ögswissen

DAS ÖGSW MAGAZIN FÜR STEUERBERATER UND WIRTSCHAFTSPRÜFER 2|2018

ÖGSW
IHR SERVICE-NETZWERK

DAS UNGELIEBTE KIND

DIE MIT 25. MAI IN KRAFT GETRETENE DSGVO WIRD VIELFACH ALS WETTBEWERBSHINDERNIS GESEHEN

PERSONALITY
Im Porträt: Hubert Fuchs ist neuer Staatssekretär für Finanzen

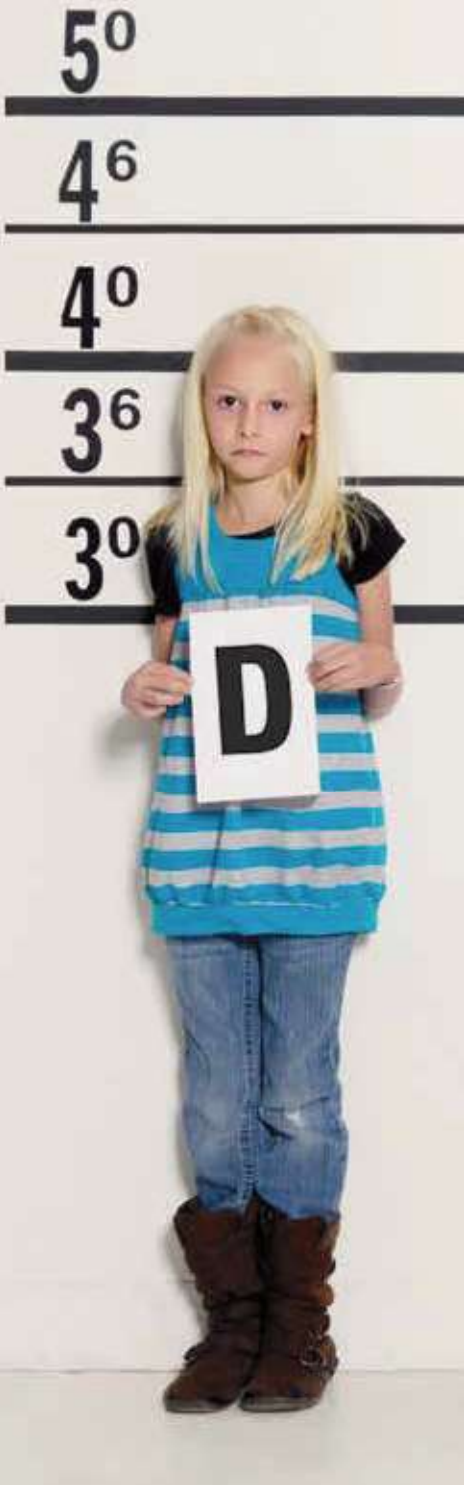
BRENNPUNKT FINANZ
Herbert Houf über Akteneinsicht und ausgeschlossene Unterlagen

SOFTSKILLS
Was Kleidung aussagt und Dresscodes für Vorteile haben

ISSN 2078-3957

Das ungeliebte Kind

WIE WICHTIG IST DATENSCHUTZ WIRKLICH? Aus unternehmerischer Sicht wird die Umsetzung der mit 25. Mai 2018 in Geltung tretenden Datenschutzgrundverordnung (DSGVO) weithin als Wettbewerbshindernis verstanden. Eine Zusammenfassung der wesentlichsten Inhalte. Von Philipp Lukas Leitner



ZUM AUTOR
Mag. Philipp Lukas Leitner, LL.B. ist Rechtsanwaltsanwärter bei SCWP Schindhelm sowie Forschungsmitglied im LIT Digital Transformation and Law Lab an der JKU Linz
p.leitner@scwp.com

Bereits in Art. 12 der Allgemeinen Erklärung der Menschenrechte aus 1948 heißt es: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr […] ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen." Auf europäischer Ebene wurde wenige Jahre später – im Jahr 1953 – in Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK) jeder Person „das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz" zugestanden. Bereits seit 1978 ist das Grundrecht auf Datenschutz – immerhin als Verfassungsbestimmung – im nationalen Datenschutzrecht verankert. Mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr wurde erstmals versucht, die seinerzeit noch uneinheitliche Rechtslage zwischen den Mitgliedstaaten zu harmonisieren und auf einen gewissen Mindeststandard zu heben.

