

Personalisierte Werbung

Inhaltsverzeichnis

I. Einleitung.....	24
1. Symbiose von Angebot und Werbung.....	25
2. Angebots- und Preispersonalisierung.....	25
3. Personalisierung der Werbung	26
II. „Privacy Paradox“ und Risiken der personalisierten Werbung.....	28
III. Steigende Anforderungen an Datenschutz und Datensicherheit.....	30
1. Personendaten und Profiling.....	30
2. Entwicklungen in der Schweiz und in der EU	31
2.1 Unterschiedliche Regelungsansätze in der Schweiz und in der EU.....	31
2.2 Extraterritoriale Anwendbarkeit der EU-DSGVO.....	32
2.3 Revision des DSG.....	33
a) Neuer Stand der Technik	33
b) Kernpunkte der DSG-Revision.....	34
2.4 Neuregelung für die personalisierte Werbung	36
a) Transparenz und Information	36
b) Dokumentation	39
c) Auskunftsrecht	40
d) Einwilligung und Widerspruch	41

* Dr. iur., Rechtsanwalt, Zürich.

** Rechtsanwältin, Zürich.

e) Rechtfertigungsgründe.....	43
f) Automatisierte Entscheide und Profiling	45
g) Erweiterter Geheimnisschutz	48
h) Datensicherheit.....	49
i) Selbstregulierung	51
j) Sanktionsrisiken	55
k) Durchsetzung	58

IV. Fazit.....	59
----------------	----

I. Einleitung

Neue Technologien erleichtern nicht nur die Personalisierung der Werbung, sondern des gesamten Angebots. Die Grenze zwischen Werbung und Produkt lässt sich kaum mehr klar erkennen. Personalisierte Werbung ist aus rechtlicher Sicht ein Querschnittthema: Es geht neben Datenschutz und Datensicherheit auch um die Lauterkeit des gewählten Vorgehens zur Datenbeschaffung, Analyse und der Absatzförderung. Kartellrechtliche Fragen zu marktmächtigen Anbietern beschäftigen auch die Wettbewerbsbehörden. Dieser Beitrag fokussiert, auch aus Aktualitätsgründen, auf das Datenschutzrecht.

Der Vorentwurf (VE) zum totalrevidierten Bundesgesetz über den Datenschutz vom 21. Dezember 2016 (DSG, SR 235.1) soll die Verpflichtungen der Schweiz aus dem revidierten Übereinkommen des Europarates zum Datenschutz (E-K 108) umsetzen. Ausserdem soll er sicherstellen, dass die Schweiz die Anerkennung der EU als ein Land mit gleichwertigem, bzw. angemessenem, Datenschutz nicht verliert, wenn im Mai 2018 die neue EU Datenschutzgrundverordnung (DSGVO, VO EU 2016/679) verbindlich wird. Die DSGVO wird aufgrund ihrer extraterritorialen Wirkung auch für viele Schweizer Unternehmen einen neuen *de facto* Standard für den Umgang mit Personendaten setzen. Der Schweizer Gesetzgeber hätte aber in vielen Bereichen Handlungsspielraum, den der VE-DSG nur ungenügend nutzt.

1. Symbiose von Angebot und Werbung

Der Stand der Technik erlaubt die Personalisierung der Werbung und des gesamten Angebots. Methoden zur Perfektionierung der Angebotspersonalisierung und der Verschmelzung von Produkt und Werbung sind auch unter dem Begriff "Growth Hacking" bekannt geworden. Vor allem für Startups im digitalen Umfeld bieten sich hier Chancen, ohne konventionelles Werbebudget und ohne herkömmliche Marketingkanäle ihr Angebot einzig auf Nutzerbedürfnisse und Wachstum auszurichten, mit dem Ziel, dass das eigene Produkt den Kundennutzen optimal bedient und sich dadurch viral verbreitet.¹ Erfolgreiche Beispiele sind die grossen Online-Plattformen Facebook, Google, YouTube oder Twitter, die sich ohne traditionelle Plakat- oder TV-Werbung etabliert haben. Diese Plattformen bauen die Werbung in das Produkt selbst ein. Durch die Einführung von Schaltflächen, welche die Nutzer auf eigenen Webseiten und Blogs einsetzen und Leser damit auf ihre Facebook-Seite führen, konnte bspw. Facebook einen massiven Wachstumsschub erzielen. Auf YouTube sieht der Nutzer nach Ende eines Videos mehrere Empfehlungen für andere Videos. YouTube setzt darauf, dass eines der gezeigten Videos dem Nutzer so gefällt, dass er es mit anderen teilt und damit YouTube wiederum mehr Besucher und Nutzer verschafft (sogenannter "viral loop"). Andere Anbieter, z.B. Dropbox, belohnen Kunden, die ihren Dienst Dritten empfehlen mit Guthaben. Solche Marketingstrategien mögen längst nicht für alle Werbetreibenden geeignet sein, sie zeigen aber die zunehmende Symbiose von Werbung und Angebot.

2. Angebots- und Preispersonalisierung

Angebotspersonalisierung kann neben "Growth Hacking" zahlreiche andere Formen annehmen. Amazon bietet z.B. jedem Nutzer eine individuelle Einstiegsseite an, auf welcher Empfehlungen gestützt auf den früher angeschauten oder gekauften Produkten erscheinen. Amazon listet personalisierte Suchergebnisse basierend auf den vermuteten Kundenpräferenzen und abgestimmt auf die Ratings vergleichbarer Kunden auf.

Produktpersonalisierung kann auch Preispersonalisierung (als Extremform des "Dynamic Pricing") einschliessen, d.h. die Festsetzung der Preise (oder

¹ MICHEL KAUFMANN, Growth Hacking: So funktioniert das Marketing der Zukunft, in: VISCHER, Digital Business Law Bites, gefunden auf: <http://createsend.com/t/r-D8273D0C75FB51EA2540EF23F30FEDED> (besucht am 9. Februar 2017).

Rabatte) je nach Kombination von Nutzerprofil mit Angaben zu Anbieterloyalität, Standort, Tageszeit, Kaufverhalten, Zahlungsmittel, vermuteten Interessen und Zahlungsbereitschaft. Nicht alle Märkte und Konsumenten sind bereit, Preispersonalisierungen zu akzeptieren. Amazon bestreitet aus Reputationsgründen, ihre Preise zu personalisieren. Gleichzeitig gibt es immer wieder Meldungen, wonach bestehende Kunden weniger Rabatte bekommen als Neukunden und sogar unterschiedliche Preise in Abhängigkeit des verwendeten Browsers bestehen.² Auch in der Schweiz testen Anbieter Preispersonalisierung, z.B. die Grossverteiler Migros und Coop. Die von der Migros ausgegebenen Rabattcoupons basierend auf dem Einkaufsverhalten der Kunden haben Medienberichte ausgelöst, wonach die Migros weniger Rabatte direkt im Laden am Produkt selbst kennzeichnen, sondern mit den Rabattcoupons eine Art personalisierte Rabattstruktur mit nutzerfokussierter Preisstruktur schaffen möchte. Auch wenn es für den Konsumenten durchaus Sinn macht, relevante Rabatte zu erhalten (z.B. Rabattcoupons für Hundefutter nur als Hundehalter), ist die Kritik vorprogrammiert: Wer Hochpreisprodukte sowieso kauft, erhält vielleicht weniger Rabattcoupons für diese Produkte als Kunden, die preissensitiver einkaufen. Auch Coop hat 2015 ein solches Modell für seinen online Shop getestet, aufgrund der öffentlichen Kritik seitens des Konsumentenschutzes den Versuch aber wieder eingestellt.

3. Personalisierung der Werbung

Nicht für alle Anbieter und Branchen ist Angebotspersonalisierung oder gar "Growth Hacking" heute möglich oder zielführend. Zudem leben auch viele Anbieter gleichzeitig vom Besuchervolumen auf ihren Plattformen, welches sie Werbekunden anbieten können. Klassische Werbung hat aber zunehmend einen schweren Stand und kämpft um Akzeptanz. Vor allem intrusive Werbeformen, wie "Spam" E-Mails, gelten als unattraktiv und gehören in vielen Branchen bereits der Vergangenheit an. Der Druck auf digitale Werbung nimmt auch aufgrund der wachsenden Verbreitung von "Ad Blockern" zu, welche das Ausspielen von herkömmlichen "Display"-Werbeformen auf

² REGINE KALKA/ANDREAS KRÄMER, Dynamic Pricing: Verspielt Amazon das Vertrauen seiner Kunden?, Absatzwirtschaft, 16. Februar 2016, gefunden auf: <http://www.absatzwirtschaft.de/dynamic-pricing-verspielt-amazon-das-vertrauen-seiner-kunden-75271/> (besucht am 9. Februar 2017); WOLF LOTTER, Eine Frage des Preises, Brand eins, 10/2000, gefunden auf: <https://www.brandeins.de/archiv/2000/design/eine-frage-des-preises> (besucht am 9. Februar 2017).

Online-Plattformen wie "Banners" oder "Skyscrapers" verhindern und auf die Preise für traditionelle Online-Werbung drücken.

Als Folge davon wird "native advertising" in Medien attraktiver für Werbetreibende. Werbung und Content verschmelzen in "sponsored stories" – d.h. durch Werbepartner finanzierte Beiträge eingebettet in den redaktionellen Teil – die aus Sicht des Werbetreibenden sehr effektiv sein können. Auch nutzen Werbeauftraggeber zunehmend die Sozialen Netzwerke ihrer Kunden und Nutzer, um Reichweite zu generieren. Nutzer stören sich im Idealfall weniger an "sponsored stories" als an klassischer Werbung, da Werbeinhalt zu Nutzerinhalt wird.³ Dies gilt umso mehr, wenn die Inhalte von ihren Freunden geteilt oder gar empfohlen wurden. Für diese Inhalte haben gerade Online-Plattformen auch keine starren Kapazitätsgrenzen. Über die Einstellmöglichkeiten der Plattformen kann der Nutzer sein Netzwerk und die geschalteten Inhalte inklusive Werbung ebenfalls personalisieren.

Unabhängig davon, ob es sich um klassische Werbung oder um "native advertising" handelt, muss Werbung für den Empfänger relevant sein, um Erfolg zu haben. Basis für erfolgreiche Online-Werbung und für ein attraktives Online-Angebot ist die Datenauswertung – "Data Analytics". Der Wert der erhobenen und verwendeten Daten ist von der Qualität und Quantität der Daten abhängig. Mögliche Quellen sind der Nutzer selbst, der Daten freiwillig zur Verfügung stellt, Maschinen, Dritte oder sogar andere Daten aus denen neue Informationen ableitbar sind. Grosse Online-Anbieter versuchen die Aktivität ihrer Kunden über verschiedene Geräte und Plattformen hinweg zu verfolgen, um damit das Nutzerprofil zu vervollständigen.⁴ Werbenetzwerke versuchen das Bild des Werbeadressaten ebenfalls plattformübergreifend zu komplettieren. Auch die grossen Verlage generieren zunehmend Netzwerkdaten innerhalb ihrer eigenen Plattformen. Geräte- oder plattformübergreifendes Verfolgen ("Tracking") der Nutzer erschwert die Schaffung oder Beibehaltung von Transparenz.

³ FLORENCE THÉPOT, Market Power in online Search and Social Media Networking: A Matter of Two-Sided Markets, 36 WORLD COMPETITION Law and Economics Review 2, 195, 204.

⁴ MARTY SWANT, Google Wants to Give You Better Control Over the Personalized Ads You See, Adweek, 1. Juli 2016, gefunden auf: <http://www.adweek.com/news/technology/google-wants-give-you-better-control-over-personalized-ads-you-see-172362> (besucht am 9. Februar 2017).

Anbieter, wie Facebook, bieten Werbetreibenden relativ detaillierte Kataloge an, um die gewünschte Zielgruppe für Werbeschaltungen zu definieren. Ausreisser und Fehlinterpretationen sind häufig, doch verspricht diese personalisierte Werbung eine höhere Relevanz der geschalteten Werbung für den Nutzer und damit eine bessere Erfolgsquote. Hochwertige Werbeplätze (z.B. betreffend Sichtbarkeit, Anzeigedauer, aber eben auch angesprochenes Publikum) sind begehrt. Da immer bessere Auswertungen zu Qualitätsaspekten der Werbung möglich sind, steigen die Preise für präferierte Werbeplätze und bestimmte Nutzer.

