Vieles ist beim neuen österreichischen Datenschutzgesetz noch offen. Gefordert sind persönliche Einschätzungen und Abwägungen. Die nicht ganz klare Gesetzeslage muss sich erst in der Praxis beweisen.

# Die Pra xis wird's richten

VON KARIN LEGAT

Datenschutz-Experte Kurt Einzinger empfiehlt, personenbezogene Daten nur dann zu verwenden, wenn dies zur Ausübung einer Geschäftstätigkeit unbedingt notwendig ist.

**DER AUFTRAGGEBER** WIRD ZUM »FÜR DIE VERARBEITUNG VERANTWORTLICHEN«, DER DIENSTLEISTER WIRD ZUM »AUFTRAGSVERARBEITER«.

**Nach Vorstellung und Erklärung eines Gesetzes hat es sich nicht angefühlt**, das Seminar an der Wirtschaftskammer zum neuen österreichischen Datenschutzgesetz, basierend auf der EU-Datenschutzgrundverordnung. Mehrfach wurde auf noch offene Punkte hingewiesen, obwohl zwei Jahre Zeit für Vorbereitung und Anpassung waren. Die DSGVO wurde am 25. Mai 2016 vom Europäischen Parlament beschlossen und gilt seit 25. Mai 2018 in Österreich. Sie ersetzt damit das bislang geltende Datenschutzgesetz 2000. Dazu passend die Zahlen des KSV aus einer aktuellen Umfrage: Nur 13 Prozent der Befragten halten sich in Bezug auf die DSGVO für sehr gut informiert, 39 Prozent für eher gut, 41 Prozent für mangelhaft und sieben Prozent für nicht informiert. Das DSGVO ist zwar eine europäische Verordnung, sieht aber gewisse Spielräume vor, um nationale Änderungen und Adaptionen zu ermöglichen. Diese hat Österreich auch genutzt. Kurt Einzinger, seit 1990 Mitglied des Österreichischen Datenschutzrates, externer Datenschutzbeauftragter und Geschäftsführer von netelligenz sowie Leiter des Seminars, bemerkt dazu: »Die Vorgangsweise war aber, auf Wienerisch gesagt, recht hatschert.« Aufgrund der fehlenden Zweidrittelmehrheit im Parlament konnten die Verfassungsbestimmungen des DSG 2000 nicht geändert werden. So wurde nur mit dem Datenschutz-Anpassungsgesetz das alte Gesetz novelliert und in Datenschutzgesetz, kurz DSG, umbenannt. Die Verfassungsbestimmungen bleiben gleich. Gerhard Wagner, Geschäftsführer des Kreditschutzverbandes: »Es gibt noch keine Judikatur. 2020 werden wir für manche Themen Klarstellungen haben.«

## TIPP

### *FÜR JEDE DATENVERARBEITUNG GILT:*

- Rechtmäßigkeit – bestehende Newsletter-Adressen dürfen weiter verwendet werden, bei neuen Daten braucht es eine Einwilligung.
- Zweckbindung – Daten dürfen nur für den Zweck verwendet werden, für den es die Einverständniserklärung gibt.
- Datenminimierung – Datensammlung soll auf den Zweck beschränkt werden.
- Richtigkeit
- Sicherheit (siehe TOM, Seite 14)
- Speicherbegrenzung – Daten dürfen nur so lang aufgehoben werden wie benötigt.
- Rechenschaftspflicht – per Logbuch müssen Aktionen nachgewiesen werden, etwa die beantragte Löschung von Daten.

Fabasoft bietet mit einer »EU-DSGVO Toolbox« eine SaaS-Lösung aus der Cloud. »Ab einer gewissen Komplexität des Unternehmens macht es Sinn, sich bei der DSGVO-Konformität durch ein Software-Tool unterstützen zu lassen. Das Führen des Verzeichnisses von Verarbeitungstätigkeiten ist ein zentraler Bestandteil der Toolbox. Es können auch die Prozesse zu den Betroffenenrechten digitalisiert und verwaltet werden«, bekräftigt Andreas Dangl, Geschäftsführer Fabasoft.

Foto: thinkstock, Fabasoft, WKW/FG Werbung

### >> Grundgedanke Personenschutz <<

Die Forderung, personenbezogene Daten zu schützen, ist europaweit angekommen. Betroffen ist jedes Unternehmen, vom Großbetrieb bis zum EPU. Das neue Datenschutzgesetz sollte laut Fachleuten als Anstoß gesehen werden, sich mit gespeicherten Personendaten auseinanderzusetzen und nach eingehender Bestandsanalyse neue Prozesse und dafür notwendige IT-Strukturen einzuführen.