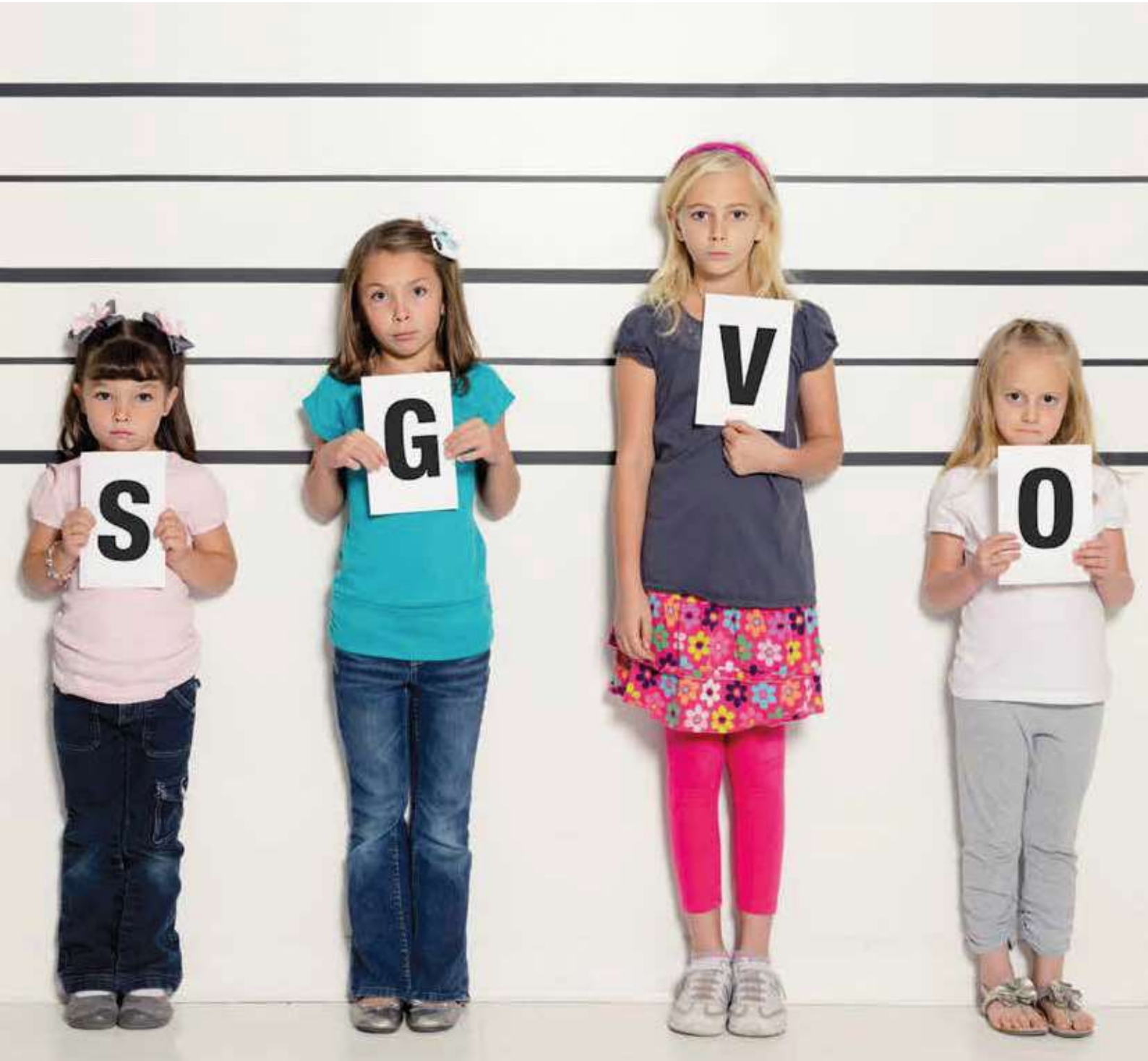
Insbesondere die bahnbrechenden technischen Entwicklungen und Innovationen der letzten beiden Jahrzehnte, der exponentielle Anstieg weltweiter Vernetzung und jederzeitiger Verfügbarkeit, aber auch die Vorfälle in jüngerer Zeit (Stichworte: NSA-Skandal, Facebook, Aufhebung des Safe-Harbor-Abkommens) haben die Notwendigkeit einer umfangreichen Neuregelung des Datenschutzrechts aufgezeigt. Als Konsequenz wurde die Datenschutz-Grundverordnung (DSGVO) beschlossen, welche eine umfangreiche Neuregelung mancher Bereiche vorsieht und Verstöße nunmehr an drakonische Strafen knüpft.

