Datenschutz newsbox

Ausgabe 07 2020

DATAKONTEXT

Editorial:

In den letzten Monaten haben sich nicht nur Anwender und Unternehmen intensiv mit Videokonferenz-Systemen beschäftigt, sondern auch immer wieder die Datenschutz-Aufsichtsbehörden.

Zwei Anbieter gerieten immer wieder in den Fokus:
Der Anbieter der Videokonferenz-Software Zoom geriet wegen fehlender Datenschutz-Features in die Kritik. Gut zu beobachten war jedoch, wie der Anbieter die wesentlichen Kritikpunkte ernst nahm, schnell nachbesserte und so die (vermeintlichen) Schwachpunkte in puncto Datenschutz und Datensicherheit durch ernsthafte und stetige Nachbesserungen zum Wettbewerbsvorteil verwandelte.
So lässt der LfDI Baden-Württemberg in einer aktuellen Mitteilung vermelden, dass nach intensiven Gesprächen zwischen dem LfDI und Zoom die angesprochenen schweren Sicherheitslücken, für welche Zoom in der Vergangenheit schon mehrfach in der Kritik stand (Tracking und Fragen der Nutzerfreundlichkeit), durch den Anbieter nachgebessert wurden.

Im Verlauf der Gespräche habe Zoom deutlich den Willen zur Verbesserung seines Dienstes gezeigt – und haben dem auch Taten folgen lassen. Wenn man bedenkt, dass manch ein Anbieter frei nach dem Motto „nicht geschimpft, ist genug gelobt" verfährt, kann Zoom wohl mit dieser Aussage gut leben.

Auch über eine weitere Videokonferenz-Software wurde in jüngster Vergangenheit öfter diskutiert. In einer zweiseitigen „Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen" warnte Berlins Datenschutzbehörde vor dem Einsatz von verbreitet eingesetzten Programmen, die bestimmte Bedingungen nicht erfüllten. Genannt werden Microsoft, Skype und Zoom.
Auch nach einer Abmahnung und der Aufforderung von Microsoft „unrichtige Aussagen so schnell wie technisch möglich zu entfernen und zurückzunehmen", steht die Aufsichtsbehörde jedoch zu ihren wesentlichen Aussagen, wie sich aus einem Brief der Berliner Aufsichtsbehörde an Microsoft ergibt.
Hier dürfte von beiden Seiten das letzte Wort wohl noch nicht gesprochen sein, vermutet

Ihr Levent Ferik.

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Smart Home und Router-Sicherheit

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE (Fraunhofer FKIE) hat im Juni 2020 die Ergebnisse eines groß angelegten Tests zur Sicherheit von Internet-Routern für Privatkunden veröffentlicht. Die Ergebnisse der Studie waren ernüchternd, da bei fast allen getesteten Geräten Sicherheitsmängel festgestellt wurden.
Die Sicherheitsmängel waren recht unterschiedlicher Natur.
Bei fast allen Geräten von insgesamt 127 getesteten Routern für Privatnutzer von sieben großen Herstellern wurden Sicherheitsmängel festgestellt, teilweise sogar ganz erhebliche. Diese reichen von fehlenden Sicherheitsupdates, über einfach zu entschlüsselnde, hartcodierte Passwörter (die vom Benutzer auch nicht geändert werden können!) bis hin zu bereits bekannten Schwachstellen, die eigentlich längst behoben sein müssten.
Die Auswertung hat ergeben, dass kein einziger Router ohne Fehler war. Manche waren sogar von Hunderten bekannter Schwachstellen betroffen. 46 Router hatten in den letzten zwölf Monaten kein Sicherheitsupdate erhalten«, berichtet IT-Security-Experte und FKIE-Wissenschaftler Peter Weidenbach. Der Extremfall unter den geprüften Geräten hatte sogar 2.000 Tage lang kein Sicherheitsupdate mehr erhalten.

