Datenschutz *Aktuell - Ausgabe Juli 2020*

Der Datenschutz-Newsletter aus Nürnberg

pb beratung & training

Sehr geehrte Damen und Herren,
liebe Leserinnen und Leser,

seit Monaten beschäftigt uns das Thema "Corona" - hierbei ist der Datenschutz verständlicherweise etwas in den Hintergurnd getreten.

Seit einigen Wochen bemerken wir wieder verstärkte Maßnahmen der Datenschutzbehörden. Es wird verstärkt geprüft. Bußgelder werden wieder verstärkt verhängt – siehe gegen die AOK in Baden-Württemberg.

Viele Unternehmen haben während der Pandemiephase, oder auch noch andauernd, auf home office umgestellt. Achtung auch hierbei ist der Datenschutz zu beachten.

Zum Schluß noch eine Abhandlung zum Thema „Privacy Shield“ (Datenaustausch mit den USA). Diese Vereinbarung mit den USA wurde gestern 16.07.2020) vom EuGH gekippt.

Nun beginnen neue langwierige Verhandlungen - Folgen derzeit noch nicht absehbar.

Ich wünsche Ihnen viel Spaß beim Lesen und bleiben Sie weiterhin gesund

Ihr Peter Brandmann

Datensicherheit im Homeoffice

Arbeiten im Homeoffice war für viele ein lang gehegter Wunsch. Kommt es aber tatsächlich dazu, ist die Umsetzung gar nicht so einfach. Das gilt auch für die Einhaltung der Datenschutzvorgaben, die am heimischen Schreibtisch genauso wie im Büro gelten.

Homeoffice zwischen Wunsch und Pflicht

Von den Berufstätigen arbeitet mittlerweile fast jeder Zweite (49 Prozent) ganz oder zumindest teilweise im Homeoffice, so eine Umfrage des Digitalverbands Bitkom. Nicht alle Unternehmen und Beschäftigten haben sich aus freien Stücken dafür entschieden.

18 Prozent durften vor der Corona-Pandemie gar nicht im Homeoffice arbeiten und machen das jetzt zeitweise (15 Prozent) oder ganz (drei Prozent). Weitere 31 Prozent konnten bereits vorher im Homeoffice tätig sein und tun das jetzt häufiger (17 Prozent) oder ganz (14 Prozent). Nur 41 Prozent der Beschäftigten sagt, ihre Tätigkeit sei grundsätzlich nicht für Homeoffice geeignet.

Keine Frage: Arbeiten im Homeoffice ist eine Entwicklung, die weiter zunimmt und die auch nach den Krisenzeiten bestehen bleiben wird. Für den Datenschutz bleibt dies aber nicht ohne Folgen.

Viele waren nicht auf Homeoffice vorbereitet

„Für viele Mitarbeiterinnen und Mitarbeiter heißt es gerade: Ab sofort Homeoffice! Viele Unternehmen und Behörden kannten dies bisher gar nicht oder nur in Ausnahmefällen. Deswegen wird vielerorts gerade improvisiert, um den Betrieb am Laufen zu halten und dabei die Bedürfnisse aller Beschäftigten möglichst gut zu erfüllen“, so Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein.

Doch technische und organisatorische Sicherheitsmaßnahmen sind wichtig für das Arbeiten am Computer, mit Papierdokumenten oder auch beim Telefonieren. Für den Fall, dass doch einmal eine Datenpanne passiert, müssen alle Beschäftigten wissen, wem sie dies melden.

Wie der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ermittelt hat, steht es um die Datensicherheit im Homeoffice nicht gut. So findet man wichtige Sicherheitsmaßnahmen bei Weiten nicht an allen heimischen Schreibtischen: Nur 65 % haben ihren Rechner passwortgeschützt, 63 % haben das WLAN passwortgeschützt, 61 % haben ein Virenschutzprogramm installiert, 41 % nutzen E-Mail-Verschlüsselung und 37 % eine VPN-Verbindung. 12 % sagen sogar, sie haben keine Datensicherheit im Homeoffice.

