

# Neues Datenschutzgesetz: Mehr Augenmass statt Bürokratie

Ursula Uttinger  
Juristin, Zürich

Datenschutz und Privatsphäre sind nicht zwangsläufig mit Warnhinweisen ohne Ende verbunden. Der gesunde Menschenverstand muss im Zentrum stehen – auch nach der Inkraftsetzung des revidierten Datenschutzgesetzes am 1. September.

Wie schon im Mai 2018, als die europäische Datenschutz-Grundverordnung (DSGVO)<sup>1</sup> in Kraft trat, kamen auch dieses Jahr viele Datenschutzexperten zu Wort und boten Beratungen zum aktuellen Handlungsbedarf gemäss dem revidierten Schweizer Datenschutzgesetz (DSG) an. Aus dem ganzen deutschsprachigen Raum gab es jede Menge Empfehlungen für Schweizer Unternehmen – und Experten empfahlen sich selbst.

Deren Sachkenntnis überzeugt jedoch nicht immer. So schreibt etwa eine Anwaltskanzlei aus Deutschland entgegen der gesetzlichen Regelung: «Unternehmen und Organisationen müssen Datenschutzbeauftragte ernennen, die dafür verantwortlich sind, die Einhaltung der Datenschutzvorschriften zu überwachen und sicherzustellen.»<sup>2</sup> Ein Blick ins Gesetz genügt, um festzustellen, dass hier etwas nicht stimmen kann: Artikel 10 DSG spricht von Datenschutzberaterin oder -berater, und eine Pflicht zur Ernennung besteht nur für Bundesorgane.

Zu solchen groben Fehlaussagen kommt es glücklicherweise nicht oft. Was jedoch selten fehlt, sind ausführlichste Beratungen und ausgeklügelte Tools, die ohne Beratung nicht nachvollziehbar sind.

Dabei fasste der eidgenössische Datenschutzbeauftragte Adrian Lobsiger Inhalt und Zweck des revidierten Gesetzes so zusammen: «Die schweizerische Gesetzgebung beschränkt sich auf Wichtiges, sie regelt es generell-abstrakt und technologieneutral. Der Vorteil dieser Rechtsetzungskultur ist, dass ihre Anwendung nicht in ers-

ter Linie Wissen, sondern Denken voraussetzt. Mit der Bereitschaft, sich gedanklich in die Haut der Kundinnen und Kunden zu versetzen und mit einer Prise gesundem Menschenverstand kann jedes Unternehmen mit dem knapp gehaltenen Text von Gesetz und Verordnung vertretbare Lösungen finden.»<sup>3</sup>

## Risiko von Bussen ist klein

Datenschutz ist nicht nur eine Compliance-Aufgabe, bei der es einzig um das Abarbeiten einzelner Pflichten geht. Die einzelnen Grundsätze müssen interpretiert, auf das Unternehmen und die Branche hin verstanden und umgesetzt werden. Ohne Branchenkenntnisse ist eine gute Beratung kaum möglich.

Das Datenschutzgesetz selbst ist ein *lex generalis*: Die Spezialgesetze der einzelnen Branchen müssen zwingend beachtet werden. Es gilt der unter älteren Juristen noch bekannte Satz «*lex specialis derogat legi generali*»: Eine spezialgesetzliche Regelung geht dem allgemeinen Gesetz vor und hat damit Anwendungsvorrang.

Das revidierte Datenschutzgesetz brachte Änderungen. Vieles blieb aber gleich, nur einzelne Formulierungen änderten sich. Die Grundsätze sind nicht neu, auch das Konzept des Erlasses blieb gleich. Eine Datenbearbeitung braucht nicht, wie in Artikel 6 DSGVO gefordert, grundsätzlich einen Rechtfertigungsgrund. Das Schweizer Gesetz ist sowohl für private Personen wie für Bundesorgane anwendbar. Einzig das fünfte

<sup>1</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

<sup>2</sup> Kolb-blickhan-partner.de/author/s-ilk, besucht am 14.9.2023.

