NEWS BOX DATENSCHUTZ

AUSGABE

11/2022

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Wie Sie in einem der nachfolgenden Newsbeiträgen lesen können, versucht der BITKOM bestehende Wissensdefizite zum Thema Datenschutz und Datensicherheit auch im privaten Bereich, insbesondere im Bereich Smart Home, mit einer neuen Orientierungshilfe zu reduzieren. Angesicht der Komplexität der Geräte und der Datensammelwut zeichnet sich jedoch ab, dass dies in einer Sisyphusarbeit für die Verbraucher enden dürfte.
Gefahren für die Persönlichkeitsrechte können bspw. Hobbyköchen durch ein manipuliertes (elektronisches) Kochbuch über den Umweg einer Küchenmaschine drohen. Und geparkte Fahrzeuge der Firma Tesla liefern nach Straftat Fahndungsfotos an die Polizei.
Es kann auch sein, dass Videoaufzeichnungsdaten von Ihrer smarten Haustür-Überwachungsanlage bzw. Ihrer smarten Türklingelanlage auch ohne richterliche Anordnung an die Polizei herausgegeben werden, wenn Sie die Geräte aus der Produktpalette der Serie „Ring“ nutzen.

Ungewollte Datenabflüsse können aber auch in Situationen und bei Tätigkeiten erfolgen, die auf den ersten Blick nicht sonderlich problematisch im Sinne des Datenschutzes erscheinen. Oder würden Sie ohne weiteres auf die Idee kommen, dass eine aktivierte automatische Rechtschreibprüfung unter bestimmten Umständen dazu führen kann, dass Online-Passwörter Unberechtigten zur Kenntnis gelangen können?
Daher wird der Nutzer nicht umhinkommen, bei steigender Komplexität der genutzten Anwendungen, sein Wissen bzgl. Technik und Datensicherheit up to date zu halten. Und er wird sich nicht darauf verlassen können, dass Geräte oder Anwendungen per Design oder per Default so konstruiert bzw. konfiguriert sind, dass der Schutz der Privatsphäre als oberstes Gebot bedacht wurde, fürchtet Ihr
Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: wachiwit, Adobe Stock

OLG Frankfurt verlangt „hinreichende Erheblichkeit" für Schadensersatzanspruch

Das OLG Frankfurt entschied in einem Berufungsverfahren, dass ein Facebook-User kein Recht auf Schadensersatz für den von ihm vorgetragenen Verstoß gegen datenschutzrechtliche Bestimmungen hat. Der Nutzer hat sog. *hate speech* verbreitet, die zur Löschung des Posts sowie zur vorübergehenden Einschränkung des Accounts führte.

Weiter auf DataAgenda lesen

Bußgeld wegen missbräuchlicher Verwendung von Grundbuchdaten

Eine der tragenden Säulen der DS-GVO ist der Grundsatz der Fairness und Transparenz. Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Der Verantwortliche soll der betroffenen Person alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.

Weiter auf DataAgenda lesen

Foto: Michael Ebardt, Adobe Stock

Foto: Anke Thomass, Adobe Stock

Digitalisierung in Schulen – Behörden begleiten konstruktiv

Insbesondere als viele Schulen während der Hochphase der Corona-Pandemie geschlossen wurden und auch längere Zeit geschlossen bleiben mussten, suchten viele Schulen bei den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Beratung (bspw. LfDI RLP, HBDI, LfD Sachsen-Anhalt), mit welchen datenschutzkonformen Instrumenten sowohl schulisches Miteinander als auch Lerninhalte transportiert werden können.
Aufsichtsbehörden reagierten teilweise unterschiedlich und es wurden pragmatische oder weniger pragmatische Lösungen für die Probleme und Sorgen der Schulen gefunden. Einige Lösungen, die von Schulen praktiziert wurden, wurden von den Aufsichtsbehörden „geduldet", bis belastbare und datenschutzkonformere Konzepte etabliert werden konnten.

