

# Jusletter

## Das revidierte Datenschutzgesetz (DSG) – Was kommt auf wen zu?

### Tagungsbericht zur 1. Basler Datenschutzrechtstagung

**Autoren/Autorinnen:** Michael Balmer / Joël Kämpf

**Beitragsart:** Tagungsberichte

**Rechtsgebiete:** Datenschutz

**DOI:** 10.38023/af095dc2-ba9a-4047-881e-be420ed26818

**Zitiervorschlag:** Michael Balmer / Joël Kämpf, Das revidierte Datenschutzgesetz (DSG) – Was kommt auf wen zu?, in: Jusletter 14. August 2023

*Die Revision des Bundesgesetzes über den Datenschutz (DSG) dauerte lange und das Ergebnis ist kontrovers. Am 1. September 2023 wird das revidierte DSG und die – ebenfalls umstrittene – Verordnung zum DSG in Kraft treten. Anlässlich der ersten Basler Datenschutzrechtstagung wurde ein Überblick zum Inhalt und den Hintergründen der neuen Datenschutzrechtsordnung verschafft. Dabei wurden einzelne Themen vertieft behandelt sowie auch Auswirkungen auf einzelne Rechtsgebiete beleuchtet.*

### Inhaltsverzeichnis

1. Veranstaltungsrahmen
2. Die einzelnen Referate
  - 2.1. revDSG: Neuerungen, Hintergründe und die Bedeutung in der Praxis
  - 2.2. Automatisierte Einzelentscheide
  - 2.3. Meldepflicht von Datenschutzvorfällen
  - 2.4. Die Datenschutzaufsicht nach dem revDSG
  - 2.5. Diskussion mit den Referierenden des Vormittags
  - 2.6. Tour d'horizon durch die privatrechtlichen Bestimmungen – Fokus auf die neuen Transparenzvorschriften
  - 2.7. Aufgaben und Stellung des Datenschutzberaters
  - 2.8. Datenschutz im Sozialversicherungsrecht – Was könnte oder wird sich ändern mit der Revision?
  - 2.9. Auswirkungen revDSG auf das Arbeitsrecht (privatrechtliche und öffentlich-rechtliche Anstellungen)
  - 2.10. Diskussion mit den Referierenden des Nachmittags
3. Ausblick

#### 1. Veranstaltungsrahmen

[1] Am Freitag, 21. April 2023, fand zum ersten Mal die Basler Datenschutzrechtstagung unter der Leitung von Prof. Dr. iur. KURT PÄRLI<sup>1</sup> statt. Diese Veranstaltungsreihe ist Teil von «**Recht aktuell**», dem Weiterbildungsformat der Juristischen Fakultät Basel. Ziel dieser Tagung war es, den Teilnehmenden einen Überblick über den Inhalt und die Hintergründe der kontroversen Revision des Bundesgesetzes über den Datenschutz zu verschaffen. Zudem wurden auch Auswirkungen auf einzelne Rechtsgebiete näher beleuchtet.

[2] Die Tagung wurde als Präsenz- und Online-Veranstaltung (mit Livestream) durchgeführt und fand im Congress Center Basel der MCH Messe Basel statt. Insgesamt verfolgten rund 180 Teilnehmende die Tagung und brachten sich in die am Vormittag und am Nachmittag angesetzten Diskussionen mit den Referierenden aktiv ein.

## 2. Die einzelnen Referate

### 2.1. revDSG:<sup>2</sup> Neuerungen, Hintergründe und die Bedeutung in der Praxis

[3] Den Tagungsaufakt gestaltete Herr Dr. iur. BRUNO BAERISWYL<sup>3</sup> mit seinem Referat zu den Neuerungen, Hintergründen und der Bedeutung der Revision für die Praxis. Einleitend erklärte er, wie es überhaupt zum neuen DSG gekommen sei. Die Geschichte des neuen DSG begann im Jahr 2011, als eine Evaluation eine abnehmende Wirkung des DSG festgestellt habe. Insbesondere seien zunehmende Risiken für die Wahrung der Grund- sowie Persönlichkeitsrechte festgestellt worden. Drei Jahre später habe ein Normkonzept zur Revision des DSG vorgelegen. Nach der parlamentarischen Debatte sei das revidierte DSG am 25. September 2020 verabschiedet worden.

[4] Auf die Entstehung des revDSG habe das europäische Datenschutzrecht einen wesentlichen Einfluss ausgeübt. Im Vordergrund stand dabei die Europaratskonvention 108.<sup>4</sup> Diese wurde modernisiert, wobei diese modernisierte Konvention 108+ von der Schweiz mit dem Inkrafttreten des revDSG ratifiziert werde.<sup>5</sup> Auswirkungen habe die Konvention beispielsweise auf die Einwilligung gehabt. Ebenfalls wichtig sei die Richtlinie 2016/680 gewesen.<sup>6</sup> Die Schweiz müsse die Richtlinie aufgrund der Schengen Assoziierung umsetzen. Dieses Schengen Datenschutzgesetz (SDSG) werde jedoch per Inkrafttreten des revDSG am 1. September 2023 wieder ausser Kraft gesetzt. Der Referent führte aus, dass die Bestimmungen der Richtlinie Eingang in das neue allgemeine schweizerische Datenschutzrecht fanden. Die DSGVO<sup>7</sup> sei nicht anwendbar in der Schweiz. Es sei denn, die Anwendbarkeit der DSGVO sei aufgrund des Marktortprinzips gegeben. Zusammenfassend hielt der Referent fest, dass das europäische Datenschutzrecht harmonisiert ist, weshalb bei den durch das revDSG übernommenen Bestimmungen auch die Rechtsprechung des EGMR und des EuGHs zu beachten sein wird.

[5] Nach diesem Einstieg fuhr der Referent mit den wesentlichen Neuerungen des neuen DSG fort. Allerdings sei nicht alles neu. So seien das Konzept, die Grundprinzipien und die Trennung zwischen dem privatrechtlichen und öffentlich-rechtlichen Datenschutz gleichgeblieben. Im Gegensatz zur DSGVO seien in der Schweiz Datenbearbeitungen weiterhin grundsätzlich erlaubt.

[6] Eine erste Änderung finde sich im Ingress des Gesetzes. Das DSG stütze sich neu auf Art. 97 der Bundesverfassung<sup>8</sup>, der den Bund zu Massnahmen des Konsumentenschutzes verpflichte. Ausdruck des Konsumentenschutzes sei beispielsweise Art. 28 revDSG, der das Recht auf Datenausgabe oder -übertragung statuiere. Ebenfalls neu sei das in den Art. 3 Abs. 1, Art. 14 und Art. 15 revDSG verankerte Marktortprinzip. Das Gesetz gelte also für Sachverhalte, die sich in der Schweiz auswirkten, auch wenn sie im Ausland veranlasst würden.

[7] Ebenfalls neu seien die Begriffe *Profiling*<sup>9</sup> und *Profiling mit hohem Risiko*<sup>10</sup>. Die Unterscheidung habe einen Einfluss auf die Form und den Inhalt der Einwilligung. Der Referent erklärte, dass die Begriffe der Richtlinie 2016/680 entstammen. Fraglich sei, ob der Schutz beim normalen *Profiling* kleiner sei als beim *Profiling mit hohem Risiko*. Nach der Meinung des Referenten ist dem nicht so. Der Schutz soll der gleiche sein.

[8] Weiter widmete sich der Referent Art. 6 Abs. 6 und Art. 7 revDSG. Die Einwilligung setze eine angemessene Information der betroffenen Person voraus. Zudem müsse die Einwilligung für die Bearbeitung von besonders schützenswerten Daten, ein *Profiling mit hohem Risiko* durch eine private Person oder ein *Profiling* durch ein Bundesorgan ausdrücklich erfolgen.

[9] Nach Art. 9 Abs. 1 lit. b revDSG dürften Personendaten von einem Auftragsbearbeiter nur so bearbeitet werden, wie es der Verantwortliche tun dürfte. Das bedeute, dass die Bearbeitung nur auf Weisung hin erfolgen dürfe. In Art. 9 Abs. 1 lit. b revDSG finde sich ein Swiss Finish aus dem noch geltenden DSG, gegen den mittlerweile Rechtsvertreter von Auftragsbearbeitern anrennen. Im Rahmen der Bestimmung müssten die gesetzlichen und vertraglichen Geheimhaltungsverpflichtungen ausgelegt werden, um beurteilen zu können, ob eine Auslagerung erlaubt oder verboten ist. Dabei handle es sich um eine Rechtsfrage und nicht um eine Beurteilung des Risikos, ob allenfalls ein Dritter auf die Daten zugreifen könne.