Erheben, ordnen, speichern

Von der DSGVO betroffen sind sämtliche natürlichen und juristischen Personen, die ganz oder teilweise automatisierte Verarbeitungen personenbezogener Daten durchführen. Darüber hinaus ist auch die nichtautomatisierte Verarbeitung derjenigen Daten erfasst, die in einem „Dateisystem" (d.h. in Form einer nach gewissen Kriterien – wie etwa dem Alphabet – sortierten Aktenablage) „gespeichert" sind. Dabei ist ersichtlich, dass sämtliche Vorgänge im Lebenszyklus der Daten von der Definition der Verarbeitung umfasst sein sollen; beispielhaft werden genannt: das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Klassische Beispiele von Verarbeitungstätigkeiten sind etwa die Protokollierung der IP-Adresse sämtlicher Besucher eines Web-Servers, die Erfas-

Bahnbrechende technische Entwicklungen und Innovationen der letzten Jahrzehnte, der Anstieg der weltweiten Vernetzung, aber auch die Vorfälle der jüngsten Zeit (NSA, Facebook etc.) haben die Notwendigkeit einer Neuregelung des Datenschutzes aufgezeigt.



sung von Daten in einem Webformular oder Papierformular, wenn es danach in ein Datensystem eingeordnet oder digital verarbeitet wird, das Verfassen sowie Versenden von E-Mails, das Einlegen von Dokumenten in einen (organisierten) Papierakt, das Löschen von Dateien oder Schreddern von Aktenbestandteilen; ebenso die Bearbeitung von Daten mit FiBu-Software.

Ausgenommen sind (analoge) Akten bzw. Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind. Überdies ausgenommen ist die Verarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Grund für diese Ausnahme ist, dass der Unionsgesetzgeber nicht dem einzelnen Bürger die Verpflichtungen der DSGVO auferlegen wollte; sobald jedoch ein Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit gegeben ist, soll die DSGVO hingegen anwendbar sein.

Zu unterscheiden sind zudem die Begriffe des Verantwortlichen und des Auftragsverarbeiters; sie beide unterscheidet, dass der Verantwortliche grundsätzlich selbst über „Zwecke" und „Mittel" der Verarbeitung personenbezogener Daten entscheiden kann. Diese Freiheit hat der Auftragsverarbeiter nicht, er verarbeitet Daten „im Auftrag" des Verantwortlichen und unterliegt dessen Weisungen.

Die DSGVO, die Datenschutzgrundverordnung, ist seit 25. Mai 2018 in Geltung.

Abgrenzung in der Praxis

Spannend ist die tatsächliche Abgrenzung in der Praxis, wobei die Diskussion über die konkrete Rollenverteilung teilweise philosophische Ausmaße annimmt; dementsprechend unterschiedliche Meinungen werden in der Literatur vertreten. Die genaue Abgrenzung, ob man nun Verantwortlicher oder Auftragsverarbeiter ist, ist auch für Steuerberater und Wirtschaftsprüfer notwendig, zumal diese – je nach

Einordnung – unterschiedliche Pflichten treffen. Vereinzelt wird vertreten, dass Steuerberater Auftragsverarbeiter seien, da sie im Auftrag des Kunden tätig werden und demnach an konkrete Verarbeitungszwecke gebunden sind. Als Gegenmeinung (vgl. insbesondere Pilgermair, Zur datenschutzrechtlichen Stellung von freien Berufen und gewerblichen Dienstleistern nach der alten und neuen Rechtslage, RdW 2017/544) wird angeführt, dass Steuerberater auch Beratungs- und Hinweiskompetenz haben und nicht (blind) die Anweisungen ihrer Mandanten ausführen dürfen. Damit würden Steuerberater und Wirtschaftsprüfer, genauso wie Rechtsanwälte, deren Eigenverantwortlichkeit sich schon aus der standesrechtlichen Vorschrift des § 9 Abs. 1 RAO ergibt, als Verantwortliche zu qualifizieren sein. Tatsächlich müsste eine gesonderte Betrachtung für jede einzelne Verarbeitungstätigkeit innerhalb des konkreten Mandats durchgeführt werden, was jedoch weder sinnvoll noch praxisnah erscheint. Im Ergebnis wird jedoch eher der Gegenmeinung zu folgen sein, wonach Steuerberater und Wirtschaftsprüfer als eigenständige Verantwortliche zu erachten sind.