Mittlerweile hatten die Beteiligten Zeit, die drängenden Fragen strukturierter betrachten und abarbeiten zu können. Als Ergebnis der Erfahrungen der jüngsten Vergangenheit hat die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) ein Papier dieser Überlegungen vorgestellt, welches als Grundstein für die notwendige Digitalisierung in den Schulen verstanden werden soll.

Flankiert werden diese Überlegungen durch die letzten beiden Änderungen des Schulgesetzes Nordrhein-Westfalen (SchulG). Darin hat der Landesgesetzgeber in §§ 120, 121 SchulG die datenschutzrechtlichen Voraussetzungen dafür geschaffen, dass die Schulen digitale Systeme im Schulunterricht rechtssicherer einsetzen können.
Der dauerhafte Einsatz von Systemen für den digitalen Unterricht soll den bestmöglichen Ausgleich zwischen Praxistauglichkeit und Gewährleistung eines angemessenen Datenschutzniveaus bieten. Das Grundsatzpapier beschreibt, wie die Einsatzbedingungen datenschutzgerecht zu gestalten sind. Die Informationen sollen den verantwortlichen Stellen dabei helfen, diese Ziele umzusetzen.

Das Grundsatzpapier der LDI NRW beschäftigt sich insbesondere mit diesen Fragestellungen:

1. Wer ist wofür zuständig? Wer ist für was verantwortlich?
2. Welche rechtlichen Rahmenbedingungen sind im Schulbereich zu beachten?
3. Welche weiteren Anforderungen müssen erfüllt werden?
4. Dürfen Lehrkräfte ihre privaten PCs zur Verarbeitung von Daten der Schüler*innen einsetzen, und wie sollen Schüler*innen die Daten digital verarbeiten?

Quelle: LDI NRW

11. GDD-Winter-Workshop

für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister

30.–31. Januar 2023 | Garmisch Partenkirchen

Praxisthemen:

- ✓ Aktuelle Entwicklungen im Datenschutz
- ✓ Datenschutz und künstliche Intelligenz
- ✓ Datenschutz bei begrenzten Ressourcen rechtssicher und pragmatisch umsetzen
- ✓ Aktuelles zum Beschäftigen-Datenschutz

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: HQUALITY, Adobe Stock

Smart Home & Datenschutz für Bürger

Immer mehr Menschen digitalisieren und vernetzen ihr Zuhause. Jedes neue internetfähige Gerät eröffnet aber Cyber-Kriminellen auch neue Angriffsmöglichkeiten. Ob die Nutzung von smarten Thermostaten, von Ambiente-Beleuchtung, diversen Sensoren, Aktoren, Überwachungskameras, smarten Türklingeln, elektronischen Schließsystemen oder digitalen Assistenten – jedes dieser smarten Geräte vergrößert auch die Komplexität des zu administrierenden privaten Netzwerks. Zusätzlich werden Unmengen von personenbezogenen Daten über die Nutzer oder auch reine Maschinendaten bzw. Sensordaten ohne Personenbezug generiert. Es entsteht ein ähnlich komplexes System wie im gewerblichen und professionellen Bereich – mit dem Unterschied, dass im privaten Bereich oftmals die zeitlichen oder fachlichen Ressourcen für eine angemessene Administration oder den Schutz der personenbezogenen Daten vorhanden sind.

Auch im Bereich Smart Home bewegen sich Anwendungsszenarien in einem rechtlich geregelten Rahmen. Wozu Daten, die im Smart Home entstehen, genutzt werden dürfen, hängt insbesondere davon ab, ob es sich um personenbezogene oder nicht-personenbezogene Daten handelt. Insbesondere dann, wenn im Smart Home personenbezogene Daten der Nutzerinnen und Nutzer verarbeitet werden, entfalten die datenschutzrechtlichen Regelungen ihre Wirkung und sollten die betroffenen Personen schützen.

