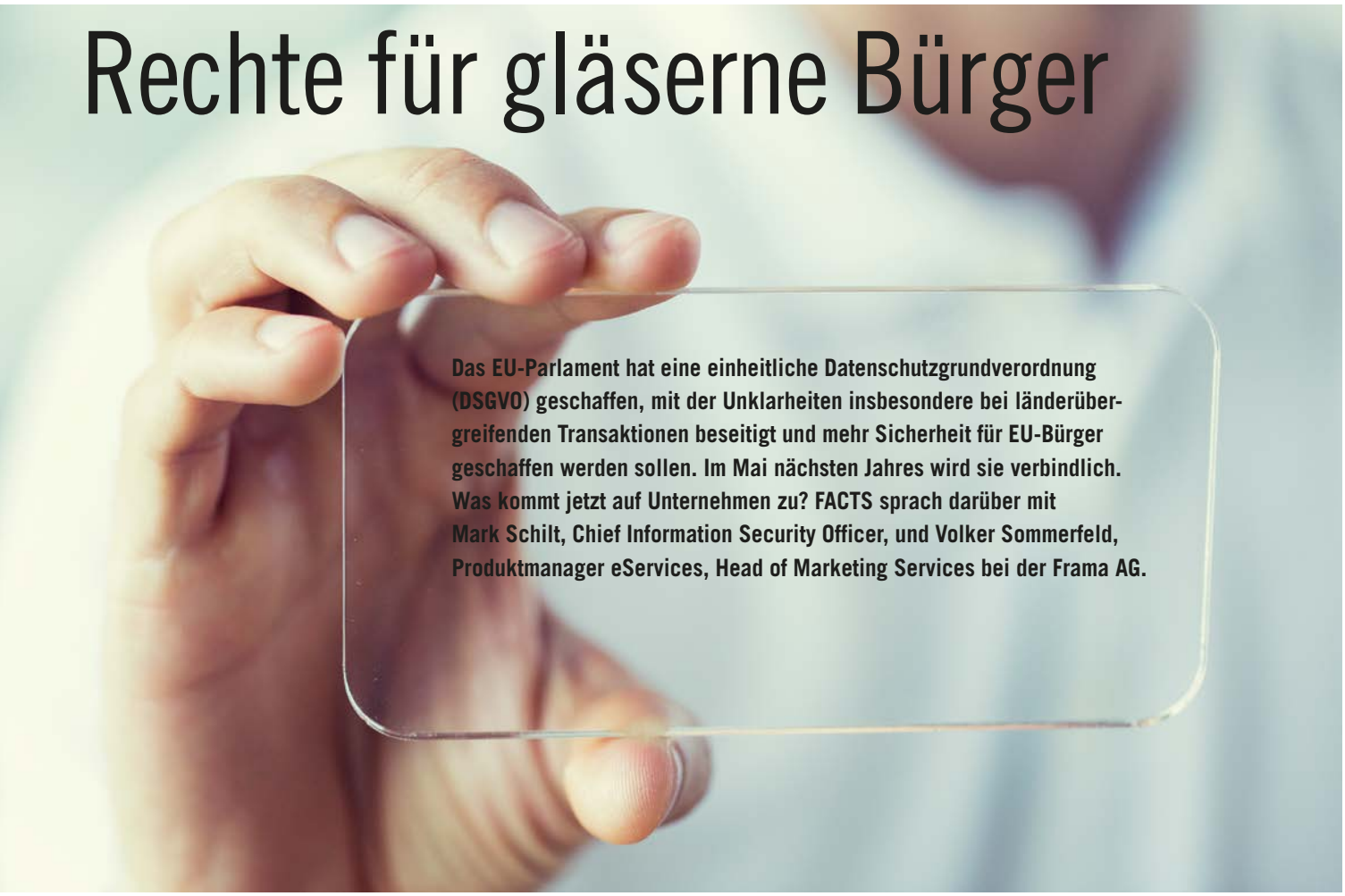
Rechte für gläserne Bürger



Das EU-Parlament hat eine einheitliche Datenschutzgrundverordnung (DSGVO) geschaffen, mit der Unklarheiten insbesondere bei länderübergreifenden Transaktionen beseitigt und mehr Sicherheit für EU-Bürger geschaffen werden sollen. Im Mai nächsten Jahres wird sie verbindlich. Was kommt jetzt auf Unternehmen zu? FACTS sprach darüber mit Mark Schilt, Chief Information Security Officer, und Volker Sommerfeld, Produktmanager eServices, Head of Marketing Services bei der Frama AG.

FACTS: *Mitte 2018 tritt die neue Datenschutzgrundverordnung in Kraft, die in der gesamten EU Wirkung haben soll. Was sind Ihrer Meinung nach ihre wichtigsten Merkmale bezüglich Chancen und Risiken?*

Mark Schilt: Vorweg ein wenig trockene Kost, denn wir müssen uns zuerst um den Begriff „Verordnung" kümmern. Verordnungen aus Brüssel gelten in der gesamten EU. Es ist Sache der jeweiligen Parlamente der Mitgliedsstaaten, geltendes nationales Recht an diese Verordnung anzupassen. Deutschland hat das bereits erledigt, am 12.05.2017 passierte das neue Bundesdatenschutzgesetz den Bundesrat und ersetzt ab dem 25.05.2018 das bestehende BDSG.

Volker Sommerfeld: In der Praxis heißt das, dass die Brüsseler DSGVO weitreichende Auswirkungen hat, denn sie regelt die Erhebung, das Abfragen, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, die Verwendung, die Übermittlung und Verbreitung sowie das Löschen von personenbezogenen Daten von – und hier liegt der Hase im Pfeffer – EU-Bürgern. Damit erstreckt sich der Wirkungsbereich weit über die EU hinaus! Denn das bedeutet, dass eine Firma mit Sitz zum Beispiel in den USA, die personenbezogene Daten von EU-Bürgern besitzt oder auch nur bearbeitet, ebenfalls an die Bestimmungen der DSGVO gebunden ist.

