SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

seit drei Jahren gilt sie nun, die Datenschutz-Grundverordnung (DSGVO). Ein Grund zum Feiern? Ja und nein, denn die DSGVO hat den Datenschutz einen deutlichen Schritt vorangebracht. Doch es gibt weiterhin Herausforderungen bei der Umsetzung.

In dieser Ausgabe dreht sich alles um den Stand der Umsetzung der DSGVO. Sie erfahren, wie es um die Datentransfers in das Drittland USA steht und warum die Datensicherheit die Fülle der Datenpannen, über die die Medien berichten, scheinbar nicht verhindern kann.

Die weiteren Artikel betrachten, ob sich die gefürchteten Geldbußen nach der DSGVO als echtes Risiko erwiesen haben und wie es um die richtige Identifizierung von Auskunftssuchenden steht.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

Juni_2021

1 DATENTRANSFER IN DIE USA – EINE DAUERBAUSTELLE?

Die DSGVO gilt seit nunmehr drei Jahren. Ihr wesentlicher Zweck besteht darin, Rechtssicherheit im Datenschutz zu bewirken. Für Datentransfers in die USA ist dies bisher nicht gelungen. Hier liegt eine große Herausforderung für die Zukunft.

Ohne Übermittlungen in die USA geht kaum etwas

Die meisten Unternehmen können gar nicht anders, als personenbezogene Daten in die USA zu übermitteln. Manche gehören zu einem Konzern mit einer Konzernmutter in den USA und müssen deshalb dorthin berichten. Nahezu alle Unternehmen nutzen Internetservices, die Daten in den USA speichern. Aktuelles Beispiel hierfür sind Systeme für Videokonferenzen. Meist laufen sie über Server in den USA.

Die USA – ein Drittland

Ein Unternehmen, das Daten in die USA übermittelt, muss die Vorgaben der DSGVO einhalten. Die USA sind bekanntlich kein Mitglied der EU, sondern ein sogenanntes Drittland. Das US-Recht orientiert sich nicht an den Vorgaben der DSGVO. Deshalb sind Maßnahmen nötig, damit „das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird." (so wörtlich Art. 44 Satz 2 DSGVO).

Der goldene Weg: generelle Regelungen

Ideal wäre es für Unternehmen, wenn es generelle Vorgaben der EU gäbe, die dies gewährleisten. Dann könnte die Europäische Kommission nämlich feststellen, dass diese Vorgaben ein angemessenes Schutzniveau für Datenübermittlungen in die USA sicherstellen („Angemessenheitsbeschluss" gemäß Art. 45 DSGVO). Diesen Weg hat die EU im engen Zusammenwirken mit der US-Seite zweimal zu beschreiten versucht.

„Safe Harbour" und „Privacy Shield" sind Geschichte

Zunächst sollten die „Safe-Harbour-Regelungen" buchstäblich einen sicheren Hafen für Datenübermittlungen in die USA schaffen. Später sollte der „Privacy Shield" ein Schutzschild für DSGVO-konforme Datenübermittlungen in die USA darstellen.

Beides waren umfangreiche Regelungswerke. Beide fanden beim Europäischen Gerichtshof keine Gnade. Seine Entscheidungen sind unter den Kurzbegriffen „Schrems I" und „Schrems II" bekannt. Herr Schrems, ein österreichischer Jurist, hatte jeweils die Verfahren in die Wege geleitet, die zu den Entscheidungen geführt haben.

Der aktuelle Stand: Ratlosigkeit

Im Augenblick herrscht in den Unternehmen eine gewisse Ratlosigkeit. Das spüren alle Mitarbeiterinnen und Mitarbeiter, die mit Datenübermittlungen in die USA zu tun haben, in ihrem beruflichen Alltag. Aufforderungen, solche Übermittlungen auf das Notwendigste zu beschränken, sind Standard. Von der EU entworfene „Standardvertragsklauseln" dienen häufig als Rechtsgrundlage für Datentransfers, sind aber aufwendig zu handhaben. Einwilligungen betroffener Personen taugen nicht als breit anwendbare Rechtsgrundlage. Der Aufwand ist schlicht zu hoch.

