Datenschutz *aktuell - Ausgabe 04-2021*

Der Datenschutz-Newsletter aus Nürnberg

Liebe Leserin, lieber Leser,

nicht nur durch die Corona-Pandemie erlebt die IT und damit auch der Datenschutz viele Veränderungen. Im rechtlichen Bereich gibt es ebenfalls Entwicklungen, die den Schutz personenbezogener Daten betreffen. Ihr Datenschutz-Newsletter bringt Sie auf den aktuellen Stand.

So wandelt sich die Arbeitswelt erneut, Beschäftigte kehren teilweise aus dem Homeoffice in ihr Büro zurück oder pendeln zwischen den Arbeitsorten. Für den Datenschutz bedeutet dies, dass sowohl die Maßnahmen für sichere Datenzugriffe als auch der Schutz vertraulicher Papierdokumente angepasst werden müssen.

Zudem gibt es eine neue Rechtsprechung zum Auskunftsrecht nach der Datenschutz-Grundverordnung.

Wie Sie ein VPN einrichten und nutzen

Ob im Homeoffice oder unterwegs: Für den Zugriff auf das Unternehmensnetzwerk soll nicht das offene Internet, sondern ein Virtual Private Network (VPN) genutzt werden. Doch wie funktioniert das in der Praxis? Lesen Sie wichtige Hinweise zur Einrichtung und Nutzung.

Flexible Arbeit hat Folgen für den Datenschutz

Nach dem Ende der Homeoffice-Pflicht sind bereits viele Beschäftigte in ihr bisheriges Büro zurückgekehrt. In vielen Fällen besteht aber weiterhin die Möglichkeit, zeitweise im Homeoffice zu arbeiten. Gleichzeitig finden wieder mehr Vor-Ort-Termine statt. Dadurch nimmt die mobile Arbeit wieder zu.

Die flexible Arbeitsumgebung hat aber Konsequenzen für den Schutz personenbezogener Daten. Die Datenrisiken im Büro, im Homeoffice und unterwegs können sehr verschieden sein. Die Maßnahmen für den Datenschutz sollten den jeweiligen Schutzbedarf berücksichtigen und damit auch den Arbeitsort.

Eines aber haben die Arbeitsorte außerhalb des Büros gemeinsam: Ist ein Zugriff auf das Unternehmensnetzwerk, auf betriebliche Applikationen oder auf Daten in der Unternehmens-Cloud nötig, kommt ein Dienst zum Aufbau eines VPN (Virtual Private Network) ins Spiel.

Sicherer Netzwerkzugang mit Virtual Private Networks

Nutzen Sie im Homeoffice oder bei der mobilen Arbeit VPN, kommt es zuerst einmal darauf an, den richtigen, vom Unternehmen freigegebenen VPN-Dienst zu verwenden. Im Internet kursieren viele Angebote für kostenlose VPN-Dienste. Doch VPN kann gegen Lauschangriffe durch Dritte auf die Verbindung zum Unternehmen schützen, nicht aber gegen denkbare Zugriffe durch den VPN-Anbieter selbst.

Es ist deshalb entscheidend, einen vertrauenswürdigen, sicheren VPN-Dienst einzusetzen. Die Auswahl trifft Ihr Arbeitgeber, nachdem er den VPN-Service geprüft hat. Sie selbst als Nutzer sollten deshalb keinen anderen VPN-Dienst als den jeweils freigegebenen verwenden. Wissen Sie nicht, welcher das ist, fragen Sie danach bei der im Unternehmen zuständigen Stelle.

VPN im Homeoffice

Sind Sie im Homeoffice tätig und wollen auf das Unternehmensnetzwerk zugreifen, verwenden Sie den VPN-Dienst in aller Regel über Ihren Desktop-PC oder Ihr Notebook. Je nach VPN-Service wird dazu einmalig ein VPN-Client auf dem Endgerät eingerichtet, der VPN-Dienst im Browser oder im Internet-Router konfiguriert oder in den Betriebssystemeinstellungen. Fragen Sie Ihre IT-Administration nach der entsprechenden Anleitung.