Schilt: Genau, aber da es pro Land eine spezifische Umsetzung der DSGVO gibt, könnte hier eine Herausforderung für die Akzeptanz der Verordnung bei Unternehmen vorliegen. Ein Beispiel: Die DSGVO fordert bei der Einwilligungspflicht zur Datenverarbeitung, dass Kinder unter 16 Jahren die Einwilligung ihrer Eltern benötigen, länderspezifisch kann dieses Alter auf 13 Jahre gesenkt werden. Ich bin gespannt, wie global tätige Unternehmen mit diesem Punkt umgehen werden.

Die neue Verordnung bringt aber viel Gutes und Chancen mit sich. Drei Beispiele: Neu gibt es eine Pflicht zur unverzüglichen Anzeige von Datenschutzverletzungen. Dass ein Diebstahl von mehreren Millionen E-Mail-Accounts erst zwei Jahre später an die Öffentlichkeit kommt, sollte somit nicht mehr vorkommen. Bei Verletzungen des Datenschutzes muss der Vorfall innerhalb einer Frist von 72 Stunden an die zuständige Aufsichtsbehörde gemeldet werden, je nach Schwere der Datenpanne sind unter Umständen direkt die betroffenen Personen zu benachrichtigen.

Neu ist auch die aktive Rechenschaftspflicht der an den Daten verarbeitenden Prozessen beteiligten Firmen gegenüber dem Bürger, um die Einhaltung des Datenschutzes zu demonstrieren. Angenommen, eine Person vermutet eine sie betreffende Datenschutzverletzung, so ist die verantwortliche Unternehmung in der Pflicht, jederzeit aufzeigen zu können, dass der Umgang vollumfänglich korrekt war.

