1/21

Beiträge | Contributions

Berichterstattung | Comptes-rendus

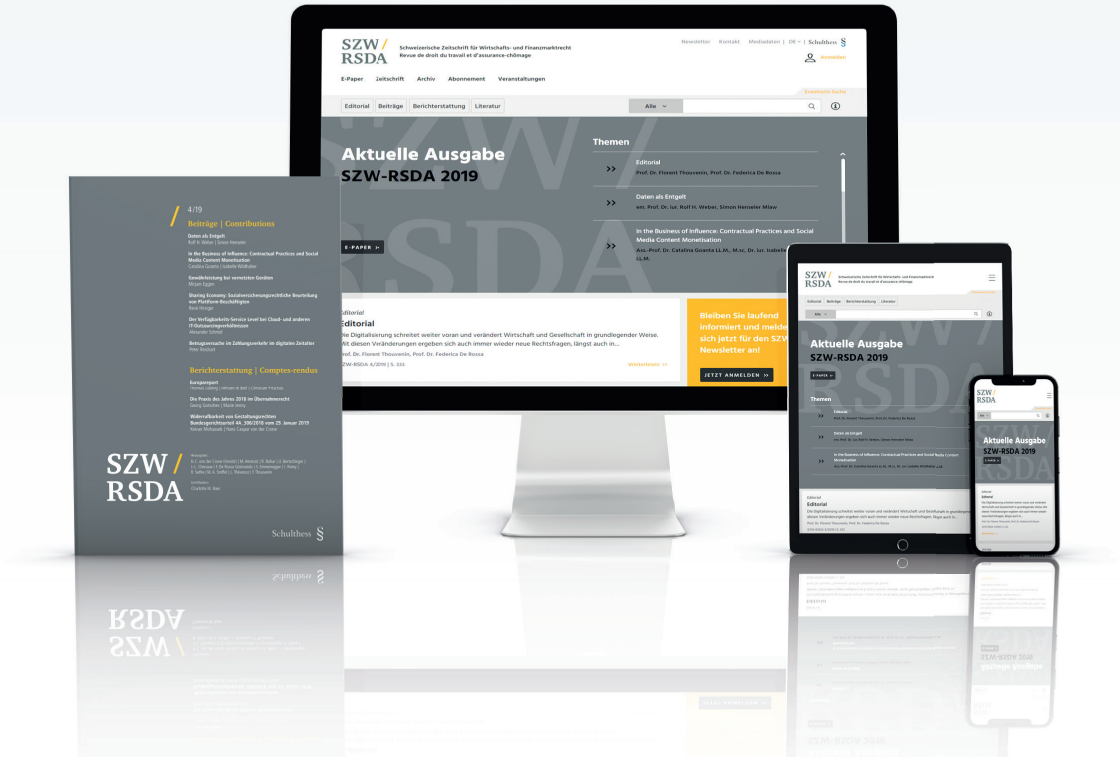
SZW / RSDA

Herausgeber:
H. C. von der Crone (Vorsitz) | M. Amstutz | R. Bahar | U. Bertschinger | I. Chabloz | J.-L. Chenaux | F. De Rossa Gisimundo | S. Emmenegger | I. Romy | L. Thévenoz | F. Thouvenin

Schriftleiterin:
Charlotte M. Baer

Schulthess §

Lesen Sie die SZW neu auch online.



- SZW Printausgabe – weiterhin alle zwei Monaten im Briefkasten
- SZW E-Paper – bequem digital im Printlayout lesen NEU
- SZW E-Recherche – schnelles Finden im Online-Archiv NEU

www.szw.ch

Alle SZW-Abonnenten profitieren ab sofort vom neuen Online-Angebot der SZW
Sie erhalten Ihre persönlichen Zugangsdaten per E-Mail und können sich damit unter www.szw.ch einfach anmelden.

Sie möchten die neue SZW kennenlernen?
Testen Sie jetzt die SZW im kostenlosen Probeabonnement. Sie erhalten zwei Printausgaben sowie für 2 Monate einen Testzugang zu www.szw.ch.
Mehr Infos unter www.szw.ch/abonnement

Schulthess Juristische Medien AG · Zwingliplatz 2 · CH-8021 Zürich · Tel. +41 (0)44 200 29 29 · service@schulthess.com

Schulthess §

Inhalt | Table des matières

Die Strafbestimmungen des neuen DSG

David Rosenthal | Seraina Gubler*

As soon as the revised Swiss Federal Act on Data Protection (DPA) will come into force, the cantonal prosecuting authorities will be entitled to impose heavy fines of up to CHF 250 000 on the person responsible for non-compliant behavior. While this may seem to be a low figure compared to the high figures provided for by the GDPR, the fines under the revised DPA are of personal nature and may not be covered by the company. This will make the DPA fines very effective. Unlike under the GDPR, however, these sanctions only apply in a relatively small number of cases. The violation of the basic principles of the DPA are not sanctioned, for example. The fines cover in essence the violation of obligations with regard to the data protection notice obligation, the right of access, data security, controller-processor relationships and data exports. But only intentional violations can be prosecuted. Most of the new data protection governance obligations, such as data breach notices or data protection impact assessments, are not enforced by fines. A further difference to the GDPR is, that it is not the data protection authority who imposes fines. The cantonal prosecutors, who notably have little or no experience in the field of data protection, do this. Last but not least, special attention should be given to a provision not yet known by the GDPR: The revised DPA provides for a «professional secrecy for everyone». The intentional violation thereof may, upon request, result in a criminal sanction.

Inhaltsübersicht

I. Einleitung

Verstösse gegen den Datenschutz galten bisher noch nicht einmal als Kavaliersdelikt. Das DSG sieht zwar seit jeher Bussen vor, doch werden sie in der Praxis kaum verhängt. Diese Betrachtung dürfte sich mit den vergleichsweise happigen Bussendrohungen im revidierten Schweizer Datenschutzgesetz («revDSG») ändern.[1/2] Der Gesetzgeber hat die Maximalbusse auf das 25-fache der bisherigen Busse von CHF 10 000[3] erhöht. Diese Stärkung des Datenschutzes ist jedoch nicht nur intrinsisch motiviert, sondern zusätzlich von zwei externen Faktoren getrieben. Zum einen musste der Schweizer Gesetzgeber die Vorgaben des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten umsetzen,[4] welches die Schweiz als Vertragspartei in Art. 10 dazu verpflichtet, geeignete Sanktionen gegen Verletzungen nationaler Datenschutzvorschriften festzulegen. «Geeignet» ist eine Sanktion laut Art. 57 der EU-Richtlinie 2016/680[5], welche auf dem

* *David Rosenthal,* lic. iur., und *Seraina Gubler,* Rechtsanwältin, beide Zürich.

1 BBl 2020 7639.
2 Eine erste Kommentierung des gesamten revidierten Datenschutzgesetzes findet sich bei *David Rosenthal,* Das neue Datenschutzgesetz, Jusletter 16. November 2020.
3 Art. 34 und 35 DSG (SR 235.1) i.V.m. Art. 106 Abs. 1 StGB (SR 311.0).
4 SR 0.235.1 (für die Schweiz in Kraft seit 1. Februar 1998).
5 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

Übereinkommen aufbaut und für die Schweiz als Weiterentwicklung des Schengen-Besitzstands[6] gilt,[7] wenn sie «abschreckend» wirkt.[8] Zum Anderen legte der Schweizer Gesetzgeber bei der Ausarbeitung des neuen Datenschutzgesetzes grossen Wert darauf, der Europäischen Kommission[9] keine Gründe zu liefern, der Schweiz die überfällige Erneuerung des Angemessenheitsbeschlusses zu verweigern.[10] Eine Verweigerung hätte zur Folge, dass beim Datenaustausch über die Schweizer Grenzen hinaus beidseitig ein administrativer Mehraufwand entstünde und die Schweiz in einer zunehmend digitalisierten Welt somit einen Wettbewerbsnachteil erleiden würde.

