EU-DSGVO
Höchste Zeit zu handeln

Ab dem 25. Mai 2018 wird die EU-Datenschutz-Grundverordnung die bisherigen nationalen Datenschutzgesetze der EU-Mitgliedstaaten verdrängen. Eine Verordnung, die es in sich hat: Ob verschärfte Wahrung von Betroffenenrechten oder massiv erhöhte Bußgelder – die EU-DSGVO bedeutet vor allem eines: viel Vorarbeit und Sorgfalt in punkto Implementierung. Stand heute bleiben faktisch gerade 11 Monate zur Umsetzung der Bestimmungen. Tilman Dralle und Thomas Werner, beide Juristen und Experten für Datenschutzmanagement bei TÜV Rheinland, im Interview, wie sich Unternehmen auf die Verordnung aus Brüssel einstellen sollten.

Tilman Dralle, Jurist und Experte für Datenschutzmanagement bei TÜV Rheinland

Thomas Werner, Jurist und Experte für Datenschutzmanagement bei TÜV Rheinland

? Herr Werner, warum jetzt wieder eine Verordnung aus Brüssel?

Werner: Faktisch ging es darum, ein einheitliches, hohes Datenschutzniveau herzustellen: Das war das Ziel, das der europäische Gesetzgeber mit der Datenschutz-Grundverordnung (EU-DSGVO) verfolgte. Doch die erwünschte EU-weite Vereinheitlichung des Datenschutzrechts wurde nicht in allen Punkten konsequent umgesetzt. Denn die neue EU-DSGVO beinhaltet rund 60 sogenannte „Öffnungsklauseln", die es den Mitgliedstaaten in vielen Bereichen erlauben, unter gewissen Voraussetzungen von den europäischen Standards abzuweichen. Diese Möglichkeit hat Deutschland auch genutzt: mit dem „BDSG 2018".

? Herr Dralle, könnten Sie einmal näher erläutern, was Unternehmen mit Blick auf die AusnahmeregEU-DSGVO: Höchste Zeit zu handeln

Dralle: Ab dem 25. Mai 2018 wird die EU-Datenschutz-Grundverordnung die bisherigen nationalen Datenschutzgesetze der EU-Mitgliedstaaten verdrängen. Eine Verordnung, die es in sich hat: Ob verschärfte Wahrung von Betroffenenrechten oder massiv erhöhte Bußgelder – die EU-DSGVO bedeutet vor allem eines: viel Vorarbeit und Sorgfalt in punkto Implementierung. Stand heute bleiben faktisch gerade 11 Monate zur Umsetzung der Bestimmungen. Tilman Dralle und Thomas Werner, beide Juristen und Experten für Datenschutzmanagement bei TÜV Rheinland, im Interview, wie sich Unternehmen auf die Verordnung aus Brüssel einstellen sollten.

? Herr Werner, warum jetzt wieder eine Verordnung aus Brüssel?

Werner: Faktisch ging es darum, ein einheitliches, hohes Datenschutzniveau herzustellen: Das war das Ziel, das der europäische Gesetzgeber mit der Datenschutz-Grundverordnung (EU-DSGVO) verfolgte. Doch die erwünschte EU-weite Vereinheitlichung des Datenschutzrechts wurde nicht in allen Punkten konsequent umgesetzt. Denn die neue EU-DSGVO beinhaltet rund 60 sogenannte „Öffnungsklauseln", die es den Mitgliedstaaten in vielen Bereichen erlauben, unter gewissen Voraussetzungen von den europäischen Standards abzuweichen. Diese Möglichkeit hat Deutschland auch genutzt: mit dem „BDSG 2018".

? Herr Dralle, könnten Sie einmal näher erläutern, was Unternehmen mit Blick auf die Ausnahmeregelungen im „Bundesdatenschutzgesetz 2018" beachten sollten?

Dralle: Das BDSG 2018 enthält zahlreiche Bestimmungen, die die EU-DSGVO ergänzen, konkretisieren bzw. modifizieren. Alle datenverarbeitenden Unternehmen in Deutschland sollten sich eingehend mit den neuen Regelungen auseinandersetzen. Insbesondere die Reichweite der komplexen Ausnahmetatbestände sollten sie gewissenhaft und im Zweifel mit Hilfe externer Sachverständiger prüfen.
Denn nach der EU-DSGVO verstößt ein privates Unternehmen auch dann gegen die Verordnung, wenn es nationale Anpassungs- bzw. Umsetzungsregelungen verletzt, die auf der Grundlage von Öffnungsklauseln erlassen wurden.