II. „Privacy Paradox“ und Risiken der personalisierten Werbung

Auf Nutzerseite zeigt sich zunehmend eine Diskrepanz zwischen Ansprüchen an die Datenbearbeiter und eigenem Verhalten, die auch als "Privacy Paradox" bezeichnet wird: Einerseits waren noch nie so viele Nutzer um ihre Privatsphäre besorgt. Nutzer wünschen sich mehr Information zum Umgang mit ihren Daten und mehr Kontrolle über ihre Daten.⁵ Andererseits schlägt sich dieses Bedürfnis nach Kontrolle nicht im Nutzerverhalten nieder. Die Information scheitert oft schon daran, dass Nutzer die Datenschutzerklärungen nicht lesen. Dies liegt nicht zuletzt an der Länge und der mangelnden Leserfreundlichkeit dieser Dokumente. Wenn z.B. eine Person in den USA Datenschutzerklärungen von allen von ihr in einem Jahr besuchten Webseiten lesen würde, bräuchte sie volle 25 Tage à 24 Stunden.⁶

Jeder Nutzer schliesst pro Jahr zahlreiche Verträge über die Nutzung einer App oder Online-Plattformen ab und "akzeptiert" damit mehrseitige Allgemeine Geschäftsbedingungen (AGB) und Datenschutzerklärungen. Nutzer erstellen von den Dokumenten keine Markup-Version und senden diese dem Anbieter zurück, um über das Kleingedruckte zu verhandeln. Entweder

⁵ LINDSEY PEACOCK, While consumers want control, they're willing to share personal data: study, itbusiness.ca, 6. November 2015, gefunden auf: <http://www.itbusiness.ca/news/while-consumers-want-control-theyre-willing-to-share-personal-data-study/61227> (besucht am 9. Februar 2017).

⁶ ALEXIS C. MADRIGAL, Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days, The Atlantic, 1. März 2012, gefunden auf: <http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/> (besucht am 9. Februar 2017).

nutzt der Kunde einen Dienst nach den Bedingungen des Anbieters oder nicht.

Plattformbetreiber internalisieren die "Störung" des Nutzers durch Werbung sowie die Datenbeschaffung als Gegenleistung für den kostenlosen Zugang.⁷ Soziale Netzwerke bieten in der Regel keine zahlungspflichtigen Alternative ohne Werbung und Datensammlung an. Die Daten sind die Gegenleistung des Nutzers im Tausch gegen die Dienstleistung, auch wenn dieser Austausch vom Anbieter nicht transparent kommuniziert wird.⁸ Die Masse an Personendaten hat massgeblichen Anteil an der Werthaltigkeit der Sozialen Netzwerke. Als einige der wenigen Gegenbeispiele musste kürzlich Evernote aufgrund einer Welle heftiger – und öffentlichkeitswirksamer – Reaktionen aus den Nutzerkreisen eine angekündigte Änderung der Datenschutzerklärung zurückziehen, gemäss welcher Mitarbeitende die von den Nutzern beim Dienst erfassten Inhalte hätten lesen können. Evernote entschuldigte sich bei den Nutzern für die schlechte Kommunikation diesbezüglich.⁹

Selbst Nutzer, die sich durch die Datenschutzerklärungen kämpfen, machen selten von den angebotenen Kontroll- und Einstellmöglichkeiten Gebrauch. Noch nie wurden so viele private und gar intime Informationen von den Nutzern selbst und freiwillig über Soziale Netzwerke verbreitet. Wenn nun also mehr Daten offenbart und analysiert werden, liegen die massgeblichen Risiken heute vor allem in den Bereichen Datensicherheit und automatisierte Entscheide: Die Kehrseite der umfassenden Datenbeschaffung und Analyse sind potentiell weitreichendere Folgen bei Datenmissbrauch und Datenlecks. Massnahmen zur Datensicherheit müssen Schutz vor ungewollter Verbreitung persönlicher Daten mit dem Risiko von Missbrauch zu kriminellen Zwecken gewährleisten. Noch fehlen adäquate, durchgesetzte Beispiele der guten Praxis für "guten" Datenschutz und "gute" Datensicherheit, weshalb

⁷ THÉPOT (Fn 3), 202.

⁸ EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER EDÖB, Erläuterungen zu Sozialen Netzwerken, gefunden auf: <https://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=de> (besucht am 19. Dezember 2016).

⁹ CHRIS O'NEILL, A Note From Chris O'Neill about Evernote's Privacy Policy, Evernote, 15. Dezember 2016, gefunden auf: <https://blog.evernote.com/blog/2016/12/15/note-chris-oneill-evernotes-privacy-policy> (besucht am 9. Februar 2017).

der Ruf nach Regulierung stärker wird.¹⁰ Mehrseitig tätige Plattformen (z.B. Uber, Airbnb, Facebook) haben zudem eine Tendenz zur Monopolbildung, was zu Marktversagen führen kann. Ähnlich wie bei Preisdiskriminierung kann das zu Fällen der "Datendiskriminierung" führen: Automatisierte Entscheide oder Angebote (z.B. Medienfilter oder Kreditentscheide) ohne Transparenz und Kontroll- und Korrekturmöglichkeiten gefährden die Rechte des Einzelnen, sind aber auch rechtsstaatlich problematisch.

III. Steigende Anforderungen an Datenschutz und Datensicherheit

1. Personendaten und Profiling

Hochstehende Datenanalysen müssen nicht zwingend Personendaten, d.h. Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSGVO), zum Gegenstand haben. Auch vollständig anonymisierte Daten können Grundlage für aussagekräftige Auswertungen darstellen.

Bereits aus der Kombination von wenigen Personendaten und Metadaten (z.B. grobe geografische Herkunft der IP-Adresse, Aktivität, Verweildauer und Bewegung auf einer Webseite etc.) lassen sich aber auch anonymisierte Daten wieder zu identifizierbaren Profilen aggregieren, die für den Webseitenbetreiber und Dritte wertvoll sein können.¹¹ Im Zeitalter von "Big Data" können immer mehr Daten aus verschiedenen Quellen (z.B. klassische Personendaten des Datensubjekts, Sensordaten, geographische Daten, Gerätedaten etc.) für detaillierte Auswertungen kombiniert werden. Ursprünglich anonyme Daten werden so Teil eines Profils, das sehr genaue Aussagen über das Nutzerverhalten erlaubt. In der Kombination von bisher nicht zusammenhängenden Daten liegt der besondere Wert von "Big Data Analytics".¹²

¹⁰ GÜNTHER KARJOHT, Weder Anonymität noch Radiergummi – Datenschutz und Identitätsmanagement im Internet: ein Rückblick auf zehn Jahre in vier Bildern, *digma* 2010, 146-151, 151.

¹¹ EDÖB (Fn 8); KARJOHT (Fn 10), 147.

¹² FLORENT THOUVENIN, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Big Data und Datenschutz – Gegenseitige Herausforderungen, Rolf H. Weber/Florent Thouvenin (Hrsg.), ZIK

Diese Datenkombinationen erfolgen nicht immer transparent, wie jüngst der Fall von Turn Inc., einer kalifornischen Gesellschaft zur Personalisierung der Werbung, zeigte. Diese hat gekaufte und unterscheidbare Wireless-Daten des Anbieters Verizon mit anderen Identifikationsmerkmalen verbunden (z.B. "Cookies", Geräte-Identifikatoren) und konnte so die Nutzer für personalisierte Werbung avisieren, selbst nachdem die Nutzer "Cookies" etc. gelöscht bzw. zurückgesetzt hatten. Vor allem letzteres war für die Nutzer aufgrund Turn Inc.'s Kommunikation nicht eindeutig ersichtlich.¹³ Sobald Personendaten gesammelt und bearbeitet werden, greifen die jeweiligen nationalen und regionalen Datenschutzgesetze und -regulierungen.

2. Entwicklungen in der Schweiz und in der EU

Obwohl Werbung und Märkte bereits grenzüberschreitend und zunehmend global sind, ist die Regulierung zum Datenschutz und zur Datensicherheit noch immer national oder höchstens regional. Durch die Internationalisierung der Geschäftstätigkeit und der Datenströme, z.B. für die personalisierte Werbung, unterwirft sich eine datenbearbeitende Organisation – meist unbewusst – verschiedenen Jurisdiktionen und Regelwerken.

2.1 Unterschiedliche Regelungsansätze in der Schweiz und in der EU

Die Datenschutzregulierungen in der EU und in der Schweiz unterscheiden sich schon im grundsätzlichen Ansatz: Während die DSGVO jede Bearbeitung von Personendaten untersagt, sofern kein Erlaubnisatbestand greift (Verbot mit Erlaubnisvorbehalt), erlaubt das geltende Schweizer Recht die Datenbearbeitung grundsätzlich, knüpft diese Bearbeitung aber an Voraussetzungen und untersagt gewisse Bearbeitungen. Das geltende DSG sanktioniert Datenbearbeitungen entgegen den Bearbeitungsgrundsätzen (Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Erkennbarkeit, Zweckbindung, Art. 4 DSGVO), aber nicht eigenständig mit Bussenandrohung. Die Schweiz stellt auch die Persönlichkeitsverletzung an sich nicht unter Strafe. Eine Datenbearbeitung, welche eine widerrechtliche Persönlichkeitsverlet-

– Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Bd./Nr. 59, Zürich/Basel/Genf 2014, 61-83, 62.

¹³ FEDERAL TRADE COMMISSION (FTC), Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices, Pressemitteilung vom 20. Dezember 2016, gefunden auf: <https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively> (besucht am 9. Februar 2017).

zung darstellt, hat aber zivil- und administrativrechtliche Folgen (Art. 28 Schweizerisches Zivilgesetzbuch, SR 210, ZGB; Art. 42 f. VE-DSG). Demgegenüber sanktioniert die EU Verstösse gegen die DSGVO an sich (Art. 83 DSGVO) und bietet auch eine zivilrechtliche Haftungsgrundlage aufgrund der Verletzung allgemeiner Datenschutzgrundsätze (Art. 82 DSGVO) – unabhängig davon, ob die (Persönlichkeits-)Rechte der betroffenen Person tatsächlich verletzt wurden.

Zivilrechtliche Ansprüche sind nach Schweizer Ansatz nur an jene Datenbearbeitungen geknüpft, die eine widerrechtliche Persönlichkeitsverletzung darstellen. Ein Verbot mit Erlaubnisvorbehalt für die ein Rechtfertigungsgrund nachgewiesen werden muss, kennt das DSG nur in zwei Fällen: Erstens bei der Bearbeitung entgegen dem ausdrücklichen Willen der betroffenen Person (Art. 12 Abs. 2 lit. b DSG) und zweitens bei der Bekanntgabe von besonders schützenswerten Daten oder Persönlichkeitsprofilen an Dritte (Art. 12 Abs. 2 lit. c DSG).

2.2 Extraterritoriale Anwendbarkeit der EU-DSGVO

Für viele Schweizer Anbieter dürfte die DSGVO ab Verbindlichkeit im Mai 2018 aufgrund ihrer extraterritorialen Wirkungen direkt anwendbar werden: Die DSGVO greift auch für Anbieter ausserhalb der EU unmittelbar, sofern Datensubjekte in der EU betroffen sind und die Datenverarbeitung entweder mit dem Angebot von Waren oder Dienstleistungen im Zusammenhang steht oder die Verhaltensbeobachtung der Personen in der EU umfasst (Art. 3 Abs. 2 DSGVO). Noch nicht als Anbieten von Waren und Dienstleistungen gilt das blosses Zugänglichmachen einer Webseite in der Union, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die auch in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist. Der Einsatz einer Sprache oder Währung eines Mitgliedstaats kombiniert mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache oder Währung zu bestellen, oder auch die Erwähnung von EU-Kunden oder Nutzern, können auf das Anbieten von Waren oder Dienstleistungen in der EU hinweisen (Erw. 23 DSGVO). Als Verhaltensbeobachtung gilt z.B. die Erfassung der Internetaktivitäten und die Profilerstellung als Grundlage für Entscheidungen, Analysen oder der Voraussage persönlicher Vorlieben, Verhaltensweisen oder Gepflogenheiten einer Person (Erw. 24 DSGVO). Schweizer Anbieter mit einer englischen Bestellseite in Euro, unterstehen der DSGVO ebenso wie Anbieter von online Werbeplätzen, die von Nutzern mit EU-IP-Adresse Profile erstellen.

