



ONLINEKOMMENTAR
DER FREI ZUGÄNLICHE
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

Art. 7 DSGVO

Eine Kommentierung von Samuel Klaus

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

Stand der Bearbeitung: 16.09.2023

PDF erstellt am: 06.10.2026

DOI: 10.17176/20230824-172340-0

ZITIERVORSCHLAG

Samuel Klaus, Kommentierung zu Art. 7 DSGVO, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Kurzzitat: OK-Klaus, N. XXX zu Art. 7 DSGVO.

Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

¹ Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

² Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

³ Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

GLIEDERUNG

In Kürze	3
I. Allgemeines.....	3
A. Vorbemerkungen und Hintergrund.....	3
B. Adressat.....	4
II. Datenschutz durch Technik / Privacy by Design (Abs. 1-2)	4
A. Begriff und Hintergrund	4
B. Inhalt und Umfang (Abs. 1).....	5
C. Angemessenheit (Abs. 2).....	6
D. Umsetzung in der Praxis	7
1. Internationale Normen	7
2. Leitfäden und Orientierungshilfen	8
3. Beispiele möglicher Massnahmen	10
III. Datenschutzfreundliche Voreinstellungen / Privacy by Default (Abs. 3).....	11
A. Begriff.....	11
B. Inhalt und Umfang.....	12
C. Umsetzung in der Praxis	13
IV. Folgen bei Pflichtverletzung.....	14
V. Übergangsbestimmungen	14
Literaturverzeichnis.....	15
Materialienverzeichnis	16

IN KÜRZE

Privacy by Design und Privacy by Default dienen als Leitprinzipien zur Umsetzung des Datenschutzes. Gemäss dem Prinzip von Privacy by Design sollen vorausschauend bereits ab der Planung einer Datenbearbeitung angemessene Massnahmen vorgesehen werden, um einen systemischen Datenschutz zu gewährleisten. Stehen den Betroffenen bzw. Nutzenden mehrere Einstellungs-/ Wahlmöglichkeiten zur Verfügung, soll das Prinzip von Privacy by Default sicherstellen, dass die Voreinstellung die datenschutzfreundlichste Kombination an Einstellungsmöglichkeiten abbildet.

I. ALLGEMEINES

A. Vorbemerkungen und Hintergrund

- 1 Die Prämisse, dass datenschutzrechtliche Vorgaben mittels passender technischer Massnahmen umzusetzen sind, galt grundsätzlich schon unter bisherigem Recht, da sich anderweitig die Vorgaben von Art. 4 aDSG (Grundsätze) und Art. 7 aDSG (Datensicherheit) gar nicht erreichen liessen. Das revidierte Datenschutzgesetz bringt dies nun explizit in Art. 7 DSG zum Ausdruck mit den beiden Prinzipien «**Privacy by Design**» (Datenschutz durch Technik, Art. 7 Abs. 1-2 DSG) und «**Privacy by Default**» (Datenschutzfreundliche Voreinstellungen, Art. 7 Abs. 3 DSG). Inhaltlich ist Art. 7 DSG zu lesen in Zusammenhang mit Art. 6 DSG (Grundsätze) und Art. 8 DSG (Datensicherheit): Die technischen und organisatorischen Massnahmen, die durch Privacy by Design («**PbDesign**») eingesetzt werden, sollen insbesondere die Umsetzung der Grundsätze gemäss Art. 6 DSG ermöglichen, und die Gewährleistung der Datensicherheit (Art. 8 DSG) stellt dabei - nebst anderen - einen der relevanten Fokuspunkte dar. Speziell erwähnt wird in Art. 7 Abs. 3 DSG mit dem Prinzip von «Privacy by Default («**PbDefault**») auch ein wichtiger Unteraspekt von PbDesign.
- 2 Der **Normzweck** von Art. 7 DSG ist stark programmatisch geprägt und damit in der konkreten Umsetzung schwer zu fassen:¹ Die Absicht hinter PbDesign liegt darin, die systemischen Voraussetzungen zu schaffen für die Erfüllung und (dauerhafte) Gewährleistung des Datenschutzes. Ob dies angesichts des eingeschränkten Adressatenkreises (vgl. unten Abschnitt B) zielführend ist, wird sich zeigen müssen.
- 3 Rechtsdogmatisch geht die Einführung von PbDesign und PbDefault zurück auf Art. 10 Abs. 2-4 der **ER-Konv 108+**,² welche mit Inkrafttreten des revidierten DSG ratifiziert wird.³ Für Bundesorgane wurden PbDesign und PbDefault im Anwendungsbereich des SDSG⁴ bereits seit 1. März 2019 (Art. 5 SDSG) vorgeschrieben. Das SDSG wird mit Inkrafttreten des revidierten DSG aufgehoben, die Verpflichtung zu PbDesign und PbDefault wird dann für alle Adressaten im DSG geregelt. Art. 7 DSG setzt die Vorgaben von Art. 10 Abs. 2-4 der ER-Konv 108+ um (vgl. dazu Art. 4 Abs. 1 der ER-Konv 108+),⁵ in ähnlicher, aber nicht identischer Weise wie dies in Art. 25 DSGVO für die EU-Mitgliedstaaten erfolgt.
- 4 Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) setzt somit dieselben generellen Vorgaben um, unter Verwendung derselben Begriffe und mit gleicher Stossrichtung - aber vor dem leicht anders geprägten Hintergrund der DSGVO-

1. SHK DSG-Baeriswyl, Art. 7 N. 10 spricht von einem «wohlgemeinten Rat des Gesetzgebers».

2. SHK DSG-Baeriswyl/Pärli, S. 9 N. 28.

3. SHK DSG-Baeriswyl/Pärli, S. 7 N. 17.

4. Schengen-Datenschutzgesetz, SR 235.3, <https://www.fedlex.admin.ch/eli/cc/2019/112/de>, besucht am 2.7.2023.

5. SHK DSG-Baeriswyl/Pärli, S. 7 Fn. 47.

Systematik. Bei der Anwendung, Auslegung und Umsetzung von Art. 7 DSG kann somit die **Literatur und Rechtsprechung zu Art. 25 DSGVO** hilfreich sein,⁶ wobei gewissen Unterschieden Rechnung zu tragen ist: Insbesondere die unterschiedliche Ausgangslage bezüglich Datenbearbeitungen (Verbotsprinzip mit Erlaubnisvorbehalt unter der DSGVO gegenüber grundsätzlich erlaubter Datenbearbeitung mit Einschränkungen und Rechtfertigungsmöglichkeit unter dem DSG) ist bei der analogen Anwendung von für die Umsetzung von Art. 25 DSGVO entwickelten Leitlinien zu berücksichtigen. Ob sich daneben im Laufe der Zeit bei der Umsetzung der Prinzipien von PbDesign und PbDefault unter dem DSG massgebliche Unterschiede zu derjenigen unter der DSGVO ergeben werden, wird sich zeigen müssen. Aus pragmatischer Sicht wäre dies zugunsten einer möglichst einheitlichen Anwendung dieser grundlegenden Prinzipien zu vermeiden.