Es existiert zwar ein Standard für nachweisbare Sicherheit bei vernetzten Geräten im Smart Home (ETSI EN 303 645). Der Standard ist jedoch lediglich eine Empfehlung an die Hersteller, Internet-of-Things-Geräte von Anfang an sicher zu entwickeln (Security by Design) und zugleich eine international anerkannte Messgröße, um zu beurteilen, ob die Geräte über ein Mindestmaß an Cyber-Sicherheit verfügen. Die Spezifikation beschreibt, wie die Konformität definiert und gemäß den Anforderungen aus dem Sicherheitsstandard strukturiert und umfassend getestet werden kann. Mit ETSI TS 103 701 werden Prüfergebnisse der Sicherheitseigenschaften von IoT-Geräten vergleichbar. So wird IoT-erfahrenen Personen eine entsprechende Sicherheitsbewertung ermöglicht. Hersteller können die Testspezifikation für einen Selbsttest nutzen oder ihr Produkt durch eine Prüfstelle evaluieren lassen.

Der BITKOM versucht nun, das bestehende Wissensgefälle im Bereich der reinen Privatnutzer von Smart Home zu begradigen. Hierzu hat der BITKOM den Leitfaden „Neue Mehrwerte im Smart Home durch Daten – Wie Daten im Smart Home gesammelt, genutzt und verarbeitet werden“ veröffentlicht. Ziel der Autoren ist es auch, ein klares und verständliches Bild von der Bedeutung von Daten und ihrer Nutzung für den Erfolg von Smart Home-Technologie zu zeichnen. Der Leitfaden soll zeigen, wie Verbraucherinnen und Verbraucher mit Transparenz und Kontrolle über ihre Smart Home-Daten die Hoheit über ihre Privatsphäre behalten.

Quelle: BITKOM

Foto: VideoFlow, Adobe Stock

Frist für Umstellung auf neue Standard-datenschutzklauseln endet bald

Der europäische Gesetzgeber hat vor dem Hintergrund der Ausweitung des internationalen Handels die Übermittlung personenbezogener Daten an Datenempfänger in Drittländern unter besondere datenschutzrechtliche Anforderungen gestellt, um Rechte und Freiheiten von Betroffenen zu schützen. Ziel ist es, das durch die Datenschutz-Grundverordnung (DS-GVO) unionsweit gewährleistete Schutzniveau für natürliche Personen nicht zu untergraben, wenn personenbezogene Daten in ein Drittland transferiert werden. Die Art. 44 ff. aus Kapitel V der DS-GVO geben die Bedingungen vor, nach denen Verantwortliche oder Auftragsverarbeiter, die der DS-GVO unterliegen, personenbezogene Daten in Drittländer übermitteln dürfen.

Adressaten der DS-GVO, die personenbezogenen Daten in ein Drittland übermitteln möchten, haben die sog. 2-Stufen-Prüfung zu durchlaufen. Dies ergibt sich aus Art. 44 S. 1 DS-GVO, der von Verantwortlichen oder Auftragsverarbeitern die Einhaltung der Vorgaben von Kapitel V sowie die Einhaltung der „sonstigen Bestimmungen dieser Verordnung“ verlangt.

Weiter auf DataAgenda lesen

Foto: peshkova, Adobe Stock

Kündigung aufgrund der Verletzung einer „Clean-Desk-Policy“

Die DS-GVO fordert von Verantwortlichen und Auftragsverarbeitern in Art. 32 DS-GVO ein Schutzniveau, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen ist. Dabei sollen zur Gewährleistung der Sicherheit insbesondere die Risiken berücksichtigt werden, die aus einer Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten, der an deren Verarbeitung beteiligten IT-Systeme, Dienste und Fachprozesse, hervorgehen können. Ziel ist es, diese Risiken einzudämmen, indem wirksame technische und organisatorische Maßnahmen (TOM) umgesetzt werden. Aufgrund der technikneutralen Formulierung des DS-GVO finden sich darin keine konkreten Maßnahmen, die Schritt für Schritt abgearbeitet werden können. Stattdessen steht es grundsätzlich jedem Verantwortlichen frei, selbst diejenigen TOM auszuwählen, die passend zu der eigenen Art der Verarbeitung und Unternehmensgröße sind, sofern damit ein wirksames angemessenes Schutzniveau erreicht werden kann.