In der EU müssen Verantwortliche und Auftragsverarbeiter von ausserhalb der EU grundsätzlich einen Vertreter im jeweiligen Mitgliedstaat bestimmen,

in dem sich die betroffenen Personen befinden (Art. 27 Abs. 3 DSGVO). Dieser gilt als Ansprechperson für die Aufsichtsbehörden sowie die betroffenen Personen.

2.3 Revision des DSG

a) Neuer Stand der Technik

Das DSG stammt aus dem Jahr 1992, als vor allem Risiken der Persönlichkeitsverletzung und der Schutz des Privat- und Familienlebens im Vordergrund standen. Zentral war insbesondere das Bedürfnis nach Schutz vor dem Staat im Nachgang zur "Fichenaffäre" der 1980er Jahre unter gleichzeitiger Wahrung des Föderalismus und der Kompetenzen der Kantone. Resultat war das DSG für Private und Bund, während jeder Kanton für seine Behörden ein eigenes DSG mit eigenen Verantwortlichkeiten schuf. Das DSG adressiert die heutigen Risiken nicht mehr adäquat, was auch an der seither erfolgten Digitalisierung und Vernetzung der Datenverarbeitung, insbesondere über das Internet, liegt. Technologische Entwicklungen, wie Videoaufzeichnungen, automatische Zugangskontrollen, die Bedienung von Geräten und Anlagen, das automatische Lesen von Kreditkarten und Zweiwegkommunikationssysteme, galten damals als neu.¹⁴ Das geltende DSG passt damit nicht mehr ohne weiteres zur heutigen technologischen und wirtschaftlichen Realität. Die digitale Kommunikation hinterlässt Spuren ohne Ablaufdatum. Datenbanken verschiedenster Art können verknüpft werden und ganz neue Rückschlüsse über einzelne Personen ermöglichen. Je grösser die Datenmengen, desto grösser sind die Gefahren bei unautorisiertem Zugriff oder bei Datenlecks infolge mangelnder Datensicherheit. Ausserdem ermöglicht die Datenanalyse nicht nur personalisierte Angebote, sondern auch automatisierte Entscheide. Diese können für den Einzelnen gravierende Auswirkungen haben, ohne dass er sich dessen bewusst ist und sich dagegen zur Wehr setzen kann. Daten sind aber auch zunehmend der Rohstoff für neue Geschäftsmodelle in vielen Branchen, etwa im Finanzwesen, bei Versicherungen oder auch in der (Tele-)Kommunikation. Es ist daher durchaus richtig, wenn das Datenrecht (nicht nur der Datenschutz) einer kritischen Würdigung und Anpassung unterzogen wird.

Dabei sollte aber die Schweizer Rechtstradition Richtschnur bleiben: Wie im geltenden DSG sollten allgemeine Anforderungen an die (im Grundsatz er-

¹⁴ Botschaft des Bundesrates vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 413, 417.

laubte) Datenbearbeitung im Zentrum stehen statt auf den Einzelfall ausgerichtete Detailpflichten, die nach kurzer Zeit nach Gegenmaßnahmen oder neuen Anpassungen rufen. Auch sollte der Schweizer Gesetzgeber nicht vergessen, dass sich die dem Schweizer Recht unterworfenen Personen grundsätzlich an gesetzliche (und auch vertragliche) Pflichten halten. Zur Durchsetzung dieser Pflichten bedarf es keiner „abschreckenden“ Sanktionen in Form von Bussen und Geldstrafen in einem Ausmass, wie sie etwa die DSGVO vorsieht. Illustrativ ist der Vergleich mit Unterlassungserklärungen, z.B. infolge von Schutzrechtsverletzungen: Während eine Unterlassungserklärung gemäss der Schweizer Rechtstradition als verbindlich und damit genügend gilt, muss eine solche Erklärung in Deutschland strafbewehrt sein, damit die Wiederholungsgefahr als beseitigt gilt.

b) Kernpunkte der DSG-Revision

Nach den Revisionsbemühungen in der EU, insbesondere mit dem Erlass der neuen DSGVO und dem Entwurf zur Überarbeitung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates vom September 2016 (E-K 108), ist nun auch das DSG in Revision. Der Bund hat den Vorentwurf (VE-DSG) am 21. Dezember 2016 zur Vernehmlassung publiziert. Interessierte Kreise konnten sich bis zum 4. April 2017 zum Vorschlag äussern. Das neue DSG soll die Verpflichtungen aus der von der Schweiz unterzeichneten revidierten E-K 108 umsetzen und die Aufrechterhaltung der Gleichwertigkeit des Schweizer Datenschutzniveaus mit der EU gewährleisten, um weiterhin internationale Datenflüsse zu ermöglichen.¹⁵

Der Vorentwurf des DSG sieht Verschärfungen gegenüber dem geltenden Recht vor, geht aber vor allem bezüglich Verwaltungssanktionen weniger weit als die Regelung in der EU. Im Grundsatz soll das neue Datenschutzgesetz in der Schweiz an der Zulässigkeit der Datenbearbeitung und der Relevanz einer Persönlichkeitsverletzung festhalten. Wie unter geltendem Schweizer Recht sollen auch künftig unter dem DSG Widerhandlungen nicht automatisch eine Persönlichkeitsverletzung darstellen. Eine Persönlichkeitsverletzung liegt gemäss Vorentwurf insbesondere in folgenden Fällen vor (Art. 23 Abs. 2 VE-DSG):

¹⁵ BUNDESAMT FÜR JUSTIZ (BJ), Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, 17 f. und 32.

1. Bearbeitung von Personendaten entgegen den Grundsätzen des DSG in Art. 4-6 sowie Art. 11;
2. Bearbeitung von Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person;
3. Bekanntgabe von besonders schützenswerte Personendaten an Dritte;
4. Profiling ohne ausdrückliche Einwilligung der betroffenen Person.

Keine Persönlichkeitsverletzung soll regelmässig dann vorliegen, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 23 Abs. 3 VE-DSG).

Gleichzeitig soll aber der Sanktionskatalog gemäss Vorentwurf massiv ausgeweitet und rein administrative Pflichten sollen strafrechtlich sanktioniert werden.

Die Revision soll nach dem Willen des Gesetzgebers dem sog. risikobasierten Ansatz folgen und Aktivitäten mit erhöhtem Risiko anders behandeln als Bearbeitungen, von denen kaum eine Gefährdung der Rechte der Betroffenen ausgeht.¹⁶ Die Umsetzung dieser an sich sinnvoll erscheinenden Grundsätze ist allerdings nur teilweise gelungen. Der VE-DSG enthält gar unnötige Verschärfungen gegenüber der DSGVO, beispielsweise im Bereich der Informations- und Auskunftspflichten sowie Einwilligungen, welche die personalisierte Werbung in der Schweiz – sogar gegenüber der EU – erschweren würden.

Kernpunkte des Vorentwurfs sind die folgenden:

1. Erweiterte Informationspflichten (Information als Bringschuld);
2. Stärkung des Auskunftsrechts (mehr Informationen);
3. Dokumentationspflichten;
4. "Herrschaft" der Betroffenen über ihre Daten (Recht auf Berichtigung und Löschung);
5. Datenschutzfreundliche Grundeinstellungen ("Privacy by Design" und "Privacy by Default");
6. Prüf- und Genehmigungspflichten (Datenschutzfolgenabschätzung bei Bearbeitungen mit erhöhtem Risiko, unternehmensinterne Datenschutzvorschriften zum Transfer ins Ausland, Pflicht zur dauernden Prüfung und Berichtigung von Daten);

¹⁶ BJ, Erläuternder Bericht (Fn 15), 18.

7. Meldepflichten bei Verletzungen der Datensicherheit ("Data Breach Notification");
8. Stärkung der Selbstregulierung ("Best Practice"-Empfehlungen);
9. Ausweitung der Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB (Erlass vorsorglicher Massnahmen, Verwaltungsmassnahmen, Amtshilfe);
10. Bussen in der Höhe von maximal CHF 500'000 bei Verletzung von Administrativpflichten des DSG.

2.4 Neuregelung für die personalisierte Werbung

Besonders relevante Neuregelungen für die personalisierte Werbung finden sich vor allem in den Bereichen der Anforderungen an die Transparenz und Information sowie an die Einwilligung. Im Gegensatz zur DSGVO fordert der VE-DSG gar eine ausdrückliche Einwilligung für Profiling. Weitere Neuerungen betreffen Rechtfertigungsgründe für die Bearbeitung von Personendaten, den Umgang mit automatisierten Entscheidungen und die Datensicherheit. Der VE-DSG sieht explizit Raum für Selbstregulierung vor. Das neue DSG soll mit griffigeren Sanktionsregeln den gesetzlichen Anforderungen zur besseren Durchsetzung verhelfen.¹⁷

a) Transparenz und Information

Vor allem für "Big Data Analytics" stellen die geforderte Erkennbarkeit und Zweckbindung der Datenbeschaffung Herausforderungen dar, z.B. weil die Bearbeitung zu einem anderen als dem ursprünglich angegebenen Zweck bei der Kombination und Auswertung von "Big Data" üblich ist.¹⁸ Die DSGVO enthält detaillierte Transparenz- und Informationspflichten. Information ist unter der DSGVO eine Bringschuld und Voraussetzung einer gültigen Einwilligung und rechtmässiger Bearbeitung der Daten (Art. 13 und 14 DSGVO).

Auch in der Schweiz sollen die Informationspflichten ausgeweitet werden (Art. 13-15 VE-DSG). Besondere Informationspflichten sollen neu auch bei der indirekten Datenbeschaffung über Dritte greifen. Dazu gehören zeitliche Vorgaben. Der Betroffene soll bereits bei der ersten Speicherung der von Dritten beschafften Daten informiert werden, nicht erst bei deren Nutzung.

¹⁷ BJ, Erläuternder Bericht (Fn 15), 46.

¹⁸ THOUVENIN (Fn 12), 63 f.

Der später Beworbene müsste also zeitnah nach der Beschaffung seiner Information – mithin vor der eigentlichen Werbemassnahme – darüber informiert werden, dass er künftig beworben wird (Art. 13 Abs. 5 VE-DSG). Die DSGVO gewährt dem datenbearbeitenden Dritten eine Frist von einem Monat ab Datenerhebung bzw. verlangt die Information zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person oder der Offenlegung an einen anderen Empfänger – d.h. abhängig davon welche Bedingung zuerst eintritt (Art. 14 Abs. 3 DSGVO). Der Katalog der aktiv zu liefernden Informationen umfasst im Wesentlichen die Identität und die Kontaktangaben des Verantwortlichen, die bearbeiteten Personendaten oder die Kategorien der Daten, den Zweck der Bearbeitung und die allfälligen Empfänger oder Empfängergruppen¹⁹ (Art. 13 VE-DSG). Zwar ist die Information unbestritten eine Grundvoraussetzung für die betroffene Person, um ihre Rechte zum Datenschutz und zur Datensicherheit wahrzunehmen. Die im VE-DSG enthaltene Pflicht zur Ankündigung möglicher künftiger Werbemassnahmen bei der ersten Speicherung von Personendaten verursacht jedoch sowohl beim Betroffenen als auch beim Bearbeiter zusätzlichen Aufwand, ohne dass damit das Risiko von Persönlichkeitsverletzungen reduziert würde. Eine Benachrichtigung im Zeitpunkt der ersten Werbemitteilung würde den Zweck mit weniger Aufwand auch erfüllen.

Als weitere Besonderheit sieht der Schweizer Vorentwurf die Information zur Identität und den Kontaktangaben des Auftragsbearbeiters vor, d.h. des Auftragnehmers des Verantwortlichen (Art. 13 Abs. 4 VE-DSG). So müsste jeder Wechsel des IT-Anbieters oder der Werbeagentur dem Datensubjekt gemeldet werden. Die EU sieht keine solche Pflicht vor. Der Vorschlag für die Schweizer Revision lässt sich in diesem Punkt daher nicht mit der Gleichwertigkeit zur Regelung in der EU begründen.

Der Verantwortliche und der Auftragsdatenbearbeiter sollen gemäss VE-DSG Empfänger der Personendaten auch informieren, wenn sie die Daten berichtigen, löschen oder vernichten – aus welchen Gründen auch immer – und wenn eine Verletzung des Datenschutzes erfolgt oder die Bearbeitung eingeschränkt wird (Art. 19 lit. b VE-DSG). Diese administrative Anforderung hätte das Potential, die Datenbearbeitung in der Praxis zum Erliegen zu bringen. Sie beruht vermutlich auf einer Fehlinterpretation von Art. 19 DSGVO. Mit dieser Bestimmung sollte dem in der EU geforderten "Recht auf Vergessen" zum Durchbruch verholfen werden. Wann immer ein derartiger

¹⁹ Die DSGVO spricht von "verarbeiten", der VE-DSG in der Tradition des DSG von "bearbeiten". Inhaltlich besteht kein Unterschied.