Die maximale Bussenhöhe von CHF 250 000 mag im Vergleich zu EUR 20 Mio. bzw. bis zu vier Prozent des weltweiten Jahresumsatzes gemäss DSGVO[11] auf den ersten Blick weniger abschreckend wirken. Es muss jedoch beachtet werden, dass sich die DSGVO-Bussen gegen das jeweilige Unternehmen, die revDSG-Bussen hingegen gegen die verantwortliche natürliche Person richten. Dieser Unterschied rührt daher, dass in der Schweiz – anders als im EWR-Raum – kein eigentliches Prozessrecht für Verwaltungssanktionen mit pönalem Charakter existiert. Damit fehlen die notwendigen rechtssicheren Regelungen der strafprozessualen Garantien, was unter anderem zur Folge hätte, dass die verfahrensrechtliche Stellung von natürlichen Personen ausgehöhlt würde.[12]

Die Schweizer Bussen sind freilich nicht weniger abschreckend als diejenigen unter der DSGVO. Im Gegenteil, sie sind nach Ansicht der Autoren sogar schärfer, denn nach verbreiteter Auffassung können die revDSG-Bussen weder versichert noch vom Unternehmen übernommen werden.[13] Sie zielen auf den Mann bzw. die Frau hinter einer Entscheidung. Wer im Rahmen seiner beruflichen Tätigkeit noch bereit sein mag, Risiken für seinen Arbeitgeber einzugehen, ist dort, wo ihn die Konsequenzen persönlich treffen können, aller Erfahrung nach sehr viel zurückhaltender. Damit wird letztlich auch begründet, warum solche Bussen nicht vom Arbeitgeber bezahlt werden dürfen: Sie müssen höchstpersönlich bleiben, ansonsten würde die Straffunktion vereitelt (was wiederum strafbar sein kann).

II. Strafbarkeitsvoraussetzungen

1. Vorbemerkung

Die Strafbestimmungen des revidierten DSG finden sich in den Art. 60–66 revDSG. Neuerdings sind wesentlich mehr Tatbestände strafbewehrt als bisher (vgl. Ziff. II.2). Wer Personendaten bearbeitet, d.h. Daten, die Rückschlüsse auf eine bestimmbare Person zulassen, sollte sich bewusst sein, dass die Strafbewehrung sofort ab Inkrafttreten des revDSG gilt. Sämtliche relevanten Übergangsbestimmungen hinsichtlich der neuen DSG-Pflichten wurden vom Parlament in den Beratungen gestrichen. Einzig für die Einhaltung der Grundsätze von *Privacy by Design* und *Privacy by Default* (Art. 7 revDSG) und für die Pflicht zur Vornahme einer Datenschutzfolgenabschätzung (DSFA) in den Art. 22 und 23 besteht eine solche (deren Verletzung ist aber nicht strafbar).[14] Revidiert wurde auch Art. 179^{novies} StGB und neu eingeführt Art. 179^{decies} StGB, die beide ebenfalls direkt den Umgang mit Personendaten betreffen.

durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl L 119/89).

6 SR 0.362.31.

7 Erw. 102 der EU Richtlinie 2016/680.

8 Vgl. auch S. 7099 der Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941.

9 Zuständigkeit für die Angemessenheitsbeurteilungen gemäss Art. 45 Abs. 1 DSGVO (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [ABl L 119/1]).

10 Die Kommission überprüft das Datenschutzniveau der Schweiz insbesondere im Hinblick auf das revidierte DSG. Die Kommission hätte gemäss einer internen provisorischen Agenda eigentlich am 3. Juni 2020 einen Entscheid treffen sollen: <*https://www.inside-it.ch/de/post/eu-kommission-beurteilt-schweizer-datenschutz-20200522*> (Stand 10. Januar 2021).

11 Art. 83 DSGVO.

12 Vgl. BBl 2017 7098 f.

13 *Vera Delnon/Bernhard Rüdy,* in: Basler Kommentar, Strafgesetzbuch II, 4. Aufl., Basel 2018, Art. 305 StGB, N 20, m.w.H.; gegen die Tatbestandsmässigkeit einer Vollstreckungsbegünstigung: *Damian K. Graf,* Art. 305, N 9, in: ders. (Hrsg.), Annotierter Kommentar StGB, Bern 2020.

14 Art. 69 revDSG.

2. Sanktionierte Tatbestände

2.1 Vorbemerkung

Nicht alle Verstösse gegen das revDSG sind bussenbewehrt, sondern nur die in den Artikeln 60–63 aufgeführten Tatbestände. Die ungerechtfertigte Verletzung der Bearbeitungsgrundsätze an sich ist im revidierten DSG zum Beispiel nicht strafbar.[15] Ebenso wenig sind die meisten der neu eingeführten Governance-Pflichten (wie z.B. die Meldepflicht für Verletzungen der Datensicherheit, das Führen eines Verzeichnisses der Bearbeitungstätigkeiten oder die Durchführung einer Datenschutzfolgenabschätzung) strafrechtlich abgesichert, was etwas erstaunt. Damit unterscheidet sich das revidierte DSG von der DSGVO, die für fast jede Verletzung der DSGVO eine Busse vorsieht.[16] Wer also beispielsweise eine Verletzung der Datensicherheit nicht wie vorgeschrieben dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) meldet, muss anders als unter der DSGVO nicht mit Strafe rechnen. Im Gegenteil kann er sich damit sogar Ärger ersparen. Erfahrungsgemäss dürften Schweizer Unternehmen dennoch grundsätzlich bemüht sein, sich an die neuen Bestimmungen zu halten – und sei es nur, weil sie das bereits für die DSGVO tun oder gar nicht realisieren, dass Sanktionen fehlen.

2.2 Verletzung der Informations- und Auskunftspflicht (bisher)

Auf den ersten Blick nicht verändert hat sich im revDSG die Strafbewehrung der vorsätzlich falschen, unvollständigen oder unterlassenen Information über die Datenbearbeitung[17] im Zeitpunkt der Beschaffung (Art. 60 Abs. 1 i.V.m. Art. 19 revDSG). Allerdings gilt diese Informationspflicht neuerdings nicht mehr nur für das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen,[18] sondern neu für das Beschaffen irgendwelcher Personendaten. Sie ist somit inhaltlich umfassender geworden, was das Strafbarkeitsrisiko massiv ausweitet. Es geht hier um die Pflicht zur korrekten und vollständigen Datenschutzerklärung – also eine Pflicht mit Aussenwirkung, deren Befolgung von kritischen oder missliebigen Zeitgenossen auch entsprechend leicht geprüft werden kann. Hier ist daher mit Bussen zu rechnen.

Abgesehen von der Höhe der Maximalbusse unverändert bleibt die Strafbarkeit der Abgabe einer vorsätzlich falschen oder unvollständigen Information bzw. das gänzliche Unterlassen einer solchen, wenn die betroffene Person ihr Auskunftsrecht geltend macht (Art. 60 Abs. 1 Bst. a i.V.m. Art. 25–27 revDSG).[19] Auskunftserteilende sollten sich deshalb nicht zur Abgabe einer Vollständigkeitserklärung hinreissen lassen; es gibt keine Pflicht hierzu. Auch die ungerechtfertigte Verweigerung einer Auskunft bleibt straffrei. Das ist mit ein Grund, warum es schon bisher kaum Bussen gab.

2.3 Mangelhafte Kooperation mit dem EDÖB (bisher)

Ebenfalls gleich bleibt, dass das Erteilen falscher Auskünfte oder die Verweigerung der Mitwirkung im Rahmen einer Untersuchung des EDÖB strafbar sind.[20] Auch hier zeigt die Praxis: Bussen gibt es so gut wie keine – normalerweise wird mit dem EDÖB kooperiert.

2.4 Verletzung der Informationspflicht über automatisierte Einzelentscheide (neu)

Neu hinzugekommen ist im revidierten DSG die Pflicht des Datenbearbeiters, die betroffene Person bei einem abschlägigen Entscheid, der mit einer erheblichen Beeinträchtigung der betroffenen Person verbunden ist, über die Tatsache zu informieren, dass der Entscheid ausschliesslich automatisiert erfolgt ist. Die Mitteilung muss zudem auf das Recht auf «menschliches Gehör» (Überprüfung der Entscheidung durch einen Menschen) hinweisen. Wird eine dieser Informationen vorsätzlich falsch, unvollständig oder gar nicht erteilt, droht eine Busse (Art. 60 Abs. 1 Bst. a i.V.m. Art. 21 revDSG). Hingegen ist die Nichtgewährung des menschlichen Gehörs nicht

15 Verstösse gegen die Bearbeitungsgrundsätze (Art. 6 und 8 revDSG) können aber auf dem Zivilweg geltend gemacht werden (Art. 32 Abs. 2 i.V.m. Art. 30 Abs. 1 und 2 Bst. a revDSG i.V.m. Art. 28 ff. ZGB [SR 210]).

