SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

der Datenschutz berührt alle Bereiche unseres beruflichen und privaten Lebens. Das macht diese neue Ausgabe wieder sehr deutlich. Ob Sie in ein Parkhaus einfahren, in dem es kein Parkticket gibt und stattdessen die Kennzeichen erfasst werden, oder ob es um neue technologische Entwicklungen rund um Künstliche Intelligenz (KI) geht, überall können personenbezogene Daten betroffen sein, die geschützt werden müssen.

Ihre neue Ausgabe behandelt neben modernen Parkhäusern und den Hinweisen zur Nutzung von KI auch Online-Shops und Web-Formulare, die nach persönlichen Daten fragen, mitunter mehr, als notwendig sind und als Sie preisgeben sollten.

Nicht zuletzt geht es auch um Cyberattacken und die Lehren aus einem solchen IT-Sicherheitsvorfall. Auch hier ist der Datenschutz aktiv und fragt nach, um die Privatsphäre der Betroffenen wirksamer zu schützen.

Seien Sie gespannt auf die Vielfalt, die der Schutz personenbezogener Daten mit sich bringt, im Alltag wie auch in Extremsituationen wie bei einem Cyberangriff!

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

August 2024

1 KENNZEICHENERFASSUNG BEIM PARKEN

Immer mehr Parkhäuser verzichten auf die klassischen Parktickets. Stattdessen erfassen sie bei der Einfahrt das Autokennzeichen. Ist das vom Datenschutz her so in Ordnung?

Das neue Verfahren ist sehr praktisch

Die Windschutzscheibe herunterfahren? Danach mühsame Verrenkungen, um an ein Parkticket zu kommen? Alles Vergangenheit! Stattdessen erfasst eine Kamera das Autokennzeichen. Dann hebt sich die Einfahrtsschranke. Vor dem Bezahlen am Automaten gibt man das Kennzeichen ein. An der Ausfahrt erkennt das System das Kennzeichen. Dann hebt sich die Ausfahrtschranke.

Kennzeichen sind pseudonym, aber personenbezogen

Ein Kfz-Kennzeichen gehört zu den pseudonymen Daten. Mit ihm allein lässt sich nicht feststellen, wer der Halter des Fahrzeugs ist. Aber die Datenbanken mit den Fahrzeughaltern enthalten die nötigen zusätzlichen Informationen, um es dem Fahrzeughalter zuordnen. Die rechtlichen Schranken für einen solchen Zugriff sind recht niedrig. Dies führt zu dem Ergebnis, dass Kfz-Kennzeichen als personenbezogen gelten.

Weitere personenbezogene Daten sind notwendig

Um die Parkgebühr berechnen zu können, muss das System Datum und Uhrzeit der Einfahrt genauso erfassen wie Datum und Uhrzeit der Ausfahrt. Auch diese Daten stellen personenbezogene Daten des Fahrzeughalters dar. Dies gilt selbst dann, wenn jemand anders als der Halter das Fahrzeug benutzt. Denn dann lässt sich aus ihnen ablesen, wann er einer anderen Person die Benutzung seines Autos erlaubt hat.

Die DSGVO ist anwendbar

Damit kommt die DSGVO ins Spiel. Sie gilt immer, wenn personenbezogene Daten verarbeitet werden. Eine Verarbeitung liegt dabei schon deshalb vor, weil das Autokennzeichen und die Verweildauer des Fahrzeugs im Parkhaus erfasst werden. Daran schließen sich weitere Verarbeitungsvorgänge an, insbesondere die Berechnung der Parkgebühr.

Eine Rechtsgrundlage ist notwendig

Rechtsgrundlage für die Verarbeitung der Daten ist der „Parkvertrag“. Ihm liegen meist Allgemeine Geschäftsbedingungen zugrunde. Sie müssen gut zugänglich aushängen, damit sie jeder lesen kann, bevor er ins Parkhaus einfährt. An der Einfahrtsschranke selbst müssen sie aber nicht angebracht sein. Denn sonst würden „eifrige Leser“ die Einfahrt immer wieder blockieren.

Der Grundsatz der Erforderlichkeit gilt

Die DSGVO lässt die Speicherung von Daten nur zu, soweit das erforderlich ist. Daraus folgt: Sobald die Parkgebühr ordnungsgemäß bezahlt ist und ein Fahrzeug das Parkhaus wieder verlassen hat, müssen die Daten gelöscht werden. Das bedeutet andererseits: Im Nachhinein kann auch keine Quittung mehr erstellt werden. Wer eine Quittung benötigt, muss sie gleich beim Bezahlen anfordern.