Anspruch erfolgreich geltend gemacht wurde, soll der Verantwortliche auch allen Empfängern der Daten die Anpassungen bzw. Löschungen mitteilen – damit diese die Daten der betroffenen Person ebenfalls anpassen bzw. löschen. Der VE-DSG verzichtet zwar erklärermassen auf die explizite Statuierung eines "Rechts auf Vergessen". Gemäss Ansicht des Bundesrates ist ein solches in den Grundzügen bereits im geltenden DSG und vor allem im Persönlichkeitsschutz angelegt.²⁰ Eine weitergehende Regelung (zumindest gegenüber privaten Datenbearbeitern) sieht der Vorentwurf bewusst nicht vor. Der Vorentwurf will gemäss Wortlaut aber gegenüber Drittempfängern eine Informationspflicht des Verantwortlichen für jede Änderung oder Löschung von Daten etablieren – unabhängig davon, aus welchen Gründen die Anpassung der Daten beim Verantwortlichen selbst erfolgte und ob die Änderungen auf Wunsch der betroffenen Person erfolgten oder nicht – was bei der Dynamik der Datenbearbeitung im digitalen Umfeld weder praktikabel noch aus der Sicht der Betroffenen wünschbar sein kann.

Die Information hat gemäss DSGVO in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form und in einer klaren und einfachen Sprache zu erfolgen (Art. 12 Abs. 1 DSGVO). Der Schweizer Vorentwurf enthält keine expliziten sprachlichen Anforderungen, verlangt aber eine Form, die dem Zweck einer transparenten Datenbearbeitung gerecht wird.²¹

Weder die EU noch die Schweiz scheinen in ihrem Pflichtkatalog für Mindestinhalte der Information den teils begrenzten Platz für Text zu berücksichtigen, z.B. bei Angeboten, die auf dem Smartphone abrufbar sind. Immerhin anerkennen die Schweiz und die EU, dass längere Texte nicht zwingend mehr und besser informieren. Die Kombination mit standardisierten Bildsymbolen oder Piktogrammen soll erlaubt sein, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln (Erw. 60 DSGVO).²² Die Kreativität der Anbieter ist gefragt, um die gesetzlichen Vorgaben in eine attraktive Kommunikation umzuwandeln. Denkbar sind z.B. "layered notices", bei denen eine übersichtliche Einstiegsseite mit Symbolen dem Nutzer einen raschen Überblick verschafft. Wer sich detaillierter informieren will, ruft den entsprechenden Abschnitt mit weiteren Informationen und Verlinkungen zu Einstellmöglichkeiten etc. auf. In der EU wird das Verfah-

ren zur Definition der Piktogramme weitgehend durch die Kommission festgelegt (Art. 12 Abs. 8 DSGVO). Vor allem in der Schweiz bieten sich hier Möglichkeiten für Best Practice-Selbstregulierungen.

Beide Regelwerke sehen Ausnahmen von der Informationspflicht vor und anerkennen, dass der Aufwand für die Information verhältnismässig bleiben muss (Art. 14 Abs. 2 lit. b, Art. 19 lit. b VE-DSG, Art. 14 Abs. 5 lit. b und Art. 19 DSGVO). Wo diese Grenze zu ziehen ist, wird die Praxis zeigen, die Ausnahme ist aber eng auszulegen.²³ Auch überwiegende Interessen Dritter oder des Verantwortlichen können die Informationspflicht unter Umständen einschränken, aufschieben oder ausschliessen (Art. 14 Abs. 3 lit. b und Abs. 4 lit. a VE-DSG). Die EU sieht Einschränkungen zugunsten des Berufsgeheimnisses explizit vor (Art. 14 Abs. 5 lit. d DSGVO). Insgesamt würde unter den neu vorgeschlagenen Regeln der Aufwand für die rechtskonforme Datenauswertung zur personalisierten Werbung massiv steigen, insbesondere aufgrund der unaufgefordert und gar vorab zu liefernden Informationen.

Die EU droht bei Verletzung der Informationspflicht mit Busse (Art. 83 Abs. 5 lit. b DSGVO). Vorsätzliche falsche oder unvollständige Informationen sollen neu in der Schweiz strafrechtlich sanktioniert werden (Art. 50 Abs. 1 und 3 VE-DSG).

b) Dokumentation

Die EU verlangt bestimmte Dokumentierungen, z.B. im Zusammenhang mit der Auftragsdatenverarbeitung, der Weitergabe ins Ausland (Art. 46 Abs. 2 lit. a, Art. 49 Abs. 6 DSGVO) oder bei der Verletzung des Datenschutzes (Art. 33 Abs. 5 DSGVO). Zum Nachweis der Einhaltung der DSGVO müssen der Verantwortliche und der Auftragsverarbeiter je ein Verzeichnis führen über die Verarbeitungstätigkeiten in ihrer Zuständigkeit (Art. 30 DSGVO), u.a. mit Angabe der Namen und Kontaktdaten des Verantwortlichen bzw. des Auftragsverarbeiters, der Zwecke der Verarbeitung, der Kategorien von Verarbeitungen im Auftrag, einer Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, der Kategorien von Empfängern, Drittländern, sowie der technischen und organisatorischen Massnahmen (Art. 30 Abs. 1 und 2, Erw. 82 DSGVO).

Dieser allgemeinen Verzeichnispflicht "ähnlich" sein soll die Dokumentationspflicht unter dem VE-DSG, wonach der Verantwortliche und der Auf-

²⁰ BJ, Erläuternder Bericht (Fn 15), 37 und 71.

²¹ BJ, Erläuternder Bericht (Fn 15), 56.

²² BJ, Erläuternder Bericht (Fn 15), 56.

²³ BJ, Erläuternder Bericht (Fn 15), 58.

tragsbearbeiter ihre Bearbeitung zu dokumentieren haben (Art. 19 lit. a VE-DSG). Diese Pflicht soll an die Stelle der Meldepflicht an den EDÖB unter dem geltenden Schweizer Recht für Datensammlungen treten. Die Dokumentation muss den Verantwortlichen und den Auftragsbearbeiter in die Lage versetzen, ihren Informations- und Meldepflichten (z.B. bei Verletzungen des Datenschutzes) nachzukommen. Anders als in der EU sieht der VE-DSG aber nicht vor, welche konkreten Informationen zu dokumentieren sind und verweist auf die Verordnung zum neuen DSG.²⁴ Diese offene Regelung beinhaltet für Werbenetzwerke und Werbetreibende eine grosse Unsicherheit hinsichtlich der zu erfassenden Informationen in der Dokumentation.

Sowohl die EU als auch der Schweizer Vorentwurf stellen die Verletzung der Dokumentationspflicht selbständig unter Strafe (Art. 51 Abs. 1 lit. f VE-DSG; Art. 83 Abs. 4 lit. a DSGVO). Da die in der Schweiz vorgesehene Grundlage im Gesetz im formellen Sinn aber keinen konkreten Umfang der Dokumentation enthält, ist fraglich, ob eine Bestrafung überhaupt dem strafrechtlichen Bestimmtheitsgebot (Legalitätsprinzip) standhalten würde.

c) Auskunftspflicht

Die betroffene Person hat sowohl gemäss DSGVO als auch nach dem VE-DSG ein Auskunftsrecht insbesondere über den Zweck der Datenverarbeitung, die Kategorien der verarbeiteten Personendaten, die Dauer der Speicherung und die Empfänger der personenbezogenen Daten (Art. 15 Abs. 1 DSGVO, Art. 20 Abs. 1 und 2 VE-DSG). Die Regelung in der EU sieht an sich vor, dass eine betroffene Person die jeweils erfragten Informationen und nicht automatisch Auskunft über alle vorhandenen Daten erhält. Um den Aufwand für die Verantwortlichen auf ein zu bewältigendes Mass zu reduzieren, darf ein Verantwortlicher verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftersuchen bezieht (Erw. 63 DSGVO). Gemäss VE-DSG beinhaltet der gesetzliche Katalog das Mindestmass an Informationen, die dem Auskunftssuchende "in jedem Fall" zuzustellen sind.

Auskunftspflichtig ist der Verantwortliche (Art. 20 Abs. 5 VE-DSG; Art. 15 Abs. 1 DSGVO). Gemäss Schweizer Vorentwurf soll eine betroffene Person die Auskunft auch direkt vom Auftragsbearbeiter verlangen können, wenn dieser den Verantwortlichen nicht bekannt gibt oder der Verantwortliche seinen Sitz im Ausland hat (Art. 20 Abs. 5 VE-DSG).

²⁴ BJ, Erläuternder Bericht (Fn 15), 65.

Die EU sieht vor, dass der Verantwortliche "nach Möglichkeit" einen Fernzugang zu einem sicheren System bereitstellen soll, welcher der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde (Erw. 63 DSGVO). Der Schweizer Vorentwurf regelt das Format der Auskunft nicht.

Sowohl in der Schweiz als auch in der EU sind Auskünfte grundsätzlich unentgeltlich (Art. 20 Abs. 1 VE-DSG; Art. 12 Abs. 5 DSGVO) zur Verfügung zu stellen. Die EU sieht jedoch vor, dass der Verantwortliche bei offenkundig unbegründeten oder exzessiven Anträgen (z.B. häufige Wiederholungen) entweder ein angemessenes Entgelt verlangen oder sich weigern kann, aufgrund des Antrags tätig zu werden (Art. 12 Abs. 5 DSGVO). Die Schweiz sieht keinen Kostenersatz vor, wodurch Auskunftsbegehren die Auskunftspflichtigen stark belasten können.

Überwiegende Interessen Dritter und allenfalls des Verantwortlichen, Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software – sowie in der Schweiz explizit formelle gesetzliche Grundlagen – bleiben vorbehalten, dürfen aber in der EU – anders als in der Schweiz – nicht zur gänzlichen Auskunftsverweigerung führen (Art. 21 VE-DSG; Erw. 63 DSGVO). So darf z.B. der Algorithmus einer automatisierten Entscheidung geheim gehalten werden, nicht aber das Ergebnis der Einzelentscheidung und wie sich diese auf die rechtliche oder tatsächliche Stellung der Person auswirkt.²⁵

Die EU sanktioniert Verletzungen der Auskunftspflicht mit Busse (Art. 83 Abs. 5 lit. b DSGVO). Die Schweiz sieht für die vorsätzliche falsche oder unvollständige Auskunft ebenfalls Busse vor (Art. 50 Abs. 1 lit. a VE-DSG), wobei der Bussenbetrag gegenüber der geltenden Regelung massiv erhöht werden soll.

d) Einwilligung und Widerspruch

Als Grundlage für eine rechtmässige Datenverarbeitung steht in der EU und mit dem neuen DSG die Einwilligung der betroffenen Person im Vordergrund (Art. 6 Abs. 1 lit. a DSGVO, Art. 24 Abs. 1 VE-DSG). Die Einwilligung muss wie bis anhin nach entsprechender Information freiwillig erfolgen, (Art. 6 Abs. 1 lit. a DSGVO, Art. 4 Abs. 6 VE-DSG). Die DSGVO fordert eine "echte und freie Wahl", d.h. die betroffene Person muss in der Lage sein, "die

²⁵ BJ, Erläuternder Bericht (Fn 15), 67.

Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden" (Erw. 42 DSGVO). Damit ist, z.B. die Koppelung einer Wettbewerbsteilnahme mit der Zurverfügungstellung und Verwendung der Daten zu Marketingzwecken in der EU nicht mehr möglich. Massgeblich ist, "ob unter anderem die Erfüllung eines Vertrags, einschliesslich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind" (Art. 7 Abs. 4 DSGVO). In der Schweiz ist mit dem Vorentwurf noch völlig offen, wie streng die Anforderungen an die Freiwilligkeit interpretiert werden.

Auch die Aufforderung zur Einwilligung untersteht den Anforderungen an eine verständliche und leicht zugängliche Form und einer klaren und einfachen Sprache (Art. 7 Abs. 2 erster Satz DSGVO). Sie muss "von anderen Sachverhalten klar zu unterscheiden" sein (Art. 7 Abs. 2 erster Satz DSGVO). Die Einwilligung z.B. in Allgemeinen Geschäftsbedingungen ist daher speziell hervorzuheben.