16 Vgl. Art. 83 DSGVO.

17 Der Mindestinhalt der Information ergibt sich aus Art. 19 Abs. 2 revDSG (bzw. Art. 14 Abs. 2 DSG).

18 Vgl. Art. 34 Abs. 1 i.V.m. Art. 14 DSG.

19 Vgl. Art. 34 Abs. 1 i.V.m. Art. 8–10 DSG.

20 Vgl. Art. 60 Abs. 2 i.V.m. Art. 49 Abs. 3 revDSG; Art. 34 Abs. 2 Bst. b i.V.m. Art. 29 DSG.

strafbar, da der Tatbestand von Art. 60 revDSG nur von einer falschen «Information» bzw. «Auskunft» spricht. Die bisherigen Erfahrungen der DSGVO zeigen: Relevante Fälle gibt es in diesem Bereich in der Praxis kaum. Mit Bussen ist hier kaum zu rechnen.

2.5 Nichtbefolgen einer Verfügung des EDÖB (neu)

Neu ist auch, dass die Strafbehörden eine Busse aussprechen können bei fehlendem Folgeleisten einer Verfügung des EDÖB oder eines Entscheids der Rechtsmittelinstanzen, sofern diese unter Bussenandrohung gemäss Art. 63 revDSG ergangen sind. Diese Norm zielt auf die Durchsetzung von Verfügungen nach Art. 51 revDSG ab, also den vom EDÖB *nach* erfolgter Untersuchung angeordneten Massnahmen. Die Bussendrohung nach Art. 60 revDSG hingegen will die Erteilung von Auskünften und die Mitwirkung sicherstellen, die der EDÖB *im Rahmen einer Untersuchung* verlangt hat.

2.6 Verletzung der Datensicherheit und Exportrestriktionen (neu)

Die Verletzung der Bearbeitungsgrundsätze und weiterer Regeln der Datenbearbeitung an sich – also was, wie, wozu und wie lange bearbeitet werden darf – bleibt für sich selbst weiterhin straffrei, was viele Verantwortliche erleichtern dürfte. Eine Ausnahme stellt einzig die Verletzung der Datensicherheit und die Verletzung der Vorgaben im Rahmen einer Bekanntgabe von Daten in Länder ohne angemessenen gesetzlichen Datenschutz dar. Bisher blieb straflos, wer sich gar nicht um diesen Schutz kümmerte; bestraft wurde nur, wer sich zwar um einen Schutz in Form eines Vertrags kümmerte, diesen Vertrag dem EDÖB aber nicht meldete.[21] Neu macht sich strafbar, wer vorsätzlich Daten in ein Land ohne angemessenen Datenschutz exportiert und weder eine hinreichende Datenschutzgarantie vorweisen noch sich auf eine Ausnahme gemäss Art. 17 revDSG stützen kann.[22] Die bisherige Meldepflicht wird hingegen abgeschafft.

Angesichts der Tatsache, dass die Einhaltung des Datenschutzes bei Datenexporten in der Schweizer Datenschutz-Compliance aufgrund mangelnder Konsequenzen im Fall einer Verletzung bisher im Allgemeinen vergleichsweise stiefmütterlich behandelt wurde, wird die neue Strafnorm für viele Unternehmen ein Weckruf sein – sofern sie sich nicht bereits durch die Diskussionen rund um das EuGH-Urteil zu «Schrems II»[23] mit dem Thema auseinandergesetzt haben.[24] Der Wortlaut von Art. 16 Abs. 2 revDSG birgt da durchaus Risiken, denn der Abschluss anerkannter Standardvertragsklauseln genügt nicht zwangsläufig, sondern nur, falls diese einen «geeigneten» Datenschutz auch tatsächlich gewährleisten. Hier wird sich 2021 zeigen, wie hoch die Messlatte nach «Schrems II» wirklich liegt – und damit auch das neue Strafbarkeitsrisiko. Damit haben Datenexporteure in der Schweiz im Gegensatz zur DSGVO noch eine Schonfrist bis voraussichtlich Mitte 2022, wenn das neue DSG in Kraft treten soll.

Noch unklar ist, welche Verletzungen im Rahmen der Datensicherheit sanktioniert werden können.[25] Die Bestimmung verweist auf eine Verletzung der Mindestanforderungen des Bundesrates, doch liegen Letztere derzeit noch nicht vor. Es ist zu befürchten, dass diese ähnlich generisch ausfallen werden, wie in der bisherigen Verordnung zum DSG,[26] womit kaum etwas gewonnen wäre: Es könnte jeden treffen, dessen Massnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten nicht überall dem Stand der Technik entsprechen – was eine Vielzahl von Unternehmen sein wird. Hierbei handelt es sich um ein abstraktes Gefährdungsdelikt; zu einem «Data Breach» muss es nicht gekommen sein. Umgekehrt impliziert ein solcher auch nicht eine Strafbarkeit, da ein Data Breach auch bei angemessener Datensicherheit vorkommen kann. Trotzdem ist bereits heute absehbar, dass die IT-Sicherheitsanbieter die Sanktionierung in ihren Verkaufsbemühungen ausschlachten werden. Kaum ein Geschäftsführer wird es wagen, das für eine angemessene Datensicherheit angeblich erforderliche Budget nicht zu genehmigen, setzt er sich doch sonst einem Strafbarkeitsrisiko aus. Demgegenüber ist aus gut informierten Quellen in Bundesbern zu vernehmen, dass die Strafnorm letztlich nur die krassen Fälle erfassen soll. Eine solche Einschränkung ergibt sich allerdings

21 Art. 6 Abs. 3 DSG.
22 Vgl. Art. 61 Bst. a revDSG.
23 Entscheid des EuGH vom 16. Juli 2020, C-311/18 (Facebook Ireland und Schrems).
24 *<https://www.vischer.com/know-how/blog/schrems-ii-waser-fuer-unternehmen-in-der-schweiz-bedeutet-38295/>* (Stand 10. Januar 2021).
25 Art. 61 Bst. c i.V.m. Art. 8 Abs. 3 revDSG.
26 Art. 8 VDSG.

aus dem Wortlaut der Norm nicht, und wie dies auf dem Weg der Verordnung erreicht werden soll, ist noch unklar.

2.7 Mangelhafte Bestellung des Auftragsbearbeiters (neu)

Teils überlappend dazu ist die ebenfalls neu eingeführte Strafbarkeit des Verantwortlichen, der sich nicht an die Vorgaben zur Bestellung eines Auftragsbearbeiters nach Art. 9 Abs. 1 und 2 revDSG hält.[27] Die Verletzung von Abs. 3 – die Pflicht des Auftragsbearbeiters, sich neue Unterauftragsbearbeiter vom Verantwortlichen absegnen zu lassen – wird hingegen nicht sanktioniert. Für die Verletzung von Abs. 1 und 2 kann aufgrund des Wortlauts zudem nur der Verantwortliche bestraft werden, nicht der Auftragsbearbeiter. Das muss auch für die Weitervergabe durch den Auftragsbearbeiter gelten; strafbegründende Normen sind eng auszulegen. Den Verantwortlichen wird dementsprechend zugutekommen, dass die Vorgaben von Art. 9 revDSG (im Vergleich zur Parallelregelung von Art. 28 DSGVO) weiterhin sehr offen und unscharf formuliert sind.

2.8 Verletzung der beruflichen Schweigepflicht (bisher, ausgeweitet)

Eine Veränderung im Vergleich zum bisherigen DSG erfährt zuletzt auch das «kleine Berufsgeheimnis» (Art. 62 revDSG), dessen Geltungsbereich ausgebaut wurde (vgl. Ziff. III).

2.9 Unbefugte Datenbeschaffung (bisher)

Veränderungen bringt das Inkrafttreten des neuen DSG auch für das StGB. Bei Art. 179^{novies} StGB (unbefugtes Beschaffen von Personendaten) wurde die Tatbestandsvariante einer unbefugten Beschaffung von Persönlichkeitsprofilen gestrichen, da es diesen Begriff im DSG offiziell nicht mehr gibt; die Bestimmung stellt die unbefugte Beschaffung von besonders schützenswerten Personendaten, die nicht jedermann frei zugänglich sind, unter Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (Vergehen).[28] Anders als Art. 143 StGB (unbefugte Datenbeschaffung), verlangt Art. 179^{novies} StGB weder, dass die Daten elektronisch gespeichert sind, noch dass der Täter eine Bereicherungsabsicht hegt.[29] Damit fallen mehr Fälle von unbefugter Datenbeschaffung unter diesen Artikel. Unbefugt ist eine Beschaffung von Personendaten, wenn sie in einer Verletzung der Persönlichkeit der betroffenen Person resultiert[30] und sich nicht auf einen Rechtfertigungsgrund gemäss Art. 31 Abs. 1 revDSG stützen kann (Gesetz, Einwilligung oder überwiegendes Interesse). Da neu auch genetische Daten als besonders schützenswerte Personendaten gelten (Art. 5 Bst. c revDSG) und ebenso biometrische Daten, die eine natürliche Person eindeutig identifizieren, sind hier neue Tatvarianten denkbar, wie etwa der Fall, in welchem einer Person für die Zwecke einer heimlichen Genanalyse eine Haarwurzelprobe entwendet wird.