Mehr Datensicherheit im Homeoffice

Der Digitalverband Bitkom hat Empfehlungen zusammengestellt, wie das Arbeiten am Schreibtisch daheim sicherer wird, darunter:

- aktuelle Softwareversionen sowie Antivirensoftware verwenden und regelmäßig Updates installieren
- VPN-Zugang nutzen, falls keine Cloud-basierten Dienste eingesetzt werden
- komplexe Passwörter benutzen, um den Rechner zu entsperren, und für Online-Dienste, die man damit nutzt
- wo immer möglich Zwei-Faktor-Authentifizierung einsetzen
- Festplatten verschlüsseln, insbesondere in Notebooks
- Rechner sperren, wenn man nicht am Schreibtisch sitzt

Ohne eine solche Datensicherheit kann eine datenschutzkonforme Arbeit im Homeoffice nicht gelingen. Aber selbst mit einer dem Risiko angemessenen IT-Sicherheit gibt es Einschränkungen für die Arbeit im

Homeoffice: Nicht alle Tätigkeiten dürfen im Homeoffice geleistet werden, beispielsweise schließen dies einige Auftragsverarbeitungsverträge aus. Die Datenschutzvorgaben müssen weiter eingehalten werden, sie bleiben nicht zurück im Büro, sondern kommen mit ins Homeoffice.

Achten Sie auf den Datenschutz im Homeoffice? Machen Sie den Test!

Frage: Wenn der Arbeitgeber ein sicheres Notebook für das Homeoffice mitgibt, sind die Anforderungen an die Datensicherheit automatisch erfüllt. Stimmt das?

1. Nein, es müssen mehr Maßnahmen erfolgen, um sicheres Arbeiten im Homeoffice zu ermöglichen.
2. Ja, dann ist die Sicherheit die gleiche wie im Unternehmen selbst.

Lösung: Die Antwort 1. ist richtig. Nur wenn das Firmen-Notebook keine Verbindung zum Internet oder ins Firmennetzwerk aufnimmt und keine Speichermedien oder weiteren Geräte angeschlossen werden, könnte man von einem sicheren Notebook ausgehen. Ansonsten müssen die Datenverbindungen und alle Schnittstellen zusätzlich abgesichert werden.

Frage: Im Homeoffice dürfen alle Arbeiten erledigt werden, die man auch sonst im Büro durchführt. Stimmt das?

1. Ja, immerhin nutzt man ja das Firmen-Notebook.
2. Nein, es gibt Einschränkungen. Denn nicht alle Daten dürfen einfach mit ins Homeoffice genommen werden.

Lösung: Die Antwort 2. ist richtig. Es muss genau festgelegt und geregelt werden, welche personenbezogenen Daten das Unternehmen verlassen und im Homeoffice verarbeitet werden dürfen. Hierzu müssen Verträge und Rechtsgrundlagen überprüft werden. Ebenso muss bedacht werden, dass das Homeoffice mit zusätzlichen Risiken verbunden ist, die ohne entsprechende Gegenmaßnahmen eine Verarbeitung bestimmter Daten nicht möglich machen.

Ein Tipp der Aufsichtsbehörden: Die grundlegende Frage, die Sie sich stellen sollten, ist die, ob Sie überhaupt dringend an Aufgaben mit personenbezogenen Daten arbeiten müssen. Wenn Sie zunächst an Aufgaben ohne Personenbezug und ohne andere sensible Daten arbeiten, können Sie sich an die neue Situation gewöhnen und Erfahrungen sammeln. Dann gewinnen Sie auch Zeit für die Umsetzung der Regeln.

Was ist der Privacy Shield?

Wer in einem Unternehmen arbeitet, das Daten in die USA übermittelt, muss ihn kennen. Aber auch jeder Normalbürger sollte zumindest einmal davon gehört haben. Die Rede ist vom Privacy Shield, auf Deutsch etwa „Schutzschild für das Persönlichkeitsrecht“. Er kann seit dem 1. August 2016 genutzt werden. Viele Unternehmen hatten dringend darauf gewartet.

Eine Herausforderung: Datenübermittlungen in die USA

Will ein Unternehmen Daten von Kunden oder auch Daten von Mitarbeitern an ein US-Unternehmen übermitteln, geht das nicht „leicht und locker“. Und zwar auch dann nicht, wenn es sich bei dem US-Unternehmen beispielsweise um die „US-Mutter“ handelt.

Bekanntlich gehören die USA nicht zur EU. Deshalb erlauben die EU-Regelungen zum Datenschutz den Transfer von Daten in die USA nur dann, wenn dort ein angemessenes Datenschutzniveau herrscht. Was als angemessen anzusehen ist, bestimmt sich dabei natürlich nach den Vorstellungen der EU.

Datenschutz in den USA: durchaus, aber ...

Damit beginnen in der Praxis die Probleme. Zwar gibt es in den USA sehr wohl Datenschutzvorschriften. Deshalb sollte man gegenüber Kollegen aus den USA auch nie zu überheblich davon sprechen, die USA würden sowieso keinen Datenschutz kennen.