Diese TOM können und werden von Verantwortlichen in sog. „Clean-Desk-Policies“ zusammengefasst und für die Einhaltung durch die Beschäftigten in Kraft gesetzt. Die Etablierung von TOM ist nicht nur für den Schutz von personenbezogenen Daten ein notwendiges Muss, sondern kann auch für den Schutz von sog. Geschäftsgeheimnissen eingesetzt werden.

Weiter auf DataAgenda lesen

Foto: beeboys, Adobe Stock

Handelsregister mit Datenschutzmängeln

Seit dem 1. August 2022 sind über das Portal „Handelsregister.de“ sämtliche Einträge in den Handels-, Genossenschafts-, Partnerschafts- und Vereinsregistern ohne weitere Einschränkungen kostenfrei abrufbar. Das hat auf den ersten Blick Vorteile in puncto Transparenz. Beim Handelsregister handelt es sich um die zentrale Registerplattform des Bundes für Firmen in Deutschland. Der Umstand, dass die Abrufe aus diesem Portal kostenfrei und ohne das Anlegen eines vorherigen Accounts erfolgen können, ist Ergebnis des seit dem 1. August 2022 geltenden Gesetzes zur Umsetzung der Digitalisierungsrichtlinie (DiRUG) der EU vom Juni 2019. Unter anderem wollte die EU damit Registerauskünfte vereinfachen.

Da das Handelsregister (erreichbar unter http://www.handelsregister.de/) eine Publikations-, Beweis-, Kontroll- und Schutzfunktion erfüllen soll, enthält es notwendiger- und typischerweise unter anderem Informationen über Firma, Sitz, Niederlassung und Zweigniederlassungen, den Gegenstand des Unternehmens, vertretungsberechtigte Personen, die Rechtsform des Unternehmens sowie das Grund- oder Stammkapital und den Namen des Geschäftsinhabers.

Die „neuen Vorteile“ des Portals (niedrigschwelliger Zugang und Kostenfreiheit) scheinen aber nach Meinung von Datenschützern die Nachteile deutlicher hervortreten lassen, mit denen das Portal auch deswegen behaftet ist, weil „die deutsche Verwaltung es sich (bei der Umsetzung der Digitalisierungsrichtlinie) einfach gemacht hat, und die früheren dezentralen und bisher nur mit Aufwand zugänglichen Register – eins zu eins – ins Internet gestellt hat“.

„Interessierte“ können auf der Plattform diverse Informationen einsehen, darunter auch eingescannte Dokumente, die mit den jeweiligen Firmen in Verbindung stehen, wie beispielsweise Anmeldungen oder Gesellschaftsverträge. Darin sind nicht nur Informationen zu der juristischen Person finden, sondern auch personenbezogene Daten zu Inhaberinnen und Inhabern und Gesellschafterinnen und Gesellschaftern.

Nach Erwägungsgrund 85 der DS-GVO kann eine Verletzung des Schutzes personenbezogener Daten eintreten – wenn nicht rechtzeitig und angemessen reagiert wird –, einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit der dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Foto: wichayada, Adobe Stock

Mehr Cybersicherheit für KMU

In Deutschland existieren nach EU-Klassifikation etwa 2,6 Millionen Unternehmen, die dem Bereich KMU zuzurechnen sind, das sind 99,4 Prozent aller Unternehmen in Deutschland. Viele dieser familien- bzw. eigentümergeführten Unternehmen zählen zur Gruppe der Hidden Champions, die in Deutschland etwa 1.500 Unternehmen umfasst – und damit etwa die Hälfte aller Hidden Champions weltweit ausmacht.

