



ONLINEKOMMENTAR
DER FREI ZUGÄNLICHE
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

Art. 22 DSGVO

Eine Kommentierung von Rehana C. Harasgama / Dario Haux

Herausgegeben von Thomas Steiner / Anne-Sophie Morand / Daniel Hürlimann

Stand der Bearbeitung: 20.08.2023

PDF erstellt am: 05.10.2026

DOI: 10.17176/20230820-140438-0

ZITIERVORSCHLAG

Rehana C. Harasgama/Dario Haux, Kommentierung zu Art. 22 DSGVO, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Kurzzitat: OK-Harasgama/Haux, N. XXX zu Art. 22 DSGVO.

Art. 22 Datenschutz-Folgenabschätzung

¹ Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

² Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

- a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
- b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

³ Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

⁴ Von der Erstellung einer Datenschutz-Folgenabschätzung ausgenommen sind private Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind.

⁵ Der private Verantwortliche kann von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er ein System, ein Produkt oder eine Dienstleistung einsetzt, das oder die für die vorgesehene Verwendung nach Artikel 13 zertifiziert ist, oder wenn er einen Verhaltenskodex nach Artikel 11 einhält, der die folgenden Voraussetzungen erfüllt:

- a. Der Verhaltenskodex beruht auf einer Datenschutz-Folgenabschätzung.

b. Er sieht Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Person vor.

c. Er wurde dem EDÖB vorgelegt.

GLIEDERUNG

In Kürze	4
I. Allgemeines.....	4
A. Überblick	4
B. Entstehungsgeschichte	5
C. Normzweck.....	7
II. Inhalt.....	8
A. Adressaten	8
B. Das hohe Risiko.....	8
C. Durchführung der DSFA.....	10
1. Einführung.....	10
2. Ablauf.....	10
3. Durchführung einer gemeinsamen DSFA	13
4. Organisation	13
D. Ausnahmen.....	14
III. Verletzung der Pflicht zur Durchführung einer DSFA.....	14
IV. Herausforderungen und praktische Relevanz.....	15
V. Vergleich mit dem EU-Recht	16
Literaturverzeichnis.....	17
Materialienverzeichnis	18

IN KÜRZE

Art. 22 DSG regelt die Voraussetzungen zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Der Artikel ist an die Bestimmungen der Art. 35 f. DSGVO angelehnt. Mithilfe der datenschutzrechtlichen Risikoanalyse soll bei einer geplanten Datenbearbeitung, welche voraussichtlich zu hohen Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt, vorgängig eine Bewertung dieser Risiken vorgenommen werden. Damit sollen vor Beginn der Datenbearbeitung angemessene Massnahmen zur Risikominimierung definiert und ergriffen werden. Ein hohes Risiko liegt gemäss Gesetz insbesondere bei (i) der umfangreichen Bearbeitung besonders schützenswerter Daten (z.B. Gesundheitsdaten) oder (ii) der systematischen umfangreichen Überwachung von öffentlichen Bereichen (z.B. der Installation von Überwachungskameras in einem Park) vor. Die Liste der in Art. 22 genannten hohen Risiken ist jedoch nicht abschliessend. Typischerweise werden sich hohe Risiken durch den Einsatz neuer Technologien und Prozesse ergeben, wie z.B. algorithmische Systeme («Künstliche Intelligenz»), DLT-Systeme oder Big Data Analytics. Die geplante Bearbeitungstätigkeit kann jedoch auch aufgrund anderer Faktoren als hohes Risiko für die Persönlichkeit oder für die Grundrechte der betroffenen Personen eingestuft werden, z.B. weil Kinder betroffen sind, automatisierte Einzelentscheide gefällt oder Personendaten an ein komplexes Netzwerk von Auftragsbearbeitern weitergegeben werden. Direkt strafbewehrt ist die Verletzung der Pflicht nach Art. 22 jedoch nicht.

I. ALLGEMEINES

A. Überblick

- 1 Das revidierte DSG sieht im Gegensatz zur DSGVO keine allgemeine Rechenschaftspflicht vor. Eingeführt wurde jedoch die **Pflicht, eine Datenschutz-Folgenabschätzung (DSFA) für Datenbearbeitungen mit hohen Risiken durchzuführen**, was im Endeffekt eine Rechenschaftspflicht für bestimmte Datenbearbeitungen darstellt. Die DSFA ist nicht nur auf Bundesebene, sondern auch in zahlreichen Kantonen gesetzlich verankert. In Zürich findet sich die entsprechende Pflicht beispielsweise in § 10 Abs. 1 IDG, in Verbindung mit einer Vorabkontrolle (vgl. zum Vorabkonsultationsverfahren auf Bundesebene die Kommentierung zu Art. 23).
- 2 Die DSFA wird mit der Revision im Schweizer Datenschutzgesetz für alle Verantwortlichen verankert – für **private Verantwortliche sowie für Bundesorgane**. Aus diesem Grund umfasst der Wortlaut der Bestimmung sowohl hohe Risiken für die Persönlichkeit (für die Datenbearbeitung durch private Verantwortliche) als auch für die Grundrechte (für die Datenbearbeitung durch Bundesorgane) der betroffenen Personen. Die DSFA dient dazu, die potenziellen Risiken einer geplanten Datenbearbeitung frühzeitig zu erkennen, zu bewerten und risikomindernde Massnahmen zu definieren sowie zu implementieren. Diese Schritte müssen vorgenommen werden, bevor mit der geplanten Datenbearbeitung begonnen wird (siehe zum Zweck weitergehend N. 8 ff.). Die Anwendung des Art. 22 ist Ausfluss des risikobasierten Ansatzes des DSG, der in der Umsetzung der Art. 22 und 23 besonders deutlich in Erscheinung tritt.¹
- 3 Der DSFA wird eine steigende Bedeutung zugesprochen. Begründet wird dies vor allem mit der zunehmenden Verbreitung von fortgeschrittenen algorithmischen Systemen² oder vergleichbaren neuen Technologien in allen Lebensbereichen, wie z.B. Distributed-Ledger-Technologien oder dem

1. Siehe dazu Lobsiger, S. 312.

2. Siehe zu den technischen Grundlagen Früh/Haux, passim.

Internet der Dinge.³ Bei zahlreichen der genannten Anwendungen sind Personendaten betroffen und es ist nicht auszuschliessen, dass die Persönlichkeit oder die Grundrechte der betroffenen Personen beim Einsatz dieser Technologien hohen Risiken ausgesetzt sind. In diesen Fällen wird somit eine DSFA erforderlich. Der oder die Verantwortliche wird dazu angehalten, sich vorgängig analytisch mit der geplanten Datenbearbeitung auseinanderzusetzen.⁴ Gleichzeitig ist zu beachten, dass insbesondere bei algorithmischen Systemen bestimmte Vorgänge kaum nachvollziehbar sind und ihr Potenzial nicht abschliessend definierbar ist (sog. «**Black Box**» **Problematik**).⁵ Entsprechend lassen sich die bearbeiteten Personendaten und Bearbeitungszwecke im Einzelfall ggf. nicht klar definieren und abgrenzen, zumal oftmals viele Auftragsbearbeiter und andere Dritte zur Bearbeitung der Daten hinzugezogen werden und die den Systemen zugrundeliegenden Big Data-Analysen ein noch nicht absehbares Potenzial bieten. So kann es sich bei der DSFA in diesen Fällen durchaus um ein «ambitiöse(s) Unterfangen»⁶ handeln, deren Durchführung jedoch umso ernster genommen werden muss.⁷ Je besser dies gelingt, desto eher kann ein vertrauenswürdiger und transparenter Einsatz von solchen Technologien gewährleistet werden.⁸

B. Entstehungsgeschichte

- 4 Das Schweizer DSG sah vor der Totalrevision keine explizite Pflicht für private Datenbearbeiter vor, eine DSFA durchzuführen. Bundesorgane waren jedoch bereits unter dem alten DSG verpflichtet, dem internen Datenschutzverantwortlichen oder dem EDÖB Projekte zu melden, welche die automatisierte Bearbeitung von Personendaten zum Inhalt hatten (Art. 20 Abs. 2 aVDSG). Diese Meldung war damit verbunden, dass die jeweiligen Bundesbehörden für die geplante Datenbearbeitung ein Informationssicherheits- und Datenschutz-Konzept («ISDS-Konzept») erstellen mussten. Dieses Vorgehen war gemäss Botschaft mit der DSFA vergleichbar.⁹ Für private Verantwortliche wurde die DSFA in Einzelfällen u.U. auf Art. 7 aDSG gestützt.¹⁰ Zudem erforderten die Datenbearbeitungsgrundsätze schon immer, dass die **Folgen einer Datenbearbeitung stets mitberücksichtigt** werden müssen.¹¹ Ausserdem verlangte der EDÖB im Rahmen seiner Beratung von privaten Datenbearbeitern in bestimmten Fällen bereits in der Vergangenheit die Vorlage einer DSFA, insbesondere wenn es sich um risikoreiche Datenbearbeitungen handelte. Bedingt wurde die Einfügung der Pflicht zur Durchführung einer DSFA nicht zuletzt durch EU-weite Vorgaben gemäss Art. 8^{bis} E-SEV 108 sowie Art. 27 f. der Richtlinie (EU) 2016/680.¹² Art. 35 f. DSGVO enthält analoge Vorschriften für Verantwortliche, die in den Anwendungsbereich der DSGVO fallen, aber die Schweiz im Rahmen der Rechtssetzung nicht direkt verpflichten.
- 5 International baut das Instrument auf einer **langjährigen Vorgeschichte auf, die bis in die 1990er Jahre zurückreicht**.¹³ In diesem Zeitraum wurden sowohl in der EU-Datenschutzrichtlinie (Art. 20, Richtlinie 95/46/EG), welche von der DSGVO abgelöst wurde, als auch im angelsächsischen Raum erste «Privacy Impact Assessments»¹⁴ entwickelt. Weitere EU Mitgliedstaaten wie Frankreich¹⁵ und Deutschland haben aufgrund der Richtlinie 95/46/EG entsprechende Empfehlungen herausgegeben.¹⁶

3. Klaus, S. 86 f.; Schönbachler, S. 190.

4. Schönbachler, S. 190.

5. Siehe dazu mit Bezug auf die Vorgaben der DSGVO, Schürmann, S. 317.

6. Lobsiger, S. 312.

7. Zum Umgang mit neuen Technologien im Datenschutzrecht als «faktische Herausforderung» siehe Pfaffinger, S. 484 ff.

8. Siehe in diesem Sinne auch Schürmann, S. 321.

9. Botschaft 2017, S. 7059.

10. Vasella/Sievers, S. 46.

11. Schönbachler, S. 189 f.

12. SHK-Blonski, Art. 22 DSGVO N. 2.

13. Zur Entstehung von Datenschutzerlassen i.A. siehe Pfaffinger, S. 96 ff.

Diese unverbindlichen Vorgaben zielten darauf ab, mögliche Risiken von vornherein zu minimieren oder wenn möglich auszuschliessen, zumal sich eine solch präventive Ausrichtung stets als einfacher und kostengünstiger erwies, als die Prozesse z.B. nachträglich zu einer Untersuchung durch die kompetente Aufsichtsbehörde anzupassen.¹⁷ Diese Ziele sollten u.a. durch eine Beschreibung der «Information Flows», den Einbezug von und den Diskurs mit «Stakeholdern» sowie durch Verfassen von Reports erreicht werden.¹⁸ Beispielhaft können zudem die Vorschriften des ehemaligen Bundesdatenschutzgesetzes (aBDSG) in Deutschland genannt werden, das in § 3 Abs. 9 aBDSG einen erhöhten Schutz für besondere Arten von Daten vorsah.¹⁹ Bei diesen besonderen Daten handelte es sich u.a. um Daten über die politische Meinung oder die Gesundheit. Bevor diese Daten von Organisationen bearbeitet werden durften, musste der zuständige Beauftragte für Datenschutz eine sog. «Vorabkontrolle» vornehmen, um den sachgemässen Umgang sicherzustellen (§ 4d Abs. 5 aBDSG).

- 6 An all diese Entwicklungen knüpfte der Gesetzgebungsprozess in der Schweiz offenbar an, indem in allen Vorversionen zum totalrevidierten DSGVO eine DSFA vorgesehen war. Im Vorentwurf waren Art. 22 und der dazugehörige Art. 23 DSGVO in einem Artikel 16 VE-DSG zusammengefasst. Art. 16 Abs. 3 VE-DSG war jedoch strenger gefasst als die nun geltende Vorschrift. Der Artikel sah vor, dass sowohl das Ergebnis als auch die ergriffenen Massnahmen von jeder DSFA dem EDÖB gemeldet werden müssen. Im E-DSG wurde die Folgenabschätzung sodann in zwei Artikel gefasst und an die Struktur von Art. 35 DSGVO angepasst. Die Liste von Bearbeitungen mit hohem Risiko, welche somit zwingend die Durchführung einer DSFA voraussetzen, umfassten im Entwurf ebenfalls das Profiling (Art. 20 Abs. 2 lit. b E-DSG). Dieser Bearbeitungsprozess wurde im finalen Gesetzestext aufgrund der parlamentarischen Beratungen und im Einklang mit der geltenden Gesetzessystematik jedoch wieder aus der Liste von Datenbearbeitungen mit hohem Risiko gestrichen. Dieser Schritt ist zu begrüßen, zumal **in vielen Fällen das Profiling nicht als besonders heikel** einzustufen sein wird und eine DSFA somit nicht gerechtfertigt wäre.²⁰
- 7 Die DSFA wird nunmehr in Art. 22 DSGVO normiert und ist sowohl auf private Verantwortliche als auch Bundesorgane anwendbar.²¹ Damit geht die Gesetzesnorm über die zuvor bestehende Pflicht für Bundesorgane aus Art. 20 Abs. 2 VDSG hinaus und weitet sie aus.²² Im Rahmen der mit der Totalrevision neu eingeführten Norm fehlt es – mit Ausnahme von Art. 14 DSGVO zur Aufbewahrungspflicht von zwei Jahren – an weiteren Ausführungsbestimmungen,²³ welche die Umsetzung in der Praxis vereinfachen könnten.

14. Information Commissioner's Office, Conducting privacy impact assessments code of practice, <https://web.archive.org/web/20160813010840/ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>, passim, besucht am 5.6.2023.

15. Commission Nationale de l'Informatique et des Libertés, Privacy Impact Assessment (PIA), <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>, besucht am 5.6.2023, passim.

16. Siehe dazu Widmer, S. 224.

17. Information Commissioner's Office, Conducting privacy impact assessments code of practice, <https://web.archive.org/web/20160813010840/ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>, besucht am 5.6.2023, S. 5. <https://web.archive.org/web/20160813010840/ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>.

18. Information Commissioner's Office, Conducting privacy impact assessments code of practice, <https://web.archive.org/web/20160813010840/ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>, besucht am 5.6.2023, S. 11 ff. <https://web.archive.org/web/20160813010840/ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>.

19. www.dejure.org/gesetze/BDSG_a.F./3.html, besucht am 5.6.2023.

20. Rosenthal, N. 158.

21. Botschaft 2017, S. 7059.

22. Schönbachler, S. 189.

23. Lobsiger, S. 312.

C. Normzweck

- 8 Die Einhaltung der Voraussetzungen des Art. 22 dient dazu sicherzustellen, dass eine geplante Datenbearbeitung nicht zu einer Verletzung des DSG führt. Die DSFA soll beim Verantwortlichen ein erhöhtes Bewusstsein für Datenbearbeitungen mit hohem Risiko, wie z.B. beim Einsatz von algorithmischen Systemen («Künstliche Intelligenz») oder Big Data Analytics, bei der Nutzung von Gesichtserkennungssoftware, bei der Einführung einer Patientendatenbank oder im Rahmen von Profiling mit hohem Risiko, schaffen. Es handelt sich mithin um eine «datenschutzrechtliche Selbstbeurteilung»²⁴ bei besonders risikoreichen Datenbearbeitungen. Art. 22 ist Ausfluss der Datenschutzgrundsätze sowie des Grundsatzes von Datenschutz durch Technik und datenschutzfreundlicher Voreinstellungen (Art. 7). So geht es darum, Risiken in einem ersten Schritt zu erkennen und diese in einem zweiten Schritt analytisch zu bewerten. Der Verantwortliche soll dabei eine **Prognose über die möglichen Folgen einer geplanten Datenbearbeitung für die betroffenen Personen machen**.²⁵ Dabei kommt es darauf an, wie und in welchem Umfang sich die geplante Datenbearbeitung auf die betroffenen Personen auswirkt.²⁶ Schliesslich zielt die Norm darauf ab, ausgehend von den Ergebnissen der durchgeführten Analyse, angemessene Massnahmen zu entwickeln und zu implementieren, um (i) die identifizierten Risiken der geplanten Datenbearbeitung zu mildern, (ii) langfristige Schlüsse daraus zu ziehen sowie (iii) sich insgesamt datenschutzkonform zu verhalten.²⁷ Gelingt dies, bietet die DSFA zudem die Möglichkeit, die Einhaltung von Vorschriften aus dem Datenschutzrecht gegenüber dem EDÖB nachzuweisen und langfristig Kosten zu sparen.²⁸ In diesem Sinne fordert der Art. 22 vom Verantwortlichen ein selbständiges Weiterdenken und Prüfen der sich ergebenden Risiken in Bezug auf die geplante Datenbearbeitung: Ist die geplante Datenbearbeitung mit den Vorgaben der Datenschutzgesetzgebung im Einklang? Werden die allgemeinen Datenschutzgrundsätze eingehalten? Ist die Datenbearbeitung verhältnismässig? Ist die Datensicherheit durch die geplante Bearbeitung gefährdet? Ergeben sich weitere Risiken für die Persönlichkeit oder Grundrechte der betroffenen Personen? Diesen Fragen ist dabei ungeachtet der Höhe des Risikos nachzugehen,²⁹ wodurch der Gesetzgeber zu einem Grossteil auf eine «Hands-on-Mentalität» setzt. Dies soll dazu dienen, die mit der Datenbearbeitung zusammenhängenden Risiken auf ein als angemessen empfundenes Niveau zu senken.³⁰
- 9 Die Dokumentations- und die Aufbewahrungspflicht nach Art. 14 DSV ergänzen die Pflicht eine DSFA bei Datenbearbeitungen mit hohen Risiken durchzuführen. So wird der Verantwortliche verpflichtet, eine durchgeführte **DSFA zu dokumentieren und nach Beendigung der Datenbearbeitung während mindestens zwei Jahren aufzubewahren**. Dadurch sieht sich der Verantwortliche im Falle einer Untersuchung durch den EDÖB in der Lage, die risikoreiche Datenbearbeitung zu rechtfertigen und aufzuzeigen, wie den hohen Risiken entgegnet wird. Aus dieser Bestimmung geht der Charakter der DSFA als ergänzende Rechenschaftspflicht sowohl gegenüber dem EDÖB als auch gegenüber betroffenen Personen hervor.

24. Rosenthal, N. 148.

25. Botschaft 2017, S. 7059.

26. Botschaft 2017, S. 7059 f.

27. Zum Vorstehenden Lobsiger, S. 316.

28. Botschaft 2017, S. 7059.

29. Lobsiger, S. 316.

30. Lobsiger, S. 318.

II. INHALT

A. Adressaten

- 10 Art. 22 adressiert vor allem zwei **Akteure: Bundesorgane sowie private Verantwortliche**,³¹ da es sowohl um eine Risikoeinschätzung der betreffenden Datenbearbeitung in Bezug auf die Persönlichkeit als auch die Grundrechte der betroffenen Personen geht. Bundesorgane hatten bereits im aDSG eine ähnliche Pflicht. Private Verantwortliche wie auch Bundesorgane sind von dieser Pflicht betroffen, wenn sie gem. Art. 3 Abs. 1 in den Anwendungsbereich des DSG fallen. Dies bedeutet, dass auch private Verantwortliche mit Sitz im Ausland dieser Pflicht unterliegen, sofern sich ihre Datenbearbeitungstätigkeit gem. dem Auswirkungsprinzip in der Schweiz auswirkt und die weiteren Voraussetzungen von Art. 22 erfüllt sind (vgl. zum Auswirkungsprinzip ausführlich die Kommentierung zu Art. 3).
- 11 **Auftragsbearbeiter sind zu Recht nicht von der Pflicht zur Durchführung einer DSFA erfasst**, zumal sie die Daten im Auftrag eines Verantwortlichen bearbeiten und der Verantwortliche grundsätzlich über den Zweck und die Mittel einer Datenbearbeitung entscheidet. Die Risikoeinschätzung liegt somit grundsätzlich nicht in ihrer Sphäre. Während im DSG im Gegensatz zu Art. 28 Abs. 3 lit. f DSGVO keine Unterstützungspflicht der Auftragsbearbeiter gegenüber den Verantwortlichen bei der Durchführung einer DSFA verankert ist, kann eine Unterstützungspflicht der Auftragsbearbeiter jedoch auch in ihrem Sinne sein. In der Praxis wird eine entsprechende Pflicht häufig Bestandteil der vertraglichen Abreden zwischen dem Verantwortlichen und dem Auftragsbearbeiter sein. Aus den Datenschutzgrundsätzen in Art. 6 lässt sich jedoch eine Pflicht für Auftragsbearbeitende ableiten, sicherzustellen, dass die ihnen übertragene Datenbearbeitung im Einklang mit den Datenschutzgrundsätzen erfolgt. Trifft dies nicht zu, ist der Verantwortliche darüber in Kenntnis zu setzen, dass die Datenbearbeitungstätigkeit angepasst werden sollte. Gegebenenfalls sollte gar die Durchführung einer DSFA vorgeschlagen werden.

B. Das hohe Risiko

- 12 Abs. 2 sieht vor, dass die DSFA in jedem Fall durchzuführen ist, sofern ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person anzunehmen ist. Dementsprechend ist nicht für jede Datenbearbeitung eine DSFA durchzuführen. Dies entspricht dem **risikobasierten Ansatz des DSG**, wobei vorliegend die Risiken für die betroffenen Personen spezifisch im Vordergrund stehen und nicht Risiken, die sich für die Verantwortlichen ergeben.
- 13 Das hohe Risiko ergibt sich aus der **Art, dem Umfang und den Umständen sowie dem Zweck der Datenbearbeitung**. Diese Kriterien sind vergleichbar mit den Risiken, die im Rahmen der Festlegung von Datensicherheitsmassnahmen gemäss Art. 1 Abs. 3 DSV berücksichtigt werden müssen. In diesem Sinne liegt das hohe Risiko insbesondere dann vor, jedoch nicht ausschliesslich, wenn neue Technologien eingesetzt werden. Je umfangreicher und sensibler diese Handlungen und Datenbestände sind, desto eher kann vom Vorliegen eines hohen Risikos ausgegangen werden. Die geplante Datenbearbeitung muss u.a. im Hinblick der Einwirkung auf die Identität, Selbstbestimmung oder Würde der betroffenen Person untersucht werden. Das hohe Risiko muss sich nicht effektiv manifestieren: Es geht darum potenzielle Risiken zu erkennen und zu bewerten, die im Rahmen der Datenbearbeitung auftreten könnten.
- 14 Gemäss den lit. a und lit. b liegt ein hohes Risiko im Sinne einer Fiktion dann vor, wenn (i) **besonders schützenswerte Personendaten umfangreich bearbeitet** (z.B., wenn Strafregisterinformationen in

31. Botschaft 2017, S. 7059.

einem öffentlichen Register publiziert werden, beim Einsatz von Gesundheitsapplikationen, die Auswertungen

der Daten vornehmen und Diagnosen erstellen, oder bei klinischen Versuchen) oder (ii) **öffentliche Bereiche umfassend und systematisch überwacht werden** (z.B. die Überwachung eines öffentlichen Spielplatzes oder Parks oder die systematische Überwachung der Internetnutzung von Mitarbeitenden). Das Gesetz listet keine weiteren Datenbearbeitungen auf, für welche zwingend eine DSFA durchgeführt werden muss. Im Gegensatz dazu sieht die DSGVO bspw. weitergehend vor, dass Aufsichtsbehörden Listen über Datenbearbeitungen publizieren müssen, welche zwingend einer DSFA bedürfen.

- 15 Weder das Profiling mit hohem Risiko noch die automatisierte Einzelentscheidung werden gemäss Wortlaut von Art. 22 Abs. 2 als Datenbearbeitungstätigkeit eingestuft, die zwingend eine DSFA verlangen. Dies erscheint auf den ersten Blick überraschend, zumal das Profiling mit hohem Risiko per Definition ein hohes Risiko für die betroffene Person mit sich bringt und die automatisierten Einzelentscheide zu Rechtsfolgen oder anderen Folgen führen, welche die betroffene Person erheblich beeinträchtigen. Vor diesem Hintergrund ist für ein **Profiling mit hohem Risiko stets eine DSFA durchzuführen**. Bei automatisierten Entscheiden stellt sich die Lage hingegen anders, komplexer dar, zumal eine DSFA die Datenbearbeitung an sich bewertet, welche bei diesen automatisierten Einzelentscheidungen nicht zwingend heikel ist. Heikel ist hier primär das Ergebnis der Entscheidung, welche in Art. 21 geregelt ist. Eine DSFA ist dennoch durchzuführen, wenn die Datenbearbeitung, die zur automatisierten Einzelentscheidung führt, an sich ein hohes Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person führen könnte.
- 16 In der Botschaft werden weitere Datenbearbeitungen aufgeführt, die zu einem hohen Risiko führen könnten, namentlich im Falle der Bearbeitung grosser Datenmengen, der Übermittlung von Daten in Drittstaaten (in diesem Zusammenhang ist auf das sog. Data Transfer Impact Assessment hinzuweisen; vgl. die Kommentierung zu Art. 16 f.) oder sofern eine grosse Vielzahl an Personen auf die Daten zugreifen können.³² Im Einzelfall ist jedoch stets zu prüfen, ob tatsächlich ein hohes Risiko vorliegt.
- 17 Weder das DSG noch die DSV enthalten genauere Vorgaben in Bezug auf die Bestimmung des hohen Risikos. So muss stets anhand der konkret geplanten Datenbearbeitung geprüft werden, ob eine DSFA durchzuführen ist. Als Hilfestellung können dabei die EU-Leitlinien dienen, welche für die Regelung in Art. 35 f. DSGVO **neun Kriterien** vorsehen, nach welchen die Ermittlung eines hohen Risikos

32. Botschaft 2017, S. 7060.

erfolgen kann.³³ Sobald eine geplante Datenbearbeitung zwei dieser neun Kriterien erfüllt, soll gemäss der Leitlinie die Pflicht bestehen, eine DSFA durchzuführen. Die neun Kriterien lauten wie folgt:

- Bewertung oder Einstufung von Personen oder Persönlichkeitsaspekten mithilfe von Daten;
- Automatisierte Entscheidungsfindung mit Rechtswirkung gegenüber natürlichen Personen oder ähnlich bedeutsamer Wirkung;
- Systematische Überwachung;
- Bearbeitung von vertraulichen oder höchstpersönlichen Daten;
- Datenbearbeitung in grossem Umfang;
- Abgleichen oder Zusammenführen von verschiedenen Datensätzen, sofern nicht damit zu rechnen war;
- Datenbearbeitung von schutzbedürftigen Personen (z.B. Kinder, Arbeitnehmenden oder Patienten);
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen (z.B. künstliche Intelligenz, Big Data Analytics oder Blockchain-basierte Technologien), da deren datenschutzrechtliches Risiko oft noch nicht genau eruiert worden ist; und
- Fälle, in denen die Datenbearbeitung die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert.

Während die Leitlinien aus der EU in der Schweiz nicht anwendbar sind, können sie aufgrund der vergleichbaren gesetzlichen Voraussetzungen zur Durchführung einer DSFA im Schweizer und EU-Datenschutzrecht beigezogen werden. Es ist zudem nicht auszuschliessen, dass der EDÖB ähnliche Leitlinien publizieren oder die Listen von Datenbearbeitungsvorgängen der verschiedenen EU-Aufsichtsbehörden gem. Art. 35 Abs. 4 DSGVO, welche zwingend eine DSFA verlangen, analog auf die Schweiz anwenden wird. Die Praxis wird in Bezug auf die Beurteilung des hohen Risikos für mehr Rechtssicherheit sorgen.

C. Durchführung der DSFA

1. Einführung

- 18 Art. 22 macht klare Vorgaben, in welchen Fällen der Verantwortliche eine DSFA durchführen muss und was bei der Durchführung zu beachten ist. Dazu gehört, dass die **Risikobewertung strukturiert durchgeführt³⁴ und dokumentiert** werden muss. Die Dokumentation muss zudem der Konsultation des EDÖB standhalten, wenn trotz der implementierten Massnahmen die Datenbearbeitung weiterhin ein hohes Risiko für die Persönlichkeit oder Grundrechte der betroffenen Personen zur Folge hat (Art. 23 Abs. 1; vgl. hierzu ausführlich die Kommentierung zu Art. 23).

2. Ablauf

- 19 Die DSFA ist von dem Verantwortlichen vor Aufnahme einer neuen oder aktualisierten Datenbearbeitungstätigkeit durchzuführen. Dies dient dazu, die Risiken der geplanten

33. Artikel 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 «wahrscheinlich ein hohes Risiko»<https://www.datenschutz-bayern.de/technik/orient/wp248.pdf>, besucht am 5.6.2023.

34. Siehe in diesem Sinne Pfaffinger, S. 114.

Datenbearbeitung vorgängig zu erkennen und entsprechende Massnahmen zu implementieren, bevor es zu Rechtsverletzungen kommt.³⁵ Dabei gilt: **je früher, desto besser**. Die einmalige, anfängliche Durchführung des DSFA reicht indes nicht aus. Vielmehr sind auch während des jeweiligen Projekts weitere Durchläufe erforderlich, um zu überprüfen, ob etwaig vorgenommene Anpassungen der Datenbearbeitungen zu einer anderen Einschätzung führen und somit andere Massnahmen sachgemässer oder gar obsolet erscheinen.

- 20 Inhaltlich setzt die DSFA drei Schritte voraus, die in Abs. 3 definiert werden. Dies ist, erstens, die Vorbereitungsphase, in welcher die Bearbeitung der Daten möglichst präzise beschrieben wird. Zweitens werden in der Bewertungsphase die Risiken bewertet, um darauf aufbauend in einem dritten Schritt, Massnahmen zum Umgang mit bzw. zur Bewältigung dieser Risiken zu treffen.
- 21 Bevor diese drei Schritte ausgeführt werden, sollten private Verantwortliche jedoch prüfen, ob sie gesetzlich zur Datenbearbeitung verpflichtet sind. Sofern eine gesetzliche Bearbeitungspflicht besteht, sind sie von der Pflicht zur Durchführung einer DSFA ausgenommen (Art. 22 Abs. 4). Ausserdem sollte die Bundesbehörde oder der private Verantwortliche zuerst eine **Vorabeinschätzung** durchführen. Dabei handelt es sich um eine allgemeine, eher oberflächliche Risikoeinschätzung, zur Prüfung, ob potenziell ein hohes Risiko bei der geplanten Datenbearbeitung vorliegen könnte (vgl. zum hohem Risiko N. 12 ff.). Auf diese Weise lässt sich vorab klären, ob eine DSFA überhaupt notwendig ist.³⁶ Kommt der Verantwortliche zum Schluss, dass die geplante Datenbearbeitung voraussichtlich nicht zu einem hohen Risiko führen wird, ist keine DSFA erforderlich. Ein solcher Entscheid sollte jedoch zu Beweis Zwecken dokumentiert und aufbewahrt werden. Sofern der Verantwortliche jedoch aufgrund dieser Vorabeinschätzung zum Schluss gelangt, dass die betreffende Datenbearbeitung zu einem hohen Risiko führen könnte, ist die DSFA grundsätzlich durchzuführen. Eine Ausnahme liegt nur in den Fällen des Art. 22 Abs. 5 vor.
- 22 Die **Vorbereitungsphase umfasst eine detaillierte Darstellung der (geplanten) Datenbearbeitungstätigkeit**. Das Gesetz legt weder fest, was diese Beschreibung umfassen, noch wie detailliert sie ausfallen muss. Je nach Komplexität der geplanten Datenbearbeitungstätigkeit kann die DSFA somit länger oder kürzer ausfallen. Die Beschreibung sollte jedoch mindestens die Art der bearbeiteten Daten und Kategorien der betroffenen Personen, die Darlegung des verfolgten Zwecks, die Aufbewahrungsdauer, die Bearbeitungsvorgänge, die Empfänger sowie den Ort der Bearbeitung und Aufbewahrung umfassen. Eine vollständige Risikoabschätzung ist andernfalls nicht möglich. Aus dieser Beschreibung sollte hervorgehen, warum welche Personendaten wie bearbeitet werden sollen. Im Rahmen dieser Darstellung ist auf die zugrundeliegenden Technologien und Systeme einzugehen sowie auf relevante Rechtsgrundlagen, damit darauf aufbauend ein möglicher gesetzgeberischer Handlungsbedarf frühzeitig erkannt und umgesetzt werden kann.³⁷
- 23 Daran schliesst die **Bewertungsphase, während der die Notwendigkeit und Verhältnismässigkeit der Datenbearbeitung in Bezug auf die möglichen Risiken** in Relation gesetzt werden. Bewertet werden damit die negativen Folgen der Datenbearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Person. Hohe Risiken oder negative Auswirkungen der Datenbearbeitung können sich hierbei auf unterschiedliche Weise manifestieren: So kann eine Datenbearbeitung zu einer Rufschädigung führen oder aber die Bearbeitung falscher Daten zur Folge haben, dass fehlerhafte Prognosen oder Diagnosen im medizinischen Umfeld erstellt werden. Vorstellbar sind auch Situationen, in denen eine Person ungerechtfertigt entlassen wird oder Vertrauensverluste gegenüber Behörden, dem privaten Verantwortlichen oder gegenüber Freunden

35. Blonski, S. 29; Botschaft 2017, S. 7059.

36. Botschaft 2017, S. 7061.

37. Zu dieser «Rechtsgrundlagenanalyse» siehe SHK-Blonski, Art. 22 DSGVO N. 16.

und Familie entstehen. Zudem kann sich die Datenbearbeitung auch finanziell auswirken.³⁸ Diese und vergleichbare Risiken gilt es in der Bewertungsphase auf ihre Wahrscheinlichkeit und Schwere hin zu analysieren.

- 24 Bei der Bewertung der Risiken sind die Datenschutzgrundsätze – vor allem jene der Datenminimierung, des Datenschutzes durch Technik sowie der datenschutzfreundlichen Voreinstellungen – zu beachten (siehe dazu N. 4). Der informationellen Selbstbestimmung der betroffenen Person kommt ebenfalls eine besondere Wichtigkeit zu, nicht jedoch den Interessen des Verantwortlichen.³⁹ Eine Interessenabwägung im Hinblick auf die zu ergreifenden Massnahmen zwischen den Interessen der betroffenen Person (Datenschutzinteresse, Interesse an der Verfügungsfreiheit über die eigenen Daten) und des Verantwortlichen (Datenbearbeitungsinteresse) darf jedoch zu einem späteren Zeitpunkt erfolgen.⁴⁰ Obschon es sich bei den für die DSFA relevanten Daten nicht zwingend um «besonders schützenswerte» handeln muss, ist die «heikle Natur» der Daten im Rahmen der jeweiligen DSFA und der zu ergreifenden Massnahmen zu berücksichtigen.⁴¹ Entsprechend sind die Anzahl sowie die Sensitivität der Daten in dieser Phase zu berücksichtigen. Die Bewertungsphase umfasst die Einschätzung der Schwere der Risiken und Wahrscheinlichkeit des Eintritts dieser Risiken. Obwohl in dieser Phase ein potenziell hohes Risiko erkannt werden soll, können sich die Risiken auch erst im Anschluss an die Durchführung der DSFA ergeben.⁴² In diesem Sinne lassen sich die drei genannten Phasen nicht strikt voneinander abgrenzen.
- 25 Nachdem in der Bewertungsphase beurteilt wurde, ob die Bearbeitung der Daten mit einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person einhergeht,⁴³ werden in der dritten **Phase Massnahmen zur Risikoverminderung** definiert. Der Verantwortliche muss sich in dieser Phase somit nicht nur im Klaren darüber sein, welche Risiken bestehen, sondern muss eine Entscheidung treffen, wie diesen Risiken entgegengetreten wird. Bei den Massnahmen kann es sich um organisatorische, technische oder rechtliche bzw. vertragliche Massnahmen handeln. Der Verantwortliche muss analysieren, wie die geplante Datenbearbeitungstätigkeit angepasst werden kann, damit das hohe Risiko auf ein angemessenes Mass reduziert wird. Solche Massnahmen können z.B. die Einschränkung der Datenkategorien, die Beschränkung der Zugriffe auf die Daten, die Verschlüsselung von Daten, der Wechsel eines involvierten Auftragsbearbeiters, die Änderung des Bearbeitungsortes, die Aufnahme bestimmter Pflichten in den Verträgen mit Dritten in Bezug auf die Datenbearbeitung, usw. sein. Die Massnahmen müssen aber geeignet sein, die spezifisch identifizierten Risiken zu mindern und können nicht *per default*, d.h. allgemein in Bezug auf alle Risiken von Datenbearbeitungstätigkeiten, welche eine DSFA erfordern, angewendet werden. Sie müssen einzelfallabhängig definiert werden.
- 26 Das DSGVO bestimmt nicht, ob die Durchführung einer DSFA nur einmalig oder regelmässig erfolgen muss. Dies hängt von der Datenbearbeitungstätigkeit ab: Ist sie einmalig, reicht eine einmalig durchgeführte DSFA aus. Wird die Datenbearbeitung jedoch über einen längeren Zeitraum hinweg ausgeführt und ergeben sich aufgrund veränderter Umstände neue oder höhere Risiken, sollte die DSFA wiederholt werden. Grundsätzlich sollte die DSFA jedoch in etwa **alle drei Jahre wiederholt** werden.⁴⁴ Ob sich diese Empfehlung angesichts schnell voranschreitender und immer umfassenderer

38. Vgl. für weitere Beispiele von negativen Folgen Rosenthal, N. 149.

39. Schönbachler, S. 191.

40. Botschaft 2017, S. 7060 f.

41. Vasella, S. 177.

42. Lobsiger, S. 316.

43. Wobei gemäss Rosenthal, N. 154 Unternehmen nach Durchführung der DSFA in der Regel zum Schluss kommen werden, dass kein hohes Risiko mehr vorliegt.

44. Rosenthal, N. 154 m.w.H.

technologischer Neuerungen langfristig bewährt, bleibt abzuwarten, erscheint aus derzeitiger Perspektive jedoch eher unwahrscheinlich.

- 27 Zeitlich ist zudem noch die Aufbewahrungsfrist zu beachten. Gemäss Art. 14 DSGVO ist die erforderliche **Dokumentation der DSFA für zwei Jahre aufzubewahren**. Die Frist beginnt mit dem Ende der Datenbearbeitung zu laufen.

3. Durchführung einer gemeinsamen DSFA

- 28 Der Verantwortliche hat das Recht **bei mehreren vergleichbaren Datenbearbeitungsvorgängen eine gemeinsame DSFA** durchzuführen.⁴⁵ Dies gilt jedoch nur dann, wenn sowohl die Risiken als auch die Gegenmassnahmen ähnlich sind. Diese Möglichkeit dient dazu, den Aufwand und die Kosten für den Verantwortlichen zu reduzieren. Ob dieses Recht tatsächlich zu einer Entlastung der Verantwortlichen führen wird, ist jedoch zweifelhaft; es sei denn eine bestimmte Bearbeitungsplattform oder Anwendung wird in verschiedenen Sektoren oder Projekten eingesetzt.

4. Organisation

- 29 Die Durchführung einer DSFA obliegt nicht nur einer bestimmten Person, Stelle oder Abteilung beim Verantwortlichen. Wie jede andere Risikoanalyse handelt es sich um einen **Prozess, an dem mehrere Personen, Stellen und Abteilungen übergreifend beteiligt werden** müssen. Innerhalb eines Unternehmens werden für die DSFA üblicherweise die Projektleitung, die IT-Abteilung und/oder der Chief Information Security Officer, die Datenschutzstelle oder der Datenschutzberater, die Rechtsabteilung, die Risiko- und Compliance-Abteilung sowie andere Schlüsselpersonen beigezogen. Jede beteiligte Person ist für bestimmte Schritte der DSFA essenziell. So ist die Projektleitung für die Vorbereitungsphase besonders wichtig, weil sie die (geplante) Datenbearbeitung am besten beschreiben kann. Der Datenschutz- und Rechtsabteilung obliegt es, die Risiken gemäss Datenschutz und anwendbarem Recht zu beurteilen.⁴⁶ Andere Abteilungen sind für die Bestimmung der risikomindernden Massnahmen von besonderer Relevanz. Auftragsbearbeiter, die bei dem geplanten Datenbearbeitungsvorgang eingesetzt werden, sollten im Rahmen der DSFA auch mit einbezogen werden. Wie bei jedem Projekt ist es besonders bedeutsam, dass eine Person, Stelle oder Abteilung die Leitung der DSFA übernimmt und den Überblick über den gesamten Prozess behält. Diese Leitung übernimmt in der Regel die Datenschutzberaterin oder die Projektleiterin auf operativer Ebene. Auftragsbearbeiter, die bei dem geplanten Datenbearbeitungsvorgang eingesetzt werden, sollten im Rahmen der DSFA miteinbezogen werden.
- 30 Aus Sicht des Verantwortlichen ist es deshalb sinnvoll **eine Stelle oder Abteilung zu definieren**, welche die rechtlichen Anforderungen an eine DSFA kennt und über die notwendigen Fachkenntnisse zur Durchführung einer DSFA verfügt. Dies ist in der Regel die für den Datenschutz zuständige Stelle oder Abteilung. Je nach Fokus oder Businessmodell der Verantwortlichen, kann es hilfreich sein, eine Vorlage inkl. Anleitung für die Durchführung einer DSFA zu erstellen, auf die im Einzelfall zurückgegriffen werden kann. Auf diese Weise werden die rechtlichen Anforderungen eingehalten, ohne dass bestimmte Aspekte vergessen gehen.

45. So auch Rosenthal, N. 151.

46. Gl.M. Rosenthal, N. 152.

D. Ausnahmen

- 31 Neben der allgemeinen Pflicht zur Durchführung einer DSFA in Fällen, in denen eine Datenbearbeitung zu einem hohen Risiko für die betroffenen Personen führt, definieren **Abs. 4 und 5** einige **Ausnahmen**.
- 32 Art. 22 Abs. 4 sieht vor, dass private Verantwortliche in Einzelfällen von der Pflicht zur Durchführung der DSFA ausgenommen sein können, sofern sie **gesetzlich zur Bearbeitung der Daten verpflichtet** sind. Im Gesetzgebungsprozess wurde diese Ausnahme damit begründet, dass mögliche Risiken in diesen Fällen bereits abgewogen wurden und somit kein weitergehender Bedarf zur Durchführung einer DSFA besteht.⁴⁷ Zu Recht wird jedoch darauf hingewiesen, dass sich der Ausnahmetatbestand einzig auf die Frage der Zulässigkeit der Datenbearbeitung bezieht, nicht auf die Art und Weise der jeweiligen Bearbeitung von Daten.⁴⁸ So ist die DSGVO in dieser Hinsicht strenger und verlangt, dass die im Rahmen der Gesetzgebung durchgeführte Risikoanalyse sich auf die konkrete Bearbeitungstätigkeit beziehen muss, damit die Ausnahme greift (vgl. N. 40). Darüber hinaus sind auch diejenigen Fälle zu beachten, in denen die Bearbeitung von Daten nicht ausschliesslich zur Erfüllung der jeweiligen gesetzlichen Pflicht erfolgt.⁴⁹ Gesetzliche Pflichten zur Bearbeitung von Daten durch Private finden sich z.B. im Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Art. 30 GwG) oder die Weitergabe von Mitarbeiterdaten durch einen Arbeitgeber zur Erfüllung sozialversicherungsrechtlicher Pflichten (Art. 84 KVG). Es liegt auf der Hand, dass Bundesbehörden von dieser Ausnahmeregelung nicht umfasst sind: Sie dürfen Daten stets nur gestützt auf eine gesetzliche Grundlage bearbeiten.
- 33 Art. 22 Abs. 5 sieht sodann eine weitere Ausnahme vor. Demzufolge können private Verantwortliche von der Erstellung der DSFA absehen, wenn bestimmte Voraussetzungen in Bezug auf die **Zertifizierung einer Datenbearbeitung oder die Einhaltung genehmigter Verhaltenskodizes** erfüllt sind. Diese Ausnahmen gelten nicht für Bundesbehörden. Zum einen ist dies der Fall, wenn der Verantwortliche ein System, Produkt oder eine Dienstleistung einsetzt, welche(s) für die Verwendung nach Art. 13 zertifiziert ist (siehe hierzu ausführlich die Kommentierung zu Art. 13 DSGVO). Zum anderen entfällt die Pflicht in den Fällen, in denen der Verantwortliche einen Verhaltenskodex i.S.v. Art. 11 einhält, (i) der auf einer DSFA beruht, (ii) spezifische Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Personen trifft und (iii) dem EDÖB vorgelegt wurde.⁵⁰ Derzeit existieren keine solchen Verhaltenskodizes in der Schweiz. Vorstellbar sind solche jedoch für Branchen, in denen die Branchenteilnehmerinnen eng zusammenarbeiten und standardisierte Prozesse gemeinsam entwickeln, wie z.B. bei Banken und Versicherungen, in Technologie- oder Medienunternehmen oder in der Werbebranche. In der EU richtet sich die Erarbeitung vergleichbarer Verhaltenskodizes bzw. – regeln nach Art. 40 DSGVO, wobei aktuell u.a. der EU Cloud Code of Conduct, welcher als harmonisierter Verhaltenskodex für die Cloud-Industrie innerhalb der EU dient, bekannt ist.

III. VERLETZUNG DER PFLICHT ZUR DURCHFÜHRUNG EINER DSFA

- 34 Führt ein Verantwortlicher keine DSFA durch, obwohl gemäss Art. 22 eine entsprechende Pflicht bestünde, ist Art. 51 Abs. 3 lit. d zu beachten. Diesem Artikel zufolge kann der **EDÖB unter Strafandrohung verfügen**, dass der Verantwortliche eine DSFA vornehmen muss. Im Gegensatz

47. Botschaft 2017, S. 7061 f.

48. SHK-Blonski, Art. 22 DSGVO N. 6 m.w.H.

49. SHK-Blonski, Art. 22 DSGVO N. 6 m.w.H.

50. Siehe dazu Botschaft 2017, S. 7062.

dazu haben betroffene Personen jedoch keinen Anspruch, die Durchführung einer DSFA klageweise durchzusetzen.⁵¹

- 35 Stellt der EDÖB im Rahmen einer Untersuchung fest, dass eine Datenbearbeitung zu einem hohen Risiko führt, kann er verfügen, dass die Datenbearbeitung angepasst, suspendiert oder ganz abgebrochen wird, bis eine DSFA durchgeführt wurde (Art. 51 Abs. 1 i.V.m. Art. 49 f). Dies kann zu erheblichen Verzögerungen beim Verantwortlichen führen, was wiederum hohe Kosten und zusätzlichen Aufwand für den Verantwortlichen mit sich bringt. Da die Ergebnisse einer Untersuchung vom EDÖB zudem veröffentlicht werden können (Art. 57 Abs. 2), bestehen zudem erhebliche **Reputationsrisiken** für den Verantwortlichen.
- 36 Die Verletzung der Pflicht zur Durchführung einer DSFA wird nicht eigenständig einer Busse unterstellt. Diese Regelung erscheint vor dem Hintergrund, dass es sich bei dieser Pflicht primär um eine Sorgfaltspflicht (bestehend aus einer Dokumentations- und Rechenschaftspflicht) handelt, sinnvoll. In der EU wird dies hingegen anders gehandhabt (vgl. N. 40 ff.). Es ist jedoch davon auszugehen, dass Verantwortliche ihre Pflichten gemäss DSGVO dennoch einhalten werden. Zum einen da Behörden bereits unter dem aDSG eine solche Pflicht berücksichtigen mussten. Zum anderen führten auch private Verantwortliche, insbesondere Konzerne, vor Inkrafttreten des totalrevidierten DSGVO ebenfalls DSFAs durch, z.B. weil die betreffende Datenbearbeitung unter die DSGVO fiel oder der EDÖB dies verlangt hatte.⁵²

IV. HERAUSFORDERUNGEN UND PRAKTISCHE RELEVANZ

- 37 Mit dem Inkrafttreten des neu gefassten Art. 22 zeigt sich, dass die normativen Voraussetzungen für eine DSFA einen hohen Komplexitätsgrad aufweisen. Dies gilt insbesondere bei der Umsetzung durch kleine und mittlere Unternehmen (KMU), denen in der Schweiz eine wirtschaftliche nicht zu unterschätzende Bedeutung zukommt. Für sie dürfte es sich als herausfordernd erweisen, die einzelnen Schritte im Einklang mit Art. 22 durchzuführen. Dies gilt insbesondere für die Vorbereitungs- sowie die Massnahmenphase (siehe dazu N. 18 ff.), welche sich allein schon aufgrund der notwendigen analytischen Vorgehensweise als zeitaufwendig gestalten. Dies dürfte in Einzelfällen erhebliche Kosten generieren. Es ist entsprechend davon auszugehen, dass der Bedarf an **Vorlagen, Beratung und Hilfestellungen seitens des EDÖB zeitnah in hohem Masse zunehmen** wird.⁵³ In dieser Hinsicht ist die Pflicht der europäischen Aufsichtsbehörden Listen zu publizieren, in denen definiert wird, wann eine DSFA zwingend notwendig ist, als Schritt in diese Richtung zu beurteilen (Art. 35 Abs. 4 DSGVO; vgl. N. 43).
- 38 Mit dem zunehmenden Einsatz von algorithmischen Systemen und anderen Anwendungen (siehe N. 2) wird auch die DSFA an Bedeutung gewinnen. Verantwortliche müssen im Einzelfall genau abwägen, welche Risiken angemessen erscheinen und ob sich der Einsatz solcher Systeme lohnt. Diese analytische Herangehensweise vor dem eigentlichen Projektstart dürfte vor allem für grosse Unternehmen nicht neu sein, zumal bereits vor der Totalrevision entsprechende Privacy Impact Assessments durchgeführt wurden (siehe N. 4 f. und 35) und sie auf EU-Ebene durch die DSGVO vergleichbare Pflichten kennen dürften.
- 39 Die DSFA macht zudem deutlich, dass sich im Bereich neuer disruptiver Technologien die verschiedenen Rechtsbereiche überschneiden und eine zunehmende Vermengung von rechtlichen

51. Rosenthal, N. 159.

52. Rosenthal/Gubler, S. 54.

53. Der EDÖB wird im Sommer 2023 ausführliche Hinweise zum Inhalt und Voraussetzungen für eine DSFA publizieren. Siehe <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/dsfa.html>, besucht am 5.6.2023.

Fragen und solcher bzgl. der eingesetzten Technologie zu beobachten ist. Ein Beispiel für diese Entwicklung sind die Diskussionen rund um den Artificial Intelligence Act («AI Act»)⁵⁴. Vergleichbar mit der DSFA nach Art. 22 DSGVO, liegt dem zuletzt diskutierten Text⁵⁵ ein stark risikobasierter Ansatz zugrunde, wonach zwischen einem begrenzten, hohen und inakzeptablem Risiko differenziert wird. So ist vor allem bei hochriskanten Anwendungen, die im Anhang III des AI Acts definiert werden, nach Art. 43 AI Act ein Konformitätsbewertungsverfahren durchzuführen, das sich u.a. nach Anhang VI richtet. Diese Vorgaben sind wie die DSFA gemäss dem DSGVO als **präventiver, fortlaufender Prozess zu verstehen, der sowohl rechtliche als auch technische Aspekte beinhaltet** sowie weitergehend der Transparenz und damit dem Vertrauen der Nutzerinnen dient.

V. VERGLEICH MIT DEM EU-RECHT

- 40 Im Allgemeinen ist die Durchführung der DSFA gemäss dem DSGVO mit den EU-weiten Vorgaben der DSGVO vergleichbar. Gleichzeitig sind **Art. 22 f. DSGVO weniger strikt ausgestaltet als Art. 35 f. DSGVO**.⁵⁶ In der EU ist eine DSFA etwa auch durchzuführen, wenn eine Datenbearbeitung zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen kann. Im Gegensatz zu Art. 22 DSGVO sieht Art. 35 Abs. 3 lit. a DSGVO zudem eine DSFA explizit für automatisierte Einzelentscheide vor.
- 41 Die lit. a bis d von Art. 35 Abs. 7 regeln vergleichbare Schritte wie Art. 22 DSGVO, welche berücksichtigt werden müssen, wenn eine DSFA durchgeführt wird. So ist die vorbereitende Phase mit lit. a vergleichbar, die Phase der Bewertung mit den lit. b und c sowie die Phase der Implementierung der Massnahmen mit lit. d.⁵⁷ Obschon in der Schweiz ebenfalls davon auszugehen ist, dass eine DSFA im Rahmen der Datenbearbeitung aufgrund veränderter Umstände gegebenenfalls nochmals durchgeführt werden muss, sieht dies Art. 35 Abs. 11 DSGVO in bestimmten Fällen sogar explizit vor.
- 42 Während Art. 35 Abs. 2 DSGVO eine Pflicht zur Konsultation des Datenschutzbeauftragten («Data Protection Officer») beinhaltet, jedenfalls sofern ein solcher ernannt wurde, sieht Art. 35 Abs. 9 DSGVO sogar vor, dass der Verantwortliche bei der Durchführung der DSFA die betroffenen Personen konsultieren kann. Eine solche Bestimmung enthält das DSGVO nicht. Die Konsultation des Datenschutzbeauftragten hat auf die DSFA inhaltlich keinen Einfluss, zumal die **Rolle des Datenschutzbeauftragten nicht konkretisiert** wird.⁵⁸ Die Einholung des Standpunktes der betroffenen Personen hingegen hat die Transparenz seitens des Verantwortlichen sowie die Selbstbestimmung der betroffenen Personen zum Ziel.⁵⁹ Diese Konsultationen verstärken den Sinn und Zweck der DSFA, indem nochmals aufgezeigt wird, dass die zu beurteilenden Risiken, solche der Datenbearbeitung für die betroffenen Personen und somit nicht in erster Linie Risiken für den Verantwortlichen sind.
- 43 Anders als in der Schweiz schreibt Art. 35 Abs. 4 DSGVO den Aufsichtsbehörden vor, eine Liste über die Verarbeitungsvorgänge zu führen, bei denen eine DSFA in jedem Fall durchzuführen ist (sog. **Positivlisten**).⁶⁰ Dem Grunde nach statuiert der europäische Verordnungsgeber damit eine faktische

54. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 21.4.2021, <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>, besucht am 5.6.2023.

55. European Parliament, Draft Compromise Amendments on the Draft Report, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf, besucht am 5.6.2023.

56. Siehe für einen Vergleich zwischen den Vorgaben des DSGVO sowie der DSGVO Baeriswyl, S. 7.

57. Siehe zum Vorstehenden Blonski, S. 28 f.

58. Kühling/Buchner/Jandt, Art. 35 DS-GVO N. 18.

59. Kühling/Buchner/Jandt, Art. 35 DS-GVO N. 54.

Pflicht zur Durchführung einer DSFA in den von den Aufsichtsbehörden definierten Fällen.⁶¹ Ausserdem werden Aufsichtsbehörden ermächtigt fakultativ auch Listen von Datenbearbeitungstätigkeiten zu führen, für die keine DSFA erforderlich ist (sog. **Negativlisten**; Art. 35 Abs. 5 DSGVO). Diese Listen unterstehen dem Kohärenzverfahren, wenn sie «Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten» (Art. 35 Abs. 6 DSGVO). Eine Pflicht zur Führung von Positiv- oder Negativlisten sieht das DSG nicht vor, obschon dies der Rechtssicherheit zuträglich wäre.

- 44 Während Art. 22 Abs. 5 DSG explizit besagt, dass eine DSFA nicht durchgeführt werden muss, wenn ein Verhaltenskodex gem. Art. 11 DSG eingehalten wird und die zusätzlichen Voraussetzungen nach Abs. 5 erfüllt sind, sind solche **Verhaltensregeln gemäss DSGVO nur im Rahmen der Beurteilung der Auswirkungen der betreffenden Datenbearbeitung** in der DSFA zu berücksichtigen. Sie entbinden den Verantwortlichen jedoch nicht von der Pflicht, eine DSFA durchzuführen, wenn diese gesetzlich zwingend erforderlich ist.
- 45 Schliesslich sieht Art. 35 Abs. 10 DSGVO, ähnlich wie Art. 22 Abs. 4 DSG, vor, dass keine DSFA durchgeführt werden muss, wenn eine Datenbearbeitung auf einer gesetzlichen Grundlage beruht. Die **Ausnahme in der DSGVO ist jedoch enger gefasst**: Die Ausnahme greift nur, wenn eine DSFA im Rahmen des Erlasses der Rechtsgrundlage durchgeführt wurde und die Rechtsgrundlage den konkreten Bearbeitungsvorgang bzw. die konkreten Bearbeitungsvorgänge regeln. Die praktische Bedeutung dürfte sich somit in Grenzen halten.⁶² Ausserdem besteht eine Ausnahme gem. Art. 35 Abs. 10 DSGVO, sofern die Datenbearbeitung in Erfüllung von öffentlichen Interessen oder in Ausübung öffentlicher Gewalt ausgeführt wird.
- 46 Die DSGVO sieht für die Verletzung der Pflicht zur Durchführung einer DSFA **Bussen bis zu € 10 Mio. oder bis zu 2% des gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres vor (Art. 83 Abs. 4 lit. a DSGVO). Diese Busse steht im Gegensatz zum DSG, das für eine solche Verletzung keine Busse vorsieht (vgl. N. 35).

LITERATURVERZEICHNIS

Baeriswyl Bruno, Der «grosse Bruder» DSGVO und das revDSG: Ein vergleichender Überblick, S. 8–15.

Blonski Dominika, Kommentierung zu Art. 22 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Zürich/Basel, 2023

Blonski Dominika, DSFA und Vorabkonsultation, digma 2020, S. 28–32.

Früh Alfred/Haux Dario, Foundations of Artificial Intelligence and Machine Learning, Weizenbaum Series 29, DOI: 10.34669/WI.WS/29.

Klaus Samuel, KI trifft Datenschutz – Risiken und Lösungsansätze, in: Epiney Astrid/Rovelli Sophia, Künstliche Intelligenz und Datenschutz, Zürich 2021, S. 81–95.

60. Siehe dazu Schönbachler, S. 190.

61. Baeriswyl, S. 12.

62. Gl.M. Kühling/Buchner/Jandt, Kommentar, Art. 35 DS-GVO N. 23.

Lobsiger Adrian, Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, SJZ 2023, S. 311–319.

Pfaffinger Monika, Das Recht auf informationellen Systemschutz. Plädoyer für einen Paradigmenwechsel im Datenschutzrecht, Habil., Baden-Baden 2022.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16. November 2020.

Schönbächler Matthias R., Zum neuen Schweizer Datenschutzrecht, ZBJV 2023, S. 171–195.

Schürmann Kathrin, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz: Bewertung und Minimierung der Risiken, ZD 2022, S. 316–321.

Vasella David, Widersprüche im Datenschutzrecht, digma 2020, S. 174–179.

Vasella David/Sievers Jacqueline, Der «Swiss Finish» im Vorentwurf des DSG, digma 2017, S. 44–49.

Widmer Michael, Datenschutz-Folgenabschätzung, digma 2017, S. 224–231.

Kühling Jürgen/Benedikt Buchner, Datenschutz-Grundverordnung BDSG, Kommentar, 3. Aufl., München, 2020.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW/RSDA 2021, S. 52–64.

MATERIALIENVERZEICHNIS

Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017, S. 6941 ff., abrufbar unter: <https://fedlex.data.admin.ch/eli/fga/2017/2057>, besucht am 5.6.2023.