2.10 Identitätsmissbrauch (neu)

Neu ins StGB eingefügt wird die Bestrafung des Identitätsmissbrauchs (Art. 179^{decies} StGB), landläufig auch als «Identitätsdiebstahl» («identity theft») bekannt. Tatbestandsmässig handelt jedermann, der die Identität einer anderen Person ohne deren Einwilligung verwendet (d.h. deren Personendaten unbefugterweise bearbeitet), um dieser zu schaden oder um sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen.[31] Die Strafandrohung beträgt maximal ein Jahr Freiheitsstrafe oder Geldstrafe (Vergehen).

2.11 Prognose

Da die Geltendmachung des Auskunftsrechts erfahrungsgemäss das grösste Konfliktpotenzial in sich birgt, ist davon auszugehen, dass die meisten Straffälle unter dem revDSG das Auskunftsrecht betreffen werden. Zweitplatziert dürften wie bereits erwähnt die Fälle von Verletzungen der Informationspflichten (z.B. Konsumenten, die auf diese Weise gegen grössere Unternehmen vorzugehen versuchen) und Auslandstransfers in strittigen Verhältnissen (betreffend

27 Art. 61 Bst. b i.V.m. Art. 9 Abs. 1 und 2 revDSG.

28 Art. 179^{novies} revStGB i.V.m. Art. 10 Abs. 3 revStGB.

29 *Raffael Ramel/André Vogelsang,* in: Basler Kommentar, Strafgesetzbuch II, 4. Aufl., Basel 2018, Art. 179^{novies} StGB N 4.

30 Vgl. Art. 30 Abs. 2 revDSG.

31 Vgl. ausführlich *Yannick Reber,* Der neue Tatbestand des Identitätsmissbrauchs nach Art. 179^{decies} E-StGB, ex/ante 2/2020, S. 33 ff., Zürich 2020.

die Angemessenheit der getroffenen Massnahmen) sein.

3. Subjektiver Tatbestand

Sämtliche Verstösse gegen das revDSG, wie auch die beiden Strafbestimmungen im StGB, verlangen – anders als die DSGVO[32] –, dass die Verletzung zumindest mit Eventualvorsatz begangen wurde. In der Praxis ist dies teilweise schwierig von der bewussten Fahrlässigkeit abzugrenzen. Bezüglich des Wissens um das Risiko der Verwirklichung des Tatbestands unterscheiden sich die beiden Fälle nicht. Der Unterschied liegt im Willen: Der bewusst fahrlässige Verletzer vertraut auf den Nichteintritt der Verletzung («Es wird schon nichts passieren.»). Dem eventualvorsätzlich handelnden Verletzer hingegen ist der Eintritt der Verletzung gerade recht oder er steht diesem gleichgültig gegenüber («Mir doch egal.»).[33]

Diese Gleichgültigkeit wird gerade dort, wo ein abstraktes Gefährdungsdelikt zur Diskussion steht – wie dies teilweise in Art. 61 revDSG der Fall ist – öfters anzutreffen sein. Allerdings sind hier Einschränkungen nötig, um nicht gegen den Willen des Gesetzgebers in den Bereich der «Rechtsfahrlässigkeit» (also pflichtwidrige Verbotsunkenntnis) zu gelangen.[34] Denn wir bewegen uns hier nicht im Kernstrafrecht, wo es um die Verletzung elementarer Güter und Interessen geht. Bei aller Relevanz des Persönlichkeitsschutzes ist Letzteres bei den im DSG mit Strafe belegten Delikten nicht der Fall. Die Rechtswidrigkeit des Verhaltens und damit das Verursachen einer Verletzung ist je nach Tatbestand keineswegs offenkundig, sondern Bedarf der Fachkunde. In diesem Sinne kann Eventualvorsatz bei solchen Bestimmungen des DSG erst dann bestehen, wenn der Täter um das übertretene Gebot oder Verbot gewusst oder wenigstens geahnt hat und dass sein Verhalten möglicherweise dagegen verstossen würde, er aber trotzdem so gehandelt und daher einen allfälligen Rechtsverstoss bewusst mit in Kauf genommen hat.[35]

Wenn also ein in solchen Fragen unerfahrener Gewerbler eine Datenschutzerklärung verfasst, weil alle das so machen, er sich eine Vorlage von einer bekannten grossen Firma im Internet sucht und sie etwas auf seine Verhältnisse anpasst, handelt er nicht eventualvorsätzlich, falls in der Vorlage gewisse Pflichtangaben fehlen. Er geht davon aus, dass er das Richtige tut und die Vorlage der grossen Firma sicher den Anforderungen entsprechen wird. Tut dies ein Schweizer Anwalt, so wird er Mühe haben den Richter davon zu überzeugen, dass er nicht mindestens geahnt hat, dass das DSG die Anforderungen an eine Datenschutzerklärung definiert und er einfach nicht die Lust oder Zeit hatte, dieses zu konsultieren. Allerdings wird auch der Gewerbler mit dem Vorwurf eines mindestens eventualvorsätzlichen Handelns rechnen müssen, wenn er in seiner Datenschutzerklärung Datenbearbeitungen klar falsch darstellt oder unterschlägt, weil auch ihm klar sein muss, dass eine Datenschutzerklärung inhaltlich korrekt zu sein hat. Geht er aufgrund weitverbreiteter Praxis hingegen davon aus, dass eine Datenschutzerklärung auf der Website nur die Datenbearbeitung der Website selbst abdecken muss und es sonst keine braucht, wird ihm der (Straf-)Richter dies vermutlich nachsehen.

Mit dem Vorwurf der strafbaren Gleichgültigkeit muss auch der Mitarbeiter der Personalabteilung rechnen, der einem Arbeitnehmer auf dessen Wunsch hin sein Personaldossier in Kopie zur Verfügung stellt und dabei den Eindruck erweckt, es sei vollständig, obwohl er damit rechnen muss, dass gewisse Akten daraus noch beim Kollegen auf dem Tisch liegen. Die Auskunft ist in diesem Fall unvollständig erteilt und der HR-Mitarbeiter muss davon ausgehen, dass dies die Rechte des Arbeitnehmers verletzt. Macht er einen Vorbehalt bezüglich der Vollständigkeit, wird es bereits am objektiven Tatbestand fehlen. Hat der HR-Mitarbeiter intern auf seine Rückfrage hin die falsche Auskunft erhalten, das Dossier sei vollständig, dann wird kein Eventualvorsatz vorliegen. Diesen hat möglicherweise derjenige, der intern bewusst die falsche Auskunft erteilt, wenn er weiss, dass ihm die Frage nach der Vollständigkeit des Dossiers aufgrund eines Auskunftsersuchens gestellt worden ist. Allerdings stellt sich die Frage, ob die Verweigerung einer

[32] Dort wird auch die Fahrlässigkeit geahndet, aber bei der Festlegung der Höhe einer allfälligen Busse berücksichtigt (Art. 83 Abs. 2 Bst. b DSGVO).

[33] *Marcel Alexander Niggli/Stefan Maeder,* in: Basler Kommentar, Strafgesetzbuch I, 4. Aufl., Basel 2018, Art. 12 StGB N 58.

[34] Vgl. dazu *Marc Thommen,* Art. 333 Abs. 7 StGB – Grenzenlose Fahrlässigkeit im Nebenstrafrecht?, recht 2013, S. 283.

[35] So schon BGE 60 I 412 («Darmhandels-Fall»).

Vollständigkeitserklärung tatbestandsmässig überhaupt erfasst werden kann (dazu sogleich).