In der EU muss die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Dies ist möglich etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung (Erw. 32). Akzeptiert ist z.B. das Anklicken eines Kästchens beim Besuch einer Internetseite, die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder eine andere Erklärung oder Verhaltensweise, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen keine Einwilligung dar. Auch der Schweizer Vorentwurf erlaubt weiterhin konkludentes Handeln als Form der Einwilligung. Untätig bleiben der betroffenen Person reicht als Einwilligung aber nicht.²⁶

Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in

²⁶ BJ, Erläuternder Bericht (Fn 15), 47.

klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen (Erw. 32 DSGVO).

Eine Einwilligung für das Bearbeiten von besonders schützenswerten Daten muss in der EU und in der Schweiz ausdrücklich sein (Art. 9 Abs. 2 lit. a DSGVO; Art. 4 Abs. 6 VE-DSG). Besonders schützenswerte Daten umfassen in der EU und gemäss dem Schweizer Vorentwurf Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen oder über Massnahmen der sozialen Hilfe und neu auch genetische Daten sowie biometrische Daten, die eine natürliche Person eindeutig identifizieren (Art. 4 Ziff. 13-15, Art. 9 DSGVO; Art. 3 lit. c VE-DSG).

Die betroffene Person kann unter der DSGVO jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einlegen, z.B. wenn die Bearbeitung aufgrund öffentlicher Interessen oder berechtigter privater Interessen (Art. 6 Abs. 1 lit. e und f DSGVO) erfolgt (Art. 21 DSGVO). In der Schweiz sollen betroffene Person einem bestimmten Verantwortlichen bestimmte Datenbearbeitungen explizit verbieten dürfen (Opt-out, Art. 23 Abs. 2 lit. b DSG).²⁷ Der Verantwortliche darf in der Folge die personenbezogenen Daten nicht mehr bearbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 Abs. 1 DSGVO).

Verstösse gegen die Bedingungen der Einwilligung stellt die EU unter Busse (Art. 83 Abs. 5 DSGVO). Die persönlichkeitsverletzende Bearbeitung aufgrund fehlender Einwilligung ist auch im Schweizer Vorentwurf zum DSG weiterhin nicht sanktioniert.

e) Rechtfertigungsgründe

Sofern eine Verletzung der Persönlichkeit gemäss Schweizer Recht vorliegt, soll sie nur dann widerrechtlich sein, wenn sie nicht durch Einwilligung der

²⁷ BJ, Erläuternder Bericht (Fn 15), 68; begründet wird dies mit der voraussichtlichen Anpassung des Übereinkommens vom 28. Januar 1981 des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (E-K 108).

betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt werden kann (Art. 24 Abs. 1 VE-DSG). Der VE-DSG geht, weitgehend wie unter geltendem Recht, davon aus, dass insbesondere bei folgenden Tätigkeiten die Interessen der bearbeitenden Person gegenüber den Interessen der betroffenen Person überwiegen können (Art. 24 Abs. 2 VE-DSG):

1. Bearbeitungen in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags;
2. Bearbeitungen zum Zwecke des wirtschaftlichen Wettbewerbs mit der betroffenen Person, ohne die Daten Dritten bekannt zu geben;
3. Prüfung der Kreditwürdigkeit von volljährigen Person, sofern keine besonders schützenswerten Daten betroffen sind und keine Daten Dritten bekanntgegeben werden;
4. Bearbeitungen beruflicher Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums;
5. Bearbeitungen zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik, soweit die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt sowie Dritten die besonders schützenswerte Personendaten nur so bekannt gegeben und die Ergebnisse nur in einer Weise veröffentlicht werden, welche die betroffenen Personen nicht bestimmbar sind;
6. Sammlung von Personendaten über eine Person des öffentlichen Lebens, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.

Auch in der EU sind die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder das Gesetz Rechtfertigungsgründe für eine rechtmässige Datenbearbeitung (Art. 6 Abs. 1 DSGVO). Im Ergebnis übereinstimmend mit der DSGVO soll auch das neue DSG (wenn auch nicht explizit) Direktwerbung wohl erlauben (Erw. 47 DSGVO, siehe Abschnitt III.2.4e) unten). Der Schweizer Vorentwurf äussert sich zwar nicht ausdrücklich zu dieser Möglichkeit. Gemäss erläuterndem Bericht sollen aber z.B. Adressdaten durch das empfangende Unternehmen zu Werbezwecken verwendet werden dürfen, wenn die betroffene Person die Daten im Hinblick auf den Erhalt einer Kundenkarte oder für eine Bestellung (online oder nicht) übermittelt hat. Die Weiterbenutzung dieser Adresse zu Werbezwe-

cken liegt dann im Rahmen einer anfänglich erkennbaren Zweckbestimmung und gilt als mit dem anfänglichen Zweck vereinbar.²⁸

f) Automatisierte Entscheide und Profiling

Profiling als dynamischer Prozess soll in der Schweiz den statischen Begriff des Persönlichkeitsprofils ersetzen, der im internationalen Vergleich eine schweizerische Eigenheit darstellte. Unter Profilbildung ("Profiling") fällt jede Art der automatisierten Verarbeitung von Daten, wobei in der EU nur personenbezogene Daten erfasst sind, während in der Schweiz auch nicht-personenbezogene Daten Grundlage eines Profilings sein können, wenn das Resultat des Profilings einer Person zugeordnet werden kann. Zweck des Profilings ist es Daten zu generieren, um bestimmte (Art. 4 Ziff. 4 DSGVO) bzw. wesentliche (Art. 3 lit. f VE-DSG) persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Dazu gehört insbesondere die Analyse oder Vorhersage von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person (Art. 4 Ziff. 4 DSGVO, Art. 3 lit. f VE-DSG). Beim Profiling werden Daten zu einem bestimmten Zweck ausgewertet, ohne dass diese Auswertung aber unmittelbare Wirkungen auf die betroffene Person haben muss.²⁹ Obwohl die Schweizer Definition von Profiling auch die Bearbeitung von nicht-personenbezogenen Daten umfasst, ist gemäss Schweizer Vorentwurf die Profilbildung datenschutzrechtlich nur relevant, wenn als Ergebnis Personendaten resultieren.³⁰ Für welchen Zweck das Resultat der Analyse oder Vorhersage schlussendlich eingesetzt wird (z.B. personalisierte Werbung) ist für die Begriffsdefinition von Profiling nicht relevant.

Profiling nach Schweizer Vorentwurf kann mit oder ohne Automatisierung erfolgen, wohingegen in der EU die automatisierte Verarbeitung begriffsnotwendig ist (Art. 4 Abs. 4 DSGVO).³¹ Eine entsprechende Einschränkung wäre auch für die Schweiz sinnvoll. Andernfalls droht der Anwendungsbereich auszufernen. Auch Quartierläden würden nach dem VE-DSG Profiling betreiben, wenn sie über das Einkaufsverhalten ihrer Stammkunden Buch führen.

²⁸ BJ, Erläuternder Bericht (Fn 15), 46.

²⁹ BJ, Erläuternder Bericht (Fn 15), 59.

³⁰ BJ, Erläuternder Bericht (Fn 15), 43 f.

³¹ BJ, Erläuternder Bericht (Fn 15), 44.

Im Unterschied zur EU verlangt der Schweizer Vorentwurf eine ausdrückliche Einwilligung für Profiling (Art. 4 Abs. 6 VE-DSG). Profiling ohne ausdrückliche Einwilligung gilt als Persönlichkeitsverletzung (Art. 23 Abs. 1 lit. d VE-DSG). Demgegenüber erlaubt die EU Profiling, z.B. für Direktmarketing, auch ohne Einwilligung, sofern die Marketinginteressen im Einzelfall berechnete Interessen des Verantwortlichen oder eines Dritten darstellen (Art. 6 Abs. 1 lit. f DSGVO, Erw. 47 und 69 f. DSGVO). Die EU sieht das Erfordernis einer ausdrücklichen Einwilligung – falls weder eine vertragliche noch eine gesetzliche Rechtfertigung greift – im Zusammenhang mit Profiling nur vor bei automatisierten Entscheidungen, sofern der Entscheid rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat (Art. 22 Abs. 1 und 2 DSGVO). Die EU stellt also auf die Wirkung des verwendeten Resultats von Profiling ab. Eine ausdrückliche Einwilligung oder eine gesetzliche Grundlage sind nötig, wenn der automatisierte Entscheid auf besonders schützenswerten Daten beruht (Art. 22 Abs. 4 DSGVO).

Der VE-DSG sieht mit dem Erfordernis der ausdrücklichen Einwilligung somit eine strengere Anforderung an Profiling vor, als die EU dies verlangt. Gerade für Betreiber und Anbieter von personalisierter Werbung stellt die Voraussetzung der Einwilligung einen zusätzlichen Aufwand und ein Wettbewerbsnachteil dar. Im Sinne des risikobasierten Ansatzes ist dabei auch zu berücksichtigen, dass Werbetreibende in der Regel nur an einem bestimmten, eingeschränkten Lebensbereich (z.B. bestimmte Interessen und Konsumgewohnheiten) interessiert sind. Diese Beschränkung verlangt auch bereits das Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 VE-DSG, Art. 4 Abs. 2 DSG). Bei Profiling zur Personalisierung der Werbung geht es letztlich nur um die Beantwortung der Frage, ob eine bestimmte Person mit dem Produkt oder der Dienstleistung beworben werden soll. Die Beeinträchtigung für die betroffene Person aufgrund des Profilings alleine aber auch im Hinblick auf die Nutzarmachung für personalisierte Werbung ist dabei regelmässig gering. Beträchtliche Ausmasse kann die Aussagekraft von Profilen erhalten, wenn der Nutzer sich über verschiedene Geräte und Dienste eines einzelnen Anbieters selbst zum gläsernen Nutzer macht. Diese unterschiedlichen Dimensionen von Profiling sind auseinanderzuhalten – was derzeit im Schweizer Vorentwurf nicht angelegt ist.

Für das Profiling und jegliche andere Bearbeitung von Personendaten für Direktmarketing sieht die EU ein unbedingtes Widerspruchsrecht vor, ohne Einschränkung auf bestimmte Gründe (Art. 21 Abs. 2 und 3 DSGVO). Der Schweizer Vorentwurf sieht ebenfalls ein unbedingtes Opt-out-Recht vor für jegliche Bearbeitungen von Personendaten (Art. 23 Abs. 2 lit. b VE-DSG), einschliesslich Profiling, wobei Profiling nur mit ausdrücklicher Einwilligung

überhaupt zulässig ist. Daten dürfen entgegen der ausdrücklichen Willenserklärung der betroffenen Person nicht (weiter-)bearbeitet werden. Die betroffene Person kann einem bestimmten Verantwortlichen explizit eine bestimmte Datenbearbeitung verbieten, ohne dass hierfür spezifische Voraussetzungen erfüllt sein müssten.³²

Eine automatisierte Einzelentscheidung liegt gemäss VE-DSG vor, "wenn ohne menschliches Zutun eine Auswertung von Daten erfolgt, die zu einer konkreten Entscheidung gegenüber der betroffenen Person führt".³³ Eine besondere Informationspflicht soll greifen, wenn diese Entscheidung rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat (Art. 15 Abs. 1 VE-DSG). Rechtliche Wirkungen gegenüber der betroffenen Person hat die Entscheidung, wenn sie die Rechtsstellung der betroffenen Person unmittelbar beeinflusst. Erhebliche Auswirkungen auf die betroffene Person liegen insbesondere vor bei tatsächlichen Konsequenzen, wobei diese einen gewissen – noch nicht definierten – Schweregrad erreichen müssen.³⁴ Im Falle automatisierter Entscheidungen (z.B. der Kreditgewährung alleine basierend auf Finanzdaten, Versicherungsangebot alleine aufgrund von Gesundheitsdaten³⁵) hat die betroffene Person Anspruch auf Auskunft über das Ergebnis, das Zustandekommen (Logik) und die Auswirkungen der Entscheidungen (Art. 15 Abs. 1 lit. h DSGVO, Art. 20 Abs. 3 VE-DSG).