B. Adressat

- 5 Adressat der Vorgaben von Art. 7 DSG sind die **Verantwortlichen**, wobei sowohl Private wie Bundesorgane angesprochen sind.⁷ Nicht erfasst werden hingegen Auftragsbearbeiter, vorgelagerte Dienstleister oder Hersteller: Vom Grundgedanken und Normzweck von PbDesign erfasst werden sollten an sich insbesondere auch die Planer, Hersteller und Vertreiber von Systemen, Applikationen und weiterer Hilfsmittel, die für die Datenbearbeitung eingesetzt werden. Diese werden aber vom Anwendungsbereich von Art. 7 DSG nicht bzw. nur indirekt durch die Verpflichtung der Verantwortlichen erfasst.
- 6 Während die Verantwortlichen somit direkt in der Pflicht stehen, die Vorgaben von Art. 7 DSG umzusetzen, wird der **Grundgedanke des «systemischen Datenschutzes»** gegenüber den in der Wertschöpfungskette vorgelagerten Akteuren **nur indirekt umgesetzt**: Die Verantwortlichen sind nach Art. 7 DSG verpflichtet, durch entsprechende Massnahmen dafür zu sorgen, dass vorgelagerte Dienstleistungen und Produkte so ausgestaltet sind, dass sie (die Verantwortlichen) ihre Pflicht zu PbDesign und PbDefault nach Art. 7 DSG erfüllen können. Dies ist von den Verantwortlichen z.B. mittels vertraglicher Vorgaben gegenüber Dienstleistern oder Lieferanten, entsprechender Ausgestaltung von Beschaffungsvorgaben etc. zu berücksichtigen.

II. DATENSCHUTZ DURCH TECHNIK / PRIVACY BY DESIGN (ABS. 1-2)

A. Begriff und Hintergrund

- 7 Das **Konzept von PbDesign** basiert auf der Idee, dass technische Mittel die Umsetzung der Datenschutzvorgaben nicht hindern, sondern vielmehr ermöglichen und sogar fördern sollten. Ursprünglich unter dem Stichwort von spezifischen «Privacy Enhancing Technologies (PET)» diskutiert, entwickelte sich PbDesign über die Zeit zu einem umfassenderen Konzept.⁸ Es besteht keine allgemeinverbindliche Definition, vielmehr wird der Begriff jeweils kontextabhängig verwendet.
- 8 Inhaltlich geprägt wurde der Begriff des PbDesign massgeblich durch Ann Cavoukian (Datenschutzbeauftragte von Ontario, Kanada, von 1997-2014), mit einem Konzept von PbDesign **basierend auf 7 Prinzipien** (Prinzipien in *kursiv*, Hervorhebungen in *fett* gemäss Cavoukian-Implementation):⁹

6. Ebenso SHK DSG-Baeriswyl/Pärli, S. 13 N. 48, S. 15 N. 56.

7. Botschaft 2017, S. 7029.

8. Vgl. dazu Kasper, S. 319-322; Langheinrich, S. 14 f.; Harasgama/Tamò, S. 130 f.

9. Vgl. Cavoukian-Principles, S. 2, Cavoukian-Implementation, S. 2-5 und Kasper, S. 324.

1. *Proactive not Reactive; Preventative not Remedial*: PbDesign ist als proaktives, antizipierendes Konzept zu verstehen und ist darauf ausgerichtet, Datenschutzverletzungen zu verhindern (und nicht darauf, erfolgte Verletzungen zu beheben).
 2. *Privacy as the Default Setting*: Auch wenn die betroffene Person keine speziellen Handlungen vornimmt, soll der Datenschutz möglichst umfassend gewährleistet sein, vgl. unten *III - Datenschutzfreundliche Voreinstellungen | Privacy by Default (Abs. 3)*.
 3. *Privacy Embedded into Design*: Datenschutz ist bereits bei Entwurf und Umsetzung von Systemen und Prozessen integral zu berücksichtigen.
 4. *Full Functionality - Positive Sum, not Zero-Sum*: Datenschutz soll nicht verhindern oder zu Funktionseinschränkungen führen, sondern durch dessen integrale Berücksichtigung einen Mehrwert schaffen.
 5. *End-to-End Security - Full Lifecycle Protection*: Datensicherheit ist über den gesamten Lebenszyklus der betroffenen Daten zu gewährleisten.
 6. *Visibility and Transparency - Keep it Open*: Die Transparenz und Verifizierbarkeit muss gewährleistet sein.
 7. *Respect for User Privacy - Keep it User-Centric*: Die Interessen der betroffenen Personen (Datensubjekte) sind zu berücksichtigen.
- 9 Diese Grundprinzipien können als **Leitlinien und Verständnishilfen** dienen. Aufgrund ihrer eher programmatischen Ausrichtung taugen sie kaum als konkrete Umsetzungshilfen. Im Gesetzestext lassen sich zumindest Referenzen finden auf *Prinzip 1 - Proactive/Preventative* (in Art. 7 Abs. 1 DSGVO mit dem präventiven Ansatz und dem Verweis auf die Berücksichtigung ab der Planung), auf *Prinzip 2 - Default Setting* (in Art. 7 Abs. 3 DSGVO bezüglich datenschutzfreundlicher Voreinstellungen), und auf *Prinzip 3 - Embedded* (in Art. 7 Abs. 1 DSGVO mit der Pflicht zur Ausgestaltung der Datenbearbeitung in Hinblick auf die Datenschutzvorgaben und Berücksichtigung ab der Planung). *Prinzip 5 - Full Lifecycle Protection* wird sodann in Art. 8 Abs. 2 DSGVO adressiert sowie *Prinzip 1 - Proactive/Preventative* in Art. 8 Abs. 1 DSGVO.
- 10 Bei der praktischen Umsetzung können bestehende **Leitlinien allgemeiner Art** (wie z.B. die EDSA Leitlinien 4/2019 zu Artikel 25 DSGVO oder der ISO-Standard 31700 zu Privacy by Design) sowie **sektor- oder anwendungsspezifische Leitlinien** hilfreich sein (vgl. dazu unten *Abschnitt D - Umsetzung in der Praxis*). Bei deren Umsetzung sind allfällige Unterschiede zu berücksichtigen, die sich daraus ergeben, dass viele solcher Leitlinien auf die DSGVO ausgerichtet sind.

B. Inhalt und Umfang (Abs. 1)

- 11 PbDesign bezweckt, durch technische Vorkehrungen die Gefahr von Verstößen gegen Datenschutzvorschriften auszuschliessen oder zumindest zu reduzieren, ohne aber auf eine bestimmte Technologie abzielen.¹⁰ Vielmehr sollen bei der Ausgestaltung der eingesetzten Systeme, Applikationen und Prozesse angemessene **technische und organisatorische Massnahmen («TOM»)** umgesetzt werden. Dabei ist nicht nur ein spezifisches System, eine einzelne Anwendung oder ein bestimmter technischer Aspekt zu betrachten, sondern im Sinne eines «holistischen Ansatzes» die **gesamte Datenbearbeitung**, mit Fokus auf die Umsetzung der Grundsätze gemäss Art. 6 DSGVO.