? Klingt kompliziert…

Dralle: Ist es. Insbesondere großen Unternehmen, die in mehreren EU-Mitgliedstaaten präsent sind und dort personenbezogene Daten verarbeiten, raten wir, die Bestimmungen der EU-DSGVO über weite Strecken eins zu eins umzusetzen. Die Vorteile eines klaren Bekenntnisses zum „Gold-Standard" der EU-DSGVO liegen auf der Hand: Ein einheitliches Datenschutz-Management mit klaren Regeln in allen EU-Mitgliedstaaten ist effizienter und damit kostensparender als ein geografisch fragmentierter Datenschutz-Ansatz. Nichtsdestotrotz entscheidet am Ende der Einzelfall, ob und in welchem Ausmaß eine Nutzung von Ausnahmetatbeständen im BDSG 2018 unternehmerisch

sinnvoll ist. Dies gilt sowohl für große Unternehmen als auch für KMUs.

? Welche Empfehlungen haben Sie in Bezug auf den Accountability-Ansatz? Das bedeutet einen erheblich gestiegenen Dokumentationsaufwand im Vergleich zum bisherigen Bundesdatenschutzgesetz …

Werner: Genau. Jede verantwortliche Stelle muss den Nachweis erbringen können, dass sie personenbezogene Daten rechtskonform nach den Vorgaben der DGSVO verarbeitet. Ohne Datenschutzmanagementsystem ist diese Nachweis-Pflicht nicht professionell zu meistern.
Mit der Einführung eines solchen Managementsystems können erhebliche Haftungsrisiken gleich von Beginn an vermieden werden. Außerdem spielt die Erfüllung der Rechenschafts- und Dokumentationspflicht bei Prüfungen durch die Aufsichtsbehörden oder Prüfdienstleister eine wichtige Rolle.

? Mit der EU-DSGVO wird sich der Bußgeldrahmen erheblich ausweiten: Es sind Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Vorjahresumsatzes möglich.

Werner: Richtig. Unternehmen sollten aber wissen: Die EU-DSGVO enthält einen Katalog von Kriterien, die einen Einfluss auf die Bußgeldverhängung und -bemessung haben.
Hierzu gehören u. a. frühere Verstöße, getroffene technisch-organisatorische Maßnahmen, Zusammenarbeit mit den Aufsichtsbehörden und eine Datenschutz-Zertifizierung. Unternehmen sollten diese Kriterien berücksichtigen, um Bußgeldrisiken so weit wie möglich zu minimieren.

? Wie sehen Sie die Datenschutz-Folgenabschätzung?

Dralle: Das bisherige Instrument der „Vorabkontrolle" weicht dem Konzept der Datenschutz-Folgenabschätzung (DSFA). Gibt es bei einer geplanten Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der entsprechend betroffenen Personen, muss das Unternehmen eine DSFA vor Beginn der Datenverarbeitung vornehmen. Entgegen der Auffassung einiger Juristen ist die DSFA nicht nur für neue Verarbeitungsvorgänge relevant.
Datenverarbeitenden Stellen ist zu raten, eine Folgenabschätzung auch für bestehende Verarbeitungen durchzuführen, sofern ein „hohes Risiko" besteht. Die durchgeführten Risikobewertungen müssen nachvollziehbar dokumentiert werden.

? Die EU-DSGVO sieht jetzt auch „Privacy by Design" und „Privacy by Default" vor.

Dralle: Das bedeutet, dass Datenschutz integraler Bestandteil der Entwicklung sein muss, sowohl bei Produkten, Diensten als auch Anwendungen. Und: „Maximaler" Datenschutz muss die „serienmäßige" Grundeinstellung sein und nicht mehr die Option, die der Betroffene aktiv anwählen muss. Wichtig zu wissen: Insbesondere die „Privacy by Design"-Anforderungen treffen die verantwortlichen Stellen, und nicht die Hersteller von Produkten, Diensten und Anwendungen. Hier müssen die datenverarbeitenden Unternehmen frühzeitig Druck auf diese Hersteller ausüben, um ab dem 25.5.2018 EU-DSGVO-konforme Technik im Einsatz zu haben.
Die frühzeitige Berücksichtigung der Anforderungen vermeidet in jedem Fall spätere Abweichungen von den gesetzlichen Vorgaben und verringert somit Haftungs- und Bußgeldrisiken.

? Was empfehlen Sie in Bezug auf die noch umfassender geregelten Löschpflichten?

Werner: Neben der allgemeinen Verpflichtung, Daten unter bestimmten Voraussetzungen auf den eigenen Systemen zu löschen, müssen Unternehmen zukünftig weitere Schritte unternehmen. Im Rahmen des neuen „Rechts auf Vergessenwerden" müssen Dritte, die veröffentlichte Daten verarbeiten, identifiziert und sodann über das Löschbegehren informiert werden.
Wie genau die erweiterten Löschverpflichtungen in der EU-DSGVO in der Praxis umgesetzt werden sollen, ist bislang noch weitgehend unklar. Allen Unternehmen, die regelmäßig personenbezogene Daten öffentlich machen, wird daher empfohlen, die aktuellen Entwicklungen zum „Recht auf Vergessenwerden" aufmerksam zu verfolgen. Dies betrifft insbesondere die Stellungnahmen des Europäischen Datenschutzausschusses.

