Newsletter Datenschutz

Ausgabe 10 | 2022

Die Datenschutz-Folgenabschätzung – ein spezieller Anwendungsfall der Risikoanalyse –

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,

„Welche Folgen kann das für den Datenschutz haben?“ Das sollten Sie sich weitaus häufiger fragen, als dies vermutlich heute geschieht. So kann selbst ein kaputter USB-Stick noch Daten preisgeben, obwohl Sie glauben, er sei nur noch etwas für die Mülltonne.
Auch das Nachverfolgen der Online-Aktivitäten mittels Cookies und anderer Tracking-Verfahren kann weitaus mehr ermöglichen als personalisierte Internetwerbung. Daher erklärt diese Ausgabe die häufig übersehenen Risiken durch Online-Tracking ebenso wie den richtigen Umgang mit defekten USB-Speicherstiften.
Wie ein weiterer Artikel zeigt, hilft eine sogenannte Datenschutz-Folgenabschätzung, die Auswirkungen einer Datenverarbeitung auf die Privatsphäre besser zu verstehen. Ein klarer Blick auf den Datenschutz ist auch erforderlich bei der Nutzung von Wildkameras in Wald und Flur. Sie hat ebenfalls mehr Folgen, als Sie wahrscheinlich denken.

Ich wünsche Ihnen viel Spaß beim Lesen!

Ihr Frank Berns, Datenschutzbeauftragter

Nicht einfach wegwerfen: Kaputte USB-Sticks

Erkennt der Computer den USB-Stick nicht mehr oder ist gar das Stick-Gehäuse defekt, landet das beliebte Speichermedium schnell im Müll. Doch oftmals sind die Daten auf dem Stick noch lesbar – ein unterschätztes Datenrisiko!

Der Sturz vom Schreibtisch

Manche Berichte von Dienstleistern, die sich auf Datenrettung spezialisiert haben, klingen abenteuerlich, sind aber wahr: „Der Hund hat meinen USB-Stick gefressen! – Ein Hund erlebte eine metallische Überraschung, als er einen USB-Stick mit seinem Lieblingskauspielzeug verwechselte – mit dem Ergebnis, dass der USB-Stick unlesbar wurde“.

Doch es müssen nicht die Haustiere sein, die zu scheinbar defekten USB-Sticks beitragen. Es kann bereits ein Sturz des Speicherstifts vom Schreibtisch auf einen harten Boden reichen, wenn es kein besonders stabiles Modell ist.

KONTAKT zu uns MAIL@Konzept17.de

Ganz gleich, welche Ursache es hat: Viele kennen das Problem, dass sie einen USB-Stick an den Rechner anstecken und der Rechner das Medium nicht mehr erkennt und anzeigt. Vielleicht hat sogar das Gehäuse einen Sprung. Was tun? Ab in den Müll? Lieber nicht!

Von Datenrettern und Datendieben

Tatsächlich lassen sich viele kaputte USB-Sticks noch auslesen, die Daten darauf retten. Sowohl für Privatpersonen als auch für Unternehmen gibt es Datenrettungslösungen, die die verloren geglaubten Daten in vielen Fällen wieder zum Vorschein bringen. Je nach Problem mit dem Speichermedium nennen Datenretter durchaus Erfolgsraten von 90 Prozent.

Leider können aber nicht nur seriöse Datenretter die Inhalte von defekten USB-Sticks wiederherstellen, das können auch Datendiebe. Ob der USB-Stick einen Elektronikfehler hat, es einen Wasser- oder Brandschaden gab, der Stick abgebrochen ist oder die Firmware des Speicherstifts nicht mehr funktioniert: In vielen Fällen gelangen sowohl Datenretter als auch Datendiebe noch an die Daten.

Datendieben ist kaum etwas zu teuer

Die professionelle Datenrettung ist durchaus kostspielig. Je nach betroffenen Daten aber wird man als Privatperson oder Unternehmen bereit sein, den Service zu beauftragen. Datendiebe jedoch verdienen so viel an gestohlenen Daten, dass sie den Aufwand nicht scheuen, wenn ein spannend erscheinender USB-Stick einer Firma im Müll zu finden ist.

In aller Regel übersteigt der Wert der Daten den Geldbetrag, den die Anschaffung des USB-Sticks gekostet hat, um ein Vielfaches. Deshalb sind auch USB-Sticks mit defektem Gehäuse ein beliebtes Diebesgut.

