www.jusletter.ch

Florent Thouvenin / Matthias Glatthaar / Juliette Hotz / Claudius Ettlinger / Michael Tschudin

Privacy Icons: Transparenz auf einen Blick

Die Transparenz von Datenbearbeitungen ist ein Grundpfeiler des Datenschutzrechts. Die meisten Unternehmen sind bestrebt, die betroffenen Personen durch Datenschutzerklärungen über die Bearbeitung von Personendaten zu informieren. Datenschutzerklärungen werden aber kaum gelesen, die Transparenz bleibt damit meist reine Theorie. Abhilfe können Privacy Icons schaffen. Diese geben die wichtigsten Inhalte von Datenschutzerklärungen bildlich wieder und erlauben es den betroffenen Personen, sich auf einen Blick über die Bearbeitung ihrer Daten zu informieren. Solche Privacy Icons werden nun von mehreren grossen Schweizer Unternehmen verwendet.

Beitragsart: Beiträge
Rechtsgebiete: Datenschutz

Zitiervorschlag: Florent Thouvenin / Matthias Glatthaar / Juliette Hotz / Claudius Ettlinger / Michael Tschudin, Privacy Icons: Transparenz auf einen Blick, in: Jusletter 30. November 2020

Inhaltsübersicht

1. Problem

[1] Die Transparenz von Datenbearbeitungen ist ein Grundpfeiler des Datenschutzrechts. Das gilt für das schweizerische ebenso wie für das europäische Recht. Hier wie dort ist das Schaffen von Transparenz ein zentraler Grundsatz, der als solcher geregelt[1] und in einer Reihe von Vorschriften konkretisiert wird, namentlich durch teilweise weitgehende Informationspflichten[2] und ein grundsätzlich umfassendes Auskunftsrecht[3].

[2] Versteht man das Datenschutzrecht als Umsetzung des Rechts auf informationelle Selbstbestimmung[4] oder zumindest als Mittel, den betroffenen Personen eine gewisse Kontrolle über die Bearbeitung ihrer Daten[5] zu gewähren, so ist zentral, dass die Betroffenen die Bearbeitung ihrer Daten erkennen können. Dies sicherzustellen, ist allerdings nicht ganz einfach. Die meisten Unternehmen sind bestrebt, in Datenschutzerklärungen darzustellen, welche Daten sie zu welchen Zwecken bearbeiten. Datenschutzerklärungen sind allerdings oft recht umfangreich und bisweilen wenig verständlich[6]. Es ist denn auch erwiesen, dass sie von den Betroffenen kaum gelesen werden[7]. Zwar können Datenschutzerklärungen dennoch wichtige Funktionen erfüllen, etwa weil sie Unternehmen zwingen, ihre Datenbearbeitungen offen zu legen oder weil sie interessierten Personen ermöglichen, sich mit geringem Aufwand über die Bearbeitung ihrer Daten zu informieren. Transparenz in dem Sinn, dass die betroffenen Personen ganz allgemein um die Bearbeitung ihrer Daten wissen, vermögen sie aber nicht zu schaffen.

---

1 Art. 4 Abs. 4 DSG bzw. Art. 5 Abs. 3 E-DSG; Art. 5 (1) (a) DSGVO.

2 Art. 14 DSG bzw. Art. 17 ff. E-DSG; Art. 13 f. DSGVO.

3 Art. 8 DSG bzw. Art. 23 E-DSG; Art. 15 DSGVO.

4 Siehe dazu statt vieler: Urs Maurer-Lambrou/Simon Kunz, in: Maurer-Lambrou/Blechta (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, DSG 1 N 16–19. Kritisch hierzu allerdings: Florent Thouvenin, Datenschutz auf der Intensivstation, digma 2019, 206 ff., 211 f.; Thomas Gächter/Philipp Egli, Informationsaustausch im Umfeld der Sozialhilfe, in: Jusletter 6. September 2010, Rz. 24–28; Regina E. Aebi-Müller, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Bern 2005, 609 f.

5 So ausdrücklich: E. 7, E. 68, E. 75, E. 85 DSGVO; Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 413 ff., 417 f.; siehe auch Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff., 6969, 6971, 7181.

6 Siehe z.B. die Analyse von 150 Datenschutzerklärungen durch die New York Times: New York Times, We Read 150 Privacy Policies. They Were an Incomprehensible Disaster, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

7 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policy Makers, FTC Report, März 2012, 2, 61; Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review 2013, 1880–1903, 1884 ff.; Jonathan A. Obar/Anne Oeldorf-Hirsch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, Information, Communication & Society (Vol. 23) 2020, 128–147, 140 ff.; Aleecia M. McDonald/Lorrie F. Cranor, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 2008, 543–568, 565, schätzen, dass ein US-Internetnutzer jährlich 201 Stunden mit dem Lesen von Datenschutzerklärungen der von ihm genutzten Services verbringen würde.