### >> Was ist neu? <<

Beim Datenschutzgesetz sind Abwägung und Hausverstand gefragt. Mit einer guten Erklärung kann dem Datenschutz entsprochen werden, etwa zur benötigten Dauer, zum Umfang und zum Zweck der Speicherung personenbezogener Daten. Auf der sicheren Seite ist man in jedem Fall mit einer Einwilligung der betroffenen Person. Grundsätzlich benötigen Unternehmen eine Einwilligung zum Verarbeiten personenbezogener Daten. Für bestehende E-Mail-Verteiler, für die bereits eine Einwilligung erfolgt ist, müssen Firmen jedoch keine neuerliche Einwilligung einholen.

Umstritten war beim Wirtschaftskammer-Seminar der Begriff der Datenverarbeitung, der in der DSGVO nicht definiert ist. Als Verarbeiten gilt jedes Hantieren mit personenbezogenen Daten – zum Beispiel das Erfassen, Ordnen, Speichern, Übermitteln, Ablegen und Vernichten – unabhängig davon, ob dies mittels Computer oder in Papierform erfolgt. E-Mails zählen laut Einzinger im Sinn der DSVGO aber eher als Kommunikationsmittel, ebenso ein betriebliches Adressbuch.

Klar und ersichtlich ist, wen die DSGVO betrifft: natürliche Personen. Juristische Personen wie Gesellschaften und Vereine haben nicht länger Anspruch auf Schutz personenbezogener Daten, im Gegensatz zu veröffentlichten personenbezogene Daten, die Datenschutz genießen. UnternehmerIn- ▶

## TIPP

### *INFORMATIONSPFLICHT FÜR WEBSITES*

**Neben dem verpflichtenden Impressum auf** einer Website wird eine allgemeine Datenschutzerklärung zu folgenden Punkten empfohlen: Art und Weise der Verarbeitung personenbezogener Daten, Hinweis auf Betroffenenrechte und Beschwerdemöglichkeit, Kontaktdaten des Verantwortlichen sowie eine Beschreibung, wie die Website mit personenbezogenen Daten verfährt, zum Beispiel Log-Files, Cookies oder Google Analytics. Bei Formularen, für die personenbezogene Daten erhoben werden, wie etwa die Anmeldung zu einem Newsletter, braucht es einen zusätzlichen Informationstext mit Namen und Kontaktdaten des Verantwortlichen, Zweck der Verarbeitung und der Rechtsgrundlage. Die Anführung eines zusätzlichen Links zur Datenschutzerklärung ist sinnvoll.

▶nen sollen personenbezogene Daten nur insoweit verwenden, als dies zur Ausübung ihrer Geschäftstätigkeit notwendig ist, sonst sollen sie gelöscht werden. Das erfordert laut Datenschützern einen Paradigmenwechsel in der IT. Einzinger, selbst jahrelang als EDV-Leiter tätig: »Bisher war der Grundsatz jedes Rechenzentrums und jedes Datenverarbeiters, dass nichts verlorengehen darf. Es wurde möglichst dreimal gespeichert.«

Mit der Forderung der Löschung stellt sich vielfach die Frage der Machbarkeit, etwa in großen Datenbanksystemen. Hier hat Österreich seinen Spielraum genutzt: Wenn eine Löschung aus technischen Gründen nicht möglich oder sehr schwierig umzusetzen ist, reicht eine Einschränkung der Verarbeitung, das heißt, die Daten dürfen nicht mehr verwendet, müssen aber nicht gelöscht werden.

Eine weitere Forderung des neuen Datenschutzgesetzes: Führung eines Verzeichnisses von Verarbeitungstätigkeit ähnlich den derzeitigen DVR-Meldungen. Dieser Punkt ist nicht eindeutig, da der Begriff Verarbeitung nicht ausformuliert ist, es gibt auch keine Formvorschriften. Laut Datenschutzexperten müssen im Verzeichnis folgende Punkte enthalten sein: eigene Kontaktdaten, Zweck der Verarbeitung, Beschreibung der Datenkategorien und der Kategorien betroffener Personen, Empfängerkategorien, gegebenenfalls Übermittlung von Daten in Drittländer und vorgesehene Löschungsfristen. Zudem werden die »TOMs«eingefordert, geeignete technische und organisatorische Maßnahmen zum Datenschutz (siehe Kasten).