Auch kaputte Sticks müssen zerstört werden

Sind also die Daten auf einem defekten Stick noch als Kopie oder Backup anderweitig verfügbar und macht somit eine Datenrettung für den Stick keinen Sinn, werfen Sie trotzdem den kaputten USB-Speicherstift nicht in den Müll.

Aus gutem Grund sollten Sie Dokumente und Datenträger mit zu schützenden Daten datenschutzgerecht entsorgen. Im Unternehmen regelt dies meist eine entsprechende Richtlinie. Halten Sie es privat ebenso, dass Sie wichtige Dokumente und Speichermedien nicht einfach wegwerfen, wenn sie Sie nicht mehr benötigen oder sie kaputt aussehen.

Selbst kaputte Speichermedien müssen noch einer sicheren Entsorgung zugeführt werden, also so zerstört werden, dass selbst Datenretter und damit auch Datendiebe keine Chance mehr haben. Ein schlichter Hammer oder Bohrer hat da schon so manch guten Dienst geleistet …

Kameras in Wald und Flur

Schon manche Spaziergängerin war ebenso verblüfft wie ihr Begleiter: Tief im Wald stießen sie auf eine „Wildkamera“. Ein Thema für den Datenschutz oder eher etwas für eine Jagdversammlung? Die DSGVO gilt auch in Wald und Flur! Aber sie schützt nicht gegen alles.

Das Betretungsrecht ist genau geregelt

Deutschland ist ein Land der Regeln. Deshalb verwundert es nicht, dass das Betreten von Feld, Flur und Wald gesetzlich geregelt ist. Und zwar fein säuberlich getrennt nach Feld und Flur einerseits und Wald andererseits:

- Das Betreten der freien Landschaft ist ein Thema des Bundesnaturschutzgesetzes. Es erlaubt allen, die sich erholen wollen, dies in der freien Landschaft zu tun. Dabei müssen sie sich allerdings an die Straßen und Wege halten und dürfen nicht quer über bestellte Felder trampeln. Abgeerntete Felder wiederum dürfen betreten werden.
- Das Betreten des Waldes ist laut Bundeswaldgesetz im Prinzip überall erlaubt. Allerdings können die Bundesländer für bestimmte Bereiche Betretungsverbote festlegen. Sie sollen beispielsweise neu angelegte Pflanzungen schützen.

Aufnahmen sind grundsätzlich nicht erlaubt

Das hat mehr mit dem Datenschutz zu tun, als es zunächst scheint. Denn wer das Recht hat, einen bestimmten Bereich zu betreten, muss nicht damit rechnen, dass er dabei gefilmt wird. Hier gilt in Feld, Wald und Flur dasselbe wie in der Stadt: Private Kameras, die öffentlich zugängliche Räume filmen oder fotografieren, verstoßen im Regelfall gegen den Datenschutz.

Ausnahmen bei berechtigten Interessen gibt es jedoch

Wo eine Regel ist, ist die Ausnahme meist nicht weit. So auch hier. Im Einzelfall kann es berechtigte Interessen geben, die Aufnahmen zulässig machen. Wer sich darauf beruft, muss dies konkret begründen können. Das allein genügt aber noch nicht. Vielmehr ist außerdem abzuwägen, ob möglicherweise die Interessen der Personen, die gefilmt werden, schwerer wiegen. So regelt es Art. 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DSGVO).

Reine Neugier ist kein berechtigtes Interesse

Dies hört sich zunächst recht abstrakt an. Einige Beispiele zeigen aber schnell, was das in der Praxis bedeutet:

Ein Jäger, der einfach nur wissen will, was im Wald los ist, darf mit dieser Begründung keine Kamera im Wald aufhängen. Schließlich ist der Wald weder sein Wohnzimmer noch sein privater Garten, sondern eine öffentlich zugängliche Fläche.

Auch der Wunsch eines Jägers, das Wild an einem Platz für die Wildfütterung zu beobachten, rechtfertigt dort keine Kamera. Dass bei Wikipedia unter dem Stichwort „Kirrung“ (einem Wort aus der

Jägersprache für „Futterplatz“) das Gegenteil steht, hat keine Bedeutung. Es zeigt nur, wie verbreitet diese Praxis ist.

Naturschutz kann ein guter Grund für Aufnahmen sein

Anders sieht es wiederum aus, wenn in Absprache mit den Naturschutzbehörden festgestellt werden soll, ob es in einem bestimmten Bereich tatsächlich Wölfe oder andere geschützte Tiere gibt. Das geht nicht ohne „Fotofallen“.

