in diesem Zusammenhang die SCHUFA. Es gibt aber auch kleinere Auskunfteien, die beispielsweise nur für bestimmte Branchen tätig sind.

Die Rechtsprechung zu Auskunfteien ist detailliert

Das Geschäftsmodell der Auskunfteien ist vom Grundsatz her datenschutzrechtlich in Ordnung. Sie müssen jedoch eine Vielzahl von Grundsätzen beachten, die sich aus Entscheidungen von Gerichten ergeben. Das gilt beispielsweise dafür, wie lange negative Tatsachen berücksichtigt werden dürfen. Auch hier gibt es so etwas wie ein Recht auf Vergessen. Zu früh darf dieses Vergessen aber nicht einsetzen. Sonst gefährdet das die berechtigten Interessen von Kreditgebern.

Betroffene haben Anspruch auf Auskunft

Wer von einem Score-Wert betroffen ist, kann Auskunft über den Score-Wert verlangen. Er kann auch Auskunft darüber verlangen, welche Tatsachen verwendet wurden, um den Score-Wert zu ermitteln. Die Berechnungsmethode im Einzelnen zählt allerdings zu den Geschäftsgeheimnissen. Darüber kann eine betroffene Person keine Auskunft verlangen. Score-Werte werden jedes Jahr millionenfach erstellt. Gemessen daran gibt es erfreulich wenige berechtigte Beschwerden.

Gesichtserkennung, Fingerscan & Co.: Bequem, aber nicht ohne Risiko

Passwörter muss man sich merken, seine Fingerabdrücke nicht. Entsprechend beliebt sind biometrische Verfahren bei der Anmeldung für Geräte und Applikationen. Doch der Datenschutz warnt davor, Biometrie vorschnell einzuführen. Warum eigentlich?

Werden Passwörter bald überflüssig?

In einer Umfrage von Cisco unter 500 Anwenderinnen und Anwendern zeigte sich, dass Fingerabdrücke ein beliebter Ersatz für Passwörter sind. Mehr als die Hälfte (55 Prozent) fühlt sich wohl dabei, den Fingerabdruck für den Zugang zu einem Online-Konto zu verwenden. 40 Prozent haben nichts gegen eine Gesichtserkennung einzuwenden.

Tatsächlich ersetzen Unternehmen den Passwortschutz zunehmend durch andere Sicherheitsverfahren. Das gilt vor allem für die Nutzung der Biometrie in Form von Fingerabdrücken und Gesichtserkennung. Smartphones und andere mobile Endgeräte haben Funktionen zur Anmeldung über Fingerabdruck oder Gesichtserkennung gleich an Bord. Entsprechend häufig erfolgt auch die Anmeldung darüber, wenn sich Beschäftigte im Homeoffice befinden oder unterwegs arbeiten.

Laut einer Umfrage der FIDO Alliance unter 1.000 befragten Deutschen gelten biometrische Verfahren nicht nur als bequem, sondern auch als sicherste Art der Identitätsprüfung. Viele Studien gehen deshalb davon aus, dass Passwörter kaum noch eine Zukunft haben, die Biometrie wird sie ersetzen.

Sollte sich der Datenschutz darüber nicht freuen, wo doch so große Probleme mit ausreichend starken Passwörtern bestehen? Ja und nein, lautet die Antwort.

Passwörter kann man tauschen, Fingerabdrücke nicht

Wollen Unternehmen biometrische Lösungen einsetzen, fordert der Datenschutz, die Risiken genau zu prüfen. Dafür gibt es gute Gründe: Biometrische Daten und ihre Analyse eignen sich zwar sehr gut als Identitätsnachweis. Gelangen biometrische Daten aber in die falschen Hände, lassen sie sich für einen Identitätsdiebstahl nutzen.

Haben Angreifer Passwörter gestohlen, kann und muss man sie ersetzen. Bei biometrischen Merkmalen wie den Fingerabdrücken oder dem Gesicht kann man jedoch nicht beliebig neue, eindeutige Kennzeichen wählen. Man hat nur ein Gesicht und eine begrenzte Zahl von Fingerkuppen.