Ein Fazit der Tester des Fraunhofer FKIE lautet, dass die Vielzahl der aufgeführten Schwachstellen zeige, dass die Hersteller noch viel mehr Anstrengungen unternehmen müssen, um die Geräte deutlich sicherer zu machen.
Ein Weg dorthin könnte über die neue Technischen Richtlinie des BSI für Breitband-Router gehen.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in einer Technischen Richtlinie für Breitband-Router das Mindestmaß an IT-Sicherheitsmaßnahmen definiert, das für Router im Endkundenbereich umgesetzt sein sollte. Für diese Technische Richtlinie hat das BSI nunmehr eine Prüfspezifikation erstellt, auf deren Basis Hersteller, Prüfstellen und andere Interessierte Breitband-Router detailliert auf die Einhaltung der Anforderungen der Technischen Richtlinie überprüfen können. Darüber hinaus werden die Technische Richtlinie und die zugehörige Prüfspezifikation in die Konzeption des IT-Sicherheitskennzeichens innerhalb des IT-Sicherheitsgesetzes 2.0 einfließen.

GDD-Praxishilfen nun auch in englischer Sprache

Die Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) wirbt auch auf internationaler Ebene für das bewährte Prinzip der Selbstkontrolle und bringt sich aktiv in die datenschutzrechtliche EU-Gesetzgebung ein. Da der Datenschutz inzwischen zu einem globalen Thema geworden ist, pflegt sie einen fachlichen Austausch mit Datenschutz-Kontrollstellen in den EU-Mitgliedstaaten sowie mit Experten und Verbänden weltweit.

Die Confederation of European Data Protection Organisations (CEDPO), ein europäischer Dachverband von Datenschutzorganisationen, ist nur ein erfolgreiches Beispiel dieser Anstrengungen, denn die GDD ist Gründungsmitglied der CEDPO.

Inzwischen vereint die Dachorganisation über seine nationalen Mitgliedsverbände tausende Datenschutzbeauftragte und andere Datenschutz-Praktiker aus der Europäischen Union. Die CEDPO fördert eine Stärkung der Rolle von betrieblichen und behördlichen Datenschutzbeauftragten und tritt generell für einen ausgewogenen, praktikablen und effektiven Datenschutz ein.

Da ist es nur konsequent wie zukunftsweisend zugleich, dass die GDD, ihre seit Jahren prägnanten und unmittelbar verwertbaren Handreichungen, die sie für den betrieblichen Datenschutzalltag bereitstellt und die sich größter Beliebtheit erfreuen auch für den englischsprachigen Anwender zur Verfügung stellt. Als gemeinnütziger Verein und Gründungsmitglied des europäischen Dachverbands CEDPO (Confederation of European Data Protection Organisations) will die GDD ihre Praxishilfen sukzessive nun auch in englischer Sprache veröffentlichen, um auch den europäischen und internationalen Datenschützern Hilfestellung beim Umgang mit der DS-GVO zu geben.

Die ersten beiden Übersetzungen finden Sie nun unter:
>> GDPR Good Practices – VII
Transparency obligations in data processing
>> GDPR Good Practices – XI
Confidentiality agreement

Häufig gestellte Fragen zur Auftragsverarbeitung

Nachdem die DS-GVO vor mehr als zwei Jahren Wirksamkeit erlangt hat, hatten die Verantwortlichen ausreichend Zeit, eine Anpassung ihrer Datenschutzorganisation auch im Hinblick auf die Überprüfung bestehender Vertragsverhältnisse sowie die Anpassung der Vertragsmuster für zukünftige Outsourcing-Dienstleistungen vorzunehmen.
Für den Bereich der Auftragsverarbeitung scheinen jedoch viele Einzelfragen noch in der Diskussion zu sein, sei es die Abgrenzung zur Funktionsübertragung oder zur gemeinsamen Verantwortlichkeit, das Fortbestehen der bisherigen Privilegierung von Auftragsverhältnissen oder schlicht die Anwendung auf Fernwartungsvorgänge. Diese Fragen müssen nicht nur durch Wissenschaft und Praxis, sondern auch durch die Datenschutz-Aufsichtsbehörden befriedigend gelöst werden.

Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen) hat die am häufigsten gestellten Fragen rund um das Thema gesammelt und stellt ihre Antworten in einer FAQ zur Verfügung. Dabei handelt es sich um nachfolgende Fragen:

1. Was versteht man unter einer Auftragsverarbeitung?
2. Wann ist die beauftragte Verarbeitung personenbezogener Daten eine Auftragsverarbeitung nach Art. 28 Abs. 1 DS-GVO?
3. Ist für die vom Auftragsverarbeiter vorgenommene Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich?
4. Kann es besondere Konstellationen geben, in denen ausnahmsweise keine Auftragsverarbeitung vorliegt, weil die Datenverarbeitung nur ein „ungewolltes Beiwerk“ einer (Haupt-) Dienstleistung darstellt?
5. Für den Fall, dass die beabsichtigte Datenverarbeitung eine Auftragsverarbeitung nach Art. 28 DS-GVO ist: In welcher Rolle befinde ich mich?
6. Muss eine Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter geschlossen werden?
7. Im Folgenden finden Sie Antworten zu verschiedenen Einzelfällen.
8. Müssen Behörden oder sonstige öffentliche Stellen in Niedersachsen neben Art. 28 DS-GVO Sonderregelungen zur Auftragsverarbeitung beachten?
9. Kann ein Auftragsverarbeiter seinen Sitz auch außerhalb der Europäischen Union/des Europäischen Wirtschaftsraums haben?
10. Sind „Alt-Verträge“ zur Auftragsverarbeitung anzupassen?
11. Was soll ich machen, wenn ich als Verantwortlicher unsicher bin und noch keinen Auftragsverarbeitungsvertrag abgeschlossen habe?

Mitarbeiterdaten im Unternehmensverbund nach DS-GVO

Als im Jahre 2001 das BDSG novelliert wurde, veröffentlichte die Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) die erste Ausgabe der „Praxishilfen" zu Verarbeitungsübersicht, Verfahrensverzeichnis und Vorabkontrolle. Zum Konzept der Reihe gehörten schon damals prägnante und unmittelbar verwertbare Handreichungen für den betrieblichen Datenschutzalltag. In den darauffolgenden Jahren erschienen in dieser Reihe weitere Titel zu praxisrelevanten Themen, zuletzt 2014 „Mitarbeiterdaten im Unternehmensverbund" in der 2. Auflage.
Mit Inkrafttreten der Europäischen Datenschutz-Grundverordnung am 24. Mai 2018 begann eine neue Zeitrechnung. Die GDD-Praxishilfen erscheinen seitdem in neuem, klaren Design und mit neuer Zählung und **ausschließlich als PDF-Dateien.**

Nun hat die GDD einen Klassiker neu aufgelegt:
Angesichts der Tatsache, dass weder die EU-Datenschutzrichtlinie noch die DS-GVO ein bedingungsloses „Konzernprivileg" kennen, ist die datenschutzrechtliche Zulässigkeit der Weitergabe von Mitarbeiterdaten im Unternehmensverbund häufig nicht unproblematisch. Datenflüsse innerhalb von Konzernstrukturen sind komplex und bedürfen einer gut strukturierten Datenschutz-Organisation sowie einer vertieften datenschutzrechtlichen Bewertung.

Vor diesem Hintergrund greift die GDD mit der vorliegenden Praxishilfe Grundsatzfragen und typische Personaldatenflüsse unter datenschutzrechtlichen Gesichtspunkten beispielhaft auf, um den betrieblichen Datenschutzbeauftragten die praktische Umsetzung der einschlägigen rechtlichen Vorgaben zu erleichtern und zugleich einen Beitrag zu mehr Rechtssicherheit in diesem Bereich zu leisten.
Im Vergleich zur Vorauflage wurden Zulässigkeitsfragen einer Übermittlung von Mitarbeiterdaten im Unternehmensverbund an die DS-GVO angepasst und Abgrenzungen zwischen der Auftragsverarbeitung und einer alleinigen oder gemeinsamen Verantwortlichkeit ergänzt. Praxisbeispiele sollen Organisationen dabei unterstützen, wie die Bewertung einer klassischen Datenweitergabe im Unternehmensverbund erfolgen kann.

>> Die Praxishilfe kann hier heruntergeladen werden.
>> Eine Möglichkeit zur Vertiefung der Rechtsfragen rund um die Datenübermittlung im Unternehmensverbund finden Sie hier.