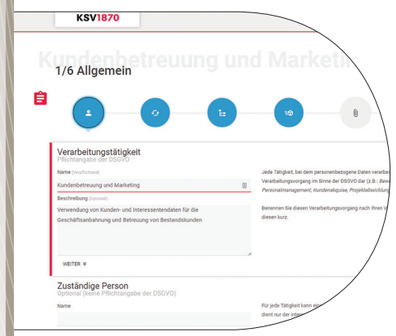
In Kooperation mit VACE IT & Security Services bietet das heimische IT-Systemhaus Navax Initialworkshops zum Thema DSGVO an. Geschäftsführer Oliver Krizek: »In weiterführenden Workshops werden gemeinsam oder einzeln erarbeitete Schritte gemäß den vier Säulen Ermitteln, Verwalten, Schützen, Berichten in die Tat umgesetzt.« Webinare zum Thema ergänzen das Angebot.

> DATENSCHUTZ UND DATENSICHERHEIT WACHSEN IMMER MEHR ZUSAMMEN – NICHT NUR IN RECHTLICHER, AUCH IN TECHNISCHER UND ORGANISATORISCHER SICHT.

Bei einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen, etwa bei Gesundheitsdaten oder im Zusammenhang mit der Kreditwürdigkeit, muss eine Datenschutz-Folgenabschätzung durchgeführt werden.

Die Verpflichtung zur Bestellung eines Datenschutzbeauftragten sieht Einzinger als gering. »Er muss nur dann ernannt werden, wenn schützenswerte Daten in größerem Volumen oder Datenverarbeitung für dauernde Überwachung der Betroffenen vorliegen.« Der Begriff »größerer Umfang« ist dabei wieder Ermessenssache.

Auch beim Recht auf Datenübertragbarkeit zeigt sich der Datenschutzexperte skeptisch. »Wie das sinnvoll angewendet werden kann, ist mir rätselhaft. Das wird sich in der Praxis zeigen.«




Der DSGVO-Assistent des Kreditschutzverbandes leitet Schritt für Schritt durch alle Unternehmensbereiche, unterstützt bei der Dokumentation von Verarbeitungsprozessen, scannt Webseiten auf offensichtlich personenbezogene Datenverarbeitung, schafft ein strukturiertes Verarbeitungsverzeichnis und liefert Hinweise, was rechtlich erforderlich ist. »Man muss sich mit dem Thema DSGVO aber bereits auseinandergesetzt haben«, rät KSV-Geschäftsführer Gerhard Wagner.

### >> Abschreckende Wirkung <<

Die angeführten Strafen »bis zu 20 Millionen Euro oder vier Prozent vom Jahresumsatz« sollen abschreckend wirken, auch für Unternehmen, die laut Kurt Einzinger Strafen von ein paar 100.000 Euro aus der Portokassa bezahlen. Der überwiegende Part der Wirtschaft muss nicht mit Strafzahlungen rechnen. »Datenschutz ist ein Zivilrecht. Jemand muss sich erst in seinen Rechten verletzt fühlen, damit die Behörde aktiv wird«, so Einzinger. Interessant: Künftig kann auch immaterieller Schaden angezeigt werden. Wie sich das entwickelt, werde man sehen. Denn bei Datenschutz ist immaterieller Schaden generell schwer festzustellen und nachzuweisen. ■

Foto: Navax

### TIPP

*»TOM«*

**> Bei der Verarbeitung personenbezogener Daten** sind technische und organisatorische Maßnahmen – TOM – zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Es braucht Kontrollen hinsichtlich Zugang zu Verarbeitungsanlagen, Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern, Verhinderung der Nutzung automatisierter Verarbeitungssysteme, Zugriffs-, Übertragungs-, Eingabekontrolle, Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können, Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können sowie Datenintegrität, d.h. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden.





## Datenschutz-Deregulierungsgesetz 2018:

# Klarstellung in letzter Minute

VON KARIN BRUCHBACHER UND CATHRINE BONDI DE ANTONI

Karin Bruchbacher ist Rechtsanwältin, Datenschutzexpertin und zertifizierte Datenschutzbeauftragte bei PHH Rechtsanwälte.