10. Botschaft 2017, S. 7029.

- 12 Aus zeitlicher Sicht ist PbDesign bereits **ab dem Zeitpunkt der Planung** der Datenbearbeitung zu berücksichtigen (Art. 7 Abs. 1 Satz 2 DSGVO). Ist eine **Datenschutz-Folgenabschätzung («DSFA»)** gemäss Art. 22 DSGVO vorzunehmen, so können die zur Umsetzung von PbDesign vorgesehenen TOM in den Prozess der DSFA einfließen und dort als Massnahmen im Sinne von Art. 22 Abs. 3 DSGVO aufgeführt werden. Die Pflicht zu PbDesign und die Pflicht zur Vornahme einer DSFA sind jedoch voneinander unabhängig, d.h. die Pflicht zu PbDesign besteht auch dann, wenn kein «hohes Risiko» im Sinne des Aufgreifkriteriums von Art. 22 Abs. 1 DSGVO zur Vornahme einer DSFA vorliegt.

C. Angemessenheit (Abs. 2)

- 13 Die im Rahmen von PbDesign umzusetzenden TOM müssen **«angemessen»** sein, was den risikobasierten Ansatz dieser Vorschrift zum Ausdruck bringt. Als massgebliche **Kriterien** zur Beurteilung der Angemessenheit erwähnt werden in Art. 7 Abs. 2 DSGVO «insbesondere» (a) der *Stand der Technik*, (b) *Art und Umfang der Datenbearbeitung*, und (c) das *Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen*. Diese Aufzählung ist nicht abschliessend, massgeblich ist die Gesamtsicht unter Berücksichtigung der spezifischen Umstände.
- 14 Der **Stand der Technik** bezeichnet einen fortschrittlichen technischen Entwicklungsstand, der sich in der praktischen Anwendung bewährt bzw. im Markt durchgesetzt hat. Dazu gehört auch die wirtschaftliche Umsetzbarkeit aus allgemeiner, objektiver Sicht (nicht derjenigen des jeweiligen Verantwortlichen). Da sich der Stand der Technik insbesondere im digitalen Bereich stets weiterentwickelt, beinhaltet die Umsetzung von PbDesign auch eine **Pflicht zur regelmässigen Prüfung**, ob die umgesetzten TOM nach wie vor dem aktuellen Stand der Technik entsprechen oder nötigenfalls anzupassen sind:¹¹ Art. 7 Abs. 1 DSGVO gibt diesbezüglich vor, dass PbDesign «ab» (und nicht bloss «bei») der Planung zu berücksichtigen ist.
- 15 Die **Art und der Umfang der Datenbearbeitung** beziehen sich auf die inhaltlichen und quantitativen Komponenten der Bearbeitung: Aus inhaltlicher Sicht ist insbesondere massgeblich, welche Daten(kategorien) in welcher Weise und zu welchem Zweck bearbeitet werden. Aus quantitativer Sicht ist sowohl der Umfang an Datensubjekten (d.h. die Zahl der betroffenen Personen) wie auch der Umfang der bearbeiteten Datenkategorien (d.h. die Zahl der betroffenen Datensätze) zu berücksichtigen.¹²
- 16 Das **Risiko für die betroffenen Personen** ist der allgemeine Massstab zur Beurteilung der Angemessenheit der TOM. Je höher das Risiko, d.h. je grösser die Eintrittswahrscheinlichkeit und die potentiellen Folgen sind, umso höher sind die Anforderungen an die technischen Vorkehren, damit sie als angemessen gelten können.¹³ Klar strukturierte und mathematisch-probabilistisch ausgerichtete Hilfsmittel können bei der Risikobeurteilung als Hilfsmittel dienen. Sie sollten aber nur als Ausgangspunkt dienen, da die Risikobeurteilung aus gesamtheitlicher, inhaltsbezogener Sicht und unter Berücksichtigung sämtlicher (nicht bloss probabilistischer) Aspekte vorzunehmen ist.
- 17 Bei der Beurteilung der Angemessenheit ist generell kein absoluter, sondern ein **risikobasierter Massstab** anzuwenden. Dabei ist das Risiko, das mit einer Bearbeitung einhergeht, in Beziehung zu setzen zu den technischen Möglichkeiten, um dieses zu verringern.¹⁴ Das Prinzip von PbDesign zielt darauf hin, für den Zielkonflikt zwischen Datenbearbeitung und Datenschutz einen angemessenen Ausgleich zu schaffen. Im Sinne des von Cavoukian formulierten *Prinzip 4 - Positive Sum, not Zero-*

11. Vgl. SHK DSGVO-Baeriswyl, Art. 7 N. 16.

12. Vgl. SHK DSGVO-Baeriswyl, Art. 7 N. 18.

13. Botschaft 2017, S. 7030.

14. Botschaft 2017, S. 7030.

Sum (vgl. oben N. 8) sollen Datenbearbeitungen nicht verhindert werden, sondern unter angemessener Berücksichtigung der Datenschutzvorgaben gerade ermöglicht werden, um damit einen Mehrwert für Verantwortliche und Betroffene zu schaffen.

D. Umsetzung in der Praxis

- 18 Ein einfaches Erfolgsrezept, wie PbDesign universell umgesetzt werden kann, gibt es nicht. PbDesign ist als projektspezifischer Prozess zu verstehen. Entsprechend gibt es auch kein allgemeingültiges Vorgehen, das sämtliche Anwendungsfälle abdecken kann. Vielmehr sind die umzusetzenden TOM (1.) auf die Besonderheiten der jeweiligen Datenbearbeitungen, (2.) auf das sektorspezifische Umfeld, in dem diese stattfinden, und (3.) auf die vorbestehenden Systeme und Prozesse, in welche diese eingebettet werden, auszurichten (wobei diese nötigenfalls auch anzupassen sind). Die erfolgreiche Umsetzung von PbDesign setzt somit voraus, dass die **projekt- bzw. bearbeitungsspezifischen Risiken und Anforderungen** erfasst und mit konkreten, auf diese zugeschnittenen Massnahmen, adressiert werden. Dabei decken die Massnahmen zur Umsetzung der Datensicherheit (Art. 8 DSGVO, Art. 1-6 DSV) nur einen (wenn auch überaus relevanten) Teilbereich ab (vgl. dazu unten N. 30).
- 19 Empfehlenswert ist ein klar **strukturiertes Vorgehen** anhand der für den Anwendungsfall einschlägigen Orientierungshilfen, ergänzt mit weitergehenden eigenen Abklärungen und Vorgaben aufgrund der projektspezifischen Besonderheiten. Dieses Vorgehen sollte genügend **dokumentiert** werden, um eine spätere Überprüfung und Aktualisierung (z.B. aufgrund technischer Änderungen, Weiterentwicklung des Stands der Technik, Anpassungen des Business Case, etc.) zu ermöglichen.
- 20 Als **Orientierungshilfe** können verschiedene Hilfsmittel beigezogen werden wie Internationale Normen, Best Practices von Branchenverbänden, Leitfäden von Datenschutzbehörden, etc. Bei der Umsetzung zu beachten ist, dass solche Orientierungshilfen als Ausgangspunkt nützlich sein können, in jedem Fall aber noch um die Anforderungen des spezifischen Anwendungsfalls und bezüglich dem derzeitigen Stand der Technik zu ergänzen sind. Ebenfalls zu berücksichtigen ist, dass viele dieser Orientierungshilfen mit Blick auf Art. 25 DSGVO formuliert wurden. Bei deren Verwendung sind deshalb allfällige Unterschiede unter dem DSGVO zu beachten, wie insbesondere die unterschiedliche Ausgangslage bezüglich Datenbearbeitungen (Verbotsprinzip mit Erlaubnisvorbehalt unter der DSGVO gegenüber grundsätzlich erlaubter Datenbearbeitung mit Einschränkungen und Rechtfertigungsmöglichkeit unter dem DSGVO).