4. Adressat der Strafbestimmungen

Wie beschrieben (vgl. Ziff. I), kann in der Schweiz in der Regel nur die für die Verletzung verantwortliche natürliche Person sanktioniert werden. Der Gehilfe wird nicht bestraft, da es sich bei den revDSG-Verstössen lediglich um Übertretungen handelt.[36] Die Verantwortlichkeit ergibt sich aus einer gesetzlichen Verpflichtung, die Einhaltung des revDSG im Unternehmen sicherzustellen (z.B. als Leitungsperson)[37] oder aus der Tatsache, dass die Person den relevanten Vorgang leitet, wobei es sich bei der Person nicht um ein Organ handeln muss.[38] Dies trifft zum Beispiel auf einen Mitarbeiter zu, der als betrieblicher Datenschutzbeauftragter eingesetzt wurde oder auf den externen Rechtsberater, der faktisch über den Inhalt der Datenschutzerklärung entscheidet. Damit handelt es sich bei den Strafbestimmungen im revDSG zwar nicht um Sonderdelikte, aber der Anwendungsbereich ist trotz allem eingeschränkt. Nicht jeder, der etwas zu einer Verletzung beiträgt, unterliegt einem Strafbarkeitsrisiko: Wer vergisst, dem Verfasser der betrieblichen Datenschutzerklärung eine bestimmte Datenbearbeitung mitzuteilen oder dazu schlicht keine Lust hatte und sie somit vorschriftswidrig nicht in der Datenschutzerklärung auftaucht, ist nicht strafbar. Eine solche Person leitete den Vorgang nicht, auch wenn sie eventualvorsätzlich handelt, und die Gehilfenschaft kann im DSG ohnehin nicht bestraft werden. Weiss der Verfasser der Datenschutzerklärung oder die Unternehmensleitung um die Unzuverlässigkeit der betreffenden Person im Betrieb, kann dies ihren Eventualvorsatz begründen. Umgekehrt wird der Rechtsberater beim Verfassen einer unvollständigen Datenschutzerklärung grundsätzlich kein Strafbarkeitsrisiko eingehen, wenn er seinen Klienten bittet, die Erklärung vor ihrer Verwendung auf Vollständigkeit und Richtigkeit der darin getroffenen tatsächlichen Aussagen über die Datenbearbeitungen zu prüfen. Tut die für die Verabschiedung zuständige Person das nicht, weil sie sich dafür keine Zeit nehmen will, setzt *sie* – und nicht der Rechtsberater – sich dem Risiko der Strafbarkeit aus. Selbst wenn der Rechtsberater darum weiss, kann er als Gehilfe nicht belangt werden, und solange nicht *er* den Freigabeentscheid trifft, was beim externen Rechtsberater regelmässig nicht der Fall sein wird, kann er auch nicht als Leitungsperson gelten.

Obwohl die Botschaft die in der Vernehmlassung geäusserte Besorgnis, dass die Strafen jeden beliebigen Angestellten treffen können, zu zerstreuen versucht,[39] wird die Strafbarkeit wohl in erste Linie nicht die Unternehmensleitung treffen, sondern diejenigen, die in ausführender Position faktisch entscheiden, was konkret gemacht wird. Erstere kümmert sich in der Regel nicht um die Einzelheiten der Informationspflicht oder einer Auskunftserteilung, sondern wird die «gesetzeskonforme» Erfüllung dieser Pflichten nach unten delegieren.

Auch die Regelung in Art. 64 Abs. 2 revDSG, wonach bei Bussen bis CHF 50 000, statt der natürlichen Person, der Geschäftsbetrieb gebüsst werden kann, dürfte der natürlichen Person selten Entlastung bringen (auch wenn die Bussen die Grenze von CHF 50 000 normalerweise nicht überschreiten werden), denn die Regelung setzt voraus, dass sich die verantwortliche Person nur mit unverhältnismässigem Aufwand ermitteln lässt. Das wird bei den bussenbewehrten revDSG-Delikten aber lediglich vereinzelt der Fall sein, da in der Regel organisatorisch klar bestimmt oder im konkreten Fall leicht zu ermitteln sein wird, wer z.B. ein Auskunftsersuchen beantwortet oder die Datenschutzerklärung freigegeben hat. Wer sein Strafbarkeitsrisiko reduzieren will, überlässt heikle Entscheidungen seinen Vorgesetzten bzw. seinen Klienten. Denn Handeln trotz Zweifeln an der Zulässigkeit kann vom Richter bereits als eventualvorsätzliche Regelverletzung gewertet werden.

5. Verfahrensfragen

Anders als unter der DSGVO werden die meisten Strafbestimmungen des revDSG (und des StGB) nur auf Antrag bestraft. Strafantragsberechtigt ist die betroffene Person, deren relevante Rechte[40] ihr nicht vollumfänglich gewährt werden. Die Antragsfrist be-

36 Art. 333 Abs. 3 i.V.m. Art. 105 Abs. 2 StGB.

37 BGE 142 IV 315, E. 2 ff.; Art. 29 StGB; Art. 6 Bundesgesetz über das Verwaltungsstrafrecht (VStrR; SR 313.0).

38 Art. 29 Bst. d StGB; Art. 6 Abs. 1 VStrR.

39 BBl 2017 7099.

40 Vgl. Ziff. II.2.b (z.B. Informationsrecht, Auskunftsrecht, Recht auf sicheren Transfer der eigenen Personendaten an Dritte).

trägt drei Monate ab Kenntnis des Täters.[41] Da den betroffenen Personen in der Regel nicht bekannt sein wird, wer im Unternehmen für den Inhalt der betreffenden Information oder der Auskunft verantwortlich ist,[42] wird die Einhaltung der Frist einem Strafantrag erwartungsgemäss nicht im Weg stehen. Der EDÖB hat kein Strafantragsrecht. Er ist lediglich berechtigt, Anzeige zu erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrzunehmen (Art. 65 Abs. 2 revDSG).[43] Daher kann bereits heute davon ausgegangen werden, dass Bussen gestützt auf die Strafbestimmungen von Art. 60 f. revDSG in der Schweiz die Ausnahme sein werden.

Das heisst aber nicht, dass die Strafbestimmungen wirkungslos sein werden. Die Vermeidung einer Busse bzw. einer strafrechtlichen Verfolgung wird in den Unternehmen – insbesondere bei Personen, die die heiklen Entscheidungen nicht weiter abwälzen können – für genügend «Motivation» sorgen den Datenschutz einzuhalten.

Für die Durchsetzung der Strafbestimmungen sind die kantonalen Strafverfolgungsbehörden zuständig (Art. 65 Abs. 1 revDSG), wobei die Verfolgungsverjährungsfrist fünf Jahre beträgt (Art. 66 revDSG). Anders als die Bussen verhängenden Datenschutzaufsichtsbehörden unter der DSGVO verfügen sie in der Regel über keine oder nur geringe Erfahrung mit datenschutzrechtlichen Fragen. Sämtliche Bussen nach dem revDSG sowie die relevanten Vergehen nach StGB können, bei Vorliegen der weiteren Voraussetzungen,[44] im Strafbefehlsverfahren oder im vereinfachten Verfahren erledigt werden. In allen anderen Fällen kommt das ordentliche Verfahren zur Anwendung. Damit stehen der verurteilten verantwortlichen Person die üblichen Rechtsmittel gemäss der Strafprozessordnung offen. Da es sich bei den revDSG-Verstössen lediglich um Übertretungen handelt, können im Berufungsverfahren keine neuen Behauptungen und Beweise mehr vorgebracht werden und die Rügegründe sind beschränkt. [45] Einen Eintrag ins Strafregister gibt es ab einer Busse über CHF 5000.[46] Der Eintrag erscheint jedoch nicht auf dem Privatauszug, den sich die verurteilte verantwortliche Person bestellen kann (z.B. um ihn einer Stellenbewerbung beizulegen).[47] Einsicht in das vollständige Vorstrafenregister können nur bestimmte Behörden[48] nehmen. Der Eintrag wird nach zehn Jahren von Amtes wegen entfernt.[49]

III. Sonderthema: Verletzung der beruflichen Schweigepflicht

1. Vorbemerkung

Das «kleine Berufsgeheimnis» oder das «Berufsgeheimnis für jedermann» in Art. 62 revDSG ist eine auf den ersten Blick unscheinbare, jedoch bedeutsame Neuerung. Das bisherige DSG kannte nur eine sehr begrenzte berufliche «Schweigepflicht», die in der Praxis deswegen eine untergeordnete Rolle spielte (vgl. Ziff. II.1.1). Terminologisch orientiert sich Art. 62 revDSG am «grossen» Berufsgeheimnis in Art. 321 StGB (z.B. für Arzt, Anwalt, Priester etc.) und am Bankgeheimnis (Art. 47 BankG). Die Verletzung von Art. 62 revDSG kann – wiederum auf Antrag – in einer Busse bis CHF 250 000 resultieren. Im internationalen Vergleich handelt es sich angesichts des weiten Anwendungsbereichs und Bussenrahmens um eine ungewöhnlich scharfe Regelung, die im Parlament interessanterweise diskussionslos blieb.