> Es müsste für jede einzelne Verarbeitungstätigkiet eine gesonderte Betrachtung durchgeführt werden, was nicht praxisnah ist. Im Ergebnis wird der Gegenmeinung zu folgen sein, wonach StB und WP als eigenständige Verantwortliche zu erachten sind.

Novelliertes Datenschutz-Deregulierungs-Gesetz 2018

Die DSGVO bezieht sich auf die Verarbeitung personenbezogener Daten. Diese sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dies stellt einen Widerspruch zum – synchron mit der DSGVO in Kraft tretenden – novellierten Datenschutzgesetz (BGBl. I N 2017/120 i.d.F. BGBl. I N 2017/24) dar, wonach sich der im Verfassungsrang stehende Schutz (weiterhin) sowohl auf natürliche als auch juristische Personen erstrecken soll. Dieser Umstand wurde im Datenschutz-Anpassungsgesetz 2018 – obwohl ursprünglich intendiert – nicht bereinigt. Informationen können entweder objektiv (d.h. überprüfbare Eigenschaften bzw. sachliche Verhältnisse) oder subjektiv sein; sie sind formatunab-

© RICHLEGG/ISTOCK

Die DSGVO bezieht sich auf die Verarbeitung personenbezogener Daten.

hängig (d.h. Texte, Fotos, Audiodateien etc.) und müssen weder wahr noch bewiesen sein. Unter besonderem Schutz stehen zudem besondere Kategorien personenbezogener Daten i.S.d. Art. 9 (Daten, aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit hervorgehen, aber auch genetische und biometrische Daten, Gesundheitsdaten sowie Daten zur sexuellen Orientierung) sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten i.S.d. Art. 10.

Zudem sind die in Art. 5 Abs. 1 dargestellten Grundsätze für die Verarbeitung einzuhalten:

- Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz): dies betrifft vor allem eine genaue Analyse der Rechtfertigungsgründe sowie Informationspflichten an die betroffene Person.
- Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden; eine außerhalb dieser Grundsätze erfolgende Weiterverarbeitung ist unzulässig (Grundsatz der Zweckbindung): hier sollte insbesondere dokumentiert werden, zu welchen konkreten Zwecken (z.B. Durchführung der Personalverrechnung) Daten erhoben und weiterverarbeitet werden. Ganz allgemein gehaltene Zwecke (z.B. Unternehmensbetrieb) reichen nicht aus.
- Die Verarbeitung muss dem Zweck angemessen sein und auf das notwendige Maß beschränkt werden (Grundsatz der Datenminimierung): es gilt daher genau zu analysieren, welche Daten für den Zweck der Verarbeitung unbedingt erforderlich sind.
- Daten müssen sachlich richtig und falls erforderlich auf dem neuesten Stand sein. Unrichtige Daten müssen durch Einführung geeigneter Maßnahmen gelöscht oder berichtigt werden (Grundsatz der Richtigkeit).
- Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die jeweiligen Zwecke erforderlich ist (Grundsatz der Speicherbegrenzung).
- Daten dürfen nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Dabei muss insbesondere durch geeignete technische und organisatorische Maßnahmen sichergestellt sein, dass die Daten vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt werden (Grundsatz der Integrität und Vertraulichkeit).