1. Internationale Normen

- 21 Die International Organization for Standardization (ISO) hat im Februar 2023 den **Standard ISO 31700 zu Privacy by Design** veröffentlicht. Dieser ist in zwei Teile gegliedert: ISO 31700-1:2023 (<https://www.iso.org/standard/84977.html>) und ISO/TR 31700-2:2023 (<https://www.iso.org/standard/84978.html>).
- 22 Der erste Teil (**ISO 31700-1:2023 - Consumer protection - Privacy by design for consumer goods and services - Part 1: High-level requirements**) enthält nebst allgemeinen Hinweisen und Begriffsdefinitionen (Abschnitte 1-3) in den Abschnitten 4-8 eine Übersicht allgemein gehaltener Anforderungen und Verfahren an die Gestaltung eines Produkts/Services über den gesamten Lebenszyklus (wie z.B. Abschnitt 4.4 - *Designing human computer interface (HCI) for privacy*, Abschnitt 7.2 - *Integrating the design and operation of privacy controls into the product development and management lifecycles*, oder Abschnitt 8.2 - *Designing privacy controls for retirement and end of use*). Da der ISO-Standard nicht auf einem bestimmten datenschutzrechtlichen Fundament aufbaut, enthält er nebst diesen designspezifischen Anforderungen auch Vorgaben zu stark vom anwendbaren (lokalen) Datenschutzrecht geprägten Aspekten (wie z.B. Abschnitt 5.2 - *Provision of privacy*

information, Abschnitt 5.4 - *Responding to consumer inquiries and complaints*, oder Abschnitt 6.2 - *Conducting a privacy risk assessment*). Derartige Vorgaben sind deshalb immer in Zusammenhang mit den jeweiligen gesetzlichen Bestimmungen zu lesen, wie z.B. Art. 19 ff. DSGVO bezüglich der Informationspflicht, Art. 22 f. DSGVO bezüglich der Datenschutz-Folgenabschätzung, etc. Sie können aber auch diesbezüglich als Grundlage für ein strukturiertes Vorgehen dienen.

- 23 Der zweite Teil (**ISO/TR 31700-2:2023 - Consumer protection - Privacy by design for consumer goods and services - Part 2: Use cases**) enthält drei illustrative Anwendungsfälle, anhand deren die Umsetzung der Vorgaben des ersten Teils aufgezeigt wird: (1) *On line retailing* (eCommerce Online Shop); (2) *Fitness company* (Fitness-Center mit Geräten, die durch Sensoren mit einer Fitness-App der Nutzenden verbunden sind); und (3) *Smart locks* (Produktlinie von elektronischen IoT-Türschlössern mit online Anbindung und zugehöriger Steuerungs-App). Durch die Use Cases werden viele praxisrelevante Aspekte abgedeckt. Die klar strukturierte Umsetzung der Vorgaben des ersten Teils in den Use Cases kann somit nicht nur der Einarbeitung in die Thematik dienen, sondern auch direkt als Checkliste bei der Umsetzung einzelner relevanter Aspekte.
- 24 Als Fazit lässt sich festhalten, dass die ISO-Standards 31700-1/2 zwar aufgrund ihrer allgemeingültigen Ausrichtung auf einem hohen Abstraktionsniveau gehalten sind. Dennoch können sie dank ihrer klaren Strukturierung als gute Grundlage dienen. Die praxisorientierten Use Cases können zudem auch im Sinne von Checklisten für vergleichbare Aspekte in anders gelagerten Anwendungsfällen hilfreich sein.

2. Leitfäden und Orientierungshilfen

- 25 Allgemeine Leitfäden und Orientierungshilfen gibt es deren viele. Die nachfolgende Auflistung kann als Einstiegshilfe und Ausgangspunkt eigener Recherchen dienen. Für einen konzeptionellen Überblick eignet sich z.B. die *EDSA-Leitlinie 4/2019 zu Artikel 25 [DSGVO]* des Europäischen Datenschutzausschusses (EDSA), während für einen eher pragmatischen Einstieg z.B. die *Privacy Patterns* dienen können:

- **EDSA-Leitlinie 4/2019 zu Artikel 25 - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen** (EDPB - European Data Protection Board / EDSA - Europäischer Datenschutzausschuss, Version 2.0 vom 20.10.2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de, besucht am 11.6.2023).
- **Privacy Patterns (privacybydesign.digital)** (Bayern Innovativ [Bayerische Gesellschaft für Innovation und Wissenstransfer mbH], Bayrisches Landesamt für Datenschutzaufsicht [BayLDA], 2023, <https://privacybydesign.digital/>, besucht am 20.5.2023).
- **Data Processing by Design and Default** (ICO - Information Commissioner's Office [UK], <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-processing-by-design-and-default/>, besucht am 21.5.2023).
- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)** (bvitg - Bundesverband Gesundheits-IT e.V. Arbeitsgruppe Datenschutz & IT-Sicherheit, GMDS - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. Arbeitsgruppe Datenschutz und IT-Sicherheit im Gesundheitswesen, GDD - Gesellschaft für Datenschutz und Datensicherheit e.V. Arbeitskreis

Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, 2018, https://www.gesundheitsdatenschutz.org/html/privacy_design_default.php, besucht am 21.5.2023).

- **OIPC (Office of the Information and Privacy Commissioner) - Privacy by Design Resources** (IAPP - International Association of Privacy Professionals), <https://iapp.org/resources/article/oipc-privacy-by-design-resources/>, besucht am 21.5.2023).
- **Manage a privacy programme - Privacy by Design (PbD)** (Digital.govt.nz - Digital Government New Zealand, 2021, <https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/>, besucht am 21.5.2023).
- **Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices** (Ann Cavoukian, 2012, <https://collections.ola.org/mon/26012/320221.pdf>, besucht am 21.5.2023).
- **Privacy and Data Protection by Design - from policy to engineering** (ENISA - European Union Agency for Networks and Information Security, 2014, <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>, besucht am 21.5.2023).