Umfangreiche Datenschutzinformationen sind geboten

Für die Datenschutzinformationen gelten die allgemeinen Regeln des Art. 13 DSGVO. Nötig ist also ein umfangreicher Aushang. Er muss unter anderem Namen und Kontaktdaten der verantwortlichen Stelle enthalten. Das ist für mögliche Beschwerden wichtig.

2 KI ALS DATENSCHUTZ-THEMA

Seit ChatGPT sind Systeme der Künstlichen Intelligenz, kurz: KI-Systeme, in aller Munde. Sobald sie personenbezogene Daten verarbeiten, kommt die DSGVO ins Spiel. Eine Orientierungshilfe der Datenschutzkonferenz (DSK) erläutert, worauf es in Unternehmen ankommt.

Der Personenbezug stellt die Weichen

Auch für KI-Systeme gilt DSGVO nur, wenn personenbezogene Daten verarbeitet werden. Das ist keineswegs immer der Fall. So können KI-Systeme etwa ausschließlich Daten aus Produktionsprozessen auswerten, die keinerlei Bezug zu menschlichem Tun haben. Das gilt etwa, wenn sie mögliche Ausfälle von Motoren erkennen sollen, bevor es zu einem Ausfall kommt. Dabei gilt es allerdings, genau hinzusehen. Denn oft erfassen die Systeme auch Daten der Menschen, die Maschinen bedienen. Dann geht es meist doch an irgendeiner Stelle um personenbezogene Daten.

Eine Gesamtbetrachtung ist notwendig

Um festzustellen, ob personenbezogene Daten im Spiel sind, ist eine Gesamtbetrachtung des KI-Systems notwendig. Dies beginnt mit der Anmeldung, um das System nutzen zu können. Oft ist eine persönliche Anmeldung vorgesehen, um Missbrauch durch Außenstehende zu verhindern. Dies ist völlig in Ordnung. Für diese Daten gilt dann allerdings die DSGVO. Auch die Daten, die in ein KI-System eingegeben werden, können personenbezogen sein. Zwingend ist das allerdings nicht. Die Ausgabedaten sind ebenfalls näher zu beleuchten. In manchen Fällen kann ein KI-System aus nicht personenbezogenen Daten im Ergebnis durchaus personenbezogene Daten generieren.

Manchmal bestehen Gestaltungsmöglichkeiten

Manche KI-Systeme verarbeiten nur wenige personenbezogene Daten und könnten bei genauer Betrachtung durchaus auch ohne diese Daten auskommen. In solchen Fällen kann es Sinn machen, die Daten mit Personenbezug aus den Eingabedaten „herauszufiltern“ und diese Daten nicht zu verwenden. Eine sorgfältige Dokumentation ist dabei notwendig, mag sie Mitarbeiter auch manchmal „nerven“. Denn immerhin geht es darum, ob die DSGVO zur Anwendung kommt oder nicht.

Geschlossene KI-Systeme sind laut DSK vorzuziehen

Großen Wert legt die DSK auf die Unterscheidung zwischen offenen und geschlossenen KI-Systemen. Diese Differenzierung ist außerhalb des Datenschutzes bisher eher wenig üblich. Ein geschlossenes System in diesem Sinn liegt vor, wenn die Kontrolle über alle Ein- und Ausgabedaten vollständig beim Anwender bleibt. Weitere Bedingung ist, dass der Systemanbieter die Daten nicht zum Training des Systems verwendet. Es geht also darum, dass die verantwortliche Stelle möglichst vollständig die „Herrin der Daten“ bleibt. Je nach Verwendungszweck des Systems lässt sich das praktisch umsetzen oder auch nicht.

Interne Vorgaben sind unbedingt zu beachten

Beim Einsatz von KI-Systemen herrscht oft eine gewisse Aufbruchsstimmung und das ist auch gut so. Dennoch haben Unternehmen gute Gründe, wenn sie beim Experimentieren mit solchen Systemen gewisse Grenzen setzen. Das kann auch auf Vorgaben des Datenschutzes zurückgehen. So darf ein KI-System Entscheidungen, die rechtliche Wirkungen gegenüber Menschen entfalten, nicht ausschließlich automatisiert treffen. Dies ergibt sich aus Art. 22 Abs. 1 DSGVO.