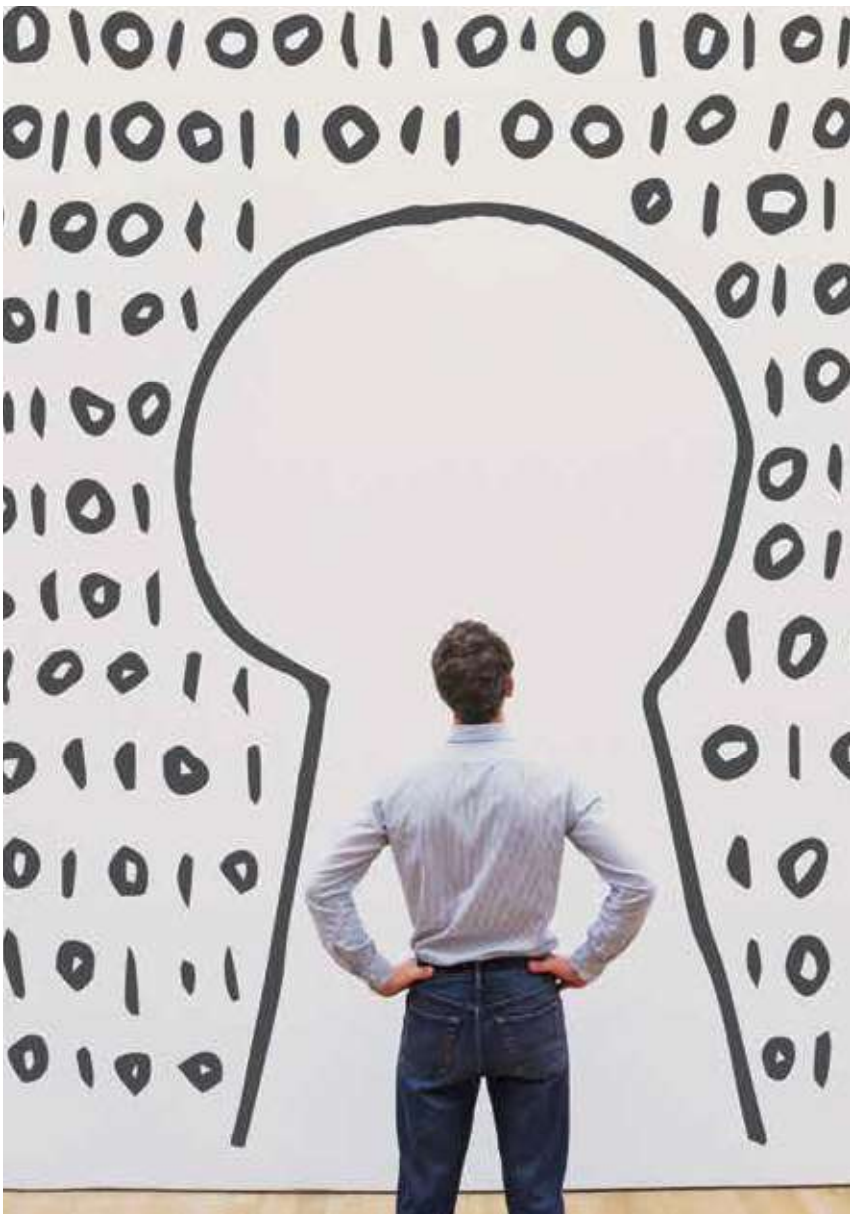
Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz).

Diese Grundsätze können schon bei der Erstellung des Verzeichnisses sämtlicher Verarbeitungstätigkeiten (Art. 30) herangezogen werden, um derzeit bestehende Prozesse, Datenflüsse bzw. Zwecke der Verarbeitung zu erfassen und ggf. adaptieren zu können. Die in Abs. 5 leg. cit. genannte Ausnahmebestimmung, wonach ein derartiges Verzeichnis nicht von Unternehmen mit weniger als 250 Mitarbeitern zu führen ist, wird auf Wirtschaftsprüfer und Steuerberater nicht zutreffen, zumal diese idR eine nicht nur gelegentliche Verarbeitung personenbezogener Daten durchführen. Insbesondere sollte daher schon auf Planungsebene eine Bestandanalyse des Ist-Zustandes vorgenommen werden, auf welche Rechtfertigungstatbestände sich der jeweilige Verarbeitungsvorgang gründet, welche Informationen (Datenschutzerklärungen) bisher veröffentlicht wurden bzw. ob ggf. die Notwendigkeit einer gesonderten Einwilligung besteht.