26 Gerade im Bereich der Software- und Applikationsentwicklung stellen sich diverse Fragen zur Umsetzung von PbDesign und PbDefault. Hilfestellung bieten können hier sowohl Leitfäden von Datenschutzbehörden wie auch branchenspezifische Orientierungshilfen, wie z.B.:

- **Privacy by Design and Privacy by Default - A Guide for Developers** (Catalan Data Protection Authority, 2023, https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD_EN.pdf, besucht am 20.5.2023).
- **Leitfaden: Entwicklung datenschutzkonformer Apps** (Datenschutzbeauftragte des Kantons Zürich, 2022, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_entwicklung_datenschutzkonformer_apps.pdf, besucht am 20.05.2023).
- **eHealth Suisse - Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer** (eHealth Suisse - Kompetenz- und Koordinationsstelle von Bund und Kantonen, 2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/Leitfaden_e-Health_Suisse_fuer_App_Entwickler.pdf, besucht am 21.5.2023).
- **Mobile Apps im Gesundheitswesen: Anforderungen aus dem Datenschutz** (GMDS - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V., DIG - Arbeitsgruppe Datenschutz und IT-Sicherheit im Gesundheitswesen, BvD - Berufsverband der Datenschutzbeauftragten Deutschlands e.V., 2022, https://gesundheitsdatenschutz.org/html/datenschutz_med_apps.php, besucht am 21.5.2023).
- **American Medical Association (AMA) - Privacy is Good Business - A case for privacy by design in app development** (2021), <https://www.ama-assn.org/system/files/privacy-principles-by-design.pdf>, besucht am 11.6.2023).
- **An Engineer's Guide to Privacy by Design** (Rachel Dulberg, 2021, <https://www.linkedin.com/pulse/engineers-guide-privacy-design-rachel-dulberg>, besucht am 21.5.2023).
- **Privacy Design Guidelines for Mobile Application Development** (GSMA - Global System for Mobile Communications, 2018, <https://www.gsma.com/publicpolicy/wp-content/uploads/2018/02/GSMA-Privacy-Design-Guidelines-for-Mobile-Application-Development.pdf>, Abruf am 21.5.2023).
- **Guidelines on Software development with Data Protection by Design and Default** (Norwegische Datenschutzbehörde Datatilsynet, 2017, <https://www.datatilsynet.no/en/about->

[privacy/virksohmhetenes-plikter/data-protection-by-design-and-by-default/](https://www.enisa.europa.eu/publications/big-data-protection), besucht am 21.5.2023).

- **Privacy by Design in Big Data** (ENISA - European Union Agency for Networks and Information Security, 2015, <https://www.enisa.europa.eu/publications/big-data-protection>, besucht am 21.5.2023).

3. Beispiele möglicher Massnahmen

- 27 Die konkreten Massnahmen sind jeweils in Abhängigkeit des spezifischen Anwendungsfalls und des zugehörigen Risikoprofils zu bestimmen. Die folgende Auflistung kann im Sinne einer beispielhaften **Übersicht möglicher Massnahmen** erste Ansatzpunkte aufzeigen. Ebenfalls hilfreich sein kann die Orientierung an konkreten Use Cases, vgl. hierzu z.B. Tamò-Larrieux, S. 203 ff. sowie die Use Cases in ISO/TR 31700-2:2023 (vgl. N. 23).
- 28 Mögliche Massnahmen lassen sich gruppieren in **Aspekte aus systemischer Sicht, eher technische Aspekte, und solche organisatorischer Art**. Die systemischen Aspekte beziehen sich (wie die Bearbeitungsgrundsätze nach Art. 6 Abs. 1-5 DSGVO) in einer holistischen Betrachtung auf den gesamten Business Case. Die technischen und organisatorischen Aspekte liegen im Schnittpunkt mit den Anforderungen an die Datensicherheit (Art. 8 DSGVO). Die systemischen, technischen und organisatorischen Aspekte überschneiden sich in vielen Bereichen und lassen sich kaum sauber voneinander abgrenzen. Indem aber mit den systemischen Aspekten gewisse übergeordnete Themen sozusagen «vor die Klammer» der technisch-organisatorischen Umsetzung gezogen werden, kann eine strukturierte Vorgehensweise erleichtert werden, insbesondere indem dadurch allgemeine, übergeordnete Aspekte frühzeitig in alle Überlegungen einfließen und in allen Projektphasen berücksichtigt werden können.
- 29 Aus allgemeiner, übergeordnet **systemischer Sicht** sind z.B. folgende Aspekte zu prüfen:
- **Datenminimierung (DSG 6 Abs. 2):**¹⁵ Die erfassten Personendaten sind inhaltlich (welche Daten(kategorien)) und umfangsmässig (wie viele Daten, z.B. in zeitlicher Hinsicht) auf das für die Bearbeitung des jeweiligen Geschäftsfalls (Business Case) zu beschränken, es soll keine «Datensammlung auf Vorrat» erfolgen.
 - **Datensegregation:** Zurückhaltung bei der Verknüpfung bzw. beim Pooling von Daten, der Zentralisierung von Datenhaltungen und der Aggregation von Datenbeständen, etc.
 - **Pseudonymisierung:** Pseudonymisierung kann zusätzlichen Schutz schaffen (im Sinne einer Segregation der Identifikationsinformation von anderen Datenkategorien), insb. falls die Verknüpfung gewisser Daten mit einer bestimmten Person nur für gewisse Bearbeitungsschritte notwendig ist.
 - **Datendeklaration:** Kennzeichnung der Datensätze (z.B. mittels Metadaten oder Deskriptoren) z.B. betreffend Herkunft, Schutzstufe, Speicherfrist («Ablaufdatum»), etc.
 - **Anonymisierung und/oder Löschung (Art. 6 Abs. 4 DSGVO):** Zur Umsetzung des Grundsatzes der Datenminimierung (z.B. mittels «Ablaufdaten» für gewisse Datensätze, durch regelmässige Anonymisierungs-/Lösch-Zyklen, etc.).
- 30 Aus **technischer Sicht** kann in erster Linie auf die zur Umsetzung der Datensicherheit notwendigen technischen Massnahmen verwiesen werden (vgl. dazu Art. 8 DSGVO und die Ausführungen dazu in Art. 1-6 DSV). Denkbar sind aber auch weitere technische Massnahmen, die nicht (nur) der

15. Vgl. Botschaft 2017, S. 7029.

Datensicherheit dienen, sondern den allgemeinen Datenschutzzielen generell. Relevant sein können z.B. insbesondere technische Massnahmen zur Umsetzung der allgemeinen Bearbeitungsgrundsätze (Art. 6 Abs. 1-5 DSGVO) und dem Prinzip der Datenminimierung (Art. 6 Abs. 2 DSGVO). Zu denken ist z.B. an die technische Umsetzung von Löschkonzepten (s. oben) oder die automatische Verpixelung von Gesichtern/Identifikationsmerkmalen bei nicht personenbezogenen Bildern/Videos, etc.