Der Verantwortliche muss der betroffenen Person alle Informationen zur Verfügung stellen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Dazu gehören in der EU aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO). Werden die personenbezogenen Daten bei der betroffenen Person erhoben, so sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde (Erw. 60 DSGVO). In der EU hat die betroffene Person neben dem Informationsrecht und dem Recht zur Stellungnahme zum automatisierten Einzelfallentscheid auch Anspruch darauf, dass eine natürliche Person seitens des Verantwortlichen auf den Entscheid einwirkt sowie das

³² BJ, Erläuternder Bericht (Fn 15), 68.

³³ BJ, Erläuternder Bericht (Fn 15), 59.

³⁴ BJ, Erläuternder Bericht (Fn 15), 59.

³⁵ BJ, Erläuternder Bericht (Fn 15), 59.

Recht, den Entscheid anzufechten (Art. 22 Abs. 3 DSGVO). In der Schweiz hat die betroffene Person bei automatisierten Entscheiden gemäss Vorentwurf lediglich das Informations- und Anhörungsrecht (Art. 15 VE-DSG). Das Anhörungsrecht liegt durchaus auch im Interesse des Verantwortlichen, "weil unzutreffende automatisierte Einzelentscheidungen auch für ihn negative Konsequenzen nach sich ziehen können, beispielsweise indem ein Vertrag mit einer Person nicht abgeschlossen wird, weil sie zu Unrecht als nicht kreditwürdig eingestuft wurde".³⁶

Die EU reguliert die Entscheidung auch inhaltlich und verlangt vom Verantwortlichen, dass er technische und organisatorische Massnahmen trifft, die eine Diskriminierung natürlicher Personen auf Grundlage von besonderen Datenkategorien verhindern (Erw. 71 DSGVO). Solche expliziten Anforderungen fehlen im Schweizer Vorentwurf.

Gemäss DSGVO und dem Schweizer Vorentwurf droht Busse bei Verletzung der Pflichten für automatisierte Entscheide (Art. 83 Abs. 5 lit. b DSGVO; Art. 50 Abs. 1 VE-DSG), wobei der VE-DSG nur die vorsätzliche falsche oder unvollständige Auskunft bzw. unterlassene Information bestrafen möchte.

g) Erweiterter Geheimnisschutz

Der VE-DSG sieht gegenüber dem geltenden Recht einen erweiterten Geheimnisschutz vor. Unter der Überschrift "Verletzung der beruflichen Schweigepflicht" wird die vorsätzliche Bekanntgabe geheimer Personendaten verboten, wenn die bekanntgebende Person die Daten erlangt hat im Rahmen der beruflichen Tätigkeit, die solche Kenntnis erfordert, oder sie die Daten selbst zu kommerziellen Zwecken bearbeitet (Art. 52 Abs. 1 lit. a und b VE-DSG). Gegenüber dem geltenden Recht soll der Vorentwurf den Geheimnisschutz auf alle geheimen Personendaten ausweiten. Bisher sind nur besonders schützenswerte Personendaten und Persönlichkeitsprofile Objekte des Geheimnisschutzes im DSG (Art. 35 DSG). Damit zielt der Vorentwurf auf eine Annäherung an Art. 321 StGB zur Verletzung des Berufsgeheimnisses, welcher ebenfalls einzig auf die Geheimniseigenschaft abstellt. Eine bedeutende Ausweitung erhält der Geheimnisschutz aufgrund der alternativen Anwendbarkeit von Art. 52 Abs. 1 lit. a und b VE-DSG: Bereits lit. a erfasst jede berufliche Tätigkeit, welche die Kenntnis der geheimen Daten erfordert. Damit sind nicht nur Berufe mit spezialgesetzlicher Schweigepflicht erfasst. Lit. b weitet die Anwendbarkeit des Verbots aber aus auf jede Person, welche

die Daten zu eigenen Zwecken kommerziell bearbeitet. Es kommt für diese Verbotsnorm also nicht darauf an, aus welchem Grund und für welche (kommerzielle) Tätigkeit die Person die Daten erhalten hat. Eine Parallel-Norm in der E-K108 oder in der DSGVO fehlt. Es handelt sich also um eine Schweizer Besonderheit, die in der politischen Diskussion noch zu reden geben dürfte. Der erläuternde Bericht zum VE-DSG nennt als Adressaten Onlinehändler und soziale Netzwerke, weil diese "derartige Informationen zu Werbezwecken kaufen und verkaufen."

Die vorsätzliche Verletzung des erweiterten Geheimnisschutzes ist strafrechtlich besonders hoch sanktioniert – mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (bis zu CHF 1'080'000; Art. 52 VE-DSG). Dienstleister im Bereich personalisierter Online-Werbung wie etwa Betreiber von Werbenetzwerken könnten solche Dienstleistungen kaum mehr in der Schweiz anbieten, wenn dieser Vorschlag ins DSG aufgenommen würde.

h) Datensicherheit

Wie unter geltendem Recht in der Schweiz und unter der DSGVO in der EU, verlangt auch der VE-DSG, dass der Verantwortliche und der Auftragsbearbeiter die Sicherheit von Personendaten gewährleisten und angemessene technische und organisatorische Massnahmen dazu treffen muss (Art. 11 Abs. 1 VE-DSG; Art. 24 DSGVO). Die EU sieht explizit die Pseudonymisierung und Verschlüsselung der Daten als geeignete Massnahmen vor (Art. 32 Abs. 1 lit. a DSGVO). Massgeblich ist auch die langfristige Integrität und Verfügbarkeit der Systeme sowie die Fähigkeit, die Verfügbarkeit von Daten und den Zugang bei einem Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. b und c DSGVO). Die Wirksamkeit der Sicherheitsmassnahmen soll zudem regelmässig überprüft, bewertet und evaluiert werden (Art. 32 Abs. 1 lit. d DSGVO). In der Schweiz sollen konkrete Mindestanforderungen in der Verordnung geregelt werden (Art. 11 Abs. 2 VE-DSG). Das stellt die Adressaten dieser Pflichten vor Rechtsunsicherheiten, da Verpflichtete (analog der Regelung in der EU gemäss Art. 83 Abs. 4 lit. a DSGVO) bestraft werden sollen, wenn sie notwendige Massnahmen nicht treffen – unabhängig davon, ob es tatsächlich zu einer Verletzung kommt oder nicht (Art. 51 Abs. 1 lit. c und Abs. 2 VE-DSG).

Zur Datensicherheit gehört nach gemeinsamem Verständnis der EU und der Schweiz künftig auch der Datenschutz durch Technikgestaltung ("Privacy by Design") und durch datenschutzfreundliche Grundeinstellungen ("Privacy by Default"). Privacy by Design verlangt eine Technikgestaltung, die Datenschutzgrundsätze inklusive Datensicherheit wirksam umsetzt (Art. 18 VE-DSG; Art. 25 Abs. 1 DSGVO). Privacy by Default soll die Masse beschaffter

³⁶ So auch: BJ, Erläuternder Bericht (Fn 15), 60.

und bearbeiteter Daten durch entsprechende Voreinstellungen auf das für den Zweck erforderliche Mass reduzieren (Datenminimierung; Art. 25 Abs. 2 DSGVO). Weitere Massnahmen sind bspw. die standardmässige und weitgehende Pseudonymisierung, Anonymisierung oder Löschung von Personendaten, restriktive Handhabung von Zugriffsrechten, transparente Informationsangaben in Bezug auf die Funktionen und die Verarbeitung von Personendaten, die Überwachung der Datenbearbeitung und die Schaffung von Sicherheitsfunktionen (Erw. 78 DSGVO).³⁷ Anbieter sind verpflichtet, Datenschutz und Datensicherheit bereits bei der Entwicklung und Gestaltung ihrer Produkte, Dienste und Anwendungen zu berücksichtigen (Erw. 78 DSGVO). Auch versäumte Massnahmen der Technikgestaltung und der datenschutzfreundlichen Grundeinstellungen sollen künftig – unabhängig von einer konkreten Verletzung – strafrechtlich sanktioniert werden (Art. 51 Abs. 1 lit. e VE-DSG; Art. 83 Abs. 4 lit. a DSGVO).

Sowohl die EU als auch der Schweizer Vorentwurf sehen eine zwingende Datenschutz-Folgenabschätzung vor, für erst vorgesehene Datenbearbeitungen, die voraussichtlich zu einem hohen (EU) bzw. erhöhten (Schweiz) Risiko für die Persönlichkeit oder die Grundrechte bzw. Rechte und Freiheiten der betroffenen Personen führen (Art. 16 Abs. 1 VE-DSG, Art. 35 Abs. 1 DSGVO). Die dazu nötige erste Beurteilung der geplanten Bearbeitung soll sich an den verwendeten neuen Technologien, der Art, des Umfangs, der Umstände und den Zwecken der Verarbeitung orientieren (Art. 35 Abs. 1 DSGVO). Unterlassene Datenschutz-Folgenabschätzungen sind strafbewehrt (Art. 51 Abs. 1 lit. d und Abs. 2 VE-DSG; Art. 83 Abs. 4 lit. a DSGVO), ebenso die unterlassene Mitteilung des Ergebnisses der Datenschutz-Folgenabschätzung an den EDÖB bzw. die Aufsichtsbehörde in der EU (Art. 50 Abs. 1 lit. c VE-DSG, Art. 83 Abs. 4 lit. a DSGVO).

Im Falle einer Verletzung des Datenschutzes (z.B. Kontrollverlust, Datenmissbrauch, unbeabsichtigte Bekanntgabe), muss der Verantwortliche seine Dokumentationspflicht erfüllen (Art. 19 lit. a VE-DSG; Art. 33 Abs. 5 DSGVO) und der zuständigen Behörde (d.h. dem EDÖB bzw. der entsprechenden Aufsichtsbehörde in der EU) die Verletzung melden (Art. 17 Abs. 1 VE-DSG; Art. 33 Abs. 1 DSGVO). Beide Regelwerke sehen vor, dass die Meldung ausbleiben kann, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt (Art. 17 Abs. 1 VE-DSG; Art. 33 Abs. 1 DSGVO). Faktisch hat der Verantwortliche aber einen grossen Anreiz, bereits beim kleinsten Zweifel über ein mög-

liches Risiko den Datenverlust zu melden, da die unterlassene Meldung eigenständig unter Strafe gestellt wird (Art. 50 Abs. 2 lit. e und Abs. 4 VE-DSG; Art. 83 Abs. 4 DSGVO).

Der Verantwortliche muss unter Umständen Verletzungen und Datenverluste auch den betroffenen Personen mitteilen (Art. 17 Abs. 2 VE-DSG; Art. 34 DSGVO). Der Schweizer Vorentwurf verlangt diese Information, "wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt hat" (Art. 17 Abs. 2 VE-DSG). Massgeblich soll sein, ob durch die Information die Risiken reduziert werden können, z.B. wenn die betroffene Person ihre Zugangsdaten oder Passwörter ändern sollte.³⁸ Es ist unklar, in welcher Form der EDÖB eine solche Mitteilung an die Betroffenen verlangen würde: Der EDÖB könnte das bekannte Instrument der Empfehlung nutzen oder unmittelbar die Mitteilungspflicht verfügen.

Die Mitteilung an den Betroffenen kann aber unter gewissen Umständen unterbleiben (vgl. zu den Ausnahmen in der Schweiz oben III.2.4a)). Die EU sieht eine zusätzliche Ausnahme vor, wenn der Verantwortliche geeignete Massnahmen zur Verminderung des Risikos getroffen hat, z.B. eine Verschlüsselung vor dem Datenleck oder nachträgliche Massnahmen (Art. 34 Abs. 3 lit. a DSGVO). Bei unverhältnismässigem Aufwand erlaubt die EU alternativ auch eine öffentliche Bekanntmachung (Art. 34 Abs. 3 lit. c DSGVO), was den Reputationsschaden wohl aber deutlich erhöhen kann.

Die Informationspflicht bei Datenschutzverletzungen bleibt vor allem im Schweizer Vorentwurf vage. Die Verletzung der Informationspflicht soll aber analog zur EU (Art. 83 Abs. 4 lit. a DSGVO) auch in der Schweiz bestraft werden (Art. 50 Abs. 1 lit. b Ziff. 1 VE-DSG). Wenn der EDÖB eine Mitteilung an die betroffene Person bloss "empfehlen" würde, wären mit dieser Regelung neu reine Empfehlungen des EDÖB strafbewehrt. Würde der EDÖB demgegenüber immer gleich eine Verfügung erlassen, käme gegen den Verstoß dieser Anordnung die selbständige Sanktionsdrohung (Art. 50 Abs. 2 lit. f. VE-DSG oder Art. 292 StGB) zur Anwendung und es bräuchte keine separate Sanktions-Regelung.

i) Selbstregulierung

Auch unter geltendem Recht war es den interessierten Kreisen freigestellt, verbindliche Regelwerke der Selbstregulierung zu implementieren. Im Be-

³⁷ BJ, Erläuternder Bericht (Fn 15), 64.