[10] Als nächstes äusserte sich der Referent zu den Art. 22 f. revDSG und damit zur Datenschutzfolgeabschätzung. Es handle sich dabei um eine Ergänzung der Risikobeurteilung. Die Verantwortlichen beurteilen in dieser die Risiken für die Persönlichkeit und Grundrechte der betroffenen Personen. Wenn man feststelle, dass die Datenbearbeitung ein hohes Risiko in sich berge, sei sie dem EDÖB<sup>11</sup> zur Vorabkonsultation vorzulegen. Die Datenbearbeitung müsse in jedem Fall rechtskonform sein. Das Risiko beurteile sich in Bezug auf die organisatorischen und technischen Massnahmen. M.a.W. sei also auch eine Datenbearbeitung mit hohem Risiko möglich.<sup>12</sup>

[11] Nach den neuen Strafbestimmungen könne sich eine Einzelperson strafbar machen. Subjektiv sei Vorsatz vorausgesetzt und bei den meisten Delikten handle es sich um Antragsdelikte. Die Strafverfolgung erfolge durch die Kantone. Um die Erfüllung des objektiven Tatbestandes beurteilen zu können, sei eine Auslegung des Datenschutzrechtes erforderlich.

[12] Zum Schluss seines Referates fragte der Referent, was denn das neue DSG sei. Es sei keine DSGVO light, aber es sei im europäischen Recht verankert. Weiter stelle es ein eigenständiges Datenschutzgesetz dar, das weiterhin den Schutz der Persönlichkeit und der Grundrechte bezwecke.<sup>13</sup> Für die Praxis stelle es ein etwas komplizierteres Datenschutzgesetz

dar. Es könne aber zweckgerichtet ausgelegt und umgesetzt werden, oder aber zu einer bürokratischen und umständlichen Handhabung führen.

## 2.2. Automatisierte Einzelentscheide

[13] Als nächste Rednerin widmete sich Prof. Dr. iur. NADJA BRAUN BINDER, MBA<sup>14</sup> den automatisierten Einzelentscheiden. Der Systematik des Gesetzes folgend, erklärte sie dem Publikum den Begriff.

[14] Die automatisierten Einzelentscheide würden eine komplette Neuerung im Schweizer Recht darstellen. Sie seien in Art. 21 revDSG geregelt. Die EU kenne einen parallelen Begriff in Art. 22 DSGVO.<sup>15</sup> Dieser sehe ein Verbot von automatisierten Einzelentscheiden vor. Art. 22 Abs. 2 DSGVO anerkenne jedoch drei Ausnahmen vom grundsätzlichen Verbot. In der Schweiz sei nun das Gegenteil vorgesehen. Automatisierte Einzelentscheide seien grundsätzlich zulässig. Die betroffene Person müsse jedoch informiert werden, wenn damit eine Rechtsfolge verbunden sei oder der Entscheid sie erheblich beeinträchtige. Nach Art. 21 Abs. 2 revDSG müsse die Information der betroffenen Person ermöglichen, ihre Rechte zu wahren. Sie müsse ihren Standpunkt darlegen können. Abs. 4 verlange sodann eine Kennzeichnung, wenn die automatisierte Einzelentscheidung durch ein Bundesorgan erfolge.

[15] Art. 21 behandle ausschliesslich automatisierte Einzelentscheide. Dabei müsse ein Personenbezug bestehen. Einfache «wenn-dann-Entscheide» seien nicht betroffen. Vielmehr seien komplexere Entscheidungen gefordert.

[16] Im Folgenden ging die Referentin näher auf Art. 21 Abs. 1 revDSG ein. Insbesondere erläuterte sie die zwei Begriffsmerkmale *automatisierte Bearbeitung* und *Rechtsfolge oder erhebliche Beeinträchtigung*.

[17] Nach der Botschaft liege eine automatisierte Einzelentscheidung vor, «wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.»<sup>16</sup> Anhand eines Beispiels aus Österreich<sup>17</sup> illustrierte BRAUN BINDER die Bedeutung einer automatisierten Bearbeitung. Das Beispiel zeigte auf, dass es nicht einfach zu beurteilen ist, ob eine vollautomatisierte Entscheidung vorliegt oder nicht.

[18] Als zweites Beispiel nannte sie mit *SCHUFA*<sup>18</sup> ein Beispiel aus Deutschland. Laut dem Generalanwalt sei die blosser Ermittlung der Wahrscheinlichkeiten bereits eine vollautomatisierte Entscheidung, auch wenn das Programm selbst keine Kredite spreche. Damit verstosse es gegen die DSGVO.<sup>19</sup> Die Referentin erwartete das Urteil mit Spannung.

[19] Die Botschaft äussere sich auch zur *Rechtsfolge oder erheblichen Beeinträchtigung*. «Die Entscheidung ist mit einer Rechtsfolge verbunden, wenn sie unmittelbare, rechtlich vorgesehene Konsequenzen für die betroffene Person nach sich zieht».<sup>20</sup> Weiter sei eine erhebliche Beeinträchtigung der betroffenen Person anzunehmen, «wenn diese auf nachhaltige Weise z.B. in ihren wirtschaftlichen oder persönlichen Belangen eingeschränkt ist.»<sup>21</sup> Auch hier präsentierte die Referentin ein Beispiel aus Europa. Sie sprach von *SyRI* aus den Niederlanden.<sup>22</sup> An diesem Beispiel sei klar ersichtlich, dass die Entscheidung erhebliche

Beeinträchtigungen nach sich ziehe (auch wenn es im konkreten Fall nicht um eine Vollautomation ging).

[20] Im Fazit prognostizierte BRAUN BINDER eine schwierige Abgrenzung zwischen automatisierten Einzelentscheiden i.S.v. Art. 21 Abs. 1 revDSG und teilautomatisierten Entscheidungen in der Praxis. Sie vertrat, dass nach den konkreten Umständen des Einzelfalls abzuwägen sei, ob bzw. wieviel Entscheidungsspielraum für eine menschliche Entscheidung bleibt. Gegen das Vorliegen einer vollautomatisierten Entscheidung seitens eines Bundesorgans würden verwaltungsinterne Weisungen, die Schulung von Mitarbeitenden und die Möglichkeit von Betroffenen, ihre Argumente vorzubringen, sprechen.

[21] Ebenfalls schwierig sei die Grenzziehung zwischen Entscheidungen, die eine erhebliche Beeinträchtigung nach sich ziehen und solchen, die es nicht tun. Dies dürfte vor allem bei automatisierten Einzelentscheiden Privater von praktischer Relevanz sein. Bei der Unterscheidung zu berücksichtigen seien die unmittelbare Auswirkung der Entscheidung auf die betroffene Person, die vorübergehende oder endgültige Wirkung der Entscheidung, der Einfluss der Entscheidung auf das Verhalten der betroffenen Person sowie die finanziellen Auswirkungen auf die betroffene Person.

### **2.3. Meldepflicht von Datenschutzvorfällen**

[22] Nach einer Kaffeepause betrat Dr. iur. DOMINIKA BLONSKI<sup>23</sup> die Bühne. Die Datenschutzbeauftragte des Kantons Zürich befasste sich mit der Meldepflicht von Datenschutzvorfällen. Diese ist in Art. 24 revDSG statuiert.

[23] Als erstes nannte die Referentin Gründe, die zur Einführung des neuen Instruments geführt haben. Die Meldepflicht solle die Wahrnehmung schärfen, zur Bewältigung von Vorfällen beitragen und zukünftige Vorfälle verhindern.

[24] Weiter ging sie darauf ein, was überhaupt zu melden sei. Nach Art. 24 Abs. 1 revDSG sei «eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt,» zu melden. Eine Verletzung der Datensicherheit liege vor, wenn Personendaten gelöscht, verändert oder offenbart würden. Gleiches gelte, wenn sie verloren gingen. Die Referentin erklärte, dass die Datensicherheit durch Dritte oder Mitarbeitende verletzt werden kann. Dabei führte sie aus, dass diese vorsätzlich oder auch unabsichtlich handeln können. Als Beispiele nannte die Datenschutzbeauftragte das Liegenlassen eines Laptops, immer noch bestehende Zugriffsrechte ehemaliger Mitarbeiter und Mitarbeiterinnen, offene Verteiler in einem Mail und Trojaner sowie Spyware. Die Referentin empfahl dem Publikum, im Zweifel eine Meldung zu erstatten. Meldepflichtig sei die verantwortliche datenbearbeitende Person.

[25] Sodann erklärte die Referentin, wem und wann zu melden sei. So führte sie aus, dass Bundesorgane und private Datenbearbeitende eine Verletzung der Datensicherheit dem EDÖB melden müssen, wohingegen sich kantonale Organe an die kantonale Datenschutzbehörde wenden müssen. Sie informierte weiter, dass letztere als Hilfsmittel auf ein Formular oder Online-Tool zurückgreifen können. Die Meldung solle nach dem Wortlaut von Art. 24 Abs. 3

revDSG «so rasch als möglich» erfolgen. Die meldepflichtigen Personen seien aufgefordert, ab dem Zeitpunkt der Kenntnisnahme ohne Verzögerung zu handeln. Insbesondere sollen sie den Vorfall auch dann melden, wenn noch nicht alle Einzelheiten bekannt sind. Die meldepflichtigen Personen können die weiteren Details nämlich auch nachreichen, sobald diese bekannt seien.