- 31 Aus **organisatorischer Sicht** müssen die internen Voraussetzungen geschaffen werden zur Umsetzung der systemischen und technischen Anforderungen. Dies kann z.B. folgende Aspekte umfassen:

- **Unternehmenskultur und gesamtheitliche Betrachtung:** Die Unternehmenskultur muss Datenschutz als Teil des unternehmerischen Handelns verstehen (und nicht wie häufig noch als extern auferlegte Einschränkung). Nötig ist somit eine «datenschutzfreundliche Mentalität».¹⁶ Zudem muss Datenschutz gesamtheitlich betrachtet werden, d.h. nicht nur punktuell auf eigene Bearbeitungen bezogen, sondern z.B. auch als Teil des Contract / Vendor Managements.
- **Prozesse, Zuständigkeiten und Dokumentation:** Die Umsetzung der datenschutzrechtlich relevanten Abläufe und Prozesse ist festzulegen und ausreichend zu dokumentieren. Wichtig sind insbesondere klare Zuständigkeiten und eine ausreichende Dokumentation. Auch wenn unter dem DSGVO kein allgemeines Prinzip der Rechenschaft («accountability») besteht,¹⁷ und u.U. keine Rechtspflicht besteht zur Erstellung eines bestimmten Dokumentes (z.B. eines Bearbeitungsverzeichnisses, vgl. Art. 12 i.V.m. Art. 24 DSGVO), so kann dessen Erstellung (zumindest in einer allenfalls vereinfachten Form) dennoch nötig oder zumindest hilfreich sein, um die Prinzipien von PbDesign umsetzen, in Zeitablauf überprüfen und nötigenfalls anpassen zu können.
- **Schulung und Sensibilisierung:** Damit die vorgesehenen TOM auch tatsächlich gelebt werden, sind die Mitarbeitenden entsprechend zu schulen und für die datenschutzrechtlichen Themen zu sensibilisieren, z.B. durch Datenschutztrainings, interne Weisungen und Reglemente, etc.
- **Technische Umsetzung:** Die technischen Massnahmen (N. 30) sind durch entsprechende organisatorische Massnahmen zu ergänzen, um deren Umsetzung sicherzustellen. So ist z.B. für eine effektive Zugriffsbeschränkung auch ein Prozess nötig, wie Zugriffsberechtigungen erteilt, deren Aktualität regelmässig überprüft, und deren Löschung (z.B. bei Stellenwechsel oder Änderung der Aufgaben von Mitarbeitenden) sichergestellt wird. Ebenso bedingt die Vorgabe einer Beschränkung der Speicherfrist bestimmter Daten einen zugehörigen Prozess zur regelmässigen Vornahme einer entsprechenden Prüfung und allfälligen Löschung.

III. DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN / PRIVACY BY DEFAULT (ABS. 3)

A. Begriff

- 32 **PbDefault** ist ein Teilgehalt von PbDesign (vgl. oben N. 8 Ziff. 2) und wurde in Art. 7 Abs. 3 DSGVO ausformuliert. Der Wortlaut ist dabei missverständlich, da keine Pflicht besteht, spezielle Einstellungsmöglichkeiten zu schaffen (vgl. dazu unten N. 35). Die Pflicht nach Art. 7 Abs. 3 DSGVO bezieht sich nur darauf, für den Fall, dass mehrere Einstellungsmöglichkeiten bestehen, bei diesen die **Voreinstellungen so zu setzen, dass die datenschutzrechtlich «minimalinvasivste» Datenbearbeitung umgesetzt wird.**

16. Kasper, S. 326.

17. Rosenthal, S. 22 N. 45.

- 33 Die Botschaft umschreibt die **Voreinstellungen** als «jene Einstellungen, insbesondere von Software, die standardmässig zur Anwendung kommen, d.h. falls keine abweichende Eingabe durch den Nutzer erfolgt».¹⁸ Zu verstehen sind darunter also die **Grundeinstellung**, **Standerdeinstellung** oder «**Default Configuration**» die jeweils dann zur Anwendung gelangt, wenn die Nutzenden nicht selber aktiv eine andere Einstellung wählen.

B. Inhalt und Umfang

- 34 Auch wenn in der Botschaft als Anwendungsfall speziell Software erwähnt wird, ist der Anwendungsbereich nicht auf Software- oder Systemeinstellungen beschränkt, sondern betrifft sämtliche Datenbearbeitungen. Erfasst werden somit generell sämtliche Einstellungsmöglichkeiten, die bei der Datenbearbeitung und insbesondere der Datenerfassung bestehen. Wo verschiedene Einstell- oder Wahlmöglichkeiten bestehen, ist **die datenschutzfreundlichste Kombination an Einstellungen** als Grundeinstellung vorzusehen.
- 35 Datenschutzfreundliche Voreinstellungen lassen sich nur dann vornehmen, wenn überhaupt verschiedene **Einstellungsmöglichkeiten** vorgesehen sind.¹⁹ Ob solche vorzusehen sind, ist unter dem Aspekt von PbDesign zu prüfen (N. 7 ff.). Die Vorgaben zu PbDefault (Art. 7 Abs. 3 DSG) jedenfalls statuieren keine spezifische Pflicht, in jedem Fall bestimmte Einstellungsmöglichkeiten zur Abstufung der datenschutzrechtlichen Eingriffsintensität vorzusehen.²⁰
- 36 Inhaltlich ist dabei qualitativ auf das **Mass des Eingriffs** in die Persönlichkeits- bzw. Grundrechte der Betroffenen abzustellen, nicht alleine (quantitativ) auf Anzahl und Umfang der bearbeiteten Daten. Der Hinweis in der Botschaft²¹ auf den Grundsatz der Datenminimierung ist als Verweis auf den Leitgedanken von PbDefault zu verstehen, und nicht als Hinweis, dass dessen Umsetzung rein quantitativ-technisch anzugehen wäre.²²
- 37 Als Massstab dient der **Zweck der Bearbeitung** (vgl. dazu den Wortlaut bezüglich der Beschränkung «auf das *für den Verwendungszweck* nötige Mindestmass»). Bei der Festlegung dieses Zwecks bleibt der Verantwortliche frei, d.h. es besteht keine Pflicht, gewisse Leistungen auch ohne Datenerfassung bzw. Datenbearbeitung anzubieten.²³ Wird z.B. eine Online-Leistung über personalisierte Werbung finanziert, so besteht keine Pflicht, eine werbelose Version dieser Leistung anzubieten. Bei der Umsetzung der Online-Leistung und der zugehörigen Datenbearbeitungen für die personalisierte Werbung müssen jedoch die Prinzipien von PbDesign und PbDefault beachtet werden.
- 38 Ausgehend von der datenschutzfreundlichsten Voreinstellung können die Betroffenen eine **andere Wahl** treffen und damit auch weitergehende Datenbearbeitungen erlauben.²⁴ Eine Pflicht, solche weitergehenden Wahlmöglichkeiten vorzusehen, besteht nicht. Der Verantwortliche dürfte dies aber in der Regel aus eigenem Interesse vorsehen, um Betroffenen die Möglichkeit zu geben, in weitergehende Datenbearbeitungen einzuwilligen, die nicht strikt für die Verwirklichung des eng eingegrenzten Verwendungszwecks nötig wären.