<sup>3</sup> Adrian Lobsiger, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, anlässlich einer Tagung in Zürich.

- 4 Wolfgang Wohlers in: Bruno Baeriswyl / Kurt Pärli / Dominika Blonski (Hrsg.), Datenschutzgesetz, 2. Aufl., Bern 2023, Art. 62 Rz 30.
- 5 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017, S. 6970.
- 6 Bundesgesetz über den Datenschutz DSG vom 19. Juni 1992, in Kraft von 1.12.2010 bis 31.8.2023.
- 7 Verordnung zum Bundesgesetz über den Datenschutz VDSG vom 14.6.1993.
- 8 BBl 7050 f.
- 9 Mitarbeiterinformation betreffend Datenschutz, Weka Business Media, Regina Arquint.
- 10 Kurt Pärli / Nathalie Flück in: Bruno Baeriswyl / Kurt Pärli / Dominika Blonski (Hrsg.), Datenschutzgesetz, 2. Aufl., Bern 2023, Art. 19, Rz. 5.
- 11 Einwilligungserklärung, Patientenformular FMH, Version 3/2023.
- 12 Rosenthal.ch: Datenschutzerklärung für KMU auf nur einer Seite (revDSG, nicht DSGVO), mit Anleitung, besucht am 16.9.2023.
- 13 Wolfgang Wohlers in: Bruno Baeriswyl / Kurt Pärli / Dominika Blonski (Hrsg.), Datenschutzgesetz, 2. Aufl., Bern 2023 Art. 60 Rz. 23.

Kapitel gilt nur für Privatpersonen, das sechste Kapitel gilt nur für Bundesorgane.

Im Vorfeld der Inkraftsetzung wurde viel mit der Angst operiert, um den Beratungsumsatz zu erhöhen. Gemäss Gesetz können Privatpersonen neu mit Bussen bis zu 250 000 Franken bestraft werden. Diese Aussage ist so zwar korrekt, doch wurde kaum erwähnt, dass es für einen Schuldspruch einen Vorsatz braucht – fahrlässiges Handeln wird nicht bestraft.

Abgesehen von Artikel 61 DSG (Verletzung von Sorgfaltspflichten) und Artikel 63 DSG (Missachten von Verfügungen) existierten die Straftatbestände schon in ähnlicher Weise im bisherigen Gesetz. Verurteilungen gestützt auf diese Normen sind nicht bekannt.

Es ist nicht davon auszugehen, dass einzig wegen der höheren Bussenandrohung mehr Strafanzeigen eingereicht werden. Diese sind Voraussetzung für ein Strafverfahren, weil auch das neue Gesetz nur Antragsdelikte enthält. Das Risiko einer Busse dürfte bei vernünftigem und nicht böswilligem Verhalten äusserst klein sein.

Übrigens: Das Amtsgeheimnis und das Berufsgeheimnis der Ärzte, Anwälte und Geistlichen sind in den Artikeln 320 und 321 des Strafgesetzbuches mit weit höheren Strafanforderungen versehen. Diese Artikel gehen dem Datenschutzgesetz vor beziehungsweise sind relevanter: Das Amtsgeheimnis als Officialdelikt, das Berufsgeheimnis als gewichtigere und speziellere Strafnorm.<sup>4</sup>

## Die wichtigsten neuen Vorgaben

Die Revision des Gesetzes brachte vor allem weitergehende Transparenzvorschriften als bisher: eine Stärkung des risikobasierten Ansatzes bei der Datenbearbeitung sowie mehr Kompetenzen für den

Datenschutz- und Öffentlichkeitsbeauftragten (Edöb).<sup>5</sup>

Datenbearbeiter müssen die weitergehenden Informationspflichten beachten (Artikel 19 und 21 DSG), allenfalls die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten (Artikel 12 DSG) sowie die Erstellung einer Datenschutzfolgenabschätzung, falls eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringen kann (Artikel 22 DSG). Dazu kommt die Pflicht der Meldung von Datensicherheitsverletzungen (Artikel 24 DSG).