Wichtig ist, dass Sie das eingerichtete VPN auch nutzen. Dazu müssen Sie die VPN-Verbindung entsprechend aktivieren. Andernfalls haben Sie zwar die Voraussetzungen für VPN, nutzen aber trotzdem das offene Internet.

VPN unterwegs

Auch außerhalb des Homeoffice, zum Beispiel auf dem Weg vom Homeoffice in Ihr Büro im Unternehmen, kann es notwendig sein, mit Ihrem mobilen Endgerät auf das Firmennetzwerk oder auf betriebliche Cloud-Dienste zuzugreifen. Dazu sollte Ihr Smartphone oder Tablet entsprechend eingerichtet sein. Je nach VPN-Dienst gibt es dazu eine spezielle VPN-App, die Sie dann jeweils zuerst starten müssen, wenn Sie sich bei Firmensystemen anmelden wollen.

Auskunftsrecht nach der DSGVO

Die DSGVO gibt Personen, deren Daten irgendwo gespeichert sind, viele Rechte. Am wichtigsten ist dabei das „Auskunftsrecht der betroffenen Person“. Wer es ausüben will, muss einige Spielregeln kennen. Der interne Aufwand für Unternehmen kann auch bei korrekten Anfragen enorm sein. Die DSGVO nimmt darauf letztlich keinerlei Rücksicht. Ob ein Antragsteller mit der Antwort inhaltlich etwas anfangen kann, ist wiederum sein Problem.

Auskunftsrecht als „Recht der Rechte“

Das Auskunftsrecht gilt als das wichtigste Recht, das die DSGVO gewährt. Ein wesentlicher Grund dafür: Nur wer weiß, wo Daten über ihn gespeichert sind, kann weitere Rechte geltend machen, etwa das Recht auf die Berichtigung von falschen Daten.

Zwei Stufen des Rechts

Genau genommen unterscheidet die DSGVO in ihrem Artikel 15 zwei Stufen des Auskunftsrechts:

- **Stufe 1:** Die betroffene Person kann Auskunft darüber verlangen, ob ein Unternehmen oder eine Behörde überhaupt über Daten verfügt, die sie betreffen. Die Antwort auf diese Frage ist im Ergebnis einfach: Ist das der Fall, lautet die Antwort „ja“ (Fall der Positivauskunft). Ist das nicht der Fall, lautet die Antwort „nein“ (Fall der Negativauskunft).
- **Stufe 2:** Falls Daten vorhanden sind, besteht ein Anspruch der betroffenen Person, diese Daten zu erhalten. Außerdem muss sie eine ganze Reihe von Informationen zu den Daten bekommen. Dazu gehört etwa die Angabe des Zwecks, zu dem die Daten verarbeitet werden.

Berechtigte Sorge der Unternehmen vor dem Aufwand

Das umfassende Auskunftsrecht ist sicher eine große Errungenschaft des Datenschutzrechts. Dennoch sind viele Unternehmen davon nicht nur begeistert. Sie haben keineswegs etwas zu verbergen, wie manche Kritiker glauben. Vielmehr fürchten sie den Aufwand, den solche Anfragen verursachen. Er ergibt sich aus mehreren Aspekten:

- Zunächst einmal muss überall im Unternehmen gesucht werden, ob Daten über die anfragende Person vorhanden sind. Hinweise darauf, wo wahrscheinlich etwas zu finden ist, erleichtern die Suche. Beispiel: Die anfragende Person gibt an, dass sie mehrfach als Zeitarbeiter im Unternehmen gearbeitet hat. Ausdrücklich verpflichtet ist sie zu solchen Angaben allerdings nicht. Sinnvoll sind sie trotzdem. Sie können eine Antwort wesentlich beschleunigen.
- Der Auskunftsanspruch betrifft auch Daten auf Papier. Dies kann den Aufwand bei der Suche vervielfachen. Die DSGVO nimmt auf die Besonderheiten von Daten auf Papier letztlich keine Rücksicht mehr.
- Der Auskunftsanspruch ist zeitlich nicht begrenzt. Er erstreckt sich auf alle Daten, die vorhanden sind – auch auf solche, die schon viele Jahre unangetastet im Firmenkeller liegen.
- Der Auskunftsanspruch besteht auch dann, wenn es um sehr große Datenmengen geht, etwa um mehrere tausend Seiten.