18. Botschaft 2017, S. 7030.

19. Rosenthal, S. 22 N. 47.

20. Vgl. Rosenthal, S. 22 N. 48.

21. Botschaft 2017, S. 7030.

22. Vgl. Rosenthal, S. 23 N. 49.

23. Vgl. Rosenthal, S. 23 N. 51.

24. Botschaft 2017, S. 7030.

C. Umsetzung in der Praxis

- 39 Ausgangspunkt bildet der **Verwendungszweck** und die zu dessen Umsetzung bzw. Erreichung nötige «minimalinvasivste» Datenbearbeitung. Ob dabei verschiedene Umsetzungsvarianten bzw. Einstellungs-/Wahlmöglichkeiten zur Verfügung stehen, hat der Verantwortliche anhand des Business bzw. Use Case und unter Anwendung der **Grundsätze von PbDesign** (N. 7 ff.) zu entscheiden. Ist dies der Fall, so ist als Vor- bzw. Grundeinstellung die **datenschutzfreundlichste Kombination an Einstellungs-/Wahlmöglichkeiten** vorzusehen, d.h. die Voreinstellung mit der geringsten Auswirkung auf die Persönlichkeits- bzw. Grundrechte der Betroffenen.
- 40 Wird den Betroffenen dabei die Möglichkeit eingeräumt, von diesen datenschutzfreundlichsten Einstellungen abzuweichen und weitergehende Bearbeitungen zu erlauben, so ist zu prüfen, ob für solche weitergehende Bearbeitungen eine **Einwilligung** im Sinne von Art. 6 Abs. 6 DSG nötig ist und damit die dort vorgesehenen Voraussetzungen (und u.U. auch diejenigen von Art. 6 Abs. 7 DSG) zu beachten sind.
- 41 Während (unter Schweizer Recht, im Gegensatz zur Situation unter der DSGVO) unter dem Aspekt der Einwilligung **vorab aktivierte Auswahlfelder** («angekreuzte Kästchen») je nach den Umständen auch als (ausdrückliche) Einwilligung gelten können, so scheint dies unter dem Aspekt von PbDefault als fraglich: Der Sinn und Zweck von PbDefault und dessen Ausformulierung in Art. 7 Abs. 3 DSG liegt gerade darin, dass sich die Betroffenen darauf verlassen können sollen, dass sämtliche Einstellungs-/Wahlmöglichkeiten in der Grundeinstellung **die datenschutzfreundlichste Variante umsetzen**.
- 42 Dies ist unter den Stichworten des *Vertrauensprinzips* und der *Ungewöhnlichkeitsregel* in Analogie zu den für Globalübernahmen von AGB entwickelten Auslegungsregeln zu beachten.²⁵ Der **Sinn und Zweck von PbDefault** gemäss Art. 7 Abs. 3 DSG liegt ja gerade darin, dass den Betroffenen nicht zugemutet werden soll, jede Einstellungsmöglichkeit einzeln zu studieren, auf ihre Datenschutzfreundlichkeit hin zu prüfen und dann individuell an- oder abschalten bzw. an- oder abwählen zu müssen. Vielmehr sollen sie sich darauf verlassen können, dass die Kombination an Einstellungs-/Wahlmöglichkeiten, die ihnen bei der Erstnutzung präsentiert wird, die **datensparsamste, datenschutzfreundlichste und damit «minimalinvasivste» Kombination an Einstellungsmöglichkeit** darstellt.
- 43 Je nach konkreter Formulierung der einzelnen Einstellungsmöglichkeiten kann dies selbstverständlich dazu führen, dass gewisse **Auswahlfelder bereits vorab aktiviert sein müssen**: Besteht eine Auswahlmöglichkeit z.B. in einer Option wie «Ich wünsche keine Zustellung von Produktinformationen», so müsste ein solches Auswahlfeld gemäss dem Prinzip von PbDefault standardmässig aktiviert sein (auch wenn eine Zustellung von Produktinformationen allenfalls gemäss Art. 3 Abs. 1 lit. o UWG aufgrund eines vorbestehenden Kundenverhältnisses zulässig wäre).
- 44 Abhängig von der konkreten Formulierung der einzelnen Einstellungs-/Wahlmöglichkeiten kann es somit sein, dass unter dem Aspekt von PbDefault *gewisse Optionen aktiviert sein müssen, während andere deaktiviert sein müssen*. Ausschlaggebend ist, dass mit der Kombination von aktivierten / deaktivierten Optionen im jeweiligen Einzelfall die **datenschutzfreundlichste Kombination an Einstellungs-/Wahlmöglichkeiten** umgesetzt wird. Die Betroffenen sollen sich darauf verlassen können, dass sie, sofern sie an diesen Voreinstellungen keine Änderungen vornehmen, stets in den Genuss der datenschutzfreundlichsten Einstellung kommen.
- 45 Gemäss der hier vertretenen Ansicht hat dies **auch für die Voreinstellung im Rahmen der Einholung von Einwilligungen** zu gelten.²⁶ Die Vorgaben zu PbDefault sind nicht auf rein

25. Vgl. dazu Reber, S. 44 ff.

technische Parameter beschränkt, sondern gemäss Art. 7 Abs. 3 DSGVO auf «die Bearbeitung der Personendaten» generell gerichtet. In einer gesamtheitlichen Betrachtung, wie sie die Konzepte von PbDesign und PbDefault voraussetzen, sind dabei auch allfällige Einholungen von Einwilligungen mitzuverstehen. Heranzuziehen ist hier die **Ungewöhnlichkeitsregel**: Bestätigen die Nutzenden AGB im Rahmen einer Globalübernahme, so werden sie dabei durch die Ungewöhnlichkeitsregel vor unerwarteten Konsequenzen geschützt.²⁷ Gleiches sollte bei der Anpassung von Einstellungsmöglichkeiten und der Einholung von Einwilligungen gelten: **Das Prinzip von PbDefault schafft bei den Betroffenen die berechnigte Erwartung, dass sie ohne Vornahme eigener Anpassungen jederzeit von der datenschutzfreundlichsten Einstellung profitieren.** Dies sollte nicht durch die Zulassung von voraktivierten Auswahlfeldern für weitergehende, nicht der datenschutzfreundlichsten Grundeinstellung entsprechende Bearbeitungen unterlaufen werden. Vielmehr sollten die Betroffenen in ihrem Vertrauen auf die umfassende Umsetzung des Prinzips von PbDefault geschützt werden. Massgeblich für die Beurteilung sind dabei die konkreten Umstände des jeweiligen Anwendungsfalls.