Die letzten beiden Punkte sind neu im Gesetz, die Pflicht zur Transparenz hingegen war bereits im bisherigen Gesetz enthalten, wenn auch weniger umfassend gefordert (Artikel 14 aDSG<sup>6</sup> bei besonders schützenswerten Personendaten). Die Risikofolgenabschätzung war in der Verordnung in Artikel 8 Absatz 2 litera c VDSG<sup>7</sup> versteckt.

Transparenz kann unterschiedlich umgesetzt werden. Die Botschaft selbst hält fest: Das Datenschutzgesetz «legt nicht fest, auf welche Weise die Information erfolgen muss. Der Verantwortliche muss aber sicherstellen, dass die betroffene Person die Information tatsächlich zur Kenntnis nehmen kann.» So könne eine allgemeine Information genügen, wenn die Personendaten bei der betroffenen Person beschafft werden. «Denkbar sind in diesem Fall eine Datenschutzerklärung auf einer Website, aber gegebenenfalls auch Symbole oder Piktogramme, soweit sie die nötigen Informationen wiedergeben.

Wird eine allgemeine Form gewählt, muss die Information leicht zugänglich, vollständig und genügend sichtbar gemacht sein.»<sup>8</sup>

Wenn man sich an die Botschaft hält, ist leicht festzustellen, dass

viele Informationspapiere zum neuen Gesetz ohne Augenmass verfasst wurden. So wurde etwa von Weka Business Media kürzlich eine zehnteilige Mitarbeiterinformation empfohlen.<sup>9</sup>

## Erklärungen oft unnötig umfangreich

Unbestritten dient die Information der informationellen Selbstbestimmung.<sup>10</sup> Wenn aber die Menge der Information so umfassend ausfällt, ist sie nicht mehr adressatengerecht. Gelungen ist demgegenüber das Beispiel des Ärzterverbands FMH, der für die Patienteninformation genau eine A4-Seite braucht.<sup>11</sup> Auch Datenschutzerklärungen von Unternehmen sind zum Teil unnötig umfangreich. Wie man sie sehr kurz halten kann, hat David Rosenthal gezeigt.<sup>12</sup>

Möglicherweise ist dieses Bedürfnis, so viel festzuhalten, auch auf die Strafbestimmung von Artikel 60 DSG zurückzuführen (Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten). Allerdings ist zu beachten, dass es bei der Informationspflicht vor allem darum geht, dass die Rechte von Artikel 19 Absatz 2 DSG geltend gemacht werden können. Dazu sind folgende Angaben nötig: Identität und Kontaktdaten des Verantwortlichen, Bearbeitungszweck und allfällige Empfängerinnen und Empfänger von bearbeiteten Daten.<sup>13</sup> Diese Angaben können kurz und prägnant erfolgen. Der Artikel 60 DSG verweist zusätzlich auf die Informationspflicht von Artikel 21 DSG (Informationspflicht bei einer automatisierten Einzelentscheidung) und die Artikel 25–27 DSG (Auskunftsrecht sowie Einschränkung des Auskunftsrecht allgemein bzw. für Medien).

Es gibt einige Vorlagen für ein Verzeichnis der Bearbeitungstätig-

keit. Für eine Datenschutzfolgeabklärung findet man vor allem bei kantonalen Datenschutzbehörden einige Hilfsmittel, bezüglich der neuen Meldepflicht bei Verletzung der Datensicherheit sind noch kaum Informationen vorhanden.