Am wichtigsten für betroffene Personen ist das gesetzlich neu verankerte „Recht auf Löschung" oder auch umgangssprachlich das „Recht auf Vergessen". Das bedeutet, dass auf

entsprechenden Antrag – falls nicht weitere bestehende Gesetze dies verhindern – Daten gelöscht werden müssen. Ob die Aussage: „Das Internet vergisst nie“ jemals hinfällig wird, ist noch ungewiss.

FACTS: *Glauben Sie, dass die DSGVO wirklich etwas verbessern kann – oder handelt es sich doch eher um einen zahnlosen Tiger?*

Sommerfeld: Das Thema wird im Hintergrund heiß diskutiert. Wir würden uns über mehr Öffentlichkeitsarbeit und über eine breitere und publikumswirksame Diskussion der verantwortlichen Stellen freuen, auch um mehr sensibilisieren zu können. Wie oft höre ich: „Datenschutz? Mir egal, ich habe doch nichts zu verbergen.“ Schon einmal darüber nachgedacht, welche Flut an personenbezogenen Daten allein das simple Buchen einer Auslandsreise mit sich bringt und was damit alles angestellt werden kann? Ich habe es selbst erlebt: Mein Reisebüro fragte an, ob ich ihm eine Kopie meines Reisepasses zumailen könnte; das tat ich, sicher verschlüsselt. Anschließend erhielt ich den Reiseverlauf per unverschlüsslter E-Mail zugestellt – das ist ein Quasi-Standard bei Fluggesellschaften. Übertragen wir das auf die analoge Welt: Niemand von uns würde seinen Pass als Postkarte versenden und niemand würde den Reiseverlauf an seine Haustür nageln zur Information für dunkle Gestalten! Nicht nur bei solch eher banalen Vorgängen greift der Gesetzgeber nun strafbewehrt ein – und das ist gut so. Und noch etwas Wichtiges: Die DSGVO gilt eben auch für das kleine Reisebüro um die Ecke, nicht nur für den Internet-Großkonzern.

„Übertragen wir den Umgang mit E-Mails auf die analoge Welt: Niemand von uns würde seinen Pass als Postkarte versenden und niemand würde den Reiseverlauf an seine Haustür nageln zur Information für dunkle Gestalten!“

VOLKER SOMMERFELD, Produktmanager eServices & Head of Marketing Services bei der Frama AG

Schilt: Da der Tiger auf dem Papier durch die möglichen hohen Geldbußen bei Verstößen – bis zu 20 Millionen Euro oder bis zu vier Prozent des globalen Umsatzes – scheinbar große Zähne hat, wird zumindest in der Wirtschaft ein gewisses Bewusstsein geschaffen. Es bleibt zu hoffen, dass die Informations- und Einwilligungspflicht auch zu einer Sensibilisierung der Bürger führen wird. Sind wir heute nicht an einem Punkt angelangt, an dem sich jede einzelne Person Gedanken darüber machen sollte, wie gläsern und berechenbar sie sich durch den zu laschen Umgang mit den eigenen Daten macht?

„Wir wünschen uns, dass die DSGVO mit Augenmaß und entsprechender Konsequenz durchgesetzt wird, ohne Sonderstatus für bestimmte Berufsgruppen, Unternehmen und Verbände.“

MARK SCHILT, Chief Information Security Officer bei der Frama AG

Ob der Tiger wirklich messerscharfe Zähne bekommt, hängt von der Durchsetzung durch die EU-Staaten und von der Auslegung durch die jeweiligen Aufsichtsbehörden ab. Wir wünschen uns, dass die DSGVO mit Augenmaß und entsprechender Konsequenz durchgesetzt wird, ohne Sonderstatus für bestimmte Berufsgruppen, Unternehmen und Verbände.