[26] Im Anschluss widmete sich die Referentin dem Inhalt der Meldung. Die Meldung solle die Art der Verletzung der Datensicherheit, den Zeitpunkt und die Dauer der Verletzung, die Kategorien und Anzahl der Personendaten sowie die Kategorien und Anzahl der betroffenen Personen enthalten. Weiter aufzuführen seien die Folgen der Verletzung für die betroffenen Personen, bereits ergriffene und geplante Massnahmen zur Beseitigung der Verletzung oder Milderung der Folgen sowie eine Ansprechperson.

[27] Nach einer eingegangenen Meldung beurteile die Datenschutzbehörde den Sachverhalt. Sie prüfe die bereits getroffenen Massnahmen und eine allenfalls erforderliche Information der betroffenen Personen. Daraus resultiere eine Stellungnahme mit zu ergreifenden Massnahmen. Die betroffenen Personen würden informiert, wenn es zu ihrem Schutz erforderlich sei oder es die Datenschutzbehörde verlange. Dagegen könne eine solche Information unterbleiben, wenn überwiegende öffentliche oder private Interessen bestehen, Geheimhaltungspflichten es verlangen, sie nur durch unverhältnismässigen Aufwand zu bewerkstelligen oder unmöglich sei. Ebenfalls könne sie unterbleiben, wenn durch nachträgliche Vorkehrungen sichergestellt sei, dass das hohe Risiko sehr wahrscheinlich nicht mehr bestehe. Die Behörde dokumentiere den Vorfall samt seinen Auswirkungen und den ergriffenen Massnahmen und bewahre die Akte während mindestens zwei Jahren auf.

[28] Gegen Ende ging die Referentin noch auf die Verwendung der Informationen für ein Strafverfahren ein. Gemäss Art. 24 Abs. 6 revDSG könne eine Meldung in einem Strafverfahren gegen die meldepflichtige Person nur mit deren Einverständnis verwendet werden.

[29] In ihrem Fazit hielt die Referentin fest, dass die Meldepflicht die Hauptaufgaben der Datenschutzbehörden vereine. Zu diesen würden die Information, Sensibilisierung, Beratung, Unterstützung, Kontrolle und Aufsicht zählen.

#### **2.4. Die Datenschutzaufsicht nach dem revDSG**

[30] Als letzter Redner des Vormittags befasste sich Herr Prof. Dr. iur. BEAT RUDIN<sup>24</sup> mit der Datenschutzaufsicht nach dem revDSG.

[31] Er begann mit den Rechtsgrundlagen und den Vorgaben aus dem europäischen Recht. Vorgaben würden aus der [Europaratskonvention 108](#), der Richtlinie 2016/680 und zum Teil aus der Datenschutz-Grundverordnung der EU stammen. Hingegen finde sich nichts in der Bundesverfassung. Die Europaratskonvention 108+ verpflichte die unterzeichneten Staaten, eine oder mehrere Aufsichtsbehörden zu schaffen. Art. 15 der Konvention nenne die Aufgaben der Aufsichtsbehörde. Unter anderem seien die Behörden verpflichtet, sich mit den Anträgen und Beschwerden zu befassen.

[32] Die EU Richtlinie sei für die Schweiz aufgrund der Schengen Assoziierung verbindlich. Die Richtlinie fordere in Art. 42 eine unabhängige Aufsichtsbehörde. Die Unabhängigkeit sei in der Schweiz nicht immer gegeben gewesen, habe doch früher der Bundesrat den EDÖB bestimmt. Der Referent betonte, dass die Behörden institutionell und materiell unabhängig sein müssen. Weiter statuiere die Richtlinie allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde.<sup>25</sup> Insbesondere hätten sie die erforderliche Qualifikation, Erfahrung und Sachkunde mitzubringen. Die Mitglieder der Behörde müssen auf Amtszeit für mindestens vier Jahre gewählt werden.<sup>26</sup> Nach Art. 45 der Richtlinie dürfe die Aufsichtsbehörde keine Aufsicht über die justizielle Tätigkeit der Gerichte ausüben. Zu den Aufgaben der Behörde gehöre die Überwachung und Durchsetzung der Durchführungsvorschriften, die Sensibilisierung der Öffentlichkeit, die Beratung des Parlaments sowie der betroffenen Personen, die Behandlung von Beschwerden betroffener Personen und die Vorabkonsultation.

[33] Da die Schweiz nicht Mitglied der EU sei, sei die DSGVO nicht verbindlich. Allerdings sehe Art. 45 DSGVO den sogenannten Angemessenheitsbeschluss vor. Die EU-Kommission habe zu beschliessen, ob ein Drittland ein angemessenes Schutzniveau biete. In die Beurteilung fliesse auch die Ausgestaltung der Aufsichtsbehörden. Nur bei einem positiven Beschluss sei der Datentransfer in ein Drittland wie die Schweiz ohne Weiteres zulässig.

[34] In einem zweiten Teil kam der Referent zur Umsetzung im revDSG. Zunächst nenne Art. 4 revDSG den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. In den Art. 43–58 revDSG finde sich sodann eine detaillierte Auflistung zur Organisation, den Aufgaben und Befugnissen. Er sei institutionell, funktionell und materiell unabhängig. Gewählt werde er von der vereinigten Bundesversammlung auf eine Amtszeit von vier Jahren, wobei er sich zwei Mal einer Wiederwahl stellen könne. Er habe ein ständiges Sekretariat und Budgethoheit. Zu seinen Aufgaben zähle die Untersuchung von Verstössen gegen Datenschutzvorschriften. Er könne Bearbeitungen anpassen, unterbrechen oder abbrechen.

[35] Zu den wichtigsten Änderungen zähle die Vorabkonsultation nach Art. 23 revDSG. Ebenfalls neu sei die Möglichkeit der verbindlichen Anordnung nach Art. 51 revDSG. Hingegen könne der EDÖB keine Sanktionen mehr aussprechen. Dies liege neu in der Kompetenz der Strafgerichte nach Art. 65 revDSG.

[36] Im dritten Teil fragte der Referent nach der Wirksamkeit der Neuerungen. Seiner Meinung nach brauche der EDÖB genügend Ressourcen, um alle Anfragen beantworten zu können. Eine weitere Gefahr bestehe in einer Überhäufung mit Meldungen zu Datensicherheitsverletzungen. Zudem habe er neu Vorabkonsultationen durchzuführen. Für die Umsetzung des revDSG seien neun neue Stellen vorgesehen.

[37] Der Referent erwartet mit Spannung, wie wirksam die Datenschutzaufsicht nach dem revDSG sein wird.

## **2.5. Diskussion mit den Referierenden des Vormittags**

[38] Die Vortragenden des Vormittags stellten sich im Anschluss an die Referate den Fragen aus dem Publikum, woraus sich eine rege Diskussion ergab.

[39] Die erste Frage aus dem Publikum betraf die rechtlichen Grundlagen der Meldepflichten und richtete sich damit an BLONSKI. Sie führte aus, dass man sich zuerst fragen müsse, welches Datenschutzgesetz anwendbar sei. In einem nächsten Schritt sei zu prüfen, ob das Gesetz bereits eine Meldepflicht vorsehe. Im Bund werde das ab dem 1. September 2023 der Fall sein. Die Kantone seien unterschiedlich weit in der Umsetzung.

[40] Eine zweite Person fragte BLONSKI, ob sie Beispiele für Bagatellfälle und schwerwiegende Fälle geben könne. Als Bagatellfall bezeichnete die Datenschutzbeauftragte des Kantons Zürich den Fall mit einer offenen Verteilerliste in einer Mail, in dem der Inhalt nicht auf die Persönlichkeitsrechte der betroffenen Person einwirke. Ganz anders wäre der Fall gelagert, wenn man anhand der Verteilerliste erfahren könne, wer an einer Krebserkrankung leide. Ein hohes Risiko liege vor, wenn sensitive Daten wie bspw. Gesundheitsdaten betroffen seien oder auch wenn viele Personen betroffen seien. Das hohe Risiko sei eine schweizerische Eigenheit. Im europäischen Recht sei grundsätzlich eine Meldung verlangt, wenn sich ein Vorfall ereigne. Im Kanton Zürich würden Bagatellfälle vermehrt nach einem Standardverfahren behandelt.

[41] Wichtig, das betonte später auch RUDIN nochmals, sei es, die Vorfälle unverzüglich zu melden. So könne die Aufsichtsbehörde Hilfe leisten und Massnahmen prüfen.

[42] Die dritte Frage betraf die Abgrenzung zwischen verantwortlichem Bundesorgan und Auftragsbearbeiterin. RUDIN erläuterte, dass die Verantwortung beim auftraggebenden öffentlichen Organ verbleibe. Bei einer Aufgabenübertragung werde der Dritte selbst zum öffentlichen Organ und damit sei der Dritte selbst verantwortlich. Dies müsse sauber auseinandergehalten werden.

[43] Die nächste Frage lautete: «Müssen Bearbeitungen von besonders schützenswerten Daten immer und ungeachtet des Umfangs dem EDÖB zur Vorabkonsultation vorgelegt werden?» RUDIN äusserte sich zur Frage. Im baselstädtischen Recht gebe es eine Bestimmung, die immer eine Vorabkonsultation verlange. Diese können sich jedoch weder die Spitäler noch die Behörde leisten. Deshalb seien in den Spitälern Datenschutzberater installiert worden. Zusammen würden sie Kriterien zur Beurteilung ausarbeiten. Solange diese Kriterien eingehalten werden, gebe sich die Behörde damit zufrieden. Bei einer Kontrolle könne immer noch genauer hingeschaut werden.