2. Objektiver Tatbestand

Vom Tatbestand erfasst ist auf den ersten Blick jede Bekanntgabe von geheimen Personendaten, die der Berufstätige in Ausübung seines Berufes zur Kenntnis genommen hat und die er zur Berufsausübung benötigt, an eine dazu unberufene Person («offenbaren»). Auch Hilfspersonen und Auszubildende können Täter sein.[50] Auf den zweiten Blick wird klar, dass der Wortlaut der Bestimmung entscheidende Fragen unbeantwortet lässt.

41 Art. 31 StGB.

42 Die Kontaktperson im Unternehmen muss nicht zwingend die für die Verletzung verantwortliche natürliche Person sein.

43 Er kann also Einstellungsverfügungen anfechten und Rechtsmittel gegen kantonale Urteile ergreifen. Gegen Strafbefehle und das Strafmass soll er hingegen kein Rechtsmittel ergreifen können (BBl 2017 7104).

44 Art. 352 Abs. 1 und Art. 358 ff. StPO (SR 312.0).

45 Art. 398 Abs. 4 StPO i.V.m. Art. 103 StGB.

46 Art. 3 Abs. 1 Bst. c Ziff. 1 Verordnung über das Strafregister (SR 331).

47 Art. 371 Abs. 1 StGB.

48 Art. 367 Abs. 2 ff. StGB.

49 Art. 369 Abs. 3 StGB.

50 Art. 62 Abs. 2 revDSG.

Was «geheime» Personendaten sind, definiert die Norm nicht. Hier ist davon auszugehen, dass derselbe Geheimnisbegriff zur Anwendung gelangt wie auch sonst im Schweizer Recht (etwa in Art. 320 ff. StGB). Geheimnisse sind demnach Informationen, die nicht allgemein bekannt sind, an denen der Geheimnisherr ein erkennbares, schutzwürdiges Geheimhaltungsinteresse hat und die er geheim halten will. Schwieriger zu beantworten ist die Frage, wer Geheimnisherr ist und wann eine Bekanntgabe von geheimen Personendaten nicht erlaubt ist, d.h. wen die Norm schützt und inwiefern eine Pflicht zur Geheimhaltung besteht.

Wer der von Art. 62 revDSG geschützte Geheimnisherr ist, ergibt sich ebenfalls weder aus dem Wortlaut noch aus der Botschaft. Die Antwort auf diese Frage liefert die Bestimmung der Rechtsnatur bzw. des Zwecks der Norm, nämlich ob es sich bei Art. 62 revDSG um eine datenschutzrechtliche Norm oder um eine Berufsgeheimnisnorm handelt. Die Bestimmung der Rechtsnatur beantwortet zugleich die Frage nach der Pflicht zur Geheimhaltung und woraus sich diese ergibt.

Würde Art. 62 revDSG als rein datenschutzrechtliche Norm betrachtet, müsste sich die Zulässigkeit einer Bekanntgabe geheimer Daten konsequenterweise aus den Grundsätzen des revDSG ergeben; getan werden darf nur, aber immerhin, was das DSG erlaubt.[51] Will ein Verantwortlicher eine Bekanntgabe mit Hilfe einer Einwilligung rechtfertigen, müsste er von jeder betroffenen Person eine Einwilligung einholen, gleichgültig, ob er mit dieser Person etwas zu tun hat oder nicht und wie er zu ihr steht. Gäbe z.B. ein Versicherter seiner Versicherung im Rahmen einer Schadensmeldung geheime Daten eines Geschädigten an, welche diese einem Schadensexperten weitergibt, so ist diese Weitergabe für den Geschädigten möglicherweise nicht erkennbar und möglicherweise auch nicht gerechtfertigt, weil der Schadensexperte diese Information nicht zu haben braucht. Um Tatbestandsmässigkeit zu vermeiden, müsste die Versicherung die Zustimmung auch des Geschädigten einholen, obwohl die Versicherung mit ihm möglicherweise (noch) keinen Kontakt hat.[52]

Wird Art. 62 revDSG hingegen aufgrund seiner vom Gesetzgeber gesuchten Nähe zu Art. 321 StGB als Berufsgeheimnis betrachtet, so engt sich der Schutzbereich ein: Geheimnisherr muss nur aber immerhin derjenige sein, der dem Berufstätigen sein Geheimnis zur Durchführung dessen Berufs anvertraut hat. Dies begründet zugleich die Basis der Schweigepflicht. Mit anderen Worten: Es wird das Vertrauen des Kunden in die Vertraulichkeit der Mitteilung an den Berufstätigen geschützt und daher ist auch nur der Bruch *dieses* Vertrauens strafbewehrt (statt jede Datenschutzverletzung). Im Beispiel gibt es dieses Vertrauen nur zwischen Versicherungsnehmer und Versicherung, nicht auch zwischen ihr und dem Geschädigten – jedenfalls solange der Geschädigte nicht direkt mit der Versicherung in Kontakt tritt und ihr Geheimnisse anvertraut. Dieses Beispiel zeigt bereits: Der Begriff des «Kunden» darf nicht eng verstanden werden; letztlich geht es um den Schutz desjenigen, der einem Berufstätigen in und für dessen Funktion etwas anvertraut. Wer sich also als Mitarbeiter einer innerbetrieblichen psychologischen Beratungsstelle anvertraut, sollte in diesem Vertrauen geschützt werden, obwohl er mit der betreffenden Person keinen Vertrag geschlossen hat (sondern ein solcher nur zwischen dem Arbeitgeber und der beauftragten Beratungsstelle besteht). Die Schweigepflicht entspringt also nicht wie beim Arzt, Anwalt oder Banker dem Behandlungs-, Mandats- oder Bankkundenverhältnis, sondern dem einem Berufstätigen entgegengebrachten Vertrauen darauf, dass er das ihm zwecks seiner Berufsausübung anvertraute Geheimnis als solches bewahrt – selbst wenn er mit ihm kein Vertragsverhältnis hat.

Dieses Verständnis von Art. 62 revDSG als «kleines» Berufsgeheimnis geht zwar nicht so weit wie wenn die Norm als datenschutzrechtliche Bestimmung ausgelegt würde, ist damit aber noch immer ausserordentlich breit und vage – so vage, dass durchaus angezweifelt werden kann, ob sie den Bestimmtheitsanforderungen von Art. 1 StGB genügt. Denn was es dazu braucht, damit ein solches straf-

[51] Art. 30 i.V.m. Art. 31 Abs. 1 revDSG: Bekanntgabe an Dritte aufgrund von Gesetz, Einwilligung oder überwiegenden Interessen.

[52] Die Versicherung wäre darauf angewiesen, dass ihr Versicherungsnehmer die erforderliche Einwilligung einholt, was allerdings unrealistisch ist. Durch eine solche Klausel in den AVB wäre eine vertragliche Überbindung dieser Pflicht zwar möglich, aber aus strafrechtlicher Sicht bleibt entscheidend, ob die seitens des Versicherers verantwortliche Person davon ausgehen konnte und ausging, dass der Versicherungsnehmer dieser Pflicht tatsächlich nachkommt.

rechtlich geschütztes Vertrauen auf Geheimhaltung vorliegt, ist bisher nicht wirklich geklärt, obwohl es die Norm – wenn auch in einer viel enger gefassten Vorläuferfassung – schon seit Jahren gibt.[53] Dass nicht jede einem Berufstätigen mitgeteilte, nicht allgemein bekannte Tatsache diesen Schutz verdient, ist klar. Auch der Geheimhaltungswille und das Geheimhaltungsinteresse können nicht entscheidend sein, denn sonst könnte der Geheimnisherr einseitig entscheiden, wer einer Schweigepflicht untersteht. Erforderlich sein muss zusätzlich, dass *erstens* aufgrund der Funktion oder Stellung des Geheimnisträgers oder aufgrund eines dem Geheimnisträger zurechenbaren Verhaltens beim Geheimnisherrn der Eindruck erweckt wurde,[54] dass sein Geheimniswille respektiert wird (Kriterium der «berechtigten Erwartung») und *zweitens* das Geheimnis dem Geheimnisträger bzw. seiner Organisation in diesem Rahmen bekanntgegeben worden ist. Das ist mit «Anvertrauen» gemeint. Erforderlich ist mit anderen Worten eine mindestens stillschweigende Vertraulichkeitsabrede, auch wenn der Wortlaut von Art. 62 revDSG, anders als etwa Art. 162 StGB, keine solche Abrede voraussetzt. Sie ist aber erforderlich, um der Norm – auch im Hinblick auf Art. 1 StGB – ein Mindestmass an Kontur zu geben.