³⁸ BJ, Erläuternder Bericht (Fn 15), 63.

reich der personalisierten Werbung gibt es sogar bereits solche Ansätze, z.B. das "IAB Framework for Online Behavioural Advertising" oder die "Coalition for better Ads" (siehe unten Abschnitt IV). Bislang haben sich solche Bestrebungen (z.B. Privacy Labels) international aber kaum durchgesetzt. Es lässt sich nicht vor der Hand weisen, dass die eher lasche Durchsetzung von datenschutzrechtlichen Anforderungen auch kaum Anreize zur wirksamen Selbstregulierung mit sich brachte. Die EU und die Schweiz wollen die Selbstregulierung im Datenschutz und in der Datensicherheit nun stärken. In den Grenzen der gesetzten Normen sollen interessierte Kreise Verhaltensregeln ausarbeiten, um die wirksame Anwendung der Datenschutzanforderungen zu gewährleisten und gleichzeitig den Besonderheiten der Sektoren und Bearbeitungen Rechnung zu tragen (Erw. 98 DSGVO). Die EU sieht insbesondere die Berücksichtigung der "besonderen Bedürfnisse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen" vor (Erw. 98 DSGVO). Auch die Schweiz plant, Empfehlungen der guten Praxis im Datenschutz und in der Datensicherheit zu stärken (Art. 8 VE-DSGVO). Damit soll einerseits das Schweizer DSG den allgemeinen, technologieneutralen Charakter beibehalten können und mittels konziseren und dynamischeren Regeln im Privatsektor für die Verantwortlichen und die Auftragsbearbeiter, aber auch für die betroffenen Personen die mit allgemeinen Regeln verbundenen Unsicherheit in Bezug auf das richtige Verhalten reduzieren.³⁹

Gemäss Schweizer Vorentwurf sind Bereiche wie die Videoüberwachung, das Cloud Computing oder Soziale Netzwerke prädestiniert für präzisere Regelungen in Form von Best Practices.⁴⁰ Aber auch bereichsspezifische Begriffsdefinitionen (z.B. das erhöhte Risiko als Auslöser der Pflicht für eine Datenschutz-Folgenabschätzung nach Art. 16 VE-DSG) und Modalitäten bestimmter rechtlicher Anforderungen (z.B. des Anhörungsrechts Art. 15 und 20 Abs. 3 VE-DSG, der Informationspflicht Art. 13 und 14 VE-DSG und der Datenschutz-Folgenabschätzung Art. 16 VE-DSG) können mittels Selbstregulierung konkretisiert werden. Die Schweiz sieht die Anwendung solcher Empfehlungen dabei nicht nur im Privatsektor vor, sondern auch zuhänden der öffentlichen Verwaltung.⁴¹ Bedürfnisse von besonders verletzlichen Personen, z.B. Minderjährige, sind zu berücksichtigen.⁴² Besonders willkommen sind gemäss Vorentwurf Lösungen im Internetbereich (z.B. Datenschutz

³⁹ BJ, Erläuternder Bericht (Fn 15), 52.

⁴⁰ BJ, Erläuternder Bericht (Fn 15), 52.

⁴¹ BJ, Erläuternder Bericht (Fn 15), 52.

⁴² BJ, Erläuternder Bericht (Fn 15), 53.

beim Betrieb sozialer Netzwerke, Benutzung von "Cookies" usw.), da dort die Rechte der betroffenen Personen durch eine rein staatliche Regulierung oftmals ungenügend geschützt seien.⁴³

Selbstregulierung in Form von Best Practice Empfehlungen und technischen Konkretisierungen bieten für Branchenverbände – insbesondere auch für Werbetreibende und Werbedienstleister – Chancen, die regulatorischen Anforderungen mitzugestalten und gleichzeitig Rechtssicherheit für Anbieter und betroffene Personen zu schaffen. Im Sinne der Transparenzbestrebungen im Datenschutz können verständlich kommunizierte Best Practice-Leitlinien auch im Verhältnis zu den betroffenen Personen helfen, deren Erwartungen zu formen und die Reputation der Werbetreibenden zu erhöhen. Wie bei der Information an die betroffenen Personen allgemein fördert eine adressatengerechte Sprache und ein entsprechender Konkretisierungsgrad der technischen Erklärungen die Durchsetzung und Etablierung der Verhaltensregeln.

In der Schweiz soll dem EDÖB eine führende Rolle bei der Ausarbeitung der Empfehlungen der guten Praxis zukommen (Art. 8 Abs. 1 VE-DSG).⁴⁴ Kommt die Initiative von Seiten der interessierten Kreise, können diese die Empfehlungen dem EDÖB zur Genehmigung unterbreiten (Art. 8 Abs. 2 VE-DSG). Doch soll auch der EDÖB selber die Initiative für Selbstregulierung ergreifen können, wobei er die betroffenen Kreise einbeziehen muss. Bei diesem von Seiten der Behörde initiierten Szenario liesse sich allerdings kaum mehr von Selbstregulierung sprechen. In der EU sollen die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission die Ausarbeitung von Verhaltensregeln fördern (Art. 40 Abs. 1 DSGVO). Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsbearbeitern vertreten, können Verhaltensregeln ausarbeiten, ändern oder erweitern, welche die Anwendung der DSGVO z.B. in folgenden Bereichen präzisieren (Art. 40 Abs. 2 DSGVO):

1. Faire und transparente Verarbeitung;
2. Berechtigte Interessen des Verantwortlichen in bestimmten Zusammenhängen;
3. Erhebung personenbezogener Daten;
4. Pseudonymisierung personenbezogener Daten;
5. Unterrichtung der Öffentlichkeit und der betroffenen Personen;

⁴³ BJ, Erläuternder Bericht (Fn 15), 53.

⁴⁴ BJ, Erläuternder Bericht (Fn 15), 52 f.

6. Ausübung der Rechte betroffener Personen;
7. Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
8. Massnahmen und Verfahren für die Sicherheit der Verarbeitung
9. Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen;
10. Übermittlung personenbezogener Daten an Drittländer.

Mit Befolgung der Empfehlungen der guten Praxis hält der Verantwortliche auch die entsprechenden rechtlichen Anforderungen an die Datenbearbeitung ein (Art. 9 Abs. 1 VE-DSG). Die EU sieht z.B. bei der Bemessung von Geldbussen explizit vor, dass die Einhaltung von Verhaltensregeln zu berücksichtigen ist (Art. 83 Abs. 2 lit. j DSGVO).

Zu beachten ist, dass Best Practice-Regeln nur so wirksam sein werden, wie sie sich als Standard durchsetzen. Um eine berechnete Erwartung der betroffenen Person zu begründen und den Datenschutz der betroffenen Person tatsächlich zu verbessern, sind praxistaugliche Empfehlungen unumgänglich. Lobend erwähnen die Erläuterungen des Vorentwurfs bestehende Ansätze zur Selbstregulierung im Bereich des Internets und der Telekommunikation, z.B. die Brancheninitiative des Schweizerischen Verbandes der Telekommunikation für verbesserten Jugendmedienschutz in den neuen Medien und zur Förderung der Medienkompetenz in der Gesellschaft sowie den Code of Conduct Hosting (CCH) der Swiss Internet Industry Association (Simsa) vom 1. Februar 2013, der Verhaltensregeln für Schweizer Hosting Provider aufstellt.⁴⁵ Bei sich wandelnden Technologien und kurzen Innovationszyklen sind die Datenbearbeiter und Anbieter der Dienstleistungen wohl am besten geeignet, die Machbarkeit und Umsetzungsfähigkeit von praktischen Handlungsanweisungen zu beurteilen. Gleichzeitig sollten Datenbearbeiter aus diversen Branchen – inklusive Werbetreibende und Werbenetzwerke – daran interessiert sein, für ihre Aktivitäten Rechtssicherheit zu schaffen und gegenüber dem Werbeadressaten und Kunden als transparenter Anbieter und Partner aufzutreten. Da Datenschutz und Datensicherheit zunehmend Reputationsfaktoren werden, sollten Datenbearbeiter damit über genügend Anreize verfügen, griffige und umsetzbare Best Practice Leitlinien, z.B. über entsprechende Labels, einzuführen und auch zu befolgen. Die Al-

⁴⁵ BJ, Erläuternder Bericht (Fn 15), 53.

ternative zu entsprechend kooperativen Bemühungen seitens der Industrie sind einseitige Empfehlungen der Aufsichtsbehörden bzw. verbindliche Verfügungen im Einzelfall.

j) Sanktionsrisiken

Das geltende DSG enthält strafrechtliche Sanktionsdrohungen für die vorsätzliche Verletzung der Auskunft- und Mitwirkungspflicht sowie der Meldepflicht für Datensammlungen (Art. 34 DSG). Zum bestehenden DSG hielt die Botschaft von 1988 fest, dass Verstösse gegen die Bestimmungen des Datenschutzgesetzes grundsätzlich nicht mit strafrechtlichen, sondern mit zivil- und verwaltungsrechtlichen Sanktionen geahndet werden.⁴⁶ Die Strafbestimmungen in Art. 34 und 35 DSG (damals Art. 28 und 29) bilden eine Ausnahme von diesem Prinzip.⁴⁷ Eine breit angelegte strafrechtliche Absicherung der Regeln über das Bearbeiten von Personendaten durch private Personen, etwa nach dem Modell des Lauterkeitsrechts, wäre auch aus der Sicht des Legalitätsprinzips unter Art. 1 StGB (Schweizerisches Strafgesetzbuch, SR 311.0) problematisch.⁴⁸

Demgegenüber sieht die DSGVO bei Pflichtverletzungen Bussen bis zum höheren Betrag von EUR 20'000'000 bzw. 4% des zuletzt gesamten weltweit erzielten Jahresumsatzes (Art. 83 Abs. 5 DSGVO) vor. Mit dem Argument der Gleichwertigkeit⁴⁹ soll gemäss Schweizer Vorentwurf ein gegenüber dem geltenden DSG massiv erweiterter Sanktionskatalog Bussen bis CHF 500'000 verankern (Art. 50 f. VE-DSG). Für die vorsätzliche Verletzung der beruflichen Schweigepflicht soll gar eine Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (bis zu CHF 1'080'000) ausgefällt werden können.⁵⁰

Die Schweiz will also auf die Übernahme der dem Kartellrecht nachempfundenen hohen Sanktionsdrohungen der DSGVO verzichten. Stattdessen sollen neu vorsätzliche und fahrlässige Verstösse gegen zahlreiche administrative Pflichten strafrechtlich sanktioniert werden. Darunter fallen Informations-,

⁴⁶ Botschaft DSG 1988 (Fn 14), 484.

⁴⁷ Botschaft DSG 1988 (Fn 14), 484.

⁴⁸ MARCEL ALEXANDER NIGGLI/STEFAN MAEDER, in: Basler Kommentar, Datenschutzgesetz – Öffentlichkeitsgesetz, Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), 3. Aufl., Basel 2014, Vor Art. 34 und 35 DSG N 3.

⁴⁹ BJ, Erläuternder Bericht (Fn 15), 79, 83.

⁵⁰ BJ, Erläuternder Bericht (Fn 15), 86.

Dokumentations-, Auskunfts-, Melde- und Genehmigungspflichten, die Pflicht eine Datenschutz-Folgenabschätzung durchzuführen und deren Ergebnis dem EDÖB mitzuteilen, Datensicherheitsmassnahmen zu ergreifen, im Verwaltungsverfahren vor dem EDÖB mitzuwirken und ganz allgemein den Verfügungen des EDÖB Folge zu leisten (Art. 50 und 51 VE-DSG). Der Vorentwurf sieht aber keine vom EDÖB verhängten Verwaltungssanktionen vor wie in der EU (Art. 83 Abs. 1 DSGVO), sondern weist die Verfolgungskompetenz den Kantonen zu (Art. 54 VE-DSG). Weiterhin nicht strafrechtlich sanktioniert werden sollen in der Schweiz Verletzungen der Bearbeitungsgrundsätze an sich (Art. 4 VE-DSG). Diese Asymmetrie von strafloser Verletzung des Kernbereichs des Datenschutzrechts bei gleichzeitig drakonischen Strafdrohungen für die Verletzung administrativer (Neben-)Pflichten lässt sich schwer begründen, auch wenn die administrativen Pflichten ebenfalls einen verbesserten Datenschutz bezwecken.