FACTS: *Wie können Unternehmen sich auf die neue Regelung vorbereiten – und was kommt an Aufwand und Kosten auf sie zu?*

Schilt: Diese Frage allgemein zu beantworten ist relativ schwer, da insbesondere die Kosten zur Umsetzung davon abhängig sind, wie weit und wie intensiv das Thema Datenschutz bisher Beachtung fand. Unternehmen, die sich bisher nicht oder nur wenig mit Datenschutz beschäftigt haben, stehen sicherlich vor einer nicht unerheblichen Herausforderung. Doch auch Unternehmen, die „im Thema“ sind, sollten Weisungen und Verträge auf Konformität prüfen, verifizieren, ob die Informations- und Einwilligungspflichten wahrgenommen werden, allfällig nötige Prozessanpassungen – insbesondere in Bezug auf das Löschbegehren – vornehmen und prüfen, ob die Dokumentations- und Nachweispflichten eingehalten werden.

Elementar wichtig ist hierbei, einen risikobasierten Ansatz zu wählen und diesen nachvollziehbar zu dokumentieren. Schon die Bedingungen für die Verhängung von Geldbußen ›


ZUSTELLUNGSNACHWEIS
EINGESCHRIEBENER NACHWEIS ÜBER ZUSTELLUNG, INHALT & ZEIT
RMail
Dieser Zustellungsnachweis ist ein verifizierbarer Nachweis Ihrer eingeschriebenen E-Mail.
Der Zustellungsnachweis ermöglicht dem Besitzer, die gesamte Transaktion inklusive Zustellung, Öffnung, Inhalt und Zeitstempeln nachzuvollziehen. Je nach Service enthält der Zustellungsnachweis auch die Angaben bezüglich Verschlüsselung und/oder elektronischer Unterschrift.
Um diesen Zustellungsnachweis zu verifizieren, leiten Sie ihn weiter an 'verify@r1.rpost.net'
Status der Zustellung
Adresse | Status | Details | Zugestellt (UTC*) | Zugestellt (lokal) | Geöffnet (lokal)
sandra.muster@frama.com | Gesendet an Postfach | Delivery confirmed by recipient mail server at | 26/01/2017 04:00:48 PM (UTC) | 26/01/2017 04:00:48 PM | 26/01/2017 04:56:54 PM
*UTC steht für Coordinated Universal Time.
Message Envelope
Von: joerg.muster@frama.com <joerg.muster@frama.com>
Betreff: Nachvollziehbare E-Mail
An: <sandra.muster@frama.com>
Cc:
Bcc:
Network ID:
Vom RMail Server empfangen: <SM21KwdUcnxO5IbvTvC000008d2@
Kundenreferenz: 03/01/2017 04:00:46 PM (UTC)
Message Statistik
Tracking-Nummer:
Größe: 980284C835825B45A4FEDCB3912CCC47064EFF20
Eigenschaften verwendet: 63588
Zustellung: Audit Trail

ZUSTELLUNGSNACHWEIS: Bei RMail kann im Nachhinein belegt werden, wer wann was mit welchem Inhalt bekommen hat.

› geben wichtige Hinweise, wo mit der Umsetzung zu beginnen ist. Unternehmen die ein etabliertes Managementsystem (zu ISO 9001, ISO27001 etc.) im Einsatz haben, sollten prüfen, wie die einzelnen Aspekte der neuen Gesetzgebung in dieses System integriert werden können. Wesentliche Aspekte zur Erfüllung der Dokumentations- und Nachweispflicht können aus bestehenden Systemen übernommen werden. Unter diesem Gesichtspunkt und unter der Voraussetzung, dass Datenschutz zuvor schon ein Thema war, sollten die Kosten für die Umsetzung aus meiner Sicht zwar spürbar, jedoch nicht gravierend sein.