Es kommt auch auf die Modalitäten an

Auch wenn eine Kamera zulässig ist, ist deshalb keineswegs „alles erlaubt“. So sind „bewegte Bilder“, also Videosequenzen, meistens nicht erforderlich. Einzelbilder, die jeweils im Abstand von einigen Sekunden aufgenommen werden, zeigen Tiere oft sogar viel genauer. Häufig genügen auch Aufnahmen während der Nacht, weil sich bestimmte Tiere nur nachts bewegen. Dann ist die Kamera entsprechend einzustellen. Kaum jemand wird tief in der Nacht mitten im Wald spazieren gehen. Dass die Aufnahmen Menschen erfassen, ist deshalb nachts nicht zu erwarten.

Grillstellen und Spielplätze sind tabu

In Bereichen rund um Grillstellen und Spielplätze sind Kameras generell unzulässig. Solche Einrichtungen sind ausdrücklich für die Benutzung durch Menschen gedacht. Mit deren berechtigten Interessen verträgt es sich nicht, dort zu filmen oder zu fotografieren.

Informationspflichten gelten auch in Wald und Flur

Wer in zulässiger Weise eine Kamera irgendwo in der Landschaft anbringt, muss selbstverständlich die Informationspflichten beachten, die Art. 13 DSGVO vorgibt. Dies bedeutet: An der Kamera muss sich gut sichtbar ein Hinweis befinden, der unter anderem den Namen und die Kontaktdaten des Verantwortlichen nennt. Hier gilt dasselbe wie bei einer Kamera an einem Laden in der Stadt.

Jägerinnen und Jäger kennen die Regeln

Manche argwöhnen, das alles sei doch reichlich Theorie, und in der Praxis würden Jägerinnen und Jäger sowieso machen, was sie wollen. Das stimmt auf keinen Fall! Gerade dieser Personenkreis ist es gewohnt, zahlreiche Rechtsvorschriften zu beachten. Die DSGVO ist dabei nur eine von vielen.

Die Datenschutz-Folgenabschätzung

Risikoanalysen vielfacher Art gehören zum Alltag in Unternehmen. Die Datenschutz-Folgenabschätzung (DSFA) ist ein spezieller Anwendungsfall der Risikoanalyse. Ein Thema nur für Spezialisten? Keineswegs!

„TOMs“ sollen Schaden vermeiden

Daten dürfen weder versehentlich gelöscht werden, noch dürfen sie in falsche Hände geraten. Aber wie lässt sich das sicherstellen? Technische Maßnahmen, etwa die Verschlüsselung von Daten, können ein wichtiger Baustein sein. Ähnliches gilt für organisatorische Maßnahmen wie etwa sichere Türschlösser. Zusammenfassend spricht man in der Praxis oft von „TOMs“, also den technischen und organisatorischen Maßnahmen.

Eine Risikoanalyse steht am Anfang

TOMs kosten meistens Geld, manchmal sogar viel Geld. Schon deshalb gilt der Grundsatz: So viel wie nötig davon, aber nicht unnötig viel! Was nach den konkreten Umständen erforderlich ist, ergibt sich aus einer Risikoanalyse. Unter der Bezeichnung „Datenschutz-Folgenabschätzung" ist sie in der DSGVO vorgeschrieben. Über kurz oder lang wird jeder, der Daten verarbeitet, damit konfrontiert.

Auch scheinbar harmlose Daten können brisant sein

Häufig hört man in Unternehmen Aussagen wie: „Jedenfalls unsere Abteilung hat nur mit harmlosen Daten zu tun. Außer Adressen von Kunden und Angaben zu den Bestellungen dieser Kunden haben wir nichts." Eine Risikoanalyse ist auch dann nicht entbehrlich. Beispielsweise sind Kundenadressen manchmal Adressen von gefährdeten Personen. Das kommt sicher nicht häufig vor. Aber wenn doch, können zusätzliche Sicherungsmaßnahmen notwendig sein.

Die Mitarbeit aller im Unternehmen ist unentbehrlich

Niemand im Unternehmen sollte genervt sein, wenn ihm Datenschutzverantwortliche scheinbar banale Fragen stellen. Nur wer selbst mit den Daten umgeht, weiß im Detail, welche Art von Daten das sind und wo ein Gefahrenpotenzial für den Datenschutz stecken kann. Das Nachdenken darüber lässt sich nicht auf andere „abschieben".