Biometrische Daten lassen sich missbrauchen

Im Gegensatz zu einem Passwort, das sich bekanntlich nicht mit der jeweiligen Person in Verbindung bringen lassen sollte, also zum Beispiel nicht den Namen enthalten soll, haben biometrische Daten sehr wohl mit der Person zu tun. So lässt sich ein Gesichtsausdruck nicht nur nutzen, um eine Person zu identifizieren. Es sind auch weitere Analysen möglich, wie eine Studie des EU-Parlaments warnt. So könnten sich darüber zum Beispiel menschliche Zustände der betroffenen Person leichter identifizieren lassen, wie Angst, Müdigkeit oder Krankheit, so die Studie.

Biometrie erfordert hohe Sicherheit

Wer also den Komfort einer Anmeldung über Gesichtserkennung oder Fingerabdruck nutzen will, muss das Verfahren besonders gut absichern. Das will der Datenschutz sicherstellen, um Missbrauch zu verhindern. Aus diesem Grund fordert der Datenschutz eine Prüfung vor der Einführung von Biometrie – nicht um die Passwort-Probleme zu erhalten, sondern um die Daten der betroffenen Personen zu schützen.

Denken Sie deshalb auch bei privater Nutzung von Fingerscan und Gesichtserkennung daran, nicht einfach jedes Verfahren zu verwenden. Stehlen Angreifer Ihre biometrischen Muster, sind Ihre privaten und beruflichen Zugänge in Gefahr, wenn sie durch Biometrie geschützt werden.

Kennen Sie die Risiken der Biometrie? Machen Sie den Test!

Frage: Die Erkennung von Fingerabdrücken ist sicher, denn einen Fingerabdruck kann niemand fälschen. Stimmt das?

1. Nein, man muss Fingerabdrücke nämlich nicht fälschen, um eine Identität vorzutäuschen. Man kann die Muster der Fingerabdrücke auch stehlen, um sie zu missbrauchen.
2. Ja, Fingerabdrücke sind im Gegensatz zu Passwörtern absolut sicher.

Lösung: Die Antwort 1. ist richtig. Aus den Fingerabdrücken der Nutzerinnen und Nutzer werden bei biometrischen Anmeldeverfahren Muster errechnet und gespeichert. Gelingt es einem Angreifer, diese errechneten Muster zu stehlen, kann er die biometrische Überprüfung der Identität täuschen und die Identität der Person übernehmen. Biometrische Verfahren müssen deshalb gegen Angriffe abgesichert sein.

Frage: Biometrische Daten lassen sich nicht für andere Zwecke missbrauchen. Stimmt das?

1. Ja, man nutzt die Fingerabdrücke und die Gesichtserkennung nur, um die Identität einer Person zu prüfen.
2. Nein, biometrische Kennzeichen können mehr über eine Person verraten als die zu prüfende Identität.

Lösung: Die Antwort 2. ist richtig. So kann man zum Beispiel aus einem Gesichtsausdruck mittels Analyse versuchen, Rückschlüsse auf Stimmungen, auf das Alter oder auf Anzeichen für Krankheiten zu ziehen. Biometrische Merkmale sind nicht nur ein möglicher Passwortersatz, sie sind Teil des menschlichen Körpers und können deshalb auch mehr über die Person aussagen als ein sinnvoll gewähltes Passwort, das bekanntlich keine personenbezogenen Angaben enthalten sollte.

Ein Tipp der Aufsichtsbehörden: Die grundlegende Frage, die Sie sich stellen sollten, ist die, ob Sie überhaupt dringend an Aufgaben mit personenbezogenen Daten arbeiten müssen. Wenn Sie zunächst an Aufgaben ohne Personenbezug und ohne andere sensible Daten arbeiten, können Sie sich an die neue Situation gewöhnen und Erfahrungen sammeln. Dann gewinnen Sie auch Zeit für die Umsetzung der Regeln.

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