Das Personalwesen bietet ein lehrreiches Beispiel

Was damit gemeint ist, erläutert die DSK an einem Beispiel aus dem Personalwesen (siehe

Randnummer 13 der Orientierungshilfe). Dort könnte jemand auf die Idee kommen, die Auswertung aller eingegangenen Bewerbungen einem KI-System zu überlassen. Ein solches System wäre ohne weiteres imstande, auf der Basis vorgegebener Kriterien selbst zu entscheiden, wer dann zu einem Vorstellungsgespräch eingeladen wird und wer nicht. Das mag vielleicht der Traum gestresster Personalstellen sein. Es verstößt jedoch eindeutig gegen die DSGVO. Denn schon wegen möglicher Diskriminierungen ist bereits die Einladung zu einem Vorstellungsgespräch rechtlich relevant.

Im Zweifel sollte man fragen und reden

Angesichts solcher Beispiele ist die Gefahr groß, dass der Datenschutz wie ein „Bremser der KI“ wirkt. Eine solche Sichtweise würde freilich ausblenden, dass nur rechtskonforme KI-Systeme ein Unternehmen voranbringen können. Deshalb gilt: Gerne kreativ sein, aber sich dann dem rechtlichen Realitätscheck stellen! Zeigen sich dabei Hürden, ist eben erneute Kreativität gefragt!

Die Orientierungshilfe ist hier zu finden

Wer den Fragen des Datenschutzes bei KI-Systemen selbst auf den Grund gehen will, findet die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ der DSK vom 6. Mai 2024 hier: https://datenschutzkonferenz-online.de/orientierungshilfen.html.

3 DATENMINIMIERUNG GANZ PRAKTISCH: WARUM WILLST DU DAS WISSEN?

Bei Registrierungen oder Bestellungen im Internet werden viele Informationen abgefragt. Doch nicht alle diese Daten werden dafür wirklich benötigt. Seien Sie deshalb kritisch, wenn Sie Angaben auf Webseiten machen sollen, aber nicht nur dann.

(K)eine Frage des Alters

Stellen Sie sich vor, Sie möchten im Internet etwas bestellen, das erst für Personen ab 18 Jahren zugänglich sein darf. Dann wird auf der Webseite nach Ihrem Alter gefragt. Doch muss der Betreiber der Webseite dafür wissen, wann Sie genau Geburtstag haben? Schließlich erwarten Sie keine Glückwünsche an diesem Tag, sondern Sie wollen nur etwas bestellen.

In der Praxis fragen aber viele Webshops oder andere Online-Dienste nach dem genauen Geburtstag. Die Angabe in den Online-Formularen ist dann nicht freiwillig, sondern ein Pflichtfeld. Die Datenschutzaufsichtsbehörde in Niedersachsen hat nun darauf hingewiesen, dass das Geburtsdatum als Pflichtfeld in Webshops oft rechtswidrig ist.

Die „neugierige“ Online-Apotheke

Beim Einkaufen in Online-Shops darf also im Rahmen eines Bestellprozesses nicht ohne Weiteres das Geburtsdatum als zwingende Angabe abgefragt werden. Dahinter steckt der Grundsatz der Datenminimierung, nach dem die Verarbeitung auf das notwendige Maß zu beschränken ist. Man darf also keine Daten abfragen, die für den jeweiligen Zweck, zum Beispiel die Bestellung, nicht erforderlich sind.

Im Beispiel einer Online-Apotheke aus Niedersachsen erfolgte die Abfrage des Geburtsdatums unabhängig von der Art der bestellten Ware, also nicht nur bei Medikamenten, sondern auch bei allgemeinen Drogerie-Produkten.

Die Datenschutzaufsicht Niedersachsen stellt klar: Die Verarbeitung des Geburtsdatums ist

datenschutzrechtlich üblicherweise nicht zur Erfüllung eines Vertrags erforderlich. Selbst für eine Prüfung, ob Minderjährige im Webshop bestellen und der Vertrag daher schwebend unwirksam sein könnte, kann der Betreiber die Volljährigkeit abfragen und benötigt nicht das genaue Geburtsdatum.

Betreiber von Webshops sollten überprüfen, ob sie im Bestellprozess das Geburtsdatum als zwingende Angabe abfragen, und zu welchen Zwecken und auf welcher Rechtsgrundlage dieses verarbeitet wird.

Sollte die Abfrage nur auf die Einwilligung als Rechtsgrundlage gestützt werden können, ist das entsprechende Eingabefeld im Bestellformular eindeutig als „freiwillig“ zu kennzeichnen und die Kundinnen und Kunden sind über die Verwendung dieses Datums umfassend zu informieren. Geben diese kein Geburtsdatum an, muss der Bestellprozess fortgesetzt werden können.

Doch nicht nur die Betreiber von Webseiten sollten die Pflichtfelder in ihren Online-Formularen genau hinterfragen, auch jede Nutzerin und jeder Nutzer sollte dies tun.