Ein dringender Geburtstagswunsch

Den dritten Geburtstag der DSGVO verbinden viele Unternehmen mit dem Wunsch, dass die EU in nächster Zeit ein besonderes Geburtstagsgeschenk bastelt: eine in der Praxis sinnvoll nutzbare Rechtsgrundlage für Datenübermittlungen in die USA! Die EU und die USA haben versprochen, sich darum in der nächsten Zeit intensiv zu bemühen.

2 WIE STEHT ES UM DIE SICHERHEIT PERSONENBEZOGENER DATEN?

Drei Jahre müssen Unternehmen und Behörden die Datenschutz-Grundverordnung nun schon anwenden. Doch scheinen die Sicherheitsvorfälle und Datenpannen noch größer und häufiger als früher zu sein. Kommt die Datensicherheit nicht von der Stelle? Kann es überhaupt Datensicherheit geben?

DSGVO fordert eine sichere Verarbeitung personenbezogener Daten

Die Datenschutz-Grundverordnung lässt keinen Zweifel. Sie fordert ausdrücklich: Die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten und die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten müssen auf Dauer sichergestellt sein.

Nun könnte man vermuten, dass drei Jahre Anwendung der DSGVO dazu geführt hätten, dass IT-Sicherheitsvorfälle und damit Verletzungen der genannten Schutzziele für personenbezogene Daten inzwischen seltener auftreten. Doch offensichtlich ist das nicht der Fall. Die Schlagzeilen der Tagespres-se sind voll von Meldungen über Datenverluste, Datenmissbrauch und Spionageangriffe auf Unternehmen und Behörden.

Ist die Forderung der DSGVO nach einer umfassenden Sicherheit der personenbezogenen Daten unrealistisch? Kann wirkliche Datensicherheit vielleicht gar nicht gelingen?

Hundertprozentige Sicherheit gibt es nicht, aber ...

Kein Sicherheitsexperte würde behaupten, dass es eine hundertprozentige Sicherheit gibt, daran kann auch die DSGVO nichts ändern. Trotzdem ist die Forderung nach Datensicherheit ein zwingender Be-standteil des Datenschutzes. Nur weil die Meldungen über Millionen von Datensätzen, die ungeschützt im Internet gefunden wurden, nicht abreißen, kann man auf die Maßnahmen des technischen Datenschutzes nicht verzichten.

Tatsächlich ist es so, dass die Maßnahmen der Datensicherheit durchaus Sicherheitsvorfälle und Datenpannen vermeiden, es also ohne diese Maßnahmen viel mehr Schaden für die Betroffenen von Datenverlust und Datenmissbrauch geben würde. Sicherheitsexperten sagen, dass selbst Basisschutzmaßnahmen helfen können, die Mehrzahl möglicher Angriffe zu verhindern.

Für besonders raffinierte Angriffe und komplexe Vorfälle braucht man dagegen besondere Schutzmaßnahmen. Doch auch diese können keine Garantie bieten.

Wirksamkeit der Schutzmaßnahmen muss dauerhaft überwacht werden

Aus gutem Grund fordert die DSGVO neben den Sicherheitsmaßnahmen auch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. So kann es durchaus sein, dass eine ergriffene Maßnahme nicht das erfüllt, was man für die Sicherheit erwartet hat. Es kann aber auch sein, dass eine Schutzmaßnahme für eine gewisse Zeit greift, dann aber keine zuverlässige Datensicherheit mehr bieten kann. Dies soll durch die Kontrolle der Wirksamkeit erkannt werden, um die Schutzmaßnahmen dann zu optimieren.

Entscheidend für die Datensicherheit ist dabei der Stand der Technik, wie die DSGVO fordert. So kann zum Beispiel eine Verschlüsselung in der Zukunft nicht mehr stark genug sein, da die Angreifer dann Mittel haben, um sie zu brechen.

Neben neuen Angriffsmethoden sind es auch die neuen Technologien, die die Datensicherheit immer wieder herausfordern. Neue Technik bringt neue Schwachstellen mit sich, die Angreifer ausnutzen könnten. Aber auch bestehende Technik kann Sicherheitslücken enthalten, die erst später bekannt werden.

Datensicherheit ist und bleibt eine Daueraufgabe

Sieht man also genauer hin, so darf man sich nicht wundern, dass auch drei Jahre nach Anwendung der DSGVO Sicherheitsvorfälle auftreten und der Datenschutz verletzt wird, weil die Datensicherheit unzureichend war. Das kann an der Wahl der falschen Maßnahmen liegen, an fehlendem Schutz, an Vorfällen, die sich technisch gar nicht verhindern lassen, aber auch an der hohen Dynamik der IT und der Bedrohungslage.

