

19.3.2018

Zeit für Regimewechsel im Datenschutz läuft aus

Axel Anderl, Nino Tlapak

In 67 Tagen müssen alle Unternehmen, die mit persönlichen Daten zu tun haben, die strengen Auflagen der Datenschutz-Grundverordnung umsetzen

Mit 25. Mai wird das bisher bekannte Regime des Datenschutzgesetzes 2000 durch die neue Rechtsordnung, nämlich die europäische Datenschutz-Grundverordnung (DSGVO) und das dazugehörige nationale Datenschutzgesetz 2018 (DSG 2018), ersetzt. Damit neigt sich die für die Vorbereitung und Implementierung der zahlreichen neuen Pflichten und Dokumentationsmaßnahmen gewährte zweijährige Übergangsfrist seit dem Inkrafttreten der Verordnung am 24. Mai 2016 dem Ende zu.



illustration: davor markovic

Wer sich bisher noch nicht mit dem neuen Rechtsrahmen der Datenschutz-Grundverordnung beschäftigt hat, wird eine vollumfängliche Implementierung aller Vorgaben ohne erhebliche Einschränkung des täglichen Geschäftsbetriebs nur noch schwer schaffen.

Wer sich bisher noch nicht mit dem neuen Rechtsrahmen beschäftigt hat und die Umsetzung im Betrieb angestoßen hat, wird eine vollumfängliche Implementierung aller Vorgaben ohne erhebliche Einschränkung des täglichen Geschäftsbetriebs nur noch schwer schaffen. Dementsprechend ist es zur Risiko- und damit Haftungsminimierung besonders wichtig, das Thema nun rasch unter Setzung der richtigen Prioritäten anzugehen.

Regimewechsel

Der große Umsetzungsaufwand unter dem neuen Datenschutzregime ergibt sich in der Praxis vorwiegend aus der bisherigen stiefmütterlichen Behandlung des Datenschutzes im unternehmerischen Umfeld, aber auch in der Verwaltung. Die Grundparameter der

datenschutzrechtlichen Zulässigkeitsprüfung haben sich – außer hinsichtlich der strengeren Prüfung von Einwilligungserklärungen – kaum verändert.

Grundsätzlich ist daher davon auszugehen, dass bisher geprüfte zulässige Systeme mit gewissen Anpassungen weiterhin rechtmäßig betrieben werden können. Da aber viele Unternehmen bislang die notwendigen Meldungen und Genehmigungen nicht gemacht bzw. eingeholt haben, besteht auf der materiellen Ebene eine aufzufüllende Lücke.

Dazu kommt der hinsichtlich des Dokumentations- und Meldewesens grundsätzlich geänderte Zugang: Nach dem noch geltenden alten Regime sind neue Prozesse vor Inbetriebnahme bei der Datenschutzbehörde zu melden. Darüber hinaus erfordern risikogeneigte Datenanwendungen – also besonders bei der Verwendung sensibler oder strafrechtlich relevanter Daten – zusätzliche behördliche Vorabprüfungen und Datentransfers ins EU-Ausland – in der Praxis mit einem langen Verfahren verbundene – Genehmigungen.

De facto haben jedoch nur die wenigsten Unternehmen – mit Ausnahme der Banken, Versicherungen und des Health-Care-/Pharmabereichs – in der Vergangenheit die Melde- und Genehmigungspflichten hinreichend ernst genommen. Dementsprechend sind die meisten Unternehmensmeldungen im online zugänglichen Datenverarbeitungsregister (DVR) lückenhaft.

Mit Anwendbarkeit der DSGVO müssen sämtliche personenbezogene Daten verarbeitenden Prozesse statt der Schleife über die Behörde vom verarbeitenden Unternehmen selbst umfassend dokumentiert, auf ihre datenschutzrechtliche Zulässigkeit geprüft und gegebenenfalls auf Basis einer intern durchzuführenden Risikoabschätzung adaptiert werden.

Zukünftig gibt es daher keine Vorab-Freizeichnung durch die Behörde. Stattdessen haben die personenbezogene Daten verarbeitenden Unternehmen eine eigenverantwortliche Entscheidung zu treffen, ob und in welchem Ausmaß die Verarbeitung zulässig ist. Diese ist zu dokumentieren, damit die mit erweiterten Kontrollbefugnissen ausgestattete Behörde sie im Anlassfall nachprüfen kann.

Lückenloser Überblick

Der Dreh- und Angelpunkt der DSGVO ist dabei das nach Artikel 30 zu führende Verzeichnis der Verarbeitungstätigkeiten, aus dem sich ein lückenloser Überblick über sämtliche Datenverarbeitungen und -ströme ergibt. Darauf aufbauend erfolgt dann für kritische Datenverarbeitungen eine Datenschutz-Folgenabschätzung, mit der die konkrete Zulässigkeit dokumentiert wird. Aber auch die weiteren Entscheidungen über die zusätzlichen Pflichten, wie zum Beispiel die Frage der Bestellung eines Datenschutzbeauftragten, sind für die Behörde nachvollziehbar festzuhalten.

Neben den formalen Aspekten wurden durch die DSGVO auch die Betroffenenrechte direkt und indirekt durch umfassendere Informationspflichten weiter gestärkt und besteht auch aufgrund verschärfter Bestimmungen ein Anpassungsbedarf bei den Zustimmungserklärungen zu Datenverarbeitungen sowie der bisherigen Dienstleistervereinbarungen bei der Hinzuziehung von Dritten bei der Datenverarbeitung. Insgesamt kommt daher doch ein erheblicher Anpassungsbedarf auf die Unternehmen, aber auch die öffentliche Hand zu.

Rechtsfolgen

Insgesamt stellt die Umstellung des Datenschutzregimes die Unternehmen vor große Herausforderungen. Verschärft wird dies durch die nun auch drastisch erhöhten Strafen, die bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Vorjahresumsatzes eines Konzerns ausmachen können. Die öffentliche Hand ist hier insoweit bevorzugt, als sie von den Pönalen ausgenommen ist. Dennoch wird es sich auch die Verwaltung kaum leisten können, wegen eines Verstoßes gegen das neue Regime in der Zeitung zu stehen.

Angesichts des nahenden Endes der Vorbereitungsfrist müssen Unternehmen ihre Umsetzungsprojekte zügig finalisieren oder – falls noch nicht gestartet – sofort und fokussiert angehen. (Axel Anderl, Nino Tlapak, 19.3.2018)

Axel Anderl ist Managing Partner bei Dorda Rechtsanwälte, leitet das IT/IP-Team und ist der Co-Leiter der Datenschutzgruppe.

Nino Tlapak ist Rechtsanwalt im IT/IP-Team und führend in der Datenschutzgruppe tätig. Beide werden bis zum 25. Mai mit wöchentlichen praxisnahen Beiträgen die wichtigsten Neuerungen und To-dos beschreiben.