Punkto Datensicherheit herausfordernd ist der Entscheid, ob eine Verletzung zu «einem hohen Risiko für die Persönlichkeit oder die Grundrechte» führen kann. Theoretisch könnte bereits ein einziges E-Mail mit sensiblen Personendaten wie etwa Gesundheitsdaten an eine falsche Adresse ein hohes Risiko darstellen. Würde jedoch jedes falsch versandte E-Mail mit solchen Daten dem Edöb gemeldet, würde er sehr viel mehr Ressourcen als heute benötigen.

Auch hier sollte mit gesundem Menschenverstand vorgegangen werden. Zweifelsohne meldepflichtig wäre aber etwa ein Hacking von Daten in einer Gesundheitseinrichtung und ein Auftauchen dieser Daten im Darknet. Werden einzig Mail-Adressen erbeutet, dürfte kein «hohes Risiko für die Persönlichkeit» vorliegen.

## Hilfreiche kostenlose Mustervorlagen

Ein Verzeichnis der Bearbeitungstätigkeiten ist für Datenverantwortliche eines Unternehmens hilfreich. Zwingend ist ein solches für Firmen mit mehr als 250 Mitarbeitenden (Artikel 12 Absatz 5 DSGVO) oder wenn besonders schützenswerte Personendaten in grossem Umfang bearbeitet (Artikel 24 Absatz 1 litera a DSV) beziehungsweise ein Profiling mit hohem Risiko (Artikel 24 Absatz 1 litera b DSV) durchgeführt werden.

Der Aufwand dafür hält sich in Grenzen. Es empfiehlt sich generell, ein Verzeichnis zu erstellen, auch wenn dies von Gesetzes wegen nicht zwingend wäre. Auch dafür kann man sich an kostenlo-

sen Mustervorlagen orientieren, wie man sie etwa auch beim Schweizerischen Gewerbeverband (SGV)<sup>14</sup> oder der FMH<sup>15</sup> findet.

Das Erstellen einer Datenschutzfolgeabschätzung ist komplexer, jedoch keine exakte Wissenschaft.<sup>16</sup> Der eidgenössische Datenschutzbeauftragte hat dazu ein Merkblatt<sup>17</sup> veröffentlicht, aber keine Formulare oder weiteren Hilfsmittel. Solche finden sich zum Beispiel beim Gewerbeverband<sup>18</sup> sowie bei diversen kantonalen Datenschutzbehörden – unter anderem in Zürich,<sup>19</sup> Zug,<sup>20</sup> Luzern,<sup>21</sup> Aargau<sup>22</sup> und Glarus.<sup>23</sup>

Die kantonalen Vorlagen sind unterschiedlich und als Orientierungshilfe nützlich. Sie sind auf die kantonalen Gesetze ausgerichtet und können nur bedingt übernommen werden.

Eine Datenschutzfolgeabschätzung sollte als Arbeitsinstrument verstanden werden, um systemische und sicherheitstechnische Risiken zu erkennen und Massnahmen zu ihrer Reduktion zu treffen.<sup>24</sup>

Neu gibt es auch diverse Vorlagen zu Vereinbarungen einer Auftragsdatenbearbeitung. Schon in Artikel 10 Absatz 2 aDSG hiess es, dass sich der Auftraggeber einer externen Datenbearbeitung insbesondere vergewissern muss, «dass der Dritte die Datensicherheit gewährleistet». Im revidierten DSGVO steht in Artikel 9 Absatz 2: «Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.»

Gemäss der Botschaft zum Gesetz handelt es sich nicht um wesentliche Änderungen.<sup>25</sup> Dennoch kamen ausführliche Verträge zur Auftragsdatenbearbeitung erst jetzt auf.

Wichtig ist, die Auftragsdatenbearbeitung sauber gegenüber einer Funktionsübertragung abzugrenzen, bei der Dritte die Daten in Eigenverantwortung wei-

terbearbeiten oder bei einer Datenbekanntgabe. Bei einer Auftragsdatenbearbeitung findet keine Datenbekanntgabe im datenschutzrechtlichen Sinne statt.<sup>26</sup> Denn die Herrschaft für die Daten und damit auch die Verantwortung bleiben beim Auftraggeber.