Die Sicherheit der Verarbeitung personenbezogener Daten ist also nicht etwa schlechter geworden, weil immer noch viele Datenpannen auftreten. Stattdessen kann man annehmen, dass die Zahl der gemeldeten und entdeckten Vorfälle zugenommen hat – das ist also ein gutes Zeichen für den Datenschutz, wenn man Datenschutzverletzungen nicht übersieht, sondern meldet und abstellt. Das ist durchaus als Erfolg der DSGVO zu sehen, die die Meldepflichten stärker in den Blick der Unternehmen gerückt hat.

Gleichzeitig gilt es, weiterhin die Sicherheit der Daten auf ihre Wirksamkeit hin zu untersuchen. Dazu gehört es auch, Sicherheitsfunktionen nicht zu umgehen oder zu deaktivieren, weil sie scheinbar den Komfort reduzieren. Das würde dann tatsächlich den Datenschutz verschlechtern. Das gilt heute und wird auch in Zukunft so sein.

.

3 GELDBUßEN NACH DER DSGVO – (K)EIN ECHTES RISIKO?

Die DSGVO sieht Geldbußen von bis zu 20 Millionen Euro vor. Das gab es vorher noch nie. Die Aufsichtsbehörden verhängen teils hohe Geldbußen. Die Gerichte akzeptieren das jedoch nicht ohne Weiteres.

Abschreckung als ausdrückliches Ziel

Was eine Geldbuße wegen Verstößen gegen den Datenschutz auszeichnen soll, sagt die DSGVO deutlich: Die Buße soll „wirksam, verhältnismäßig und abschreckend“ sein. So steht es in Art. 83 Abs. 1 DSGVO. Das dient der „konsequenteren Durchsetzung der Vorschriften dieser Verordnung“. So formuliert es Erwägungsgrund 148 zur DSGVO.

Ein Wettlauf um die höchste Geldbuße?

Die Richtung ist damit klar. Die DSGVO will Schluss machen mit Sanktionen eher symbolischer Art. Sie gab es vor Geltung der DSGVO häufig. Nun steigen manche Aufsichtsbehörden dagegen in einen regelrechten Wettlauf um die höchste Geldbuße ein. So kommt es zumindest manchen Beobachtern vor.

Rekordhalter ist Hamburg

„Rekordhalter“ ist bisher die Datenschutzaufsicht Hamburg. Sie verhängte gegen das Unternehmen H&M eine Geldbuße von nicht weniger

als 35.258.708 Euro. Auch wenn es um erhebliche Verstöße ging, war dies ein ordentlicher Aufschlag. Das Unternehmen akzeptierte die Geldbuße. Warum? Vielleicht wollte es vor allem weitere öffentliche Diskussionen um das Thema „Datenschutz bei H&M“ vermeiden.

Manche Unternehmen wehren sich erfolgreich

Andere Unternehmen verhielten sich weniger gefügig. Der Kommunikationsanbieter 1&1 sah sich mit einer Geldbuße in Höhe von 9.550.000 Euro konfrontiert, verhängt vom Bundesbeauftragten für den Datenschutz. Dies schien 1&1 nun doch zu viel. Das Unternehmen wandte sich an das zuständige Landgericht Bonn. Das Gericht reduzierte die Geldbuße um über 90 Prozent.

Die Zeit symbolischer Sanktionen ist vorbei

Diese Beispiele zeigen vor allem zwei Dinge:

- Zum einen machen die Aufsichtsbehörden für den Datenschutz inzwischen wirklich ernst.
- Zum anderen bilden sich aber erst noch Maßstäbe dafür heraus, was die Gerichte für angemessen halten.

Klar ist jedoch, dass Geldbußen von wenigen Tausend Euro selbst für schwere Verstöße der Vergangenheit angehören. Diese Zeiten kehren nicht mehr wieder.