[44] Als nächstes fragte eine Person nach der Strafbarkeit von Einzelpersonen, da es sich in der Praxis bei der Datenbearbeitung um einen arbeitsteiligen Prozess handle. BAERISWYL verwies zunächst auf die Grundsätze des Strafrechts: Sowohl der objektive wie auch der subjektive Tatbestand müssen von einer Person erfüllt sein, um sich strafbar zu machen. Es handle sich anders als nach der DSGVO um reines Strafrecht, weshalb ein Vergleich in diesem Bereich nicht möglich sei. RUDIN ergänzte, dass er nicht mit vielen Verurteilungen rechne.

[45] Zuletzt fragte eine Teilnehmerin noch nach den Ressourcen der Datenschutzbeauftragten und in welcher Frist mit einer Antwort gerechnet werden könne. BLONSKI verwies zunächst auf die bereitgestellten Formulare, die eine Bearbeitung erleichtern würden. Bei kleinen Meldungen könne innerhalb eines Tages mit einer Stellungnahme gerechnet werden.

[46] Nach der Diskussion entliess der Tagungsleiter PÄRLI das Publikum und selbstverständlich auch die Referierenden in die Mittagspause.

## **2.6. Tour d'horizon durch die privatrechtlichen Bestimmungen – Fokus auf die neuen Transparenzvorschriften**

[47] Der erste Teil des Nachmittagsprogramms wurde von Frau Prof. Dr. habil. MONIKA PFAFFINGER<sup>27</sup> gestaltet. Dabei ging sie auf ausgewählte Aspekte der privatrechtlichen Regelungen des revidierten DSG ein. Ein besonderes Augenmerk legte sie dabei auf die neuen Vorschriften zur Erhöhung der Transparenz. Mit ihrem Beitrag verfolgte sie das Ziel, das Bewusstsein für die Funktionsweise des DSG zu schärfen.

[48] In einem ersten Block ging die Referentin auf die Verzahnung der privatrechtlichen Bestimmungen des DSG mit dem restlichen Gesetz ein. Sie präsentierte eine Charakterisierung des DSG anhand von drei Strukturmerkmalen: Dualismus, Generalklauseln und Persönlichkeitsschutz im privaten Sektor. Dies, da diese Einbettung für das Verständnis der privatrechtlichen Bestimmungen zentral sei und insofern lange auch Fehlinterpretationen kursierten. Zunächst beschrieb sie den hybriden resp. dualen Charakter des DSG als Querschnittsgesetz, das sowohl im öffentlichen Bereich des Bundes als auch im privatrechtlichen Bereich Anwendung finde. Die Datenbearbeitung durch Privatpersonen sei im 5. Kapitel geregelt, während diejenige durch Bundesorgane im 6. Kapitel eine Regelung erfahren habe. In den vorangehenden Kapiteln befänden sich gemeinsame Vorgaben teilweise mit Differenzierungen für Private wie auch Bundesorgane. Die allgemeinen Bearbeitungsgrundsätze von Art. 6 und 8 revDSG würden für beide Bereiche gelten, seien aber gemäss dem 5. und dem 6. Kapitel in unterschiedliche Mechaniken eingebettet. Während für den öffentlichen Bereich des Bundes ein prinzipielles Bearbeitungsverbot mit Schranken aufgrund des Legalitätsprinzips gelte, greife für den privatrechtlichen Bereich die prinzipielle Bearbeitungsfreiheit mit Schranken («Dualismus» mit entgegengesetzten Ausgangspunkten). Anders dagegen die Funktionsweise der DSGVO mit monistischem Regime für öffentlichen und privaten Bereich und konsequentem grundsätzlichem Verarbeitungsverbot und notwendigen Erlaubnistatbeständen. Für die Schweiz mit ihrem dualen Regime sei immerhin bemerkenswert, dass das Verhältnismässigkeitsprinzip mit seiner öffentlich-rechtlichen Trias von Eignung, Erforderlichkeit und Verhältnismässigkeit auch im privaten Bereich gelte. Die gemeinsamen Bestimmungen für den öffentlichen und privaten Bereich seien im revDSG stark ausgebaut worden, da es für die Betroffenen nicht darauf ankomme, ob der Staat oder eine private Person Daten bearbeite, da in beiden Bereichen eine ähnliche Machtasymmetrie bestehe. Die drei Strukturmerkmale des Dualismus, des generalklauselartigen Regimes und der persönlichkeitsrechtlichen Anknüpfung im privaten Sektor blieben mit der Totalrevision bewahrt. Das revDSG reiche indes den Datenschutz zudem mit neuen Ansätzen und Instrumenten an. Das zeige sich insbesondere im Bereich der neuen Transparenzvorgaben. So sei der Datenschutz neu eine Governance- und Compliance-Aufgabe, zudem greife der risikobasierte Ansatz. Auf diese Art werde der Ball an die Datenbearbeiter gespielt, die neu in die Verantwortung genommen werden, den Datenschutz zu implementieren, zu dokumentieren und Rechenschaft abzulegen.

[49] In einem zweiten Block ging die Referentin vertieft auf die privatrechtlichen Bestimmungen i.e.S. des DSG und insb. auf die Art. 30 ff. revDSG ein. Dabei erklärte sie, dass sich der Datenschutz ebenso wenig für den privaten Bereich im **DSG** erschöpfe, sondern das weitere

Bestimmungen, namentlich Art. 328b OR<sup>28</sup>, zu beachten seien. In der Folge betonte sie, dass die Art. 30 ff. revDSG im Verhältnis zu Art. 28 ZGB als *lex specialis* zu betrachten seien.<sup>29</sup> Diese Art. 30 ff. revDSG seien konsequent persönlichkeitsrechtlich angeknüpft und damit individual- und defensivrechtlich. Bei genauerer Betrachtung entspreche Art. 30 Abs. 1 revDSG dem Art. 28 ZGB, während Abs. 2 nicht abschliessend aufzähle, wann das DSG von einer Persönlichkeitsverletzung durch Personendatenbearbeitung ausgehe. Nicht jede Personendatenbearbeitung begründe per se eine Persönlichkeitsverletzung, sondern nur die Bearbeitung qualifizierter Personendaten. Die Einwilligung sei keine grundsätzliche Voraussetzung zur rechtmässigen Personendatenbearbeitung. Art. 30 revDSG verbürge keinen Selbstbestimmungsansatz für den privaten Bereich in dem Sinne, dass es ein prinzipielles Bearbeitungsverbot gebe und die Einwilligung prioritäre Bedeutung habe. Vielmehr handle es sich um eine Missbrauchs- oder Integritätsschutzgesetzgebung. So führte die Referentin aus, dass namentlich die allgemeinen Bearbeitungsgrundsätze beachtet und ansonsten Freiräume für die Personendatenbearbeitung gewährt werden sollen. Sie geht in Kürze alsdann auf die weiteren Tatbestände der persönlichkeitsverletzenden Bearbeitung (Widerspruch; Weitergabe von besonders schutzwürdigen Angaben an Dritte) ein. Auch bei den Rechtfertigungsgründen nach Art. 31 revDSG entspreche die Gesetzessystematik weitgehend dem Konzept von Art. 28 ZGB.

[50] Im dritten Block widmete sich die Referentin ihrem eigentlichen Fokusthema, der erhöhten Transparenz, die mit der Totalrevision verfolgt wurde. Sie ging auf die Argumentation zu dieser zentralen Zielvorgabe der Totalrevision ein und liefert alsdann eine Übersicht über die zahlreichen, teilweise neuen Transparenzvorgaben und -instrumente (insb. Inventar, Datenschutzfolgenabschätzung, Dokumentation/Accountability, Informationspflichten, Meldepflichten, Auskunftsrecht usf. unter Verweis auf andere Vorträge). Welche Transparenzvorgaben im Einzelfall greifen würden, hänge von der Rolle des Personendatenbearbeiters ab (Verantwortlicher oder Auftragsbearbeiter, öffentliche Stelle oder Private). Der Forderung nach erhöhter Transparenz wurde auch durch den Bussenkatalog nach Art. 60 ff. revDSG Nachdruck verliehen. In der Folge führte die Referentin aus, welche Rechte und Pflichten die Zielsetzung der Transparenz verfolgen. Vertieft ging sie auf die neuen Informationspflichten zur angemessenen Informierung gegenüber dem Datensubjekt nach Art. 19 ff. revDSG ein. Dabei erläuterte sie, dass Art. 19 Abs. 2 revDSG Mindestinformationen bzw. Mindestinhalte aufzähle, wobei Art. 20 revDSG Ausnahmen bzw. Einschränkungen dieser Informationspflicht vorsehe. En détail wurde zudem die informierte Einwilligung besprochen. Sodann beleuchtete die Referentin das Auskunftsrecht nach Art. 25 ff. revDSG (Betroffenenrecht), wobei auch hier das Risiko von Bussen bestehe. Schliesslich wies die Referentin darauf hin, dass trotz erhöhter Transparenz ebenso Pflichten zur Geheimhaltung bestehen würden, die gleichermassen dem Datenschutz dienen würden. Dies leitete die Referentin denn auch zur Forderung über, neue Perspektiven für das Datenschutzrecht einzunehmen (Personendatenflüsse).