Quelle: Gesellschaft für Datenschutz und Datensicherheit

BfDI zeigt rechtlichen Rahmen der Anonymisierung auf

In der DS-GVO werden anonyme und anonymisierte Daten in den Sätzen 4 und 5 von Erwägungsgrund 26 adressiert. Danach sollten die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten, „d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann".
Weitere Bestimmungen hierzu enthält die DS-GVO nicht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat sein aktuelles Positionspapier zur Anonymisierung vorgestellt.
Ausgehend von der Tatsache, dass die Anonymisierung trotz ihrer hohen praktischen Bedeutung für die Praxis in der DS-GVO nur sehr oberflächlich angesprochen wird, versucht der BfDI, in seinem neuen Papier der eigentlichen Bedeutung gerecht zu werden.
Immerhin könne die Anonymisierung als ein Mittel angesehen werden, im Einzelfall eine Verarbeitung von Daten gar erst zu ermöglichen, wenn die Verarbeitung bei bestehendem Personenbezug datenschutzrechtlich unzulässig wäre, so der BfDI.
Das neue Positionspapier bezweckt daher das Mittel der Anonymisierung über die kurze Erwähnung in den Sätzen 4 und 5 von des Erwägungsgrund 26 der DS-GVO hinaus, die Bedeutung zu verschaffen, die es aufgrund seiner Praxisrelevanz für bspw. Forschungsprojekte oder Geschäftsmodelle haben sollte.
Bedeutsam dürfte auch die Feststellung im Rahmen des Positionspapiers sein, dass die Anonymisierung selbst ebenfalls eine Verarbeitung darstellt und damit als solche einer Rechtsgrundlage bedarf.

Das Positionspapier beantwortet unter anderem Fragen wie: Ist die Anonymisierung personenbezogener Daten rechtfertigungsbedürftig? Und auf welche Rechtsgrundlage lässt sich die Anonymisierung stützen?

Quelle: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Evaluationsbericht zur DS-GVO

In der DS-GVO ist vorgesehen, dass die Kommission erstmals nach zwei Jahren und anschließend alle vier Jahre einen Bericht über die Bewertung und Überprüfung der Verordnung vorlegt.

Dementsprechend hat die EU-Kommission nach etwas mehr als zwei Jahren seit Wirksamwerden der DS-GVO einen Bewertungsbericht veröffentlicht. Nicht besonders überraschen ist, dass die Kommission der DS-GVO ein gutes Zeugnis ausstellt und feststellt, dass die meisten mit der DS-GVO verknüpften Ziele erreicht worden sind.

Insbesondere die leistungsstarken, durchsetzbaren Vorschriften für die Bürgerinnen und Bürger und das durch die DS-GVO neu geschaffene europäische Governance- und Durchsetzungssystem sei ein Faktor für den Erfolg der DS-GVO. Auch bei der Unterstützung digitaler Lösungen in unvorhersehbaren Situationen wie der COVID-19-Krise habe sich die DS-GVO als flexibel erwiesen.

Auch beim Thema Harmonisierung attestiert die Kommission der DS-GVO die gewünschte Wirkung erzielt zu haben. Die Harmonisierung in den Mitgliedstaaten habe zugenommen, auch wenn ein gewisses Maß an Fragmentierung eingeräumt wird, das ständig überwacht werden müsse. Ferner wird festgestellt, dass Unternehmen eine Compliance-Kultur entwickeln und einen starken Datenschutz immer häufiger als Wettbewerbsvorteil nutzen.

In dem Bericht werden folgende Aspekte als die wichtigsten Ergebnisse der Überprüfung der DS-GVO betrachtet:

- Die Bürgerinnen und Bürger sind in ihren Rechten gestärkt und besser sensibilisiert
- Die Datenschutzvorschriften sind zeitgemäß
- Datenschutzbehörden nutzen ihre erweiterten Abhilfebefugnisse
- Die Zusammenarbeit der Datenschutzbehörden im Europäischen Datenschutzausschuss (EDSA) kann noch besser werden
- Möglichkeiten der freien und sicheren Datenübermittlung an Drittstaaten und internationale Organisationen optimal nutzen
- Internationale Zusammenarbeit fördern

Wie in Artikel 97 Absatz 2 der DS-GVO festgelegt, bezieht sich der veröffentlichte Bericht insbesondere auf die Datenübermittlung an Drittstaaten bzw. internationale Organisationen und die Kooperations- und Kohärenzverfahren.