IV. FOLGEN BEI PFLICHTVERLETZUNG

- 46 Die Verletzung der Pflichten von Art. 7 DSGVO hat **keine direkten Sanktionsfolgen** (vgl. Art. 60 ff. DSGVO).²⁸ Auch stellt eine solche Verletzung der Pflicht zur Umsetzung von PbDesign und PbDefault per se (noch) keine Persönlichkeitsverletzung dar: In Art. 30 Abs. 2 lit. a DSGVO wird explizit nur auf Art. «6 und 8» (und nicht «6 bis 8») verwiesen: «Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn: (a) Personendaten entgegen den Grundsätzen nach den Artikeln 6 und 8 bearbeitet werden».
- 47 Hingegen kann eine Verletzung der Pflichten von Art. 7 DSGVO **indirekte Sanktionsfolgen** haben, wenn die einer Bearbeitung zugrundeliegenden Systeme, Applikationen und Prozesse die Erfüllung der Datenschutzvorgaben aufgrund ungeeigneter Planung und/oder Umsetzung verunmöglichen oder einschränken. Wenn z.B. gespeicherte Personendaten nicht personenbezogen aufgerufen (und nötigenfalls bearbeitet, korrigiert oder gelöscht) werden können, und dies dem Verantwortlichen bekannt ist (oder sein muss), so ist es nur noch ein kleiner Schritt zur (eventual-)vorsätzlichen Erteilung einer falschen oder unvollständigen Auskunft im Sinne von Art. 60 Abs. 1 lit. a DSGVO.
- 48 Eine ungenügende Umsetzung der Grundsätze von PbDesign und PbDefault kann zudem dazu führen, dass die vorgenommenen Datenbearbeitungen generell gegen Datenschutzvorschriften verstossen, insbesondere gegen die Grundsätze von Art. 6 DSGVO. Liegen genügend Anzeichen für solche Verstösse vor, so kann der EDÖB von Amtes wegen oder auf Anzeige hin eine **Untersuchung** eröffnen (Art. 49 Abs. 1 DSGVO) und entsprechende **Anordnungen** erlassen (Art. 51 DSGVO), inklusive der **Anordnung, die Grundsätze von PbDesign und PbDefault umzusetzen** (Art. 51 Abs. 3 lit. b DSGVO). Wird dann einer Verfügung des EDÖB nicht Folge geleistet, droht eine Sanktion nach Art. 63 DSGVO (Missachten von Verfügungen).

V. ÜBERGANGSBESTIMMUNGEN

- 49 Grundsätzlich ist das DSGVO ab dessen Inkrafttreten für sämtliche Datenbearbeitungen direkt anwendbar, sofern Art. 69 ff. DSGVO keine speziellen **Übergangsbestimmungen** vorsehen. Gemäss Art. 69 DSGVO (Übergangsbestimmungen betreffend laufende Bearbeitungen) sind die Vorgaben von Art. 7 DSGVO nicht auf bereits bestehende Datenbearbeitungen anwendbar, die unverändert fortgeführt

26. A.M. OFK-Spacek zu Art. 7 DSGVO, N. 26 und Rosenthal, S. 23 N. 50.

27. Vgl. zur AGB-Kontrolle von Datenschutzerklärung Reber, S. 41 ff.

28. Rosenthal, S. 21 N. 43 und S. 23 N. 52.

werden: «Die Artikel 7, 22 und 23 sind nicht anwendbar auf Datenbearbeitungen, die vor Inkrafttreten dieses Gesetzes begonnen wurden, wenn der Bearbeitungszweck unverändert bleibt und keine neuen Daten beschafft werden.»

- 50 Die Ausnahmebestimmung von Art. 69 DSG bezieht sich somit nur auf Datenbearbeitungen mit rein statischen Datenbeständen und gleichbleibendem Bearbeitungszweck und nur auf bereits **bestehende Datenbearbeitungen**, nicht auf die dafür verwendeten Systeme, Applikationen, Prozesse oder andere Aspekte der Datenbearbeitung als solche: Sobald mit einem bestehenden System, einer bestehenden Applikation oder einem eingespielten Prozess *neue Daten* bearbeitet werden, oder *zu neuen Zwecken*, so muss sich dieses System, diese Applikation oder dieser Prozess (oder anderweitige Aspekt der Datenbearbeitung) an den neu geltenden Vorgaben von PbDesign und PbDefault messen lassen. Während somit z.B. Legacy-Systeme, die unverändert weiterbetrieben werden (wie z.B. eine rein statische Archiv-Applikation ohne neue Datenzuflüsse), unter die Übergangsbestimmungen fallen, sind bestehende operative Systeme, Applikationen und Prozesse gemäss den Prinzipien von PbDesign und PbDefault auszugestalten und kontinuierlich dem entsprechenden Stand der Technik anzupassen.

LITERATURVERZEICHNIS

Baeriswyl Bruno, Kommentierung zu Art. 7 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpfli Handkommentar, 2. Aufl., Bern 2023 (zit. SHK DSG-Baeriswyl, Art. 7).

Baeriswyl Bruno/Pärli Kurt, DSG und europäisches Datenschutzrecht, in (S. 1 ff): Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpfli Handkommentar, 2. Aufl., Bern 2023 (zit. SHK DSG-Baeriswyl/Pärli).

Cavoukian Ann, Privacy by Design - The 7 Foundational Principles, Kanada 2011, <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>, besucht am 25.4.2023 (zit. Cavoukian-Principles).

Cavoukian Ann, Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices, Kanada 2011, <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf, besucht am 25.4.2023 (zit. Cavoukian-Implementation).

Harasgama Rehana/Tamò Aurelia, Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: ZIK - Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 59 (2014), Big Data und Datenschutz - Gegenseitige Herausforderungen, S. 117-149.

Kasper Gabriel, People Analytics in privatrechtlichen Arbeitsverhältnissen - Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, in: RnT - Schriften zum Recht der neuen Technologien Band/Nr. 02, Zürich 2021, <https://www.alexandria.unisg.ch/handle/20.500.14171/111087> (Hauptseite) sowie <https://www.alexandria.unisg.ch/bitstreams/8a467009-dc08-4740-8d49-b8810c31fd35/download> (PDF), besucht am 27.4.2023.

Langheinrich Marc, Mehr Datenschutz durch Technik? - Die Umsetzung der technikbezogenen Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) in der Praxis, digma 2017, S. 14 ff.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter vom 16.11.2020, <https://www.rosenthal.ch/downloads/Rosenthal-revidiertesDSG.pdf>, besucht am 1.7.2023.

Spacek Dirk, Kommentierung zu Art. 7 DSG, in: Bieri Adrian/Powell Julian, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Orell Füssli, Zürich 2023 (zit. OFK-Spacek zu Art. 7 DSG).

Reber Yannick, Die AGB-Kontrolle von Datenschutzerklärungen, ius.full - Forum für juristische Bildung 2/2023, S. 40-53.

Tamò-Larrioux Aurelia, Designing for Privacy and its Legal Framework - Data Protection by Design and Default for the Internet of Things, in: Law, Governance and Technology Series - Issues in Privacy and Data Protection, Vol. 40, Springer, Cham 2018.

MATERIALIENVERZEICHNIS

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017, BBl 2017 S. 6941 ff., <https://www.fedlex.admin.ch/eli/fga/2017/2057/de>, besucht am 26.6.2023.

Revidierte Europaratskonvention zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 10.10.2018, BBl 2020 S. 599 ff., <https://www.fedlex.admin.ch/eli/fga/2020/62/de>, besucht am 2.7.2023 (zit. ER-Konv 108+), basierend auf ER-Konv 108 (SR 0.235.1).