Recht auf eine kostenlose Kopie

Sind die Daten gefunden, hat die anfragende Person Anspruch auf eine kostenlose Kopie. Besonders bei umfangreichen Papierunterlagen kann dies für das Unternehmen ins Geld gehen. „Eine“ Kopie ist dabei wörtlich zu nehmen. Wer eine zweite Kopie will, etwa weil er die erste Kopie verloren hat, muss dafür zahlen.

Notwendige Vernichtungsaktionen

Viele Firmen haben die DSGVO zum Anlass genommen, entbehrliche Unterlagen zu vernichten. Solche Aktionen sind bei Mitarbeitern nicht immer beliebt, aber wichtig. Wenn die gesetzlichen Aufbewahrungsfristen (beispielsweise aus dem Steuerrecht) abgelaufen sind, steht einer Vernichtung von Unterlagen nichts entgegen.

Grenzen bei Geschäftsgeheimnissen

Der Auskunftsanspruch geht zwar weit. Grenzen hat er aber trotzdem. So ist ausdrücklich festgelegt, dass „das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen“ darf. Dies wirkt abstrakt, hat aber sehr konkrete Auswirkungen. In den Erwägungsgründen der DSGVO ist als Beispiel genannt, dass der Auskunftsanspruch Geschäftsgeheimnisse nicht beeinträchtigen darf. Der Auskunftsanspruch darf sie also nicht aushebeln.

Kein Anspruch auf eine verständliche Auskunft

Wer Auskunft verlangt, erhält die Daten übrigens so, wie sie vorliegen. Ob er inhaltlich mit ihnen etwas anfangen kann, ist sein Problem. Denn einen Anspruch auf Erläuterung des Inhalts von Daten sieht die DSGVO nicht vor. Dies wird vor allem im Bereich der Medizin wichtig. In der DSGVO heißt es ausdrücklich, dass sich der Auskunftsanspruch auch auf Daten in Patientenakten bezieht. Die Verständlichkeit der dort verwendeten Fachbegriffe und Kürzel ist damit in keiner Weise garantiert. Es ist Sache des Antragstellers, wie er damit klarkommt.

Drucker, Dokumente und digitale Transformation

Auch wenn die Corona-Pandemie die Digitalisierung weiter beschleunigt hat: Papierdokumente spielen weiterhin eine wichtige Rolle und enthalten personenbezogene Daten. Vergessen Sie deshalb bei den Schutzmaßnahmen auch das Papier nicht. Gerade im Homeoffice könnte dies leicht geschehen.

Das digitale Büro bleibt Zukunft

Schon lange wird über das digitale Büro gesprochen: Alles wird digitalisiert, Aktenordner verschwinden. Doch diese Vorstellung ist auch heute noch Zukunftsmusik. Bisher verwenden erst 48 Prozent der Unternehmen Lösungen, um Dokumente zu digitalisieren, wie der Digitalverband Bitkom berichtet hat.

So kommt es auch, dass es weiterhin viele Dokumente in Papierform gibt, die personenbezogene Daten enthalten und die deshalb zu schützen sind. Dabei befinden sich die Papierdokumente nicht nur im verschlossenen Aktenschrank.

Vertrauliche Unterlagen pendeln zwischen Büro und Homeoffice

Viele Papierdokumente werden auch außerhalb des Büros und Firmengebäudes genutzt und aufbewahrt. Die Tätigkeit im Homeoffice und die mobile Arbeit unterwegs haben dies noch verstärkt. Wo in Zukunft die sogenannte Hybride Arbeit als Mischung aus Büro und Homeoffice zum betrieblichen Alltag wird, hat dies auch Folgen für die Papierdokumente.

So transportieren die Beschäftigten dann Akten und andere Dokumente in Papierform zwischen den verschiedenen Arbeitsorten. Es kann etwa sein, dass jemand einen aktuellen Kundenvorgang im Homeoffice ausdruckt und dann später mit ins Büro nimmt, um das Dokument in der entsprechenden Akte abzulegen. Bei diesem Transport jedoch könnte das Dokument verloren gehen oder gar gestohlen werden.