Quelle: Europäische Kommission

Neue Tätigkeitsberichte des Bundesbeauftragten für Datenschutz und Datensicherheit (BfDI)

Lob für positive Entwicklungen, Warnung vor überhasteten Entscheidungen, Kritik in puncto staatliche Transparenz – all das steckt im jüngsten Tätigkeitsbericht des Bundesbeauftragten für Datenschutz und Datensicherheit (BfDI). Am 17. Juni 2020 überreichte der BfDI, Ulrich Kelber, seinen Tätigkeitsbericht an den Bundestagspräsidenten. Die Position des „obersten Datenschützer Deutschlands" hat seit der Datenschutz-Grundverordnung (DS-GVO) stark an Bedeutung gewonnen, die Berichte werden daher mit entsprechend hohem Interesse begleitet.

Generell kritisiert der BfDI, dass Gesetzentwürfe übereilt beschlossen würden. Er mahnt den Gesetzgeber, sich vor allem bei tief greifenden Veränderungen genug Zeit für Beratung der Initiativen zu lassen. Ein besonderes Augenmerk sei hierbei auf Datenverarbeitung und die Vermeidung von Datenmissbrauch zu richten. Gerade in Bereichen, in denen es um sensible Daten gehe, sei eine solche Sorgfalt essenziell, um das Vertrauen in politische Prozesse zu erhalten.
In dem 28. Tätigkeitsbericht zum Datenschutz erkennt der BfDI aber auch positive Entwicklungen seit der Einführung der DS-GVO an. Eine Angleichung des Rechts habe stattgefunden, das generelle Bewusstsein für Datenschutz sei gestiegen und die Sanktionsmöglichkeiten der Aufsichtsbehörden seien gestärkt. Die von der DS-GVO bezweckten Entwicklungen seien dementsprechend weitestgehend in Gang gesetzt worden.

Jedoch sieht der BfDI in manchen Bereichen Schwierigkeiten. So funktioniere die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden zur Durchsetzung der Regelungen bei internationalen IT-Unternehmen nur schwierig. Trotzdem warnt er, angesichts der erst kurzen Geltung der Regelung, vor grundlegenden Änderungen der DS-GVO.

Schärfer fällt seine kritische Bewertung in dem 7. Tätigkeitsbericht zur Informationsfreiheit aus. Neben Angelegenheiten staatlicher Transparenz geht es darin um seine eigenen Tätigkeiten in den Jahren 2018 und 2019. In diesem Bericht kritisiert er zunächst deutlich das Informationsfreiheitsgesetz (IFG). Dessen Schutzbestimmungen gehörten nach Auffassung des BfDI überarbeitet. Zudem solle es zu einem Transparenzgesetz des Bundes weiterentwickelt werden. Ferner wünscht sich der BfDI, dass seine Ombudsfunktion auch auf das Umweltinformationsgesetz (UIG) erweitert wird.

Quelle: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

BITKOM-Leitfaden: DS-GVO-konformes Drucken

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) rundet die Sammlung seiner Leitfäden zum Thema Datenschutz und Datensicherheit mit einem weiteren Leitfaden, der unter dem Titel „DS-GVO-konformes Drucken – Drucken, Scannen, Faxen, Kopieren" veröffentlicht wird, ab.

Darin widmet sich der BITKOM einem Thema, das in Unternehmen oftmals etwas stiefmütterlich behandelt wird, obwohl den heutigen Multifunktionsdruckern vertrauliche Informationen anvertraut werden, die auch häufig personenbezogene Daten beinhalten, deren Vertraulichkeit gewahrt bleiben muss. Oftmals wird die Tatsache vernachlässigt, dass auf aktuellen Druckern Betriebssysteme laufen, die Software ausführen; in der Regel auch Festplatten verbaut sind, auf denen häufig sensible und/oder personenbezogene Daten (Druckjobs, Adressbücher, Protokolle usw.) gespeichert sind. Daraus folgt, dass Drucker ebenfalls in das IT-Sicherheitskonzept des Unternehmens eingebunden werden müssen.