## Viel und ausführlich ist nicht besser

In den Auftragsdatenvereinbarungen werden diverse Punkte geregelt, insbesondere auch die technischen und organisatorischen Massnahmen. Solche Vereinbarungen sind naturgemäss relativ ausführlich.

Auch hier findet man bereits gute Vorlagen im Umfang von vier Seiten (Vorlage SGV<sup>27</sup>). Etwas ausführlicher ist die Vorlage des Ärzteverbandes FMH,<sup>28</sup> es enthält einen Anhang, in dem die Massnahmen zu beschreiben sind.

Dabei gilt: Viel und ausführlich ist nicht besser. Das Ziel, eine Bearbeitung transparent zu machen und damit den Konsumentenschutz, auf den im Ingress des revidierten Datenschutzgesetzes verwiesen wird, zu verbessern, wird dadurch nicht erreicht. Durch die Menge der Information an die Konsumenten in seitenlangen Datenschutzerklärung werden die relevanten Informationen verwässert.

Was also bringt das revidierte Datenschutzgesetz? Auf den Punkt gebracht hat es der einstige Zürcher Datenschützer Bruno Baeriswyl: Es ist «ein etwas kompliziertes Datenschutzgesetz, das zweckgerichtet ausgelegt und umgesetzt werden kann – oder bürokratisch und umständlich gehandhabt.»<sup>29</sup>

- 14 Sgv-usam.ch/media/19654/20221222\_dsg\_muster\_datensicherheits-verzeichnis\_de.xlsx, besucht am 16.9.2023.
- 15 Fmh.ch/files/doc3/vorlage-verzeichnis-der-bearbeitungstaetigkeiten.docx, besucht am 16.9.2023.
- 16 Ursula Uttinger/Thomas Geiser, Das neue Datenschutzrecht, N 336 ff., Basel 2023.
- 17 Edöb, Merkblatt zur Datenschutz-Folgenabschätzung (DSFA) nach Art. 22 und 23 DSGVO, Stand August 2023.
- 18 Sgv-usam.ch/media/19650/20221222\_dsg\_muster\_datenschutz-folgenabschaetzung\_de.docx, besucht am 16.9.2023.
- 19 Datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutz-folgenabschaetzung, besucht am 16.9.2023.
- 20 zg.ch/de/recht-justiz/datenschutz/informationen-fuer-behoerden/datenschutz-folgenabschaetzung, besucht am 16.9.2023.
- 21 Datenschutz.lu.ch/themen/Neues\_Kantonales\_Datenschutzgesetz, besucht am 16.9.2023.
- 22 Ag.ch/media/kanton-aargau/dvi/dokumente/ges/organisation/idag/merkleaetter/20200701-merkleaetter-datenschutz-folgenabschaetzung-dsfa.pdf, besucht am 16.9.2023.
- 23 Gl.ch/public/upload/assets/45859/Merkblatt%20Datenschutz%20Folgenabsch%3%A4tzung.pdf?fp=1671792547410, besucht am 16.9.2023.
- 24 Adrian Lobsiger, «Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation», in: Schweizerische Juristenzeitung (SJZ) 6/2023, S. 311 ff.
- 25 BBl 2017, 7031.
- 26 Bruno Baeriswyl in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, 2. Aufl., Bern 2023, Art. 9, Rz. 6 ff.
- 27 Sgv-usam.ch/media/19649/20221222\_dsg\_muster\_auftragsbearbeitungsvertrag\_de.docx, besucht am 16.9.2023.
- 28 Fmh.ch/files/doc3/vereinbarung-fuer-eine-auftragsbearbeitung.docx, besucht am 16.9.2023.
- 29 Bruno Baeriswyl anlässlich einer Veranstaltung vom Schweizerischen Verein der Berufe mit Bezug zu Datenschutz im Gesundheitswesen (SHPP) vom 20.6.2023.