FACTS: *Datenschutz ist ja nicht nur etwas, das verordnet werden kann, indem der Umgang mit Fremddaten geregelt wird, sondern jede Person und jedes Unternehmen muss dafür Sorge tragen, die eigenen Daten zu schützen. Das betrifft ganz besonders elektronischen Datenaustausch bei der Kommunikation. Welche Vorteile bietet RMail gegenüber anderen Ansätzen?*

Sommerfeld: Hier müssen wir erneut anmerken, dass die DSGVO einen risikobezogenen Ansatz fährt. Die fundamentalen Rechte und die Selbstbestimmung des Einzelnen über die eigenen personenbezogenen Daten müssen gegen die Organisation und Prozesse ausbalanciert werden. Das heißt, dass jeder bestehende und neue Prozess, jeder bestehende und neue Service, der personenbezogene Daten verarbeitet, speichert oder überträgt, von Risk-Assessments und der daraus abgeleiteten Dokumentation und aktiver Demonstration der Compliance mit der DSGVO begleitet wird.

Viele gut gemeinte Ansätze zur Umsetzung des Datenschutzes in Services oder Produkten sind allerdings an der mangelnden Akzeptanz der Nutzer zugrunde gegangen. Beispiele: De-Mail, Volksverschlüsselung oder die Online-Ausweisfunktion des Personalausweises. Und noch etwas ist wichtig: Was nützt es, wenn Datenschutz an der Landesgrenze aufhört? Schon einmal versucht, eine De-Mail nach Spanien zu senden?

Mit RMail bieten wir einen interessanten Ansatz für die Belange des schriftlichen Datenaustauschs personenbezogener Daten, gemäß etwa Artikel 5, §§1f, 2 oder auch Artikel 32 DSGVO. RMail gewährleistet bei Bedarf den sicheren Datenaustausch (Compliance by Design), erreicht eine sehr hohe Akzeptanz auf Empfängerseite, da der Empfänger keinen eigenen RMail-Account benötigt, und macht an der Landesgrenze nicht Halt. RMail liefert mit dem Zustellungsnachweis einen Compliance-Record, der die Einhaltung der Anforderungen der DSGVO in Bezug auf den einzelnen Vorgang dokumentiert und aktiv nachweist (auditable Proof of Compliance).

Die Integration in bestehende Systeme ist einfach und schnell erledigt. RMail steht als Plug-in für Outlook oder Gmail zur Verfügung oder kann direkt in Unternehmenssysteme eingebunden werden, zum Beispiel über API oder Domain-Extension. Zu unseren Kunden zählen Reiseversicherungen, aber auch Kliniken, Klinikverbände, Kanzleien von Rechtsanwälten und Notaren, Arztverbände, Radiologen sowie Entwicklungsbüros und Immobilienunternehmen … Kurzum: Immer dann, wenn Informationen sicher und nachweisbar ausgetauscht werden müssen, hilft RMail, diese Aufgabe effizient zu lösen, für die DSGVO natürlich mit Compliance-Nachweis!

Anja Knies ■

INFO Am 25. Mai 2018 geht's los – die Uhr tickt!

Ab dem 25. Mai 2018 ist die DSGVO unmittelbar in den EU-Mitgliedsstaaten geltendes Recht. Der Anwendungsbereich der DSGVO ist sehr weit gefasst: Ziel ist der Schutz personenbezogener Daten (Name, Geburtsdatum, IP-Adresse etc.) als Ausfluss des Persönlichkeitsrechts jeder Person. Es ist Unternehmen dringend anzuraten, sich auf die damit verbundenen Änderungen in Bezug auf den Umgang mit personenbezogenen Daten rechtzeitig und adäquat einzustellen. Beachtlich ist insbesondere, dass die Bußgelder für etwaige Verstöße auf 20 Millionen Euro beziehungsweise im Fall von Unternehmen auf bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes angehoben wurden.


DR. STEFFEN ALBICKER

Rechtsanwalt Dr. Steffen Albicker
Fachanwalt für Arbeitsrecht
Fachanwalt für Handels- und Gesellschaftsrecht
www.bmt.eu