Vor dem Hintergrund, dass Gesetze und Vorschriften wie beispielsweise BDSG § 203 StGB oder DS-GVO konkrete Anforderungen an dieser Vertraulichkeit setzen und Verstöße nicht nur extrem teuer werden können, sondern teilweise auch mit Haftstrafen belegt sind, kann der neue Leitfaden mit hilfreichen Anregungen für die verantwortlichen Stellen aufwarten.

Damit ergänzt der neue Leitfaden das bereits 2019 erschienene Papier mit dem Titel: „Sicherheit von Drucksystemen – Die Sicherheit von Drucksystemen und Multifunktionsgeräten".
Beide Leitfäden beschreiben typische, in der Praxis vorkommende Sicherheitsrisiken und stellen Maßnahmen vor, wie man diesen Bedrohungen (proaktiv) begegnen kann.

Quelle: BITKOM

Fast alle Smart-TV verstoßen gegen die DS-GVO

Smart-TVs sind internetfähige Fernsehgeräte, mit denen die Verbraucher über das klassische Fernsehprogramm hinaus Internetangebote wie Video-Streaming und viele weitere Informationen und Funktionen nutzen können.

Smart-TVs bieten vielfältige Möglichkeiten, personenbezogene Daten zu erheben. Hiervon machen Unternehmen bislang in unterschiedlichem Ausmaß gebrauch. So können etwa das generelle Fernsehverhalten einer Person, ihre App-Nutzung, ihr Surf- und Klickverhalten oder auch biometrische Daten wie Stimme oder Cursorbewegungen sowie die im Einzelnen über den Fernseher abgespielten Inhalte erfasst und ausgewertet werden. Die Erhebung solch intimer Nutzungsdaten und ggf. deren Verwendung für personalisierte Werbung kann der Verbraucher zumeist durch Vornahme entsprechender Einstellungen an seinem Fernsehgerät verhindern.

Das Bundeskartellamt teilt im Abschlussbericht seiner sog. Sektoruntersuchung zu Smart-TVs mit, dass die Datenschutzbestimmungen der in Deutschland aktiven Smart-TV-Hersteller fast durchgehend schwerwiegende Transparenzmängel aufweisen und damit gegen Vorgaben der Datenschutzgrundverordnung (DS-GVO) verstoßen. Sie seien vor allem deshalb für die Verbraucher nicht nachvollziehbar, weil sie für eine Vielzahl von Diensten und Nutzungsprozessen gelten sollen. Diese „one fits all"-Architektur führe dazu, dass die Verbraucher nicht zuverlässig erfahren, welche personenbezogenen Daten verarbeitet werden, welche Datenverarbeitungen durch welchen Nutzungsprozess ausgelöst werden, welche Daten an Dritte übermittelt werden und wie lange einzelne Daten gespeichert werden. Die Verbraucher könnten daher ihr Anwendungsverhalten nicht so steuern, dass sie möglichst wenige private personenbezogene Daten preisgeben.
Bei etlichen Herstellern sei zudem nicht gesichert, dass der Sicherheitsstandard der Geräte auch in den Jahren nach dem Kauf durch Software-Aktualisierungen (Updates) aufrechterhalten wird. Kein Unternehmen mache verbindliche Angaben dazu, wie lange seine Produkte mit Sicherheits-Updates versehen werden. Für die Verbraucher sei diese Information jedoch unerlässlich, um einschätzen zu können, wie lange sie das Gerät uneingeschränkt gefahrlos verwenden können.

Das Bundeskartellamt kann im Bereich des Verbraucherschutzes Untersuchungen durchführen und so Defizite identifizieren. Über die Befugnis, etwaige Rechtsverstöße per behördlicher Verfügung abzustellen, verfügt das Amt hingegen nicht.

Quelle: Bundeskartellamt