Für Arbeitnehmer bedeutet dies wiederum, dass sie künftig auch ohne Sondereigenschaft wie jener eines Beamten, Anwalts, Arztes oder Bankers einer Schweigepflicht unterliegen können, die über die arbeitsvertragliche Geheimhaltungspflicht von Geschäfts- und Fabrikationsgeheimnissen (Art. 321*a* Abs. 4 OR[55]) hinausgeht und insofern auch anders gelagert ist, als dass als Geheimnisherr nicht mehr nur der Arbeitgeber und auch nicht mehr nur *Geschäfts*geheimnisse geschützt sind.

Wird Art. 62 revDSG in diesem Sinne als Berufsgeheimnis verstanden, braucht es zur Aufhebung der Schweigepflicht nur – aber immerhin – die Einwilligung des so verstandenen «Kunden» (im genannten Beispiel also des Arbeitnehmers). Das gilt natürlich nur dort, wo sich eine Berechtigung zur Bekanntgabe oder Notwendigkeit zur Aufhebung der Schweigepflicht (bzw. zur Datenweitergabe) nicht bereits aus der Funktion bzw. aus der Vereinbarung ergibt, in deren Rahmen der Berufstätige aktiv ist (vgl. dazu die Praxishinweise in Ziff. III.4 nachfolgend). Auch in diesem Punkt verweist die Botschaft auf Art. 321 StGB.[56]

Die Norm bietet trotz diesem engen Verständnis einiges an Konfliktpotenzial. Wie verhält es sich etwa mit dem Mitarbeiter der Personalabteilung, dem ein Angestellter des Unternehmens von einem innerbetrieblichen Übergriff berichtet, von ihm aber verlangt, dass er seine Identität unter allen Umständen geheim hält. Greift Art. 62 revDSG, so kann sich der Mitarbeiter der Personalabteilung strafbar machen, wenn er dieses Vertrauen verletzt und den Melder intern bekanntgibt. Umgekehrt wird sich das Unternehmen das Wissen gewisser Mitarbeiter anrechnen lassen müssen. Das Unternehmen wird daher zum einen gut beraten sein, die Vertraulichkeit solcher Meldungen vorab für alle erkennbar zu regeln oder auf deren Nichtbestehen vorgängig hinzuweisen. Der Mitarbeiter der Personalabteilung sollte sich zum anderen hüten, Vertraulichkeitszusagen abzugeben, die er möglicherweise nicht einhalten kann.[57]

Umgekehrt stellt sich die Frage, ob eine datenschutzrechtlich zulässige Bekanntgabe von Personendaten trotzdem eine Verletzung von Art. 62 revDSG darstellen kann. Sie kann es nach der hier vertretenen Auffassung im Prinzip; aber praktisch sind kaum Fälle denkbar, in welchen die Rechtfertigungsgründe des revDSG das berechtigte Vertrauen des Geheimnisherrn in die Wahrung seines Geheimnisses nicht schützen würden. Würde Art. 62 revDSG hingegen nicht als Berufsgeheimnis verstanden, könnte dies umgekehrt zu einer strafrechtlichen Sanktionierung einer datenschutzrechtlich verpönten (d.h. eine gegen die Bearbeitungsprinzipien verstossende, nicht gerechtfertigte) Bekanntgabe von Personendaten führen. Das Geheimhaltungsinteresse müsste konsequenterweise danach ausgerichtet werden, was die Bearbeitungsgrundsätze vorsehen. Die tatbestandsmässige Offenbarung läge vor, sobald eine Bekanntgabe von Personendaten die Bearbeitungsgrundsätze

53 Art. 35 DSG.

54 Die Zurechenbarkeit muss genügen, dass in arbeitsteiligen Betrieben der Geheimnisherr sein Geheimnis der einen Person anvertraut, aber davon ausgeht, dass auch die anderen Mitarbeiter dieses Geheimnis schützen werden.

55 SR 220.

56 BBl 2017 7102, wonach die für Art. 321 Ziff. 2 StGB entwickelten Grundsätze sinngemäss gelten sollen.

57 Vgl. die angelsächsisch geprägte Praxis von Rechtsvertretern in internen Untersuchungen, die Mitarbeiter eines Unternehmens darauf hinzuweisen, dass sie dem Unternehmen, nicht dem Mitarbeiter gegenüber verpflichtet sind («corporate miranda warnings»).

oder weiteren Bestimmungen von Art. 30 Abs. 2 revDSG ungerechtfertigterweise verletzen würde. Das würde wiederum zur Kriminalisierung von heute alltäglichen, aber harmlosen Datenschutzverletzungen auch innerhalb der Betriebe führen. Würde ein Mitarbeiter seinem Büronachbarn in der Mittagspause beispielsweise von seinem neusten, von ihm zu bearbeitenden Fall erzählen, würde er damit den Grundsatz der Verhältnismässigkeit verletzen, weil eine solche Bekanntgabe von Personendaten für die Berufsausübung des zuhörenden Kollegen streng genommen nicht erforderlich wäre. Gerechtfertigt wäre dies womöglich auch nicht. Weil er vorsätzlich gehandelt hätte, könnte argumentiert werden, dass dies eine strafbare unbefugte (weil datenschutzwidrige) Bekanntgabe gewesen sei. Das kann nicht sein. Es können beim «kleinen» Berufsgeheimnis keine strengeren Regeln gelten als sie es heute etwa für das Bank- oder Anwaltsgeheimnis tun, wo das Geheimnis – Ausnahmefälle vorbehalten – nur gegenüber externen Dritten zu wahren ist.

3. Subjektiver Tatbestand

Der subjektive Tatbestand verlangt das Wissen um die Geheimnispflicht, das Bewusstsein bezüglich des Geheimnischarakters, willentliches Offenbaren und Inkaufnahme der Kenntnis durch Dritte. Es genügt wiederum Eventualvorsatz. Nicht erfasst ist das versehentliche Ausplaudern von berufsgeheimnisgeschützten Daten, sondern nur die Bekanntgabe an dazu unberufene Personen, die absichtlich («Der soll das ruhig wissen.») oder gleichgültig («Schon OK, wenn der das weiss.») erfolgt. In der Praxis dürften vor allem die ersten beiden Anforderungen, also das Wissen um eine Geheimnispflicht und das Bewusstsein bezüglich des Geheimnischarakters, eine Strafbarkeit verhindern, jedenfalls soweit ein Unternehmen seine Mitarbeiter nicht entsprechend in die Geheimhaltung von Personendaten unterwiesen hat.

4. Möglichkeiten zur Handhabung in der Praxis

Auch, wenn Art. 62 revDSG «nur» als Berufsgeheimnis verstanden wird, stellt sich die Frage, wie in der Praxis mit der Norm umzugehen ist. Nach dem Gesagten kann nur die Weitergabe von geheimen Daten, d.h. Daten, die der Kunde dem Dienstleister in der berechtigten Erwartung mitgeteilt hat, dass dieser sie vertraulich behandelt, tatbestandsmässig sein.

Dienstleister können diese Erwartungshaltung steuern, indem sie z.B. in ihrer Datenschutzerklärung darauf hinweisen, mit welchen Kategorien von Dritten sie diese Daten teilen. Hat der Dienstleister den Kunden vor dessen Mitteilung geheimer Daten auf deren Weitergabe genügend klar hingewiesen, wird der Kunde normalerweise nicht mehr von einer Schweigepflicht ausgehen können und der Schutz nach Art. 62 revDSG fällt dahin. Der Vorteil dieser Lösung ist, dass keine Willenserklärung des Geheimnisherrn im Sinne eines Waivers erforderlich ist; die Datenschutzerklärung muss nicht einmal Teil der vertraglichen Abrede sein. Die Herausforderung der Praxis wird es aber sein, zu bestimmen, wann «genügend klar» informiert worden ist, denn die Anforderungen von Art. 19 revDSG an den Detailgrad einer Datenschutzerklärung (betreffend die Weitergabe von Personendaten) sind sehr tief. Es ist nicht einmal erforderlich anzugeben, welche Daten den zu nennenden Kategorien von Empfängern mitgeteilt werden.