[51] Zusammenfassend betonte die Referentin die neuen Charakterzüge des revDSG und schloss mit der Feststellung, dass es sich beim revDSG wohl nur um einen Zwischenschritt handle, der in Zukunft weiterentwickelt werden müsse.

## **2.7. Aufgaben und Stellung des Datenschutzberaters**

[52] Direkt im Anschluss setzte sich Herr Dr. iur. DAVID VASELLA<sup>30</sup> mit dem Datenschutzberater (DSB) und dessen Regelung im schweizerischen Recht auseinander. Zunächst führte er aus, dass es sich beim DSB um eine Datenschutzfunktion handle, also um eine Art Governance Instrument. Der DSB sei aus der Überlegung entstanden, dass die Datenbearbeiter aus der Optik des Gesetzgebers proaktiv handeln sollen. Dies ist aus Sicht des Referenten missglückt. Für Private handle es sich im Gegensatz zu den Bundesorganen und der Regelung in der DSGVO um eine freiwillig zu bestellende Datenschutzfunktion. Der DSB könne entweder eine externe oder eine interne Person sein, solle aber unabhängig und wirksam sein. Der DSB sei nicht dazu da, das Geschäft zu fördern, sondern stehe wie jede Compliance-Funktion in einem gewissen Spannungsverhältnis zum «Business». Der DSB bringe Erleichterungen bei Datenschutz-Folgeabschätzungen mit sich. So könne der private Verantwortliche gemäss Art. 23 revDSG von der Konsultation des EDÖB absehen, wenn er den DSB konsultiert hat. Die Anreize funktionieren nach Ansicht des Referenten nicht, da aus Unternehmensoptik eine Erleichterung betreffend die «breach notification» an das EDÖB gewünscht worden wäre. Dazu zählt der Referent verschiedene Gründe auf, die aus Sicht eines Unternehmens gegen die Meldung an das EDÖB sprechen könnten, unter anderem die Unterstellung des EDÖB unter das Öffentlichkeitsgesetz, das Strafantragsrecht des EDÖB oder das Selbstbelastungsverbot, das aus Sicht des Referenten eine Fehlkonstruktion sei, da sich das Strafverfahren gegen die natürliche Person richte und die Meldepflicht das Unternehmen treffe. Der einzige Anreiz, nämlich die Erleichterung betreffend die Datenschutz-Folgeabschätzungen bei hohen Restrisiken, sei irrelevant, da kein Unternehmen eine Folgeabschätzung mache, bei der am Ende ein hohes Risiko resultiert. Der Anreiz bestehe eher in der Kundenerwartung, der Reputation oder aufgrund von Pflichten gemäss DSGVO.

[53] An den Bestellvorgang des DSB gibt es gemäss dem Referenten keine besonderen formellen Anforderungen. Der DSB müsse sich aber seiner Funktion bewusst sein und seine Rolle solle definiert werden. Zudem müssen zum einen die Kontaktdaten des DSB veröffentlicht werden, wobei eine Veröffentlichung im Internet wohl genüge und zum anderen müsse über ein Meldeformular eine Mitteilung an das EDÖB erfolgen. Die Aufgaben des DSB seien teilweise im Gesetz zu finden. So solle er schulen und beraten, bei der Anwendung des Datenschutzrechts mitwirken, die Einhaltung des Datenschutzrechts überwachen, bei Folgeabschätzungen mitwirken, bei Erstellung des Bearbeitungsreglements mitwirken und als Anlaufstelle für Betroffene und den EDÖB figurieren. Um diese Aufgaben zu erfüllen, müsse der DSB über ausreichende Fach- und Organisationskenntnisse verfügen. Ein DSB könne auch gesellschaftsübergreifend bestellt werden, könne gleichzeitig die Funktion eines DSB nach DSG sowie eines DPO<sup>31</sup> nach DSGVO erfüllen und könne, sofern die notwendigen Fachkenntnisse vorhanden sind, auch aus dem Ausland seiner Funktion nachkommen, solange er diese Funktion effektiv ausüben könne.

[54] Auch zur Stellung des DSB sage das Gesetz nicht viel. So soll der DSB fachlich unabhängig und weisungsungebunden sein. Zur Unabhängigkeit gehöre ein Konfliktverbot (Art. 10 Abs. 3 revDSG). So dürfe der DSB keinen Tätigkeiten nachgehen, die mit den Aufgaben als DSB unvereinbar sind. Dies seien gemäss Botschaft bspw. eine Mitgliedschaft in der Geschäftsleitung, Funktionen in der Personalführung oder in der Informationssystemverwaltung oder eine Dienststelle, die selbst besonders schützenswerte Personendaten bearbeitet. Der Referent lehnte diese pauschalen Beispiele mit Ausnahme der Mitgliedschaft in der Geschäftsleitung ab und plädierte für eine Prüfung der Vereinbarkeit im Einzelfall. Von

grundlegender Bedeutung sei das Effektivitätsgebot. Demnach müssten dem DSB die nötigen Ressourcen, Informationen und Daten zur Verfügung stehen.

[55] Gemäss dem Referenten seien alle seine Ausführungen zum DSB bei Privaten reine Theorie. Dies, da es keine Pflicht zu einer bestimmten Ausgestaltung des DSB gebe. Selbst wenn der DSB völlig abhängig wäre, hätte dies keine Konsequenzen. Einzig die praktisch bedeutungslose Ausnahme von der Konsultationspflicht würde entfallen. Dementsprechend bestehe eine gewisse Flexibilität hinsichtlich der Ausgestaltung des DSB. Bei Bundesorganen würde es sich hingegen um eine Verletzung des Datenschutzrechts handeln.

[56] Sofern der DSB unabhängig sei und somit keine Entscheidungen treffe, sei er vor der Strafbarkeit gut geschützt. Am Ende entscheide eine Person aus dem Business und nehme das Risiko auf sich. Dies treffe aber nur solange zu, als die Funktionen voneinander getrennt seien. Denkbar wäre hingegen eine Haftung des DSB bei unvollständiger Datenschutzerklärung oder Datenschutzauskunft, bei fehlender oder mangelhafter Auftragsdatenverarbeitung oder bei Übermittlung von Daten in Drittstaaten ohne Absicherung, sofern auch Vorsatz vorliege. Die Strafbarkeitsrisiken dürften aber wohl gering sein. Auch eine zivilrechtliche Haftung sieht der Referent als unwahrscheinlich an, wobei er auf einen möglichen Regress durch das Unternehmen hinweist.

## **2.8. Datenschutz im Sozialversicherungsrecht – Was könnte oder wird sich ändern mit der Revision?**

[57] Herr lic. iur. KASPAR GEHRING<sup>32</sup> führte zunächst aus, dass er in seiner über 18-jährigen Tätigkeit im Bereich des Sozialversicherungsrechts nur selten Fragestellungen im Bereich des DSGVO begegnet sei, womit er zum Ausdruck brachte, dass der Einfluss des bis anhin gültigen DSGVO im Sozialversicherungsrecht (insbesondere im Leistungsrecht) gering ist. In der Folge zeigte der Referent auf, welche Aufgaben das Sozialversicherungsrecht hat und welche Daten für die Erfüllung dieser Aufgaben benötigt werden. Dabei ging er zunächst auf die Beitragserhebung und die Anschlusskontrolle ein. Dort würden beispielsweise Daten zu den Anstellungsverhältnissen, zu den Löhnen, zu den Pensionskassen, zum Alter der versicherten Person sowie zu ihrer gesundheitlichen Vorgeschichte erhoben. Bei der Leistungsprüfung und -ausrichtung würden die zu erhebenden Informationen stark vom versicherten Risiko abhängen. So würden bei der AHV Informationen zur Anzahl Kinder und zum Alter der versicherten Person, bei der UV Daten über Gesundheitszustände, Abläufe von Unfällen etc. erhoben. Bei der Leistungsüberprüfung würden weitere Daten gesammelt, die auch mittels Observation erhoben würden. Hier seien sensible gesundheitsrelevante Daten betroffen.

[58] Das revDSG sei gemäss Art. 2 Abs. 1 auf private Personen sowie auf die in Art. 5 lit. i revDSG konkretisierten Bundesorgane anwendbar. Um die Tragweite der neuen Datenschutzgesetzgebung zu ermitteln, müsse die Zuständigkeit der Durchführungsorgane geklärt werden, um dann festzustellen, ob das DSGVO auf diese Versicherungen anwendbar sei. Als Abgrenzungskriterium sei die Rechtsnatur des Grundverhältnisses und allenfalls die Trägerschaft heranzuziehen. Im Rahmen der UV<sup>33</sup> ist das revDSG sowohl auf die SUVA als auch auf private Unfallversicherer anwendbar. Gleiches gelte für die Krankenkassen und die Militärversicherung. Bei den Pensionskassen gebe es unter Umständen Fragen, wenn es sich um kantonal organisierte Pensionskassen handle. Sodann könne die Abgrenzung zwischen

obligatorischer und weitergehender beruflicher Vorsorge Unterstellungsfragen aufwerfen. Nicht anwendbar sei das revDSG auf die RAV<sup>34</sup>. Bei der AHV<sup>35</sup> müsse zwischen Verbandsausgleichskassen, die dem revDSG unterstehen und den kantonalen Ausgleichskassen, die dem revDSG nicht unterstehen, unterschieden werden. Die Stellen der IV<sup>36</sup> und der EL<sup>37</sup> seien kantonal organisiert, weshalb das revDSG darauf nicht anwendbar sei. Im Sozialversicherungsrecht lasse es sich demnach nicht generell sagen, ob das DSG anwendbar sei. Vielmehr würden entweder die kantonalen Datenschutzgesetze oder das revDSG und dabei zusätzlich die besonderen Bestimmungen für Datenbearbeitung durch Bundesorgane, die nicht privatrechtlich handeln, zur Anwendung kommen.

[59] In der Folge ging der Referent auf die besonderen Bestimmungen des revDSG für Bundesorgane ein. Von diesen besonderen Bestimmungen waren die meisten bereits im alten DSG enthalten. Besonders betonte er die Datenschutz Folgeabschätzungen nach Art. 22 revDSG. Da es sich bei den Sozialversicherungen um besonders sensible Daten handle und die Daten, sofern Dauerleistungen ausgerichtet werden, die der Revision unterstehen, nicht zerstört werden können, müsse dies in einer Datenschutz-Folgeabschätzung wohl besondere Beachtung erfahren. Hinsichtlich der Meldung von Verletzungen der Datensicherheit nach Art. 5 lit. h revDSG zeigte der Referent auf, dass es spezifische Risiken/Konstellationen im Bereich der Sozialversicherungen gebe, da die Sozialversicherungen einen Bereich der Massenverwaltung darstellen. Nicht selten seien in Dossiers von Versicherten Daten zu anderen Versicherten zu finden. Dann stelle sich die Frage, ob in jedem Fall, in welchem bspw. ein Arztbericht einer anderen Person fälschlicherweise in einem Dossier abgelegt wurde, eine Meldung zu erfolgen habe.

[60] Dass die Bestimmungen des DSG in der sozialversicherungsrechtlichen Praxis nur eine untergeordnete Rolle spielen, erklärte der Referent mit den spezifischen datenschutzrechtlichen Regelungen im Sozialversicherungsrecht, bspw. die Schweigepflicht in Art. 37 ATSG<sup>38</sup>, den Untersuchungsgrundsatz in Art. 43 ATSG, die Aktenführung in Art. 46 ATSG und Art. 8 ff. ATSV<sup>39</sup>, die Akteneinsicht in Art. 47 ATSG und Art. 8 ATSV, die Massgeblichkeit geheimer Akten nach Art. 48 ATSG, die Amts- und Verwaltungshilfe nach Art. 32 ATSG und weitere Bestimmungen in den Gesetzen zu den jeweiligen Versicherungen. Das Sozialversicherungsrecht beinhalte somit bereits eine sehr umfassende Regelung des Datenschutzes. Es stelle sich also die Frage, ob überhaupt Raum für die Anwendung des revDSG bestehe. Zum Verhältnis vom revDSG zum Sozialversicherungsrecht besage Art. 2 Abs. 3 revDSG jedoch, dass auf erstinstanzliche Verwaltungsverfahren die Bestimmungen des revDSG anwendbar seien. Zudem besage die bundesgerichtliche Rechtsprechung im Wesentlichen, dass die spezialgesetzlichen Bestimmungen des ATSG nicht ausschliessen, dass man sich auch auf das revDSG berufen könne.

[61] Abschliessend hielt der Referent fest, dass sich am Verhältnis zwischen DSG und Sozialversicherungsrecht mit der Revision nichts ändere und gemäss der Botschaft die «alte» Praxis weitergeführt werden solle. Eher vermutete der Referent, dass sich – weil mit dem neuen DSG das Thema Datenschutz wieder sehr aktuell und präsent sei – an der Bearbeitungspraxis der Sozialversicherungen insoweit etwas ändern könnte, als die Sensibilisierung für das Thema erhöht wurde. Zudem erhoffte er sich, dass betreffend Transparenz Fortschritte gemacht werden.

## 2.9. Auswirkungen revDSG auf das Arbeitsrecht (privatrechtliche und öffentlich-rechtliche Anstellungen)

[62] Im letzten Referat der Tagung ging Herr Prof. Dr. iur. KURT PÄRLI auf die Auswirkungen des revDSG auf das Arbeitsrecht ein. Er begann mit einem Zitat eines ehemaligen Datenschutzbeauftragten des Kantons Bern, der gewisse Datenschutzbestimmungen als Normeneunuchen bezeichnete und somit zum Ausdruck brachte, dass diese komplett wirkungslos seien. Der Referent sprach sich jedoch für eine korrektere Bezeichnung aus, wonach die Datenschutzbestimmungen auch eine symbolische Funktion haben würden. Wie man aus der Rechtssoziologie wisse, seien auch symbolische Bestimmungen nicht komplett nutzlos. Nichtsdestotrotz stelle sich die Frage, ob im Datenschutz der richtige Weg verfolgt werde. Auch hier untermalte der Referent seine Aussage mit einem Zitat, dieses Mal von Mark Twain: «Als wir unser Ziel aus den Augen verloren hatten, verdoppelten wir unsere Anstrengungen». Auch beim Datenschutz müsse man sich immer wieder daran erinnern, welches Ziel verfolgt wird. Es gehe nicht darum, den Datenschutz zu stärken – den Daten sei es egal, ob sie geschützt seien. Ziel sei es vielmehr, die Persönlichkeit und die Grundrechte der Menschen, deren Daten bearbeitet werden, zu schützen. Die DSGVO verfolge zudem noch einen weiteren Zweck, nämlich die Verwirklichung des Binnenmarktes durch einheitliches Datenschutzrecht, wobei den Mitgliedsstaaten im Bereich des Arbeitnehmerschutzes Freiraum für abweichende Regelungen offenstehe.

[63] Basierend auf dem arbeitsrechtlichen Unterordnungsverhältnis würden Ansprüche betreffend den Datenschutz entspringen. Bei Arbeitnehmerdaten handle es sich oft um besonders schützenswerte Personendaten. Wie bereits erwähnt, würden die Regeln des revDSG und des DSG bei Bearbeitung durch private Arbeitgeber und durch Arbeitgeber zur Anwendung gelangen, die als Bundesorgane gelten. Zu beachten sei jedoch, dass der Umstand, dass ein Arbeitgeber hinsichtlich gewisser Aspekte seiner Tätigkeit als Bundesorgan gelte, nicht bedeute, dass auch das Verhältnis zum Personal öffentlich-rechtlicher Natur sei. Kantonales Datenschutzrecht gelte für kantonale und kommunale Arbeitgebende.

[64] Der Referent unterstrich, dass das DSG nicht bei Datenbearbeitung für den persönlichen Gebrauch und nicht in Gerichtsverfahren gelte. Es gebe also keine doppelte Personalakte mehr zur Unterteilung von Daten, die bei einem Auskunftsbegehren herausgegeben werden und andere, die nicht herausgegeben werden. Wenn Daten nicht herausgegeben werden sollen, so sei dafür eine Rechtfertigung nach DSG notwendig. Betreffend Notizen zur Vorbereitung von Mitarbeitergesprächen hielt der Referent fest, dass es sich dabei solange nicht um Personendaten handle, als sie keine Person ausser derjenigen, die die Notizen gemacht hat sehe. Sobald eine andere Person einen Einblick in die Notizen erhalte, handle es sich um Personendaten und das DSG müsse eingehalten werden.

[65] Der Referent rief in Erinnerung, dass Personendaten durch eine Vielzahl von Normen zum Schutz der Persönlichkeit geschützt werden, bspw. durch Art. 8 [EMRK](#)<sup>40</sup>, Art. 28 [ZGB](#) und dessen Konkretisierung in Art. 328 und 328b [OR](#), Art. 26 der Verordnung 3 zum [ArG](#)<sup>41</sup>, strafrechtliche Bestimmungen und das DSG.

[66] In der Folge ging er vertieft auf Art. 328b [OR](#) ein. Demnach dürfe der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, sofern sie die Eignung für das Arbeitsverhältnis

betreffen oder die Durchführung des Arbeitsvertrages dies erfordere. Dies gelte bereits im Bewerbungsverfahren bis nach Beendigung eines allfälligen Arbeitsverhältnisses. Das Verhältnis zwischen Art. 328b OR und Art. 13 DSG bzw. 31 revDSG sei in der Lehre umstritten. Gemäss dem einen Teil der Lehre und der Ansicht des Referenten ist jede Datenbearbeitung ohne Arbeitsplatzbezug gem. Art. 328b OR unzulässig, da es sich dabei um eine Verbotsnorm handle. Gemäss dem anderen Teil der Lehre und dem BGer kommen die Rechtfertigungsgründe des DSG zur Anwendung.

[67] Der Referent wies darauf hin, dass gegenüber den Arbeitnehmenden im Arbeitsverhältnis eine Vielzahl von Überwachungsmöglichkeiten bestünden. Sollten diese Möglichkeiten ausgeschöpft werden, so würden sich Fragen hinsichtlich der Überwachung stellen. Art. 26 ArGV 3 halte fest, dass Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmenden überwachen sollen, nicht eingesetzt werden dürfen. Sofern die Überwachung aus legitimen Gründen notwendig sei, so sei sie derart auszugestalten, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmenden nicht beeinträchtigt würden. Da es sich also um eine Frage des Gesundheitsschutzes handle, eröffne sich der Anwendungsbereich des Mitwirkungsgesetzes, sodass die Überwachung mit der Arbeitnehmersvertretung besprochen werden müsse.

[68] Das revDSG habe mannigfaltige Auswirkungen auf das Arbeitsrecht. Zunächst sei festzuhalten, dass die Arbeitgeberin, die im Zusammenhang mit dem Arbeitsverhältnis Personendaten der Arbeitnehmenden bearbeite, Verantwortliche im Sinne des DSG sei und den entsprechenden Pflichten unterliege. Zudem seien die Betroffenenrechte minimal ausgebaut sowie neue Informationspflichten eingeführt worden, die die Einführung einer Datenschutzerklärung zur Information der Mitarbeitenden nach sich ziehen dürfte. Weitere Auswirkungen seien bspw. in der Verzeichnispflicht, dem Transfer von Daten ins Ausland, der Pflicht zur Datenschutz-Folgeabschätzung sowie der Sanktionsandrohung zu sehen.

[69] Hinsichtlich des Profilings warf der Referent die Frage auf, ob tatsächlich Änderungen vorgenommen wurden. Dabei legte er dar, dass die Bestimmung im DSG eher ergebnisorientiert, während diejenige im revDSG eher prozessorientiert sei. Bei Profiling mit erhöhtem Risiko sei eine ausdrückliche Einwilligung erforderlich, wobei Bundesorgane auch bei Profiling ohne erhöhtes Risiko eine gesetzliche Grundlage im formellen Sinn benötigen würden. Für das Arbeitsverhältnis bedeute dies, dass gewöhnliches Profiling ohne Einwilligung in den Schranken von Art. 328b OR zulässig sei. Bei Profiling mit erhöhtem Risiko sei die Einwilligung sowie Protokollierung nach Art. 4 DSV<sup>42</sup> erforderlich. Bei automatisierter Einzelentscheidung mit Ermessen, bei welcher dem Begehren der betroffenen Person nicht entsprochen werde, z.B. bei der Information, dass ein Bewerber eine Stelle nicht erhält, habe die betroffene Person gemäss Art. 21 revDSG Anspruch auf «menschliches Gehör», sofern die betroffene Person nicht ausdrücklich einwillige, dass die Entscheidung automatisiert erfolgt.

[70] Zum Auskunftsrecht hielt der Referent fest, dass im Verwaltungs- und Gerichtsverfahren, d.h. ab dem Zeitpunkt, in dem die Verfahrensordnung Anwendung findet, der Auskunftsanspruch nach DSG nicht mehr zur Anwendung komme, beispielsweise im Schlichtungsverfahren, im Arbeitsgerichtsprozess und im Schiedsverfahren. Nach Ansicht des Referenten komme das Auskunftsrecht nach DSG aber bei GAV-Streitigkeiten vor paritätischer

Kommission zur Anwendung, sofern ein Einzelunternehmer als natürliche Person betroffen sei. Gleiches gelte beim Verfahren vor dem kantonalen Arbeitsinspektorat und im Verfahren mit Sozialversicherungen bis zum Erlass einer Verfügung.

[71] Zusammenfassend hielt der Referent fest, dass die Änderungen im DSG mittelbare, unmittelbare und spezifische Auswirkungen auf die Bearbeitung von Arbeitnehmerdaten durch die Arbeitgeberin haben würden. Der Schutz der Arbeitnehmerpersonendaten erfolge aber auch durch arbeitsrechtliche Bestimmungen.

## **2.10. Diskussion mit den Referierenden des Nachmittags**

[72] Die erste Frage betraf die Vernichtung und Anonymisierung von Personendaten, wenn der Zweck nicht mehr gegeben ist. So wurde gefragt, ob es genüge, wenn man Zugriffsbeschränkungen, eine logische Löschung oder Archivierung einsetze, oder ob man die Daten gespeichert belassen könne, wobei die Identifizierbarkeit der betroffenen Person durch andere Massnahmen hinreichend reduziert würde. VASELLA führte aus, dass wenn die Daten verschlüsselt seien und man den Schlüssel wegwerfe, «crypto-shredding» vorliege und dies genüge. Dies stelle eine Anonymisierung dar, welche ausreiche, solange man die Daten auch wirklich anonymisiere. Datenschutzrechtlich gesprochen sei dies dasselbe wie Löschung. Wenn man lediglich den Zugang beschränke, dann stelle dies keine Löschung dar.

[73] Als nächstes wurde gefragt, ob Freizügigkeitsstiftungen, 3a-Stiftungen oder Wohlfahrtsfonds auch als Bundesorgane gelten, weil sie der staatlichen Aufsicht unterstellt seien. GEHRING erklärte, dass die Freizügigkeitsstiftungen grundsätzlich Aufgaben, die im Freizügigkeitsgesetz geregelt seien, wahrnehmen. Selbst wenn sie privatrechtlich organisiert seien, sei dies grundsätzlich zu bejahen, da sie eine öffentliche Aufgabe übernehmen. Dazu komme dann noch das Problem der Abgrenzung von Obligatorium und Überobligatorium, sodass man sich fragen könne, ob mit dem Überobligatorium die staatliche Durchführungsaufgabe aufhöre. Aus Praktikabilitätsüberlegungen müsse man zum Ergebnis kommen, dass sowohl der obligatorische Teil, als auch der überobligatorische Teil als Bundesorgan zu betrachten sei. PFAFFINGER stimmte ihrem Vorredner zu und unterstrich, dass dieser sozialversicherungsrechtliche Bereich äusserst komplex sei, da die Unterscheidungen schwierig seien, sodass sich ein pragmatischer Ansatz anbiete. VASELLA ergänzte, dass die Freizügigkeitseinrichtungen nach seiner Erfahrung davon ausgehen, dass sie Bundesorgane seien.

[74] Als nächstes wurde gefragt, ob bei öffentlichen Organen und KMUs die Rollen des DSB und des CISO in ein und derselben Person vereinbar sind. VASELLA führte aus, dass aus seiner Sicht der CISO auch DSB sein könne.

[75] In der Folge wurde gefragt, ob es Besonderheiten für DSB bei kantonalen Behörden gebe. VASELLA erklärte, dass dies eine Frage des kantonalen Rechts sei. Nach seinem Wissen sehen die kantonalen Gesetze keine Besonderheiten vor.

[76] Die nächste Frage zum Verzeichnis der Datenbearbeitungstätigkeiten richtete sich an PFAFFINGER. Diese habe ausgeführt, dass dieses Inventar auch dazu führe, die internen

Prozesse in einem Unternehmen besser zu verstehen. Dies stehe aus der Sicht der fragestellenden Person dem grundsätzlich pragmatischen Ansatz zur Umsetzung des revDSG entgegen. Wenn die Prozesse im Einzelnen aufgeschrieben werden müssen, führe dies zu einem riesigen Aufwand. So stelle sich die Frage, ob der Pragmatismus oder die umfassende Prozessdokumentation vorgehe. Aus der Sicht von PFAFFINGER sei es eine Tatsache, dass diese neuen Regelungen eine grosse Aufgabe darstellen würden, wenn auch die revDSG schlanker ausgefallen sei als die DSGVO. Das Inventar sei eine äusserst unbeliebte Aufgabe, aber die Inventaraufnahme sei, sofern die Voraussetzungen gegeben sind, eine Pflicht, wobei man hinsichtlich dem Detaillierungsgrad einen gewissen jedoch nicht beliebigen Pragmatismus walten lassen kann.

[77] Die nächste Frage betraf Art. 21 revDSG zur Anhörung und Information bei automatisierten Entscheidungen. So könne man, wenn man in einem Bewerbungsportal in eine automatisierte Entscheidung einwillige, die Anhörung und Information nicht mehr einfordern. VASELLA antwortete, dass er bezweifle, dass Arbeitgeber eine Art Blackbox einsetzen würden, um die Bewerber zu selektieren. Sollte eine automatische Vorselektion vorgenommen werden, so würden wohl diejenigen Bewerber aussortiert, die aus relativ naheliegenden Gründen nicht in Frage kämen. Ob die Einwilligung tatsächlich freiwillig sei, könne in Frage gestellt werden. Aber die Frage laufe seiner Ansicht nach ins Leere, da niemandem etwas weggenommen würde. PÄRLI ergänzte, dass aus seiner Sicht das Auskunftsrecht bestehen bleibe. Zudem bestehe gestützt auf das [GIG](#)<sup>43</sup> ein Begründungsanspruch bei einer Absage. Gleiches gelte im [BehiG](#)<sup>44</sup> gegenüber dem Bund. Zudem würde er im Rahmen des Bewerbungsverfahrens die Anforderungen an eine Einwilligung relativ hoch ansetzen.

[78] Als nächstes wurde gefragt, wieso ein DSB nicht im Verwaltungsrat sitzen könne, da der Verwaltungsrat für die Einhaltung des Gesetzes verantwortlich sei. Schliesslich liege es auf der Hand, dass diese Datenschutzfrage auch dem Verwaltungsrat angehängt wird. VASELLA erklärte, dass der Verwaltungsrat tatsächlich verantwortlich sei, wenn das DSG verletzt werde. Der DSB aber habe eine andere Funktion, nämlich die unabhängige Meinungsbildung, und könne deshalb nicht die Funktion eines Verwaltungsrates einnehmen. Der Verwaltungsrat dürfe die unabhängige Meinung des DSB aber jederzeit übersteuern.

[79] Als Letztes wurde angemerkt, dass das neue DSG sowohl den Stand der Technik als auch die Implementierungskosten als Erwägungspunkte bei der Festlegung von Massnahmen für die Gewährung der Datensicherheit zulasse. Auf diesem Gedanken aufbauend wurde die Frage gestellt, warum solche Erleichterungen für die Erfüllung der Datenschutzgrundsätze nicht gelten würden. VASELLA erläuterte, dass diese schon gelten, das DSG aber unter dem Konstruktionsfehler leide, dass eine Persönlichkeitsverletzung fingiert wird, wenn ein Grundsatz verletzt ist. Es gebe im Gegensatz zum übrigen Persönlichkeitsrecht keine Bagatellschwelle. Es handle sich um eine Art persönlichkeitsrechtlicher Vorfeldschutz. Jede Zweckverletzung sei zunächst persönlichkeitsverletzend, auch wenn sie harmlos sei oder der Person sogar nütze. In einem zweiten Schritt komme dann jedoch die Rechtfertigungsdiskussion. Dort könne dann eine Abwägung vorgenommen werden.

### **3. Ausblick**

[80] Wie erwähnt, verfolgte die Tagung das Ziel, einen Überblick über den Inhalt und die Hintergründe der kontroversen Revision des Bundesgesetzes über den Datenschutz zu verschaffen sowie Auswirkungen auf einzelne Rechtsgebiete näher zu beleuchten. Neben dem verschafften Überblick konnten die Referierenden eine erste Einschätzung zur Umsetzung und den Auswirkungen des revDSG abgeben. Zu einigen Punkten setzte sich jedoch auch die Einsicht durch, dass sich eine Vielzahl von Einzelfragen, wie beispielsweise zu den Strafbestimmungen des revDSG wohl erst zu einem späteren Zeitpunkt verlässlich beantworten lassen. Dies betrifft insbesondere auch Fragen im Schnittstellenbereich zum Arbeits- und Sozialversicherungsrecht. Je nach weiterem Verlauf bietet sich beispielsweise an der 7. Basler Sozialversicherungsrechtstagung<sup>45</sup> oder der 8. Basler Arbeitsrechtstagung<sup>46</sup> die Möglichkeit, auf Entwicklungen im Schnittstellenbereich zum DSG einzugehen.

---

MICHAEL BALMER, Advokat, MLaw, LL.M., ist Assistent und Doktorand am Lehrstuhl für Soziales Privatrecht der Universität Basel (Prof. Pärli). Zudem ist er bei Bangerter Friedli & Partner in Thun tätig.

JOËL KÄMPF, BLaw, ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Soziales Privatrecht der Universität Basel (Prof. Pärli).

Die Autoren danken den Referierenden herzlich für die Durchsicht des Beitrages und die wertvollen Rückmeldungen.

- 
- 1 Professor für Soziales Privatrecht (Professur Pärli) an der juristischen Fakultät der Universität Basel.
  - 2 Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020, SR 235.1, das revDSG tritt am 1. September 2023 in Kraft.
  - 3 Unabhängiger Datenschutzexperte; Präsident der Stiftung für Datenschutz und Informationssicherheit.
  - 4 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1.
  - 5 Internationale Zusammenarbeit, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/international/zusammenarbeit.html> zuletzt besucht am 11. Mai 2023.
  - 6 Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016, in Kraft seit 6. Mai 2018.
  - 7 Verordnung (EU) Nr. 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 (Datenschutz-Grundverordnung).
  - 8 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.
  - 9 Art. 5 lit. f revDSG.
  - 10 Art. 5 lit. g revDSG.
  - 11 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter.
  - 12 Vgl. dazu ADRIAN LOBSIGER, Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, SJZ 119/2023, S. 311 ff.
  - 13 Art. 1 revDSG.
  - 14 Professorin für Öffentliches Recht an der Juristischen Fakultät der Universität Basel.
  - 15 2016/679 vom 27. April 2016 (ersetzt EG-DSRL 95/46), in Kraft seit 25. Mai 2018.

- 16 Botschaft des Bundesrates vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, [BBI 2017 6941](#) (7056, 7059).
- 17 AMS – Arbeitsmarktservice Österreich.
- 18 Die SCHUFA sammelt bonitätsrelevante Daten über Personen und Unternehmen. Gegen Entgelt übermittelt sie die Daten Finanzinstituten, sodass diese die Kreditwürdigkeit von kreditinteressierten Personen überprüfen können. Um die Beurteilung der Kreditwürdigkeit zu vereinfachen, berechnet die SCHUFA mittels mathematisch-statistischem Verfahren automatisiert Wahrscheinlichkeitswerte über die Kreditwürdigkeit. Vgl. dazu: SIMON HENSELER, daten:recht, 17. März 2023, abrufbar unter: <https://datenrecht.ch/eugh-c-634-21-antraege-ga-kreditscore-der-schufa-als-automatisierte-entscheidung/>.
- 19 Schlussanträge des Generalanwalts Priit Pikamäe vom 16. März 2023, Rechtssache C-634/21.
- 20 Botschaft des Bundesrates vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, [BBI 2017 6941](#) (7057).
- 21 Botschaft des Bundesrates vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, [BBI 2017 6941](#) (7057).
- 22 Systeem Risico Indicatie (dt.: System Risiko Hinweis), SyRi sammelt Daten über Bürgerinnen und Bürger und wertet sie mit einem Algorithmus aus.
- 23 Dr. iur. DOMINIKA BLONSKI ist Datenschutzbeauftragte des Kantons Zürich.
- 24 Prof. Dr. iur. BEAT RUDIN ist Datenschutzbeauftragter des Kantons Basel-Stadt; Titularprofessor für Datenschutzrecht und Informationsrecht an der Juristischen Fakultät der Universität Basel.
- 25 Art. 43 f. Richtlinie 2016/680.
- 26 Art. 44 Abs. 1 lit. d Richtlinie 2016/680.
- 27 Professorin für Privatrecht, Informationsrecht (insb. Datenschutzrecht) sowie Recht und neue Technologien, Kalaidos Law School; Inhaberin von MP – only connect.
- 28 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, [SR 220](#).
- 29 Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, [SR 210](#).
- 30 Rechtsanwalt, Partner, Walder Wyss AG, Zürich.
- 31 Data Protection Officer.
- 32 Partner, Fachanwalt SAV Haftpflicht- und Versicherungsrecht, KSPartner Anwaltskanzlei, Zürich.
- 33 Unfallversicherung.
- 34 Regionale Arbeitsvermittlungszentren.
- 35 Alters- und Hinterlassenenversicherung.
- 36 Invalidenversicherung.
- 37 Ergänzungsleistungen.
- 38 Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) vom 6. Oktober 2000, [SR 830.1](#).
- 39 Verordnung über den Allgemeinen Teil des Sozialversicherungsrechts (ATSV) vom 11. September 2002, [SR 830.11](#).
- 40 Konvention zum Schutze der Menschenrechte und Grundfreiheiten, [SR 0.101](#).
- 41 Verordnung 3 zum Arbeitsgesetz (ArGV 3) vom 18. August 1993, [SR 822.113](#).
- 42 Verordnung über den Datenschutz (Datenschutzverordnung, DSV) vom 31. August 2022, [SR 235.11](#), tritt am 1. September 2023 in Kraft.
- 43 Bundesgesetz über die Gleichstellung von Frau und Mann (Gleichstellungsgesetz, GIG) vom 24. März 1995, [SR 151.1](#).
- 44 Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (Behindertengleichstellungsgesetz, BehiG) vom 13. Dezember 2002, [SR 151.3](#).

45 Diese findet am 10. November 2023 in Basel statt.

46 Diese findet am 2. Februar 2024 in Basel statt.

## 0 Kommentare

Es gibt noch keine Kommentare

*\* Pflichtfelder*

### Was ist Ihr Kommentar?

Titel:

Ihr Kommentar: \*

Name: \*

Senden

Ihr Kommentar wird durch eine Moderatorin bzw. einen Moderator geprüft und in Kürze freigeschaltet.