Die wichtigsten Rechtfertigungsgründe sind Einwilligung (Art. 6 Abs. 1 lit. a), Vertragserfüllung/-anbahnung (lit. b), Erfüllung einer gesetzlichen Verpflichtung (lit. c) sowie die Wahrung berechtigter Interessen (lit. f). Während die Frage der Rechtmäßigkeit mancher Verarbeitungsvorgänge wohl eher einfach zu beantworten ist (zumal die vertragskonforme und sorgfältige Durchführung einer Lohnverrechnung zwingend die Verarbeitung der vom Mandanten zur Verfügung gestellten Daten erfordert und demnach wohl auf den Rechtfertigungsgrund der Vertragserfüllung gestützt werden kann), sind andere Verarbeitungsvorgänge (z.B. Zusendung eines E-Mail-Newsletters, Veröffentlichung

von Fotos oder Kontaktdaten der eigenen Mitarbeiter auf der Unternehmenswebsite) durchaus differenzierter zu betrachten und einer gesonderten Prüfung zuzuführen. Soll eine Verarbeitung auf den Rechtfertigungsgrund der Einwilligung gestützt werden, ist auch immer das Koppelungsverbot zu beachten. Dieses pönalisiert die Verknüpfung einer Einwilligung mit der Erfüllung eines Vertrages, wenn die Einwilligung für die Erfüllung nicht erforderlich ist.

Es ist auf die Rechte betroffener Personen hinzuweisen: Neben dem Recht auf Auskunft, dem Recht auf Berichtigung, Löschung bzw. „Vergessenwerden", Einschränkung der Verarbeitung und Widerspruch ist nun auch das Recht auf Datenübertragbarkeit hinzugekommen.



Hohe Strafandrohung

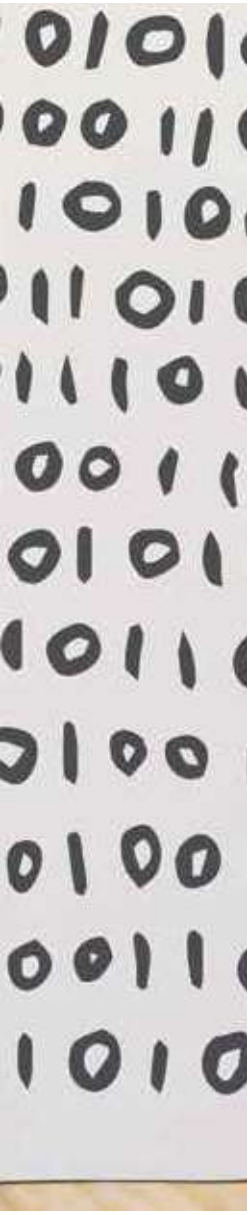
Im Lichte der hohen Strafdrohung ist auch auf die Rechte betroffener Personen hinzuweisen. Neben dem Recht auf Auskunft (Art. 15), dem Recht auf Berichtigung (Art. 16), Löschung bzw. „Vergessenwerden" (Art. 17), Einschränkung der Verarbeitung (Art. 18), und Widerspruch (Art. 21) sei insbesondere auf das neu hinzugekommene Recht auf Datenübertragbarkeit (Art. 20) hingewiesen:

Gemäß Art. 20 Abs. 1 hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen zu übermitteln, vorausgesetzt, die Verarbeitung erfolgt mittels automatisierter Verfahren und beruht auf Einwilligung oder Vertrag. Darüber hinaus sieht Abs. 2 vor, dass die betroffene Person den Verantwortlichen anweisen kann, diese Daten im Wege der Direktübertragung an einen anderen Verantwortlichen unter der Voraussetzung der technischen Machbarkeit zu übermitteln. In Zeiten moderner FiBu-Software und standardisierter Dateiformate könnte dies in extremo bedeuten, dass ein Steuerberater bzw. Wirtschaftsprüfer seine aufwändig gestalteten Rohdaten an einen anderen Wettbewerber übermitteln müsste, wenn sich der Mandant zu einem Wechsel entscheidet.