Manche Daten sind von Haus aus heikel

Manchmal ergibt sich das Risiko schon aus der Art der Daten. Typisch hierfür sind medizinische Daten. Sie sind ihrem Wesen nach vertraulich. Deshalb sind beispielsweise Daten beim Betriebsarzt immer besonders schutzwürdig. Ein PC mit solchen Daten muss deshalb speziell abgesichert werden.

Scheinbar banale Vorgänge können brisant sein

Nicht immer sind die Risiken so offensichtlich. Ein Beispiel dafür ist die Einbindung von besonderen Schriftarten auf einer Webseite. Das geschieht häufig über den Zugriff auf Dienste wie Google Fonts. Ein völlig banaler Vorgang? Leider nein, denn wenn jemand auf die Webseite zugreift, übermittelt Google Fonts Daten von ihm an Google. Google ist in den USA ansässig. Dies zieht besondere rechtliche Probleme nach sich. Es hat also gute Gründe, wenn im Rahmen einer DSFA auch Fragen nach solchen Abläufen gestellt werden.

Am Anfang steht die Frage nach den Daten

Jede Risikoanalyse läuft nach einem bestimmten Raster ab. Das ist auch bei der DSFA so. Am Anfang steht die Frage, welche personenbezogenen Daten verarbeitet werden. Normalerweise sollte sich dies schon aus dem ohnehin vorhandenen Verzeichnis der Verarbeitungstätigkeiten ergeben. Die Angaben, die dort enthalten sind, sollten allerdings bei dieser Gelegenheit überprüft werden.

Es folgt die Ermittlung des Schutzbedarfs

Personenbezogene Daten können unterschiedlich schutzbedürftig sein. Deshalb ist eine Einstufung der Daten anhand eines Rasters aus drei Kategorien üblich. Sie reichen vom geringen Schutzbedarf (etwa bei üblichen Adressdaten) über mittleren Schutzbedarf (etwa bei Angaben zum Personenstand) bis hin zu hohem Schutzbedarf (etwa bei medizinischen Daten).

Die Folgen etwaige Pannen sind wichtig

An diese Einstufung schließt sich die Frage an, welche Folgen etwaige Daten-Pannen haben können. Diese Frage ist deshalb wichtig, weil Pannen Schadensersatzforderungen, Geldbußen und andere Folgen für das Unternehmen nach sich ziehen können. Man sollte deshalb nicht voreilig davon ausgehen, dass „ohnehin im Normalfall nichts passiert".

Die DSFA bildet eine Handlungsgrundlage

Ergebnis einer DSFA ist ein umfangreiches „Risikopapier". Es bildet unter anderem die Grundlage dafür, welche Schutzmaßnahmen als notwendig anzusehen sind. Nur selten führt eine DSFA dazu, dass bestimmte Daten überhaupt nicht mehr verarbeitet werden dürfen. Viel häufiger ist es, dass bestimmte Spielregeln ergänzt oder vorhandene Spielregeln in der Praxis endlich umgesetzt werden.

Was Online-Tracking alles verraten kann

Nicht nur die Werbewirtschaft nutzt Tracking-Verfahren, um die Online-Aktivitäten von Nutzenden nachzuverfolgen. Online-Tracking macht weitaus mehr möglich als personalisierte Online-Werbung: einen genauen Blick auf die persönlichen Einstellungen.

Ist Online-Tracking wirklich so schlimm?

Eine Trendstudie des BVDW (Bundesverband Digitale Wirtschaft) untersuchte die Akzeptanz für Werbung im Internet. Demnach sind sich drei Viertel der Befragten (71 Prozent) bewusst, dass Werbung ein unverzichtbares Finanzierungsmittel der digitalen Angebote im Internet ist. Gleichzeitig empfindet mehr als die Hälfte der Befragten (58 Prozent) Werbung als grundsätzlich störend.

Jeder zweite Internetnutzende (52 Prozent) gibt an, Cookies in den eigenen Browser-Einstellungen zu löschen, so eine Umfrage des Digitalverbands Bitkom. Doch so manchem erscheint die Sorge wegen Online-Tracking übertrieben. Immerhin ist dann die Online-Werbung, die angezeigt wird, passender zu den persönlichen Interessen und aktuellen Internetsuchen.

Aber Internetwerbung ist nicht alles, wofür sich die Analysen der Online-Aktivitäten nutzen lassen.

Persönliche Eigenschaften könnten transparent werden

Tatsächlich geht es bei Online-Tracking um mehr als möglichst erfolgversprechende Online-Werbung. So zeigt der Datenschutzbericht „Risiken im Zusammenhang mit dem Tracking- und Targeting-Ökosystem im digitalen Werbemarkt" der Internationalen Arbeitsgruppe zum Datenschutz in der Technologie weitere Risiken auf, die das Tracking im Internet mit sich bringen kann.