Das Einholen einer Einwilligung des Kunden in die Bekanntgabe seiner geheimen Personendaten (z.B. in den AGB) ist zweifellos die sicherste Lösung, um Art. 62 revDSG einzuhalten. Dieser Lösungsansatz ist aber insofern nicht praktikabel, da häufig nicht von vornherein klar sein wird, welche Daten von der Norm überhaupt erfasst sind: Ist es neuerdings ein strafrechtlich geschütztes Geheimnis, was eine Familie im Dorfladen einkauft? Oder welche Haftpflichtversicherung sie abgeschlossen hat? Oder ist nur ein Geheimnis, was die Eltern im Erotikversand bestellen? Oder welche Angaben sie auf dem Gesundheitsfragebogen der Zusatzversicherung gemacht haben? In den ersten beiden Fällen handelt es sich schwerlich um berufsgeheimnisgeschützte Informationen, in den letzteren beiden Fällen hingegen schon. Um sicher zu gehen, müsste ein Unternehmen sich entweder einen «General-Waiver» geben lassen oder eine umfangreiche, jede Eventualität abdeckende Liste aller relevanten Bekanntgaben zusammenstellen und diese einzeln freizeichnen. Jeder, der schon einmal eine Datenschutzerklärung formuliert hat, weiss, dass dies gerade bei grösseren Unternehmen unrealistisch ist. Geht eine bestimmte Bekanntgabe vergessen, droht sie zudem im Hinblick auf die Präzision des spezifischen Waivers *e contrario* verboten zu sein; bereits das Vorhandensein eines Waivers vermittelt den Eindruck, dass es eine Schweigepflicht

gibt – sonst wäre er ja nicht nötig. Ein «General-Waiver» löst dieses Problem, lässt aber Art. 62 revDSG ins Leere laufen. Trotzdem dürfte er in der Praxis bevorzugt werden. Helfen können in der Praxis immerhin Vertragsformulierungen, die nicht auf die Zulässigkeit der Bekanntgabe fokussieren, sondern auf das Nichtbestehen einer Geheimhaltungspflicht.[58] Sie dürften vom Publikum leichter akzeptiert werden.

Bezüglich des gültigen Einholens einer Einwilligung zeigt sich die Relevanz der Natur der Norm ebenfalls, nämlich im Zusammenhang mit der Frage, ob für einen «Waiver» die speziellen Anforderungen an Einwilligungen nach Art. 6 Abs. 7 revDSG gelten. Dies ist nicht der Fall, da es sich bei Art. 62 revDSG eben nicht um eine datenschutzrechtliche Norm handelt und für das Einholen einer Einwilligung in die Bekanntgabe deshalb dieselben Grundsätze, wie für andere Berufsgeheimnisse gelten müssen. Diese einheitlichen Anforderungen an eine gültige Einwilligung scheinen auch deshalb nur logisch, weil eine vertragliche Regelung der Bekanntgabe dem Waiver im Ergebnis gleichgestellt ist und für diese auch keine besonderen Vorschriften gelten. Sieht die Bestellung von Sextoys den Versand über einen Paketdienst vor, darf der Versandhändler diesem die Adresse des Kunden selbstverständlich mitteilen.

Im Ergebnis bedeutet dies, dass Unternehmen gut daran tun, ihre Mitarbeiter auf die neue Strafbarkeit hinzuweisen und ihnen Leitlinien vorzugeben, wo und wie vertrauliche Informationen (auch innerbetrieblich) weitergegeben werden dürfen. Sie sollten zudem ihre Datenschutzerklärungen um detaillierte Hinweise auf kritische Bekanntgaben von Personendaten an Dritte erweitern; hierbei ist die Ungewöhnlichkeitsregel zu beachten, nach der ungewöhnliche Datenweitergaben in der Darstellung besonders hervorzuheben sind. In ihren AGB können sich Unternehmen die Bekanntgaben gemäss ihrer Datenschutzerklärung vorbehalten und auf das Nichtbestehen einer Schweigepflicht verweisen. Heiklere Bekanntgaben sind zudem vorzugsweise vertraglich vorzusehen. Einen formalen Waiver für den grossflächigen Einsatz wird es in Anbetracht dieser anderen möglichen Schutzmassnahmen eher selten brauchen; vielmehr wird er wohl im Einzelfall eingesetzt werden. Dabei ist insbesondere an Situationen zu denken, in denen Unternehmen von Dritten um Auskünfte angefragt werden. Dieses Szenario wirft viele weitere Fragen auf, die hier nicht beantwortet werden können, so etwa, ob eine Referenzauskunft, die ohne Einwilligung des (ehemaligen) Arbeitnehmers erteilt wird, künftig strafbar sein wird.

IV. Andere Sanktionen von Datenschutzverstössen

Die Bussen im revidierten Datenschutzgesetz sind nicht die einzige Art und Weise, wie datenschutzrechtliche Verstösse sanktioniert bzw. durchgesetzt werden können.[59] In der Praxis häufiger werden Interventionen des EDÖB sein, der neu auch Verfügungen erlassen kann. Diese werden teilweise wesentlich gravierendere Konsequenzen haben als eine Busse. So kann der EDÖB etwa anordnen, dass eine Datenbearbeitung eingestellt oder angepasst werden muss, die mit grossem Aufwand erstellt worden ist oder von der viel abhängt. Im Übrigen können auch andere Aufsichtsbehörden im Falle von Datenschutzverstössen einschreiten (z.B. die FINMA); mit ebenso schwerwiegenden Folgen. Durchsetzen lässt sich das DSG selbstverständlich auch auf dem Zivilweg, was künftig einfacher wird, da die Gerichtskosten wegfallen. Privatrechtlicher Natur sind ausserdem die in manchen Verträgen vorgesehenen Konventionalstrafen für den Fall von Datenschutz- und Geheimnisverletzungen.

Verletzungen des Datenschutzes sind teilweise auch in anderen Gesetzen unter Strafe gestellt. Im Laufe der Zeit wurden beispielsweise einige spezialrechtliche Datenschutzbestimmungen ins UWG eingefügt (Spamverbot, Einschränkung von Werbetelefonaten). Eine Verletzung der Pflicht zur Information über Cookies kann nach FMG gebüsst werden (Art. 45*c* i.V.m. 53 FMG). Die Datenbekanntgabe an ausländische Behörden oder in ausländischen Verfahren kann eine Sanktionierung nach Art. 271 StGB zur Folge haben, und selbstverständlich kann die unerlaubte Bekanntgabe von Personendaten – je nach Situation – auch Geheimnisschutztatbestände (z.B. Art. 162, 273 und 320 ff. StGB, Art. 47 BankG, Art. 69

[58] Etwa: «Der Kunde anerkennt, dass der Verantwortliche keiner Schweigepflicht nach Art. 62 revDSG unterliegt.»

[59] Zum Ganzen: *David Rosenthal,* Sanktionierung von Datenschutzverstössen, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, Basel, 2015, S. 203 ff.

FINIG) und Tatbestände zum Schutz der Privat- und Geheimsphäre (Art. 179 ff. StGB) verletzen.

V. Zusammenfassung und Ausblick

Die Strafbestimmungen des revDSG werden zweifellos noch für Diskussionen sorgen. Das Risiko einer persönlichen Strafbarkeit, auch auf unteren Hierarchiestufen, wird das Interesse an der Einhaltung des Datenschutzes zweifellos stark fördern. Die gute (aber oft übersehene) Nachricht für Personen, die mit der Einhaltung des Datenschutzes betraut sind, ist, dass nur wenige Verstösse strafbewehrt sind. Weil die Sanktionen jedoch solch alltägliche Aspekte wie die Datensicherheit, die Datenschutzerklärungen und den Export von Personendaten betreffen, wird bei übereilter Betrachtung des revDSG oft vergessen, dass die Verletzung vieler der neu eingeführten Bestimmungen straflos bleibt. Neben den neuen Sanktionen wird wohl auch das «kleine» Berufsgeheimnis für Unbehagen sorgen; schon die bisherigen Reaktionen zeigen, dass selbst Datenschützer Mühe haben, die Bestimmung zu «fassen» und mit ihr umzugehen. Wer Entscheidungen bezüglich der Einhaltung des Datenschutzes treffen muss, braucht jedoch nicht allzu beunruhigt zu sein angesichts der neuen Strafbestimmungen: Der Sanktionsapparat im revDSG ist zwar aufgerüstet worden. Doch den in vielen Fällen erforderliche Strafantrag können nur betroffene Personen und nicht der EDÖB einreichen. Zudem entspricht es nicht den schweizerischen Sitten und Gebräuchen, Datenschutzrecht mittels des Strafrechts durchzusetzen, obwohl das DSG schon bisher Bussenbestimmungen hatte. Wird ferner der Umstand berücksichtigt, dass die Strafverfolgung nur durch die kantonalen Strafverfolgungsbehörden erfolgt, die normalerweise nichts mit Datenschutzdelikten zu tun haben, so ist davon auszugehen, dass Bussen tendenziell weiterhin die Ausnahme bleiben werden. Und selbst der EDÖB dürfte erfahrungsgemäss primär daran interessiert sein, die ihm zu Augen oder Ohren kommenden Datenschutzverstösse zu beheben, statt zu sanktionieren.