Datenminimierung ist die Sparsamkeit mit Ihren Daten

Pflichtfelder in Online-Formularen sollten nicht einfach ausgefüllt werden, nur weil das Feld als verpflichtend gekennzeichnet wird. Geben Sie immer nur so viele Daten an, wie wirklich notwendig sind. Seien Sie also sparsam mit Ihren Daten. Der Grundsatz der Datenminimierung wurde aus gutem Grund früher auch als Datensparsamkeit bezeichnet.

Nun haben digitale Informationen die Eigenschaft, dass sie nicht „weg“ sind, wenn man sie weitergegeben hat. Bei physischen Gütern wie zum Beispiel Bargeld ist dies bekanntlich anders. Aber nur weil die Weitergabe von Daten den eigenen Bestand an Daten nicht verringert, bedeutet das nicht, dass Sie nicht sparsam sein sollten.

Die Stelle, der Sie Ihre personenbezogenen Daten gegeben haben, obwohl dies zum Beispiel für die Durchführung der Online-Bestellung gar nicht notwendig wäre, könnte mit den Daten etwas tun, was nicht in Ihrem Sinne ist. Zum Beispiel könnten die Daten für ungewollte Werbung missbraucht oder an Dritte weiterverkauft werden.

Kritisches Hinterfragen ist angebracht

Wenn Sie also das nächste Mal ein Online-Formular vor sich haben, überlegen Sie genau:

- Was möchte ich mit dieser Registrierung, mit diesem Online-Formular erreichen?
- Muss die Stelle, die nach den Daten fragt, zum Beispiel meine Postadresse wissen, wenn ich einen E-Mail-Newsletter bestellen will?
- Sind also Pflichtfelder in dem Online-Formular vorgesehen, die wenn überhaupt freiwillige Angaben sein sollten?

Stellen Sie fest, dass Daten als Pflichtfelder vorgesehen sind, obwohl die Informationen nicht notwendig erscheinen, verzichten Sie lieber auf den Newsletter oder die Registrierung. Seien Sie aber auch nicht zu freizügig mit Ihren Daten, wenn Eingabefelder auf Webseiten als freiwillig gekennzeichnet sind. Auch freiwillige Angaben lassen sich zweckentfremden und missbrauchen.

Nicht zuletzt sollten Sie nicht nur im Internet an Datenminimierung oder Datensparsamkeit denken. Auch bei Telefonaten, in klassischen Briefen oder bei Gesprächen sollten Sie nicht zu viel von sich verraten. Auch hier ist Vorsicht angezeigt. Es ist richtig, wenn Sie nachfragen, warum jemand etwas wissen will, was Ihnen merkwürdig verkommt, da es die andere Person doch eigentlich gar nicht wissen muss. Es ist kein falsches Misstrauen, sondern die richtige und notwendige Vorsicht, die Sie walten lassen sollten.

4 NACH DER CYBERATTACKE: ALLES BEIM ALTEN?

Viele Unternehmen erhöhen ihre Sicherheitsmaßnahmen erst nach einem erfolgreichen Cyberangriff. Doch Cyberattacken sind keine Warnschüsse, die zeigen sollen, dass es ernst werden kann. Aber man muss aus dem Schaden lernen, denn die nächste Attacke kommt bestimmt.

Internetkriminelle sind Wiederholungstäter

Durch die Digitalisierung wird vieles leichter, Aufwände können reduziert werden. Was für Unternehmen und Verwaltungen gilt, stimmt leider auch für die Cyberkriminellen. Anstatt in eine gut gesicherte Bank einzubrechen, versuchen sie, an das Geld direkt bei den digitalen Kontakten zwischen Bankkundinnen und -kunden mit der Bank zu gelangen. Das ist mit weitaus weniger Aufwand verbunden. Damit ist es auch möglich, viel mehr Angriffsversuche zu starten, denn die laufen inzwischen nahezu automatisiert ab.

Selbst gezielte Online-Attacken machen nicht mehr so viel Aufwand. Insbesondere die Möglichkeiten von KI (Künstliche Intelligenz) machen es einfach, die Opfer besser auszuspionieren und die Attacken sehr genau zu personalisieren.

Deshalb machen Internetkriminelle auch nicht nur einige wenige Angriffe auf Unternehmen und Behörden, sondern sie attackieren ihre Ziele fortlaufend und auf lange Dauer. Die Bedrohungen sind fortgeschritten und persistent, man spricht von Advanced Persistent Threats (APTs).

Kennen Sie die Risiken durch weitere Cyberangriffe?