Drucker sind ein mehrfaches Angriffsziel

Aber auch der Ausdruck selbst im Homeoffice birgt Risiken. Viele Drucker werden inzwischen in das WLAN im Homeoffice eingebunden. Manche sind sogar direkt über das Internet zu erreichen, damit man auch unterwegs etwas drucken kann, das dann im Homeoffice wartet.

Cyber-Attacken haben vernetzte Drucker im Visier. Es gibt aktuelle Beispiele, dass Cyberkriminelle Schwachstellen in Verbindung mit Druckern aktiv ausnutzen. Dabei bieten Drucker gleich mehrere Angriffsziele: Angreifer könnten ungeschützte Druckverbindungen abhören, ungeschützte Datenspeicher im Drucker auslesen, dort Malware deponieren und den unzureichend geschützten Drucker als heimlichen Zugang zum Endgerät und ins Netzwerk nutzen.

Mehr Datenschutz für Dokumente und Drucker

Denken Sie bei der digitalen Transformation deshalb nicht nur an den digitalen Datenschutz, sondern auch an Papierdokumente und an die Drucker, die Dokumente in Papierform ausgeben.

Andernfalls könnten Dokumente und Drucker zum Datenleck werden – sei es bei der unsicheren Lagerung, dem ungeschützten Transport oder der fehlerhaften Entsorgung über den normalen Papiermüll. Auch im

Homeoffice und unterwegs müssen angemessene Schutzmaßnahmen verfügbar sein, wie zum Beispiel ein Papierschredder, der dem Schutzbedarf der Dokumente, die entsorgt werden sollen, entspricht.

Denken Sie nicht zuletzt daran, dass der Schreibtisch im Homeoffice kein sicherer Ort ist, um Akten aufzubewahren. Ein Homeoffice-Arbeitsplatz kann viel mehr „Publikumsverkehr“ haben als so manches Büro.

Haben Sie Ihre Papierdokumente im Griff? Machen Sie den Test!

Frage: Der Datenschutz betrifft nur Dateien, nicht aber Papierdokumente. Stimmt das?

1. Nein, auch Papierdokumente können zu schützende personenbezogene Daten enthalten.
2. Ja, denn der Datenschutz gilt nur für die automatisierte Verarbeitung personenbezogener Daten.

Lösung: Die Antwort 1. ist richtig. Die Datenschutz-Grundverordnung (DSGVO) gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, aber auch für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Unter Dateisystem versteht die DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, also zum Beispiel auch gedruckte Kundenlisten in einem Aktenordner.

Frage: Drucker im Homeoffice sind über das Internet nicht zu erreichen. Stimmt das?

1. Ja, ist die Tür zum Homeoffice abgeschlossen, kann niemand an den Drucker.
2. Nein, über WLAN und teils über das offene Internet könnten Drucker für Angreifer erreichbar sein.

Lösung: Die Antwort 2. ist richtig. Inzwischen werden gerade im Homeoffice die meisten Drucker über WLAN angebunden. Schwachstellen im WLAN könnten damit Dritten Zugang zum Drucker und den darauf gespeicherten Druckdaten geben. Zudem bieten viele Druckermodelle eine direkte Verbindung ins Internet und haben eine eigene E-Mail-Adresse. Das macht es möglich, von unterwegs über das Internet darauf zu drucken. Damit sind aber auch Cyberattacken auf diese Drucker möglich. Die Daten, die auf der Festplatte des Druckers liegen, könnten auf diesem Weg ebenso in Gefahr geraten wie die Daten, die für einen Ausdruck auf den Drucker temporär übermittelt werden.

Impressum
Redaktion: Peter Brandmann (V.i.S.d.P.)
Externer Datenschutzbeauftragter - Zert. Fachkraft DSGVO
Anschrift:
pb beratung & training
Schnepfenreuther Weg 51
90425 Nürnberg

Telefon: 0911/3506118
E-Mail: peter.brandmann@pb-beratung-training.de