Anders als typische Großunternehmen beschäftigen KMU in der Regel keine dedizierten IT-Sicherheitsteams. Oftmals verfügen sie nicht einmal über einen eigenen IT-Betrieb. Daraus folgt vielfach eine mangelnde Beurteilungskompetenz für IT-Sicherheitsgefährdungen. Zudem fehlt auf Managementebene häufig das grundsätzliche Bewusstsein für die Risiken und Abhängigkeiten, die der Einsatz von Informationstechnik mit sich bringt. Dadurch sind KMU gegenüber Bedrohungen aus dem Cyber-Raum besonders anfällig. Durch den stetig zunehmenden Grad an Digitalisierung verschärft sich nach Ansicht des BSI die Gefährdungslage kontinuierlich. Dies spiegelt sich auch in den Analysen des BSI zum Updateverhalten von Unternehmen wider (Die Lage der IT-Sicherheit in Deutschland 2021).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht eine Notwendigkeit für die Stärkung der KMU in Deutschland. Dem trägt das BSI durch Ausbau seines Engagements für diese Zielgruppe Rechnung. Seit Herbst 2020 kümmert sich innerhalb der Behörde nun ein neues Referat ausschließlich um die Belange von KMU. Ein Beispiel für dieses Engagement ist die neue Veröffentlichung des BSI mit dem Titel Cyber-Sicherheit für kleine und mittlere Unternehmen (KMU). Die Broschüre bietet KMU einen leicht verständlichen Einstieg, um ihr Cyber-Sicherheitsniveau zu verbessern. Informationssicherheit wird vom BSI als notwendige Voraussetzung für eine sichere Digitalisierung bewertet.

Die Broschüre steigt mit den wichtigsten Grundlagen der IT-Sicherheit ein – kurz und knapp anhand von 14 Fragen. Sie informiert unter anderem darüber, wer für die Informationssicherheit im Unternehmen verantwortlich ist, warum Patches und Updates regelmäßig installiert werden sollten, warum ein Virenschutzprogramm notwendig und eine Datensicherung so wichtig ist.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Foto: carballo, Adobe Stock

525.000 EUR Bußgeld wegen Interessenkollision des DSB

Die DS-GVO (Art. 38 Abs. 6 Satz 2) verbietet Interessenkonflikte des Datenschutzbeauftragten.

Ein Interessenkonflikt ergibt sich regelmäßig dann, wenn der Datenschutzbeauftragte im Rahmen seiner sonstigen Tätigkeit für die gleiche Organisation Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt und sich insofern selbst überwachen müsste. So kommen insbesondere der Geschäftsführer oder der IT-, Personal- oder Marketingleiter als Datenschutzbeauftragter nicht in Betracht. Ob ein „echter" Interessenkonflikt i.S.v. Art. 38 Abs. 6 Satz 2 DS-GVO vorliegt, der die Amtsübernahme ausschließt, kann im Übrigen regelmäßig nur im konkreten Einzelfall entschieden werden.

Weiter auf DataAgenda lesen

Data Agenda Podcast Folge 23: Anonymisierungsstandards für die EU-Datenstrategie

Die neue Datenakte der Europäischen Union stehen im Zentrum der datenschutzrechtlichen Diskussion. Im Herbst 2022 ist der Data Governance Act in Kraft getreten, Data Act und KI-Verordnung gehen auf die Zielgerade und der Entwurf einer Richtlinie zur KI-Haftung wird diskutiert. Die DS-GVO wird durch die auf Datenteilung angelegten Datenakte der EU-Datenstrategie nicht berührt. Wir müssen die DS-GVO in Wechselwirkung mit dem entstehenden Recht bringen und uns um Standards für Pseudonymisierung und Anonymisierung kümmern, um den Datenbinnenmarkt ins Werk zu setzen. So lautet das gemeinsame Fazit von Frederick Richter und Steffen Weiß im Podcast.
Wie können sich Einrichtungen, wie die Stiftung Datenschutz und die Gesellschaft für Datenschutz- und Datensicherheit,w einbringen und welche Rolle spielt die Bundesregierung? Um diese und weitere Fragen geht es im Data Agenda Podcast mit Frederik Richter und Steffen Weiß. Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter