LeGes

Gabriel Gertsch / Marc Schinzel / Sandrine Wibin

40. Forum für Rechtsetzung vom 27. Oktober 2022

Neues Datenschutzgesetz und Datenschutz-Folgenabschätzung

Tagungsbericht zum 40. Forum für Rechtsetzung vom 27. Oktober 2022. Die Tagung drehte sich um das neue Datenschutzgesetz und um das Instrument der Datenschutz-Folgenabschätzung.

Beitragsart: Tagungsberichte

Zitiervorschlag: Gabriel Gertsch / Marc Schinzel / Sandrine Wibin, 40. Forum für Rechtsetzung vom 27. Oktober 2022, in: LeGes 33 (2022) 3

ISSN 2624-5477, leges.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

EDITIONS WEBLAW

[1] Dans le **premier exposé**, Fanny Matthey et Daniela Nüesch (collaboratrices scientifiques, Projets législatifs I, Office fédéral de la justice) ont présenté la **nouvelle loi du 25 septembre 2020 sur la protection des données** (nLPD/nDSG, RS 235.1) et la **nouvelle ordonnance du 31 août 2022 sur la protection des données** (OPDo/DSV, RS 235.11). En premier lieu, le *contexte ainsi que l'état de la révision du droit de la protection des données* ont été abordés. Le droit suisse de la protection des données ne peut évoluer dans un vase clos au vu de l'évolution technologique constante et du développement du droit européen dans le domaine. Il s'agit de la Directive européenne 2016/680 sur la protection des données dans le domaine du droit pénal, du Règlement européen général sur la protection des données 2016/679, et de la modernisation de la Convention 108 du Conseil de l'Europe sur la protection des données (Convention 108+) signée par la Suisse en 2019. Au niveau fédéral, la réforme du droit de la protection des données s'est concrétisée par l'adoption, en 2020, de la nLPD et, en 2022, de l'OPDo. Elles entreront en vigueur le 1*er* septembre 2023. Les lois cantonales dans le domaine devront également être mises à jour afin d'être compatibles avec la Convention 108+.

[2] En deuxième lieu, Matthey et Nüesch ont mis l'accent sur les *principales nouveautés issues de cette réforme*. Pour diverses raisons, le champ d'application matériel a été restreint, excluant dès lors les personnes morales (art. 2, al. 1 nLPD). Les données personnelles sensibles comprennent désormais notamment les « données sur l'origine ethnique », les « données biométriques identifiant une personne physique de manière univoque » ainsi que les « données génétiques » (art. 5, lit. c nLPD). Le « profil de la personnalité » (art. 3, lit. d LPD) a été remplacé par le « profilage » (art. 5, lit. f nLPD) et le « profilage à risque élevé » (art. 5, lit. g nLPD). Par ailleurs, des principes alliant technologie et droit, par exemple le « Privacy by design and by default » (art. 7 nLPD), viennent renforcer la protection des données. Les compétences requises du conseiller ou de la conseillère à la protection des données des organes fédéraux ont été révisées (art. 10, al. 3 nLPD et 25 ss. OPDo) et des registres d'activité de traitement se sont substitués à la déclaration des fichiers (art. 12 nLPD). En outre, les dispositions sur la communication de données à l'étranger prévoient dorénavant quel est le contenu minimal des garanties jugées suffisantes pour qu'un niveau de protection approprié soit assuré (art. 16, al. 2 nLPD et art. 9 ss. OPDo) ainsi que la compétence du Conseil fédéral pour déterminer (art. 16, al. 1 nLPD), sur la base des critères de l'art. 8 OPDo, quels sont les Etats présentant un niveau de protection des données adéquat (annexe 1 OPDo). Les obligations du responsable de traitement ont également été étendues. Un devoir d'information lors de décisions automatisées (art. 21 nLPD) et l'obligation d'établir une analyse d'impact dans certaines situations (art. 22 nLPD, art. 14 OPDo) ont notamment été instaurés. Enfin, il faut noter des modifications ponctuelles se rapportant aux droits de la personne concernée ainsi que de nouvelles exigences relatives aux bases légales pour le traitement des données personnelles (art. 34 ss. nLPD). Les pouvoirs d'enquête (art. 49 s. nLPD) et les compétences décisionnelles (art. 51 nLPD) du Préposé fédéral à la protection des données et à la transparence (PFPDT/EDÖB) ont eux aussi été élargis. Pour plus de détails, l'Office fédéral de la justice met à disposition un Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux (disponible à l'adresse : www.bj.admin.ch, Etat & Citoyen, Instruments de légistique).

[3] Dans un troisième temps, Matthey et Nüesch ont expliqué *comment certaines de ces modifications ont été mises en œuvre de manière concrète*. Premièrement, lors de la phase précédant le traitement des données, au moment de l'approbation du projet ou lors de la décision de le développer, l'organe fédéral responsable doit annoncer au PFPDT si le projet nécessite un traitement automa-

tisé des données personnelles (art. 31 OPDo). Deuxièmement, l'adoption de bases légales selon les art. 34 ss. nLPD, et pour les personnes morales selon les art. 57*r* ss. de la Loi sur l'organisation du gouvernement et de l'administration révisée (RS 172.010, dans le cadre de la nLPD [FF 2020 7681 ss.]), est obligatoire pour autoriser un traitement des données conforme à la Constitution fédérale (art. 13, art. 36 et art. 5 Cst. [RS 101]). A noter que les organes fédéraux impliqués dans le traitement de données de personnes morales ont un délai de cinq ans dès l'entrée en vigueur de la nLPD pour créer les normes légales nécessaires (art. 71 nLPD). De plus, chaque office doit en principe être doté d'un conseiller ou d'une conseillère à la protection des données, qui agit de manière indépendante (art. 25 ss. OPDo) et qui effectue diverses tâches, dont le contrôle du traitement des données (art. 26, al. 2, lit. a OPDo). Les organes fédéraux tiennent un registre des activités de traitement et doivent le déclarer au PFPDT (art. 12 nLPD). Enfin, après le traitement des données personnelles, les art. 24 nLPD et 15 OPDo imposent d'annoncer toute violation de la sécurité des données au PFPDT et, éventuellement, à la personne concernée.

[4] Dans le **deuxième exposé**, Véronique Jaquet et Daniela Nüesch (collaboratrices scientifiques, Unités Législation I et Projets législatifs I, Office fédéral de la justice) ont abordé le sujet de « **l'élaboration de bases légales dans le domaine de la protection des données** » et présenté le *nouveau guide de législation en matière de protection des données* (disponible à l'adresse : www.bj.admin.ch, Etat & Citoyen, Instruments de légistique). Ce guide propose entre autres une check-list pour les praticiens. Le développement de la digitalisation domine de nombreux projets législatifs et avec lui, l'augmentation de la masse des données traitées par les organes fédéraux constituent de nouveaux défis. Parmi eux, le respect du droit à l'autodétermination informationnelle, qui découle des art. 13 Cst. et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (RS 0.101), doit être assuré. Celui-ci confère à l'individu une certaine maîtrise sur ses propres données. Toute restriction à ce droit fondamental doit respecter les conditions de l'art. 36 Cst., soit notamment figurer dans une base légale, qui doit être formelle en cas de restriction grave. Ainsi, la gravité possible du risque d'atteinte aux droits fondamentaux constitue le fil conducteur lors de l'élaboration d'un acte normatif. A cet égard, les art. 34 et 36 nLPD concrétisent le principe de légalité (art. 5 et 164 Cst.) et fixent les exigences devant être respectées par les dispositions du droit sectoriel pour permettre de traiter ou de communiquer des données.

[5] Jaquet et Nüesch ont par la suite présenté la *phase initiale de l'élaboration d'un acte législatif en matière de protection des données*. Elle consiste à analyser les risques inhérents au traitement de données projeté, à l'aide de la méthode de gestion de projets HERMES et de son concept de Sûreté de l'information et protection des données (SIPD), ainsi que par le biais d'une analyse d'impact (art. 22 nLPD). A noter qu'un projet de directives du Conseil fédéral est actuellement en train d'être développé, qui a pour but de mettre en œuvre l'analyse d'impact en matière de protection des données personnelles (*Datenschutz-Folgenabschätzung*) par les organes fédéraux ainsi que de coordonner cette dernière avec la procédure législative. Ces futures directives prévoient entre autres de joindre l'analyse d'impact en matière de protection des données personnelles au projet lors de la première consultation des offices et d'en faire figurer les résultats dans le message du Conseil fédéral.

[6] Puis, Jaquet et Nüesch ont expliqué que le *niveau de la base légale* dépend de la gravité du risque d'atteinte aux droits fondamentaux, qui peut notamment résulter du type de données traitées, de la finalité de leur utilisation ou de leur mode de traitement (art. 34, al. 2 nLPD). Ainsi, selon l'art. 34, al. 2 nLPD, une base légale formelle est indispensable pour permettre le

traitement de données sensibles, d'un profilage (art. 5, lit. f et g nLPD) ou lorsque la finalité ou le mode du traitement de données personnelles est susceptible de porter gravement atteinte aux droits fondamentaux. Néanmoins, l'art. 34, al. 3 nLPD prévoit un assouplissement de l'exigence de base légale au sens formel pour le traitement de données sensibles ou pour l'élaboration d'un profilage, lorsque le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel, et que la finalité du traitement ne présente pas de risque particulier pour les droits fondamentaux de la personne concernée. S'agissant de la *densité normative*, le principe de la légalité requiert un degré suffisant de concrétisation des normes légales. Doivent ainsi figurer dans la loi : l'organe fédéral responsable du traitement, les catégories de données traitées et la finalité du traitement. En outre, dans certains cas, la base légale devrait aussi fournir des indications sur le mode de traitement, en particulier lorsque des moyens technologiques non reconnaissables pour l'administré sont utilisés. La communication de données, qui est une forme particulièrement sensible du traitement de données, doit être prévue dans une base légale spécifique et mentionner qui communique, dans quel but, quelles catégories de données et selon quel mode de communication (art. 36 nLPD).

[7] Jaquet et Nüesch se sont finalement penchées sur *certains aspects nouveaux pour la ou le légiste*. Elles ont abordé l'accès en ligne, caractérisé par le principe du « self-service » (procédure d'appel, *Abrufverfahren*) qui n'est plus expressément réglé dans la nLPD. Il s'agit néanmoins d'un mode de communication qui, à ce titre, doit figurer dans la loi, et qui présente un risque accru d'atteinte aux droits fondamentaux. L'accès en ligne à des données sensibles ou à des profilages reste prévu par une loi au sens formel. De plus, en ce qui concerne la règlementation, l'accent est moins mis sur l'architecture informatique et davantage sur les flux de données ainsi que sur l'accès en ligne. Lorsque des données sont traitées pour exécuter plusieurs tâches légales, la règlementation doit être différenciée selon ces dernières. Enfin, en cas de passage d'une solution « en silos » (systèmes informatiques séparés) à une solution de systèmes intégrés, l'analyse des risques qui en découlent pour les personnes concernées doit être approfondie, en collaboration avec les informaticiens, afin de pouvoir déterminer le niveau normatif et la densité des bases légales à élaborer.

[8] Nach der Pause hielt Adrian Lobsiger, der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, ein **Einführungsreferat** zum **neuen Instrument der Datenschutz-Folgenabschätzung** (DSFA). Die DSFA beschreibt eine geplante Datenbearbeitung, bewertet das Risiko der Bearbeitung für die Persönlichkeit oder die Grundrechte der Betroffenen und sieht Massnahmen zu deren Schutz vor. Nach dem nDSG ist der Verantwortliche verpflichtet, vor einer Datenbearbeitung eine DSFA zu erstellen, wenn die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Ein solches kann sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergeben und liegt namentlich vor, wenn umfangreiche Bearbeitungen besonders schützenswerter Personendaten vorgenommen oder systematisch umfangreiche öffentliche Bereiche überwacht werden (Art. 22 Abs. 1–3 nDSG). Ergibt die DSFA, dass die geplante Bearbeitung trotz der vorgesehenen Schutzmassnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person birgt, so hat der Verantwortliche vorgängig die Stellungnahme des EDÖB einzuholen. Dieser teilt dem Verantwortlichen innert zwei Monaten seine Einwände gegen die geplante Bearbeitung mit und schlägt ihm gegebenenfalls geeignete risikomindernde Massnahmen vor (Art. 23 Abs. 1-3 nDSG).

[9] In seinem Referat wies der Beauftragte zunächst darauf hin, dass die *Pflicht zur Vorlage der DSFA* nur dann bestehe, wenn *trotz* des Ergreifens risikomindernder Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen besteht. (Im Unterschied da-

zu besteht die Vorlagepflicht bei einer wörtlichen Auslegung der Datenschutz-Grundverordnung der Europäischen Union schon, wenn die Bearbeitung ohne risikomindernde Massnahmen ein hohes Risiko birgt.) Im Lichte dieses Grundentscheids des Gesetzgebers sei es unzulässig, eine DSFA mit dem Ziel durchzuführen, die geprüfte Datenbearbeitung möglichst nicht mit der Bewertung «hohes Risiko» zu bewerten, um so die Vorlagepflicht und das Ergreifen weitergehender Massnahmen zu vermeiden. Der gesetzgeberische Auftrag verlange vielmehr, es transparent auszuweisen, wenn als Endresultat der DSFA ein Risiko resultiert, welches die zu dessen Minderung vorgesehenen Massnahmen nicht auf ein Niveau zu senken vermögen, das nicht mehr als hoch bezeichnet werden muss.

[10] Der Beauftragte betonte weiter, dass zwar eine grosse Nachfrage nach *Software-unterstützten Checklisten und Tools* bestehe, welche die Abschätzung der Risiken erleichtern. Allerdings verlange die Durchführung einer DSFA nach einer wertenden Evaluation der Gesamtrisiken, die nicht vollständig an eine Software-unterstützte Analyse delegiert werden könne. Vielmehr sei bei der DSFA zu unterscheiden zwischen Risiken, die durch risikomindernde Massnahmen gänzlich oder immerhin teilweise beeinflussbar sind, und solchen, die durch Massnahmen nicht oder kaum beeinflussbar sind. In Bezug auf erstere Gruppe könne sich der Einsatz Software-unterstützter, quantitativer Methoden als sinnvoll erweisen. Hingegen sei es bei kaum oder gar nicht beeinflussbaren Risiken nicht immer möglich, angemessene Massnahmen zu treffen oder das Risiko überhaupt zu kalkulieren. Gerade bei der Bewertung systemischer Risiken, wie sie z.B. von fremden Rechtsordnungen ausgehen können, stünden Verantwortliche deshalb in der Pflicht, sich nicht nur auf Expertisen zu verlassen. Vielmehr müssten sie selber über die abschliessende *Bewertung des Gesamtrisikos entscheiden.* Angesichts der recht generell formulierten Begrifflichkeiten des Gesetzes komme ihnen dabei ein erheblicher Ermessensspielraum zu. Ergebe sich aus der abschliessenden Bewertung eine Vorlagepflicht, so bestehe die Rolle des EDÖB zunächst darin, zu prüfen, ob der Verantwortliche sein Ermessen pflichtgemäss ausübte. Habe der EDÖB Einwände gegen die geplante Bearbeitung, kann er Massnahmen zu deren datenschutzkonformen Ausgestaltung vorschlagen (Art. 23 Abs. 3 nDSG). Das Verfahren der Vorlage sei zu unterscheiden vom Aufsichtsverfahren nach den Art. 49 ff. nDSG, in dessen Rahmen der EDÖB entsprechende Massnahmen *verfügen* kann (Art. 50 Abs. 1 nDSG) und welches gegebenenfalls an ein Vorlage-Verfahren anschliesst.

[11] Im vierten **Referat** des Nachmittags hielt Tobias Naef (Mitarbeiter der Datenschutzbeauftragten des Kantons Zürich) eine Präsentation zur **Datenschutz-Folgenabschätzung im Rahmen der Zollgesetzrevision**. Das Zollgesetz vom 18. März 2005 (ZG, SR 631.0) befindet sich zurzeit in Totalrevision. Dabei soll das ZG zu einem reinen Abgabenerlass reduziert werden, während die Aufgaben des Bundesamts für Zoll und Grenzsicherheit (BAZG) in einem Neuerlass (BAZG-Vollzugsaufgabengesetz, abrufbar unter: https://www.efd.admin.ch/efd/de/home/das-efd/nsb-news_list.msg-id-90126.html) geregelt werden sollen. Der Bundesrat hat die entsprechenden Gesetzesentwürfe am 24. August 2022 verabschiedet und ans Parlament überwiesen. Mit diesem Rechtsetzungsvorhaben will er die Rechtsgrundlagen für das Digitalisierungs- und Transformationsprogramm (DaziT) schaffen, mit dem sämtliche Zoll-, Abgaben und Kontrollprozesse des BAZG vereinheitlicht und digitalisiert werden sollen. Täglich überqueren über 2 Millionen Personen, über 1 Million Fahrzeuge und 24'000 Lastwagen die Schweizer Grenze. Im Zuge der Kontrolle dieses Personen- und Warenverkehrs nimmt das BAZG in grossem Umfang Bearbeitungen besonders schützenswerter Personendaten vor und überwacht systematisch umfangreiche öffentliche Bereiche. Im Rahmen der Zollgesetzrevision hat das BAZG aus diesem

Grund eine umfassende DSFA zur Bewertung der dabei entstehenden Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen erstellt.

[12] Naef, der in seiner damaligen Stellung als Jurist für Digitalisierung und Datenschutz beim BAZG an diesen Analysen aus datenschutzrechtlicher Perspektive intensiv mitgewirkt hat, präsentierte seine *wichtigsten Erkenntnisse zur praktischen Erarbeitung einer DSFA*. Er fokussierte dabei auf folgende Themen: (*i*). Zur Erstellung einer DSFA werde ein interdisziplinäres Team benötigt, dem ausreichend Zeit gewährt werden müsse. (*ii*). Die DSFA müsse als feststehende Etappe nicht nur im Prozess der Rechtsetzung, sondern auch im Prozess der technischen Entwicklung angesehen werden, denn das Ergreifen risikomindernder Massnahmen setze unter Umständen Rahmenbedingungen für die technische Entwicklung. (*iii*.) Neben den Risiken, die sich aus der Liste der geplanten Datenbearbeitungen ergeben, seien auch systemische Risken zu berücksichtigten, die etwa dadurch entstehen können, dass eine Person in der flexiblen Organisation mehrere Funktionen wahrnimmt. Bei der Evaluation systemischer Risiken sei der Austausch mit der Aufsicht zu suchen. (*iv*.) Die Risikobewertung anhand feststehender Schemata (etwa entlang der Dimensionen Eintrittswahrscheinlichkeit versus Schwere des möglichen Schadens) eliminiere nicht den subjektiven Aspekt der Bewertung und sei nicht in jedem Fall zielführend. (*v*.) Bei der Evaluation von risikomindernden Massnahmen sei Mut gefragt, auch kreative Massnahmen in Betracht zu ziehen. Diese sollten konkret auf das spezifische Datenschutzrisiko eingehen und nicht nur generische (aber trotzdem wichtige) Massnahmen wie Schulungen und Zugriffskonzepte umfassen. Nur so könne man dem Prinzip «Privacy by design» wirklich Rechnung tragen. (*vi*.) Schliesslich sei es nicht möglich, durch risikomindernde Massnahmen jedes Risiko für die Persönlichkeit oder die Grundrechte vollständig auszuschliessen. Es sei deshalb notwendig und akzeptabel, Restrisiken in Kauf zu nehmen. Dazu müsse man die Restrisiken jedoch *kennen* – eine Gesamtbewertung des Restrisikos sei mit anderen Worten nur auf der Basis einer vollständigen Risikoevaluation möglich.

[13] In der abschliessenden **Podiumsdiskussion**, moderiert von Monique Cossali (Leiterin Fachbereich Rechtsetzungsprojekte I, stv. Leiterin Direktionsbereich Öffentliches Recht, Bundesamt für Justiz), diskutierten David Rosenthal (Partner bei der Anwaltskanzlei Vischer) sowie die Referenten Lobsiger und Naef über die Chancen und Risiken, Stärken und Schwächen des Instruments der Datenschutz-Folgenabschätzung, wobei auch Plenumsfragen möglich waren. Rosenthal, der selber auch schon DSFA für Bundesorgane erstellt hat, schloss sich eingangs den Erkenntnissen aus dem vierten Referat an. Entscheidend sei, dass die DSFA die *unerwünschten negativen Folgen*, *die eine Datenbearbeitung für den Betroffenen haben kann*, *umfassend* – und aus der Warte des Betroffenen, nicht des Verantwortlichen – *beurteilt*. Dabei könnten diese negativen Folgen beliebiger Art sein (z.B. Rufschädigung, Jobverlust, Gefühl der Angst, Diskriminierung usw.). Die Verletzung der Grundrechte gehöre im Falle von staatlichen Organen allerdings auch dazu, selbst wenn die Datenbearbeitung sonst keine negativen Folgen hat.

[14] Darauf angesprochen, wie die Praxis mit dem nDSG und dem Instrument der DSFA zurechtkommen werde, erwiderte Lobsiger, dass Datenschutzbeauftragte in der Schweiz keine Berührungsängste hätten, weil ihnen anders als in der EU – auch wesentliche Beratungsaufgaben zukommen. Der Gesetzgeber hätte die Regelung der DSFA dem Bundesrat überlassen oder die Kriterien für die Erstellung einer DSFA engmaschiger fassen können. Darauf verzichtete er jedoch und räumte den Verantwortlichen Spielräume ein. Am Ende obliege die Beurteilung eines Projekts den Verantwortlichen. Auch Naef betonte die Bedeutung des Austauschs zwischen Verantwortlichen und Datenschutzbeauftragten. Wie im Bund sehe auch das Zürcher Gesetz über

die Information und den Datenschutz (LS 170.4) die Erstellung von DSFA vor. Wenn sie in der DSFA besondere Risiken erkennen, so müssten die Verantwortlichen das betreffende Projekt der Datenschutzbeauftragten zur Vorabkontrolle vorlegen.

[15] Ein wichtiges Diskussionsthema war die Frage, *wie datenschutzrechtliche Risiken in der Praxis identifiziert und beurteilt* werden sollen. Das Publikum interessierte insbesondere, ob in der Praxis *Checklisten* bei der Erstellung einer DSFA hilfreich sein könnten. Cossali und Lobsiger informierten das Publikum, dass das Bundesamt für Justiz in Zusammenarbeit mit dem EDÖB, der Bundeskanzlei und dem National Cyber Security Center entsprechende Hilfsmittel für Bundesorgane erarbeiten werde. Lobsiger mahnte gleichzeitig, solche Listen seien immer nur Hilfsmittel und würden den Verantwortlichen nicht davon entbinden, das Risiko wertend zu evaluieren. Das sei nur in Kenntnis der gesetzgeberischen Weichenstellungen und unter Berücksichtigung der systemischen Risiken zu leisten. Rosenthal fügte an, dass er bereits Checklisten als Hilfestellung für die Praxis entwickelt habe und diese online zur Verfügung stellen werde. Sie seien nicht als fixe Vorgehensraster gedacht, sondern könnten den Verantwortlichen helfen, die richtigen Fragen zu stellen: Welche Risiken sind zu bedenken? Wie gross ist die Wahrscheinlichkeit ihres Eintritts? Checklisten hätten zudem den Vorteil, dass sie den Verantwortlichen zwingen, sich bei der Beurteilung an eine vorgängig festgelegte Methode zu halten, was zu besser nachvollziehbaren Ergebnissen führe als ein Entscheiden «aus dem Bauch heraus».

[16] Lobsiger und Naef wiesen schliesslich darauf hin, dass datenschutzrechtliches Denken oft mit informationsrechtlichem Denken vermischt werde. Klassifizierungen wie «geheim» oder «vertraulich» würden nicht *per se* bedeuten, dass datenschutzrechtliche Risiken vorliegen. Sind keine persönlichkeitsrelevanten Daten betroffen und drohen keine Grundrechtseingriffe, so seien sie aus einer datenschutzrechtlichen Perspektive irrelevant. Dagegen könnten weit verbreitete, öffentlich zugängliche Kommunikationsplattformen aufgrund ihrer vielfältigen Bezüge zum Persönlichkeitsschutz datenschutzrechtlich relevant sein.

[17] Sämtliche Tagungsunterlagen finden sich auf der Homepage des Bundesamts für Justiz; abrufbar unter: https://www.bj.admin.ch/bj/de/home/staat/legistik/rechtsetzungsforum/veranstaltungsthemen/40.html. Das 41. Forum für Rechtsetzung findet voraussichtlich am 27. April 2023 statt und dreht sich um die Digitalisierung.

Dr. sc. Gabriel Gertsch, wissenschaftlicher Mitarbeiter, Fachbereich Rechtsetzungsbegleitung I, Bundesamt für Justiz.

Dr. iur. Marc Schinzel, wissenschaftlicher Mitarbeiter, Fachbereich Rechtsetzungsprojekte I, Bundesamt für Justiz.

Sandrine Wibin, MLaw, wissenschaftliche Praktikantin, Fachbereich Rechtsetzungsprojekte II, Bundesamt für Justiz.