Die Datenschützer berichten, dass sich das Tracking mittlerweile über digitale Werbung hinaus nutzen lässt, etwa um Meinungsbildungsprozesse zu manipulieren. Das ist möglich, weil Online-Tracking es erlaubt, eine Sammlung persönlicher Eigenschaften und Interessen zu einer Person anzulegen. Dies könnte nicht nur die Werbewirtschaft, sondern auch ein Interessenverband oder eine Partei für sich nutzen.

Sammlungen persönlicher Eigenschaften kann man sich selbst ansehen:

- Google Ads Setting (Einstellungen für personalisierte Werbung) beispielsweise verrät Nutzenden mit Google-Konto, was bereits alles über die Person bekannt ist.
- Auch bei Facebook zum Beispiel kann man sich die „Ad Preferences" (Interessenbasierte Online-Werbung verwalten) ansehen, um dann festzustellen, dass sogar die Nähe zu einer politischen Partei dort hinterlegt sein kann.

Hohe Diskriminierungs- und Manipulationsrisiken

Die Datenschützer warnen vor den häufig übersehenen Risiken durch Online-Tracking: Das vertiefte Wissen über einzelne Nutzerinnen und Nutzer, insbesondere über die emotionale Verfassung, könne genutzt werden, um persönliche Vorurteile und Schwächen zu identifizieren. Es erlaubt Dritten, diese auszunutzen, um individuelles Verhalten zu beeinflussen oder sogar zu kontrollieren.

Der Datenschutzbericht nennt konkrete Beispiele: So beeinflusste Facebook im Jahr 2012 den Newsfeed von 1,9 Millionen seiner Nutzerinnen und Nutzer in den USA, um sie zum Wählen zu bewegen. Facebook behauptet, dass es den Anteil der Wählerinnen und Wähler innerhalb dieser Gruppe um drei Prozentpunkte erhöhen konnte. Die Datenschützer machen klar: Würden Facebook oder andere soziale Netzwerke eine solche Manipulation hypothetisch nur bei Nutzerinnen und Nutzern eines bestimmten politischen Spektrums anwenden, könnte das einen entscheidenden Einfluss auf den Ausgang von Wahlen haben.

Es gibt also sehr gute Gründe, sich über den Schutz vor heimlichem Online-Tracking genau zu informieren! Lesen Sie deshalb genau die Online-Hilfe zu Ihrem Browser, damit Sie alle verfügbaren Einstellungen kennen und einsetzen, die sich gegen ungewolltes Tracking richten.

Wissen Sie, wie Sie sich vor Online-Tracking schützen können? Machen Sie den Test!

Frage: Aktiviert man im Browser die Option „Do Not Track" (DNT), findet kein Online-Tracking mehr statt. Stimmt das?

1. **Nein, die Einstellung DNT signalisiert nur den Wunsch der Nutzerin oder des Nutzers, nicht getrackt zu werden.**
2. **Ja, dann wird das Tracking durch den Browser automatisch unterbunden.**

Lösung: Die Antwort 1. ist richtig. Tatsächlich übermittelt das DNT-Signal nur einen Wunsch. Aber es ist nicht garantiert, dass sich Werbenetzwerke und andere Tracking-Dienste daran halten. Untersuchungen haben sogar gezeigt, dass das DNT-Signal häufig missachtet wird.

Frage: Lässt man im Browser automatisch alle Cookies am Sitzungsende löschen, kann es kein längerfristiges Online-Tracking geben. Ist das so richtig?

1. **Ja, denn ohne Cookies gibt es kein Online-Tracking über mehrere Sitzungen hinweg.**
2. **Nein, denn es gibt auch andere Tracking-Verfahren.**

Lösung: Die Antwort 2. ist richtig. Selbst wenn Sie gar keine Cookies akzeptieren würden, also alle Cookies im Cookie-Manager des Browsers verbieten, können Sie im Internet getrackt werden. Möglich wird dies durch Cookie-Alternativen wie eindeutige Browser-Kennzeichen (sogenanntes Browser Fingerprinting). Die Entwicklung geht sogar weg von Tracking-Cookies hin zum sogenannten Cookieless Tracking. Es nutzt nur Cookie-Alternativen, die sich nicht über den Cookie-Manager im Browser steuern lassen.

Impressum

Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de