Gemäss Begleitbericht zum VE-DSG ist die vorgesehene Sanktionsregelung notwendig für den Erhalt des gleichwertigen Schutzniveaus: "Ein zu mildes Strafsystem könnte zur Folge haben, dass die schweizerische Regelung von der Europäischen Union nicht mehr als angemessen erachtet würde".⁵¹ Die Argumentation zum Vorentwurf stützt sich insbesondere auf den Entwurf zum Europaratsübereinkommen (E-K 108). Dessen Wortlaut sieht allerdings nur die Sicherstellung der "wirksamen" Umsetzung (Art. 4 Abs. 1) und "geeignete" Sanktionen und Rechtsmittel (Art. 10) vor. Auch die EU verlangt nicht zwingend die komplette Übernahme des Sanktionskatalogs, sondern sie verlangt selbst von ihren Mitgliedstaaten lediglich "wirksame" Rechtsbeihilfe, die im Falle von Geldbussen aber auch verhältnismässig und abschreckend sein müssen (Art. 83 Abs. 9 DSGVO, vgl. auch Art. 84 Abs. 1 DSGVO). Dass eine Abschreckung zwingend hohe Geldbussen für Administrativpflichten bedingt, ist damit aber noch nicht gezeigt. Es scheint störend, dass die EU ihren eigenen Mitgliedstaaten bewusst Spielraum einräumt, die Schweiz als Drittstaat und Nicht-EU-Mitglied diesen zumindest im Vorentwurf aber zu wenig nutzt.

Es stellt sich insbesondere bei an sich rein administrativen Pflichten, wie der Dokumentationspflicht, die Frage, ob die Sanktionsdrohungen zur Erreichung der Regelungsziele nicht überschüssend sind. Das neue DSG soll insbesondere die Kontrolle der betroffenen Person über ihre eigenen Daten sowie die Eigenverantwortung der Verantwortlichen stärken und gleichzeitig die Wettbewerbsfähigkeit der Schweiz erhalten, "indem ein günstiges Um-

feld geschaffen wird, mit dem der grenzüberschreitende Datenverkehr erleichtert und die Attraktivität unseres Landes für neue Aktivitäten im Zusammenhang mit der digitalen Gesellschaft gesteigert werden kann".⁵² Bei Nichtbefolgen der Administrativpflichten drohen dem Verantwortlichen regelmässig bereits an sich Rechtsnachteile, z.B. weil er in einem Zivilprozess oder in einer Untersuchung durch den EDÖB mangels Dokumentation keine rechtskonforme Bearbeitung oder getroffene Sicherheitsmassnahmen aufzeigen kann. Zudem sind die administrativen Pflichten im Vorentwurf sehr unbestimmt, was eine Bestrafung rechtsstaatlich problematisch erscheinen lässt (Art. 1 StGB).

In Zeiten sich rasch entwickelnder technologischer Innovationen im internationalen Umfeld braucht es zur Umsetzung wirksamer Datenschutzvorschriften nach der hier vertretenen Meinung zudem keinen extensiven Sanktionskatalog für administrative Pflichten mit massiven Bussendrohungen, sondern vielmehr die Förderung des effizienten Dialogs zwischen kompetenten Aufsichtsbehörden und Anbietern. Für die Rechtssicherheit sowie zur Durchsetzung einer einheitlichen Praxis ist die geplante Ausweitung der Verfügungskompetenz des EDÖB darum zielführender (Art. 43 VE-DSG): Datenbearbeiter und EDÖB können sich über geplante und bereits umgesetzte Massnahmen austauschen. Datenbearbeiter können eigene Risiken auch aktiv reduzieren, wenn sie sich durch einen Dialog mit dem EDÖB Rechtssicherheit verschaffen. Der EDÖB kann auf Anzeige hin oder von sich aus Untersuchungen einleiten und Empfehlungen aussprechen, wenn er Schwachstellen oder Verbesserungsbedarf vermutet. Damit würde den Zielen der Transparenz bei der Datenbearbeitung und dem Schutz der Persönlichkeit der betroffenen Person schlussendlich auch besser Rechnung getragen. Können sich der EDÖB und der Datenbearbeiter trotz Empfehlung des EDÖB nicht auf das weitere Vorgehen einigen, kann der EDÖB eine Verfügung erlassen. Der Datenbearbeiter hat dann die Wahl, die Verfügung zu akzeptieren oder sie gerichtlich anzufechten. Bei Widerhandlung gegen eine rechtskräftige Verfügung würden dann (nach Ansetzung einer Erfüllungsfrist) die Instrumente des Art. 41 VwVG (Bundesgesetz über das Verwaltungsverfahren, SR 172.021) greifen, d.h. die Ersatzvornahme auf Kosten des Verpflichteten, der unmittelbarer Zwang gegen die Person des Verpflichteten oder an seinen Sachen, sowie schliesslich die Strafverfolgung wegen Ungehorsams nach Art. 292 StGB.

⁵¹ BJ, Erläuternder Bericht (Fn 15), 83.

⁵² BJ, Erläuternder Bericht (Fn 15), 17 f.

Damit wäre der Anreiz für einen Austausch zwischen Datenbearbeitern und dem EDÖB grösser – wovon bei laufenden technologischen Neuentwicklungen und Produktinnovationen beide Seiten profitieren und dem Schutz der betroffenen Person schliesslich wirksamer zur Durchsetzung verholfen wird.

k) Durchsetzung

Die EU sieht die Beschwerdemöglichkeit für die betroffene Person an die jeweilige Aufsichtsbehörde vor (Art. 77 DSGVO), welche Verletzungen der DSGVO mit Geldbusse sanktionieren kann (Art. 83 DSGVO). Zentral für die bessere Durchsetzung des DSG wird in der Schweiz aber die Kompetenzerweiterung des EDÖB sein. Der EDÖB soll nämlich neu, neben der Möglichkeit vorsorgliche Massnahmen auszusprechen (Art. 42 VESG), eine allgemeine Verfügungskompetenz erhalten (Art. 43 Abs. 1 VE-DSG). Eine Widerhandlung gegen solche Verfügungen ist wiederum strafbewehrt (Art. 50 Abs. 2 lit. f VE-DSG). Ob es die zusätzlich vorgeschlagenen Strafdrohungen für die Missachtung von administrativen Nebenpflichten wirklich braucht, ist fraglich (siehe oben Abschnitt III.2.4j)).

Zuständig für die Durchsetzung der strafrechtlichen Sanktionen wären weiterhin die kantonalen Strafverfolgungsbehörden. Es ist vorauszusehen, dass dem Thema Datenschutz nicht alle Kantone denselben Stellenwert einräumen würden. Eine einheitliche Rechtsdurchsetzung und Praxis könnte lange auf sich warten lassen. Strafrechtliche Sanktionen richten sich in erster Linie gegen die verantwortlichen natürlichen Personen. Nur wenn die Ermittlung der strafbaren Person "unverhältnismässig" wäre, soll stattdessen der Geschäftsbetrieb mit einer Busse von maximal CHF 100'000 bestraft werden (Art. 53 VE-DSG). Je kleiner ein Unternehmen, desto einfacher lässt sich die für Datenbearbeitung verantwortliche Person eruieren. Bei grossen Konzernen und insbesondere bei globalen Online-Plattformen wäre es für die Strafverfolgungsbehörden in der Praxis kaum möglich, eine verantwortliche Person zu eruieren und eine Strafsanktion durchzusetzen. Während also die für Online Aktivitäten eines Schweizer KMU verantwortliche Personen als Täter einen Strafregistereintrag und eine happige Busse riskieren würden, kämen globale Plattformbetreiber im schlimmsten Fall mit einer im Verhältnis zum Sanktionsregime in der EU geringen Busse davon.

Der Begleitbericht zum VE-DSG geht davon aus, dass betroffene Personen ihre Rechte zum Datenschutz auch wegen der Kostenrisiken bisher insbe-

sondere im privaten Sektor kaum wahrnehmen.⁵³ Daher sieht der Vorentwurf "als zentrale Massnahme"⁵⁴ auch eine Befreiung von den Gerichtskosten für Verfahren zur Durchsetzung von Streitigkeiten nach dem DSG vor (neuer Art. 113 Abs. 2 lit. g ZPO). Zwar erwartet der Begleitbericht keinen "sprunghaften" Anstieg von Verfahren. Angesichts des breiten Katalogs vermuteter Persönlichkeitsverletzungen (z.B. bei Profiling, Art. 23 VE-DSG), besteht mit der geplanten Neuregelung allerdings durchaus Potential für vermehrte Klagen. Für Betreiber von personalisierter Werbung drohen neben strafrechtlicher Verfolgung, neu auch zivilrechtliche Konsequenzen sowie strafbewehrte Verfügungen des EDÖB.

IV. Fazit

Die Revision des DSG bietet die Chance, die durch Digitalisierung und Internet entstandenen neuen Risiken der Datenbearbeitung für die Persönlichkeit des Einzelnen zu adressieren. Dazu gehören insbesondere Anforderungen an die Datensicherheit sowie die Gewährleistung von Transparenz und Widerspruchsmöglichkeiten bei automatisierten Entscheiden, die für den Einzelnen negative Auswirkungen haben können. Die Umsetzung der Pflichten aus der revidierten Übereinkunft des Europarates zum Datenschutz gehört für die Schweiz zum Pflichtprogramm. Die Übernahme (und teilweise gar Verschärfung) zahlreicher administrativer Nebenpflichten aus der DSGVO hingegen gilt es zu vermeiden. Insbesondere die detaillierten (und teils strafbewehrten) Informations- und Einwilligungspflichten stärken den Datenschutz kaum, behindern aber Entwicklung und Einsatz von datengestützten Geschäftsmodellen in der Schweiz (etwa die Personalisierung der Angebote und der Werbung) und begünstigen indirekt die globalen Online-Plattformen.

Noch ist nicht vorhersehbar, in welche Richtung sich die Revision des DSG entwickeln wird. Werbeauftraggeber und Online-Plattformbetreiber tun aber gut daran, sich nicht auf die Zurückhaltung des Gesetzgebers zu verlassen. Letztlich hängt die Wirksamkeit von Werbeformaten von der Akzeptanz beim Publikum ab. Am 15. September 2016 haben sich die wichtigen internationalen Verbände und Betreiber von Online-Plattformen zur "Coalition for better Ads" zusammengeschlossen. Sie wollen in gemeinsamer Selbstregulierung dafür sorgen, dass die als besonders störend empfundenen Werbefor-

⁵³ BJ, Erläuternder Bericht (Fn 15), 68.

⁵⁴ BJ, Erläuternder Bericht (Fn 15), 91.

men (etwa "Pop-Ups" und "Lay-Overs") von den Bildschirmen der Medienplattformen verschwinden. Zwar steht der Tatbeweis noch aus, ob dieses Vorhaben gelingt und Werbung beim Publikum künftig vermehrt Akzeptanz findet. Werbeauftraggeber und Medienplattformen haben aber ein ureigenes Interesse daran, dass Werbung beim Publikum Akzeptanz findet.

Daneben ist aber auch der Schweizer Gesetzgeber gefragt, die vorhandenen Spielräume zu nutzen, was der VE-DSG noch nicht ausreichend macht. Im Gegenteil: Der VE-DSG schiesst in verschiedenen Belangen selbst über die hohen zwingenden Vorgaben der DSGVO hinaus. Beispiele dafür sind das auf Strafrecht gründende Sanktionsregime für die Verletzung von administrativen Datenschutzpflichten sowie auch die Bestimmungen, welche personalisierte Werbung betreffen. Dabei wären gerade Schweizer Online-Plattformen mit ihrem kleinen Heimmarkt auf flexiblere Regelungen angewiesen. Dies gilt in besonderem Masse für Medien, die ihr redaktionelles Angebot (auch) über Werbeeinnahmen finanzieren. Sie stehen im Wettbewerb mit global tätigen Online-Plattformen, welche über eine viel grössere Datenbasis für die Optimierung ihrer Angebote und die Personalisierung von Werbung verfügen. Gerade im Bereich der nationalen Medienangebote behindern starre gesetzliche Vorgaben die Finanzierbarkeit redaktioneller Medien und sie gefährden damit letztlich die Medienvielfalt.