Nur zu schnell kann es einem sonst passieren, dass diese Kollegen etwa auf Regelungen hinweisen, die die Daten von Kindern ganz besonders schützen. Die Abkürzung hierfür heißt COPPA (Children's Online Privacy Protection Rule) und ist auch den meisten Durchschnitts-Amerikanern bekannt.

Die US-Regelungen setzen die Schwerpunkte aber ganz anders als die Vorschriften der EU. Manche Aspekte des Datenschutzes, die in Europa ganz hoch gehalten werden, gelten in den USA kaum etwas. Langer Rede kurzer Sinn: Ein Datenschutzniveau, das nach den Vorstellungen der EU generell als angemessen anzusehen wäre, existiert in den USA nicht.

Individuelle Einwilligungen: nur theoretisch denkbar

Wie soll ein Unternehmen damit umgehen? Nun, es könnte beispielsweise jeden einzelnen Betroffenen um seine Einwilligung bitten und seine Daten erst dann übermitteln.

Theoretisch wäre das denkbar. In der Praxis funktioniert das aber schon wegen des Aufwands nicht. Deshalb wählt der neue Privacy Shield einen anderen Ansatz.

Der besondere Ansatz von Privacy Shield:

- Ein US-Unternehmen, das personenbezogene Daten aus der EU erhalten soll, verpflichtet sich dazu, umfangreiche Spielregeln für den Datenschutz einzuhalten. Sie sind unter dem Begriff „Privacy Shield“ zusammengefasst.
- Diese Verpflichtung erfolgt gegenüber den zuständigen US-Behörden. Das ist meist die Federal Trade Commission (FTC), eine Verbraucherschutzbehörde.
- Der Inhalt der Spielregeln ist zwischen dem US-Handelsministerium (Department of Commerce) und der Europäischen Kommission abgestimmt.
- Ist ein US-Unternehmen eine solche Verpflichtung eingegangen, gilt das Datenschutzniveau in diesem Unternehmen auch seitens der EU als angemessen.
- Die positive Folge für die europäischen Geschäftspartner solcher US-Unternehmen: Sie dürfen personenbezogene Daten an dieses Unternehmen unter denselben Voraussetzungen übermitteln, unter denen dies auch innerhalb der Europäischen Union zulässig wäre.

Keine Einwilligung der Betroffenen nötig

Die Betroffenen müssen nicht gefragt werden, ob sie damit einverstanden sind. Sie müssen aber in geeigneter Weise informiert werden. Dabei sind viele Einzelheiten zu beachten, um die sich die Spezialisten in den Unternehmen kümmern. In Deutschland sind dies die Datenschutzbeauftragten der Unternehmen.

Erinnern Sie sich noch an Safe Harbor?

Manchem wird dieses Vorgehen irgendwie bekannt vorkommen. Völlig zu Recht! Ziemlich ähnlich lief dies auch schon bei den Safe-Harbor-Regelungen ab. Sie hatten sich über zehn Jahre lang beim Transfer von Daten aus der EU in die USA bewährt – jedenfalls aus der Sicht der meisten Unternehmen.

Allerdings hatte der Europäische Gerichtshof diese Regelungen im Oktober 2015 aus verschiedenen Gründen gekippt. Das geschah gewissermaßen über Nacht, also ohne jede Übergangsfrist. Deshalb waren neue Regelungen, wie sie der Privacy Shield nun vorsieht, dringend erforderlich. Etwas vereinfacht lässt sich sagen: Der Inhalt des Privacy Shield ist neu und wesentlich ausgefeilter, als es die Regelungen von Safe Harbor waren. Der Verfahrensablauf ist aber ziemlich ähnlich.

Gegen die Spielregeln verstoßen? Lieber nicht!

Wie sieht es übrigens damit aus, dass sich die Unternehmen auch wirklich an die Spielregeln halten, zu denen sie sich verpflichtet haben? Die Chancen dafür stehen gut. Jeder weiß, wie kräftig US-Behörden bei Rechtsverstößen zupacken können. Und das gilt nicht nur, wenn es um Verstöße gegen Abgasregelungen geht. Auch Datenschutzverstöße von US-Unternehmen haben die amerikanischen Behörden schon schwer geahndet. Gehen Sie also davon aus: Privacy Shield ist ernst gemeint!

Impressum
Redaktion:

Peter Brandmann
ext. Datenschutzbeauftragter

Anschrift:
pb beratung & training
Schnepfenreuther Weg 51
90425 Nürnberg

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