Betretungsrecht der DSB

Die Österreichische Datenschutzbehörde hat bei der Wahrnehmung ihrer Aufgabe umfangreiche Untersuchungs- und Abhilfebefugnisse. So kann sie etwa eine Datenschutzüberprüfung durchführen oder den Zugang zu allen personenbezogenen Daten und Informationen, aber auch zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen und -geräte durchsetzen. Ein Unternehmen, welches gegen (insbesondere) die in Art. 25 – 39 genannten Pflichten und Grundsätze verstößt, ist mit bis zu EUR 10.000.000,– oder 2% des gesamten jährlichen weltweiten Umsatzes im Vorjahr zu bestrafen, je nachdem, welcher Betrag höher ist. Darunter fallen beispielsweise Verstöße gegen die technische Ausgestaltung der Datensicherheit bzw. gegen die Festlegung datenschutzfreundlicher Voreinstellungen (Art. 25), die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30), Missachtung von Benachrichtigungspflichten bei Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34), Nichtdurchführung einer vorgeschriebenen Datenschutz-Folgenabschätzung (Art. 35) oder Nichtbestellung eines Datenschutzbeauftragten trotz Erforderlichkeit (Art. 37).

Bei Verstößen gegen die Grundsätze für die Verarbeitung, einschließlich



der Bedingungen für die Einwilligung (Art. 5–7; 9), Betroffenenrechte (Art. 12–22) oder bestimmte Anweisungen der Datenschutzbehörde drohen Strafen bis zu EUR 20.000.000,– oder 4% des gesamten jährlichen weltweiten Umsatzes im Vorjahr, je nachdem, welcher Betrag höher ist.

Die DSGVO orientiert sich zudem am kartellrechtlichen Unternehmensbegriff (Art. 101 f AEUV), sodass für die Umsatzberechnung nicht nur dasjenige Unternehmen heranzuziehen ist, welches den Verstoß begangen hat, sondern darüber hinaus auch alle im Konzern verbundenen Unternehmen. Mit einem Abänderungsantrag wurde bei der Nationalratssitzung am 20.4. 2018 das bereits zur Beschlussfassung finalisierte Datenschutz-Deregulierungs-Gesetz 2018 angepasst. Wichtigste Änderung ist der Primat der Verwarnung vor Strafe bei erstmaligem Verstoß (Art. 11). In Hinblick darauf, dass dies als klare Handlungsanweisung an die Datenschutzbehörde zu verstehen ist, werden sich Unternehmen wohl nicht bei erstmaligen Verstößen mit den Strafandrohungen des Art. 83 DSGVO konfrontiert sehen. Dies darf jedoch nicht zur Untätigkeit verleiten. Datenschutz ist nicht nur wichtig, um Fairness und Transparenz zu wahren, sondern auch, um eigene Verarbeitungsprozesse analyisieren und optimieren zu können. ■

Was ist zu tun ?
Last-minute-checkup

- Überprüfung sämtlicher Verarbeitungsvorgänge, Prozesse, technischer (Sicherungs)maßnahmen im Unternehmen (Datenschutzaudit).
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten (als Verantwortlicher und Auftragsverarbeiter).
- Überprüfung, ob sämtliche Verarbeitungsvorgänge von einem Rechtfertigungsgrund gedeckt sind.
- Überprüfung, ob ein Datenschutzbeauftragter zu bestellen oder eine Datenschutz-Folgenabschätzung durchzuführen ist. Dokumentieren Sie die Ergebnisse dieser Prüfungen!
- Überprüfung, ob die Grundsätze der Datenverarbeitung gemäß Art. 5 eingehalten werden. Verantwortliche trifft eine Rechenschaftspflicht!
- Überprüfung, ob wirksame Verfahren bei Ausfall der Systeme bzw. bei Verletzung des Schutzes personenbezogener Daten implementiert wurden (72-Stunden-Frist!).
- Überprüfung und ggf. Überarbeitung sämtlicher Vereinbarungen mit Kunden, Auftragsverarbeitern, anderen Verantwortlichen, Mitarbeitern etc. Sind Verträge gemäß Art. 26 bzw. 28 erforderlich?
- Schulung der Mitarbeiter über Zulässigkeit der Verarbeitung, Geheimhaltungspflicht, Betroffenenrechte etc. Führen Sie Nachweise über diese Schulungen!
- Erarbeitung von Konzepten, damit Betroffenenrechte ausgeübt und wirksam bearbeitet werden können. Achten Sie auf die Skalierbarkeit.