? Bei Schwachstellen im Bereich der technisch-organisatorischen Datensicherheit, wie etwa veraltete Verschlüsselungsstandards, drohen nun auch Bußgelder und zwar drastische, mit bis zu 2 Prozent des Vorjahresumsatzes. Wie sollten Unternehmen mit der Verschärfung in Bezug auf technische und organisatorische Maßnahmen (TOMs) umgehen?

Dralle: Aus Sicht der datenschutzrechtlichen Praxis ist diese Neujustierung kaum zu überschätzen. Nützliche Best-Practice-Hinweise gibt die TOM-Liste nach IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI): Wichtig sind beispielsweise Notfallpläne im Rahmen des Business-Continuity-Managements, Identity-and-Access-Management, Rollenberechtigungen nach dem „Need to know"-Prinzip, aktuelle Verschlüsselungsverfahren sowie eine hochverfügbare Speicherung von Daten.

? Stichwort Datenportabilität: Der EU-DSGVO zufolge müssen Unternehmen personenbezogene Daten auf Antrag in einem gängigen und maschinenlesbaren Format entweder an den User oder gleich an ein anderes Unternehmen übergeben können. Für welche Unternehmen hat dieser Punkt Relevanz?

Werner: Die genaue Reichweite des Rechts auf Datenportabilität (Stichwort: interoperable Formate) kann noch nicht abschließend bewertet werden. Klar ist allerdings schon jetzt, dass es nicht nur für große Internet-Konzerne, sondern auch für mittelständische Unternehmen hohe Relevanz hat.

? Lediglich beim Thema Datenschutzbeauftragter ändert sich wenig, richtig?

Werner: Nicht ganz. Auch in Zukunft müssen alle Unternehmen, die mindestens zehn Personen mit automatisierter Verarbeitung beschäftigen, einen Datenschutzbeauftragten bestellen. In diesem Punkt gibt es tatsächlich keine Änderung.
Bei einer umfangreichen Verarbeitung besonders sensitiver personenbezogener Daten kann die Bestellpflicht künftig jedoch auch dann greifen, wenn das jeweilige Unternehmen unter der 10-Personen-Grenze liegt und bisher keinen Datenschutzbeauftragten benennen musste.
Dies könnte insbesondere ärztliche Gemeinschaftspraxen oder mit genetischen Analysen befasste Labors treffen. Hier gilt es, die weiteren Entwicklungen speziell auf Seiten der Aufsichtsbehörden genau zu verfolgen.

? Die EU-DSGVO bietet auch die Möglichkeit einer Zertifizierung.

Dralle: Das Zertifizierungsverfahren dient dem Nachweis, dass die Bestimmungen der EU-DSGVO in vollem Umfang eingehalten werden. Das Vorliegen einer entsprechenden Zertifizierung wird zukünftig eine wichtige Rolle spielen, so u.a. bei der Entscheidung über das Ob und die Höhe von Bußgeldern.
Darüber hinaus hat sie zweifelsohne großes Potenzial als wettbewerbsdifferenzierendes Element. Unternehmen, für die die Verarbeitung personenbezogener Daten Teil ihres Kerngeschäftes ist, wird geraten, Datenschutz als Wettbewerbsvorteil zu begreifen und die Vorteile und Kosten einer Zertifizierung in diesem Lichte sorgsam abzuwägen.

? Was raten Sie bei der Auswahl externer Berater zur Umsetzung der EU-DSGVO?

Die Consultants sollten die EU-DSGVO nicht allein durch die juristische Brille betrachten, sondern über Erfahrung in der Umsetzung von Managementsystemen und über ein umfassendes Verständnis informationssicherheits-technologischer Zusammenhänge verfügen.
Wer mit Blick auf den 25. Mai 2018 die Unterstützung fachkundiger Dritter sucht, sollte bald handeln, denn der Wettbewerb um qualifizierte Berater ist in vollem Gange.

? Was passiert, wenn die Umstellung bis zum Stichtag 25. Mai 2018 nicht gelingt?

Organisationen riskieren in diesem Falle empfindliche Sanktionen. Strafmildernd dürfte sich allerdings der Nachweis auswirken, dass sich das Unternehmen bereits eingehend mit der Thematik befasst hat.

Tilman Dralle, Thomas Werner, TÜV Rheinland