Cathrine Bondi de Antoni ist Rechtsanwaltsanwärterin und spezialisiert auf Datenschutzrecht.

**> Kurz vor der Anwendbarkeit der EU-Datenschutz-Grundverordnung** mit 25. Mai 2018 wurde auf Initiativantrag das Datenschutz-Deregulierungs-Gesetz 2018 beschlossen, welches in letztem Moment einige Lockerungen des Datenschutzes für Unternehmen vorsieht. Aber was bedeutet dies für betroffene Unternehmen? Ein Überblick.

Durch das Datenschutz-Deregulierungs-Gesetz werden die Auskunftspflichten der Verantwortlichen gegenüber den betroffenen Personen gelockert. Wenn es sich bei den angefragten Auskünften um »Betriebs- oder Geschäftsgeheimnisse« handelt, sind diese Informationen von der Auskunftspflicht ausgenommen. Allerdings liegt es auch weiterhin in der Beweislast des Unternehmens, nachzuweisen, dass eine angefragte Information zu einer ungewünschten Offenlegung von »Geschäfts- und Betriebsgeheimnissen« des Unternehmens oder Dritter führen würde. Eine pauschale Berufung eines Unternehmers auf den Schutz eines Betriebs- oder Geschäftsgeheimnisses ist demnach auch in Zukunft nicht möglich. Unternehmen haben stets im Einzelfall zu erklären, wieso die Verweigerung einer Auskunft aufgrund eines Betriebs- oder Geschäftsgeheimnisses gerechtfertigt ist.

> *Es kann keinesfalls so ausgelegt werden, dass bei Ersttätern stets nur eine Verwarnung ausgesprochen wird.*

### >> Videoüberwachung künftig ohne Interessensabwägung: <<

Die Videoüberwachung öffentlicher Orte, die dem Hausrecht unterliegen, ist künftig einfacher. Da die Einschränkung »wenn … kein gelinderes geeignetes Mittel zur Verfügung steht« gestrichen wurde, muss vor der Installation einer Kamera keine Interessenabwägung mehr stattfinden, ob eine andere Form der Überwachung als gelinderes Mittel möglich wäre. Allerdings gilt auch weiterhin, dass die Videoüberwachung verhältnismäßig und entsprechend gekennzeichnet sein muss.

### >> Günstigkeitsprinzip Strafbestimmungen <<

Hinsichtlich der Verhängung von Strafen für Straftatbestände, welche vor dem Inkrafttreten des DSG verwirklicht wurden, ist abzuwägen, welche Rechtslage für den Täter günstiger ist: die vor der DSGVO und des DSG oder die nach dem DSG 2000.

### >> Strafen oder Verwarnung? <<

Bereits vielerorts freudig kolportiert wurde der Wegfall der hohen Strafen bei Verletzung der Vorschriften der DSGVO. Dies lässt außer Acht, dass das Datenschutz-Deregulierungs-Gesetz 2018 lediglich zur Wahrung der Verhältnismäßigkeit bei der Verhängung von Sanktionen mahnt und in diesem Zusammenhang die Datenschutzbehörde auffordert, insbesondere bei erstmaligen Verstößen vom Verwarnen Gebrauch zu machen. Der Wortlaut der Bestimmung kann keinesfalls so ausgelegt werden, dass bei Ersttätern stets eine Verwarnung ausgesprochen wird. Nach dem Grundsatz der Verhältnismäßigkeit wird im Einzelfall jeweils auf den Gesamtkontext abzustellen sein, insbesondere ob und in welchem Ausmaß die sonstigen datenschutzrechtlichen Bestimmungen vom Unternehmen eingehalten wurden.

Erfreulich ist die Klarstellung, dass ein verantwortlicher Beauftragter nicht mehr für die Verstöße haftet, sofern bereits gegen das Unternehmen (juristische Person) für denselben Verstoß eine Verwaltungsstrafe verhängt wurde.

Die Kernbereiche der DSGVO – der Schutz der personenbezogenen Daten und die Ausübung der Betroffenenrechte – sind von diesen rein innerstaatlichen Bestimmungen nicht umfasst. Die Verpflichtung der Unternehmen, DSGVO-konform zu handeln, bleibt aufrecht. Alle Vorbereitungen, die Unternehmen bereits für die Umsetzung der Bestimmungen der DSGVO getätigt haben, sind vom Datenschutz-Deregulierungsgesetz damit nicht betroffen. ■