Die Lösungen finden Sie am Ende des Beitrags.

Frage 1: Wer einmal angriffen wurde, wird wahrscheinlich so schnell kein Ziel mehr sein. Stimmt das?

1. Nein, im Gegenteil. Erfolgreiche Attacken können schnell den nächsten Angriff nach sich ziehen.

2. Ja, bei der Vielzahl möglicher Opfer sind dann aus Wahrscheinlichkeitsgründen erst einmal die anderen dran.

Frage 2: Wenn man nach einer Ransomware-Attacke das Lösegeld bezahlt hat, ist das Risiko gebannt. Stimmt das?

1. Ja, die Angreifenden haben ja bekommen, was sie wollen.
2. Nein, man macht sich dadurch sogar für weitere Attacken noch interessanter.

Datenschutzaufsicht macht Nachprüfungen

Aus gutem Grund hat zum Beispiel das Bayerische Landesamt für Datenschutzaufsicht eine sogenannte „Ransomware FollowUp Prüfung“ gestartet, bei der insbesondere solche Unternehmen geprüft werden, die bereits einmal Opfer einer solchen Attacke mit Erpresser-Schadsoftware geworden sind.

So schreibt die Aufsichtsbehörde, dass man davon ausgeht, dass Unternehmen, die in den letzten Jahren einen Ransomware-Vorfall gemeldet haben, im Rahmen der Aufarbeitung des Vorfalls ihrerseits die Sicherheitsmaßnahmen ausgeweitet oder zumindest angemessen angepasst haben. Im Rahmen der Ransomware-Nachprüfung möchte die Aufsichtsbehörde nun den aktuellen Sicherheitsstand diesbezüglich abfragen.

Unter anderem fragt die Datenschutzaufsicht nach dem Patchmanagement, das sicherstellen soll, das Sicherheitslücken erkannt und ge-

schlossen werden, nach den System-Berechtigungen, die genau geregelt und sinnvoll begrenzt werden sollen, nach IT- und Sicherheitssystemen, die so eingestellt sein sollen, dass mögliche Angriffe besser und schneller erkannt werden, um einige Beispiele zu nennen.

Viele der Punkte, die die Datenschutzaufsicht nochmals kontrollieren will, betreffen die IT- und die IT-Sicherheitsabteilung, aber auch jede Nutzerin und jeder Nutzer ist gefragt.

Die meisten Angriffe erfolgen über uns Menschen

Damit die IT-Sicherheit nach einer Cyberattacke besser wird und der nächste Angriff möglichst keinen Erfolg mehr hat, müssen alle Beschäftigten aus dem Vorfall lernen. Allein eine verbesserte technische Sicherheit reicht nicht, denn die Angriffe starten sehr oft mit einer E-Mail oder anderen Nachricht, mit der wir Menschen getäuscht werden sollen. Ein angeklickter Link, eine heruntergeladene Datei, eine scheinbar harmlose Aktivität am PC oder Smartphone kann bereits der Beginn der nächsten erfolgreichen Attacke sein.

Das ganze Unternehmen muss aus einem Vorfall lernen, nicht nur die IT oder IT-Sicherheit. Es muss klar sein, was bei dem letzten Vorfall ausgenutzt wurde, wie man sich hätte besser verhalten können. Fehler passieren, aber wir müssen aus ihnen lernen. Angriffe passieren ebenso, und wir müssen aus ihnen lernen. Wir müssen in jedem Fall wissen, wie wir richtig reagieren, wenn es zu einem Sicherheitsvorfall gekommen ist. Dazu gehört es, den Vorfall richtig zu melden und nicht etwa etwas zu verheimlichen, was falsch gelaufen ist. Sonst lernen nur die Angreifenden dazu!

Und hier die Lösungen für die Quizfragen

Lösung Frage 1: Die Antwort 1. ist richtig. Wer erfolgreich angriffen wurde, hat den Internetkriminellen eine Verwundbarkeit gezeigt. Wenn die ausgenutzten Schwachstellen nicht umgehend erkannt und beseitigt werden, ist es wahrscheinlich, dass die gleiche Sicherheitslücke nochmals ausgenutzt wird.

Lösung Frage 2: Die Antwort 2. ist richtig. Wer Lösegeld bezahlt, finanziert zum einen weitere Angriffe, deshalb raten alle Sicherheits- und Polizeibehörden davon ab, bei Ransomware-Attacken zu bezahlen. Zudem wird man ein besonders interessantes Ziel, denn man hat offenbart, dass man bereit ist, auf eine Online-Erpressung einzugehen. Weitere Angriffe können also schon bald kommen.

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de