Geringe Akzeptanz für den „Bußgeldkatalog“

Wenig Erfolg hatten die Aufsichtsbehörden für den Datenschutz bisher damit, eine Art „Bußgeldkatalog“ durchzusetzen. In einem aufwendigen Abstimmungsverfahren haben sie sich auf entsprechende Leitlinien geeinigt. Die Leitlinien enthalten keine konkreten Beträge für Geldbußen. Sie versuchen aber, Maßstäbe dafür vorzugeben, wann ein durchschnittlich schwerer Verstoß vorliegt, wann ein leichter Verstoß gegeben ist und wann von einer schweren Verletzung des Datenschutzes auszugehen ist. Teils haben Gerichte offen erklärt, dass sie diese Leitlinien für nicht relevant halten.

Ein wichtiges Ziel: Verstöße von vornherein vermeiden!

Auch wenn es auf den ersten Blick überraschen mag: Diese Situation macht es Unternehmen nicht leichter, sondern schwerer. Denn so ist ganz schwierig abzuschätzen, welche Folgen ein konkreter Verstoß nach sich ziehen könnte. Deshalb muss umso mehr die Devise gelten, Verstöße am besten von vornherein zu vermeiden, statt sich danach über ihre Folgen unterhalten zu müssen.

Das bringt durchaus etwas

Es ist ein Irrtum, dass solche Bemühungen im Ernstfall ohnehin nichts bringen würden. Stellen sie einen Verstoß fest, differenzieren die Aufsichtsbehörden sehr wohl danach, ob es sich um ein punktuelles Versagen handelt oder ob der Verstoß Schwachstellen genereller Art belegt. Sollte Letzteres der Fall sein, wird es rasch teuer. Sollte dagegen nur ein Verstoß vorliegen, wie er immer wieder einmal passieren kann, muss die Aufsichtsbehörde nicht einmal unbedingt ein Verfahren einleiten. Sie kann es dann auch bei einer Ermahnung belassen.

Geldbußen auch gegen Mitarbeiterinnen und Mitarbeiter?

Erstaunlicherweise besteht keine Einigkeit darüber, ob die DSGVO Geldbußen gegen Mitarbeiterinnen und Mitarbeiter in Unternehmen möglich macht, wenn sie an einem Datenschutzverstoß schuld sind. Die Frage stellt sich vor allem dann, wenn es eigentlich klare Vorgaben des Unternehmens zur Einhaltung des Datenschutzes gibt, Mitarbeiterinnen oder Mitarbeiter sie aber einfach nicht eingehalten haben. Manche Juristen bejahen diese Frage, andere nicht.

Das Arbeitsrecht gilt in jedem Fall

Doch wenn jemand glaubt, mit etwas Glück könne ihm dann ja nichts passieren, droht ihm möglicherweise ein böses Erwachen. Denn arbeitsrechtliche Sanktionen sind bei Datenschutzverstößen ohne Weiteres möglich. „Datenschutz ist mir egal“ – das ist nach drei Jahren DSGVO endgültig keine Option mehr.

4 DATENAUSKUNFT ALS DATENPANNE?

Die Umsetzung der DSGVO bereitet gerade bei den Betroffenenrechten weiterhin Probleme. So haben Unternehmen oftmals noch keinen richtigen Prozess, um Auskunftsersuchen datenschutzgerecht nachzukommen. So muss etwa geklärt werden, ob die anfragende Person wirklich die betroffene Person ist.

Fristen einzuhalten ist nicht alles

Stellen Sie sich vor, Sie sollen einen Antrag auf Auskunft bearbeiten. Sie müssen feststellen, ob Ihr Betrieb personenbezogene Daten verarbeitet, die die anfragende Person betreffen. Ist das der Fall, klären Sie, welche Daten dies sind und zu welchem Zweck Ihr Betrieb sie verarbeitet. Sie bereiten nun eine Kopie der personenbezogenen Daten vor, die Gegenstand der Verarbeitung sind, um diese Informationen zur Verfügung zu stellen.

Dabei können Sie sich nicht beliebig Zeit lassen. Denn die Auskunft muss unverzüglich, also ohne schuldhaftes Zögern, erteilt werden, spätestens jedoch binnen eines Monats nach Eingang des Auskunftsersuchens. Nun darf es aber nicht passieren, dass Sie möglichst schnell die Datenkopie verschicken – sonst könnte die Datenauskunft zu einer Datenpanne werden.

Die Identität des Antragstellers muss geklärt sein

Die Aufsichtsbehörden für den Datenschutz haben mehrfach deutlich gemacht: Es muss sichergestellt sein, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten.

Das bedeutet somit, dass Sie sicherstellen müssen, dass die Person, die die Auskunft wünscht, auch tatsächlich das Recht dazu hat, also tatsächlich die betroffene Person oder eine von der betroffenen Person bevollmächtigte Person ist. Das sollte jedes Unternehmen durch einen Prozess sicherstellen. Bei vielen Unternehmen ist dem aber noch nicht so, auch wenn die DSGVO bereits drei Jahre zur Anwendung kommt.

Nicht auf die falsche Prüfung der Identität setzen

Nun gibt es verschiedene Wege, um die Identität einer anfragenden Person zu überprüfen. Dabei muss dieser Weg zum einen datenschutzgerecht sein, also zum Beispiel keine unnötigen Daten abfragen. Zum anderen muss der gewählte Weg aber auch sicher genug sein.

Wenn Sie das Verfahren in Ihrem Unternehmen noch nicht kennen, erkundigen Sie sich bitte, bevor Sie ein Auskunftsersuchen bearbeiten. Wichtig ist auch, dass Sie die Einschränkungen der Verfahren kennen, die gern in der Praxis genutzt werden.

Ob beispielsweise die Identifizierung über ein Nutzerkonto (also Benutzername und Passwort) sicher ist, hängt sehr stark vom Passwort ab, das der Nutzer vergeben hat. Ist es zu leicht zu knacken, können Angreifer Nutzerkonten übernehmen und damit weitere Daten ausspähen – womöglich dann über ein Auskunftsersuchen mit gefälschter Identität.

Kennt also eine anfragende Person das Passwort der betroffenen Person, das für einen Online-Dienst Ihres Unternehmens besteht, und kann sie sich einloggen, bedeutet dies nicht, dass es wirklich die betroffene Person ist, die die Anfrage stellt. Seien Sie also vorsichtig,

denn Identitätsdiebstahl im Internet greift um sich. So basieren die stark verbreiteten Phishing-Attacken genau auf einer gefälschten digitalen Identität, die Vertrauen erwecken und vertrauliche Daten herauslocken soll. Das Auskunftsersuchen per Mail kann also auch eine Fälschung sein.

Ist es wirklich die betroffene Person? Machen Sie den Test!

Beantragt eine Person Auskunft über eine bekannte E-Mail-Adresse, kann man davon ausgehen, dass die Anfrage echt und berechtigt ist. Stimmt das?

1. Nein, denn die Absenderangaben können gefälscht sein.
2. Ja, aber nur, wenn es sich um eine verschlüsselte, signierte E-Mail des Absenders handelt.

Lösung:

Die Antworten 1 und 2 sind richtig. Absenderangaben bei E-Mails lassen sich fälschen, dafür muss man nicht einmal das E-Mail-Passwort des Betroffenen haben, es reicht das Editieren der Absenderangaben im Mail-Programm des (kriminellen) Absenders. Konnten Angreifer aber das E-Mail-Passwort stehlen, kann die E-Mail sogar echt sein. Doch die Identität ist eine gestohlene und stimmt nicht. Der Bundesdatenschutzbeauftragte schreibt zum Auskunftsrecht: Es empfiehlt sich, die Auskunft schriftlich oder in einer sicheren elektronischen Form (etwa per De-Mail oder mittels verschlüsselter E-Mail über das Programm Pretty Good Privacy (PGP) oder GnuPG) anzufordern.

Die Kopie eines Personalausweises darf keine geschwärzten Stellen enthalten, wenn eine anfragende Person damit ihre Identität im Auskunftsersuchen nachweisen soll. Stimmt das?

1. Ja, die Kopie muss vollständig und gut zu lesen sein.
2. Nein, die Kopie muss leserlich sein, sie darf aber bestimmte Stellen enthalten, die geschwärzt wurden, weil sie für die Identitätsprüfung nicht notwendig sind.

Lösung:

Die Antwort 2 ist richtig. Die Aufsichtsbehörden für den Datenschutz haben zum Thema „Kopie des Personalausweises“ darauf hingewiesen, dass man als Betroffener die nicht erforderlichen persönlichen Daten auf der Kopie des Ausweises (wie Augenfarbe, Größe, ID-Nummer, Unterschrift) schwärzen sollte. Andere Daten wie der Name und der Vorname dürfen natürlich nicht unkenntlich gemacht sein.

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de