2. Lösungsansatz

[3] Mit Blick auf die fundamentale Bedeutung und das weitgehende Fehlen echter Transparenz im Datenschutz haben sich vor drei Jahren in der Schweiz einige Juristinnen und Juristen in einer informellen Projektgruppe zusammengeschlossen, um eine Lösung zu entwickeln. Der Ansatz lag rasch auf der Hand: Statt langer Texte sollten einfache «Privacy Icons» Transparenz schaffen. Diese Idee ist nicht neu. Vielmehr gibt es bereits verschiedene Icons, die von unterschiedlichen Organisationen und Gruppierungen entwickelt worden sind, um Datenbearbeitungen bildlich darzustellen. Als Beispiele können das Mozilla Privacy Icons Project[8] und das Data Protection Icon Set (DaPIS) der Universität Bologna[9] genannt werden[10]. Auch die DSGVO enthielt im Entwurf des Europäischen Parlaments vom 12. März 2014 eine Reihe von Icons[11] und die Botschaft zum neuen DSG weist ausdrücklich auf die Möglichkeit hin, die in Datenschutzerklärungen enthaltenen Informationen durch Symbole oder Piktogramme darzustellen[12]. Die bisherigen Versuche sind allerdings alle gescheitert. Zwei Gründe dürften dafür entscheidend sein: Zum einen ist es nicht trivial, Datenbearbeitungen durch Icons darzustellen. Während gewisse Aspekte recht einfach bildlich wiederzugeben sind (z.B. verschiedene Arten von Personendaten wie biometrische Daten oder Standortdaten), ist dies bei anderen Aussagen ungleich komplexer (z.B. die Bearbeitung zu weiteren Zwecken oder die automatisierte Einzelentscheidung). Vor allem aber dürften die meisten Icons am Anspruch gescheitert sein, zugleich selbsterklärend zu sein und die ganze Komplexität der Fragestellungen abbilden zu können. An diesem Punkt setzen die im Rahmen dieses Projekts neu entwickelten Privacy Icons an:

[4] Zum einen müssen Privacy Icons nicht selbsterklärend sein, um zu funktionieren. Der Anwender der Icons kann vielmehr davon ausgehen, dass Adressaten deren Bedeutung rasch lernen werden, wenn sie den Icons nur genügend oft begegnen. Denn obwohl sich kaum behaupten lässt, dass ein roter Kreis um eine weisse Fläche für sich allein eine bestimmte Aussage vermittelt, wissen wir alle, dass dieses Zeichen ein allgemeines Fahrverbot zum Ausdruck bringt. Voraussetzung für einen solchen Lerneffekt ist, dass Icons häufig und stets einheitlich verwendet werden. Das Ziel des Projekts bestand deshalb von Anfang an darin, Privacy Icons nicht nur zu entwickeln, sondern auch als faktischen Standard in der Schweiz zu etablieren.

[5] Zum andern kann nicht erwartet werden, dass Privacy Icons in der Lage sind, Datenschutzerklärungen vollumfänglich wiederzugeben und die Darstellung der Datenbearbeitungen durch Text gänzlich durch Bilder zu ersetzen. Vielmehr können Privacy Icons nur dann einen relevanten Beitrag zur Transparenz von Datenbearbeitungen leisten, wenn sie sich auf Kernaussagen beschränken, die es den betroffenen Personen erlauben, sich in wenigen Sekunden einen Überblick über die in Frage stehenden Datenbearbeitungen zu verschaffen. Ist die Zahl der Icons zu hoch oder sind die Aussagen zu komplex, wird dieses Ziel verfehlt. Dies bedeutet zugleich, dass

8 Privacy Icons, https://wiki.mozilla.org/Privacy_Icons; https://wiki.mozilla.org/Privacy_Icons_v0.2.

9 DaPIS: the Data Protection Icon Set, http://gdprbydesign.cirsfid.unibo.it/dapis-2/.

10 Zudem gibt es verschiedene Forschungsprojekte zu diesem Thema, vgl. z.B. The Privacy Icons Forum, https://privacyiconsforum.eu.

11 Legislative Entschliessung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Anhang.

12 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 6941–7192, 7050.

Privacy Icons die klassischen Datenschutzerklärungen in Textform nicht ersetzen, sondern nur ergänzen können. Im Sinn des zunehmend postulierten «*layered approach*»[13] sollen Privacy Icons eine weitere Informationsschicht bilden[14], die es Unternehmen erlaubt, mit einfachen Mitteln sicherzustellen, dass den betroffenen Personen zumindest der Umstand und die wichtigsten Aspekte der Datenbearbeitung bekannt sind.

3. Inhalt der Privacy Icons

[6] Der erste und zugleich wichtigste Schritt bei der Erarbeitung von Privacy Icons besteht in der Auswahl derjenigen Aspekte von Datenschutzerklärungen, die mit Icons abgebildet werden sollen. Als Leitlinien dienten dabei die folgenden Überlegungen: (1) Die Privacy Icons sollten nur die relevanten Inhalte und nicht die gesamte Datenschutzerklärung abbilden. Damit lässt sich die Zahl der verwendeten Icons reduzieren und die effektive Transparenz erhöhen, die umso grösser sein dürfte, je knapper und konziser die mit Icons gemachten Aussagen sind. (2) Die Relevanz der Inhalte ist aus Sicht der betroffenen Personen zu beurteilen, nicht aus Sicht der Unternehmen oder des Datenschutzrechts. Bei den Privacy Icons zu den Arten der bearbeiteten Daten wird deshalb nicht nach «normalen» und «besonders schützenswerten» Personendaten unterschieden[15], sondern zwischen allgemeinen Personendaten, Finanzdaten, Gesundheitsdaten, Standortdaten, biometrischen Daten und Daten über die Privat- und Intimsphäre. (3) Mit Privacy Icons werden grundsätzlich nur Aspekte der Datenbearbeitung abgebildet, die nicht ohnehin immer gegeben sind bzw. durch jeden Datenbearbeiter sichergestellt werden müssen. So gibt es bspw. keine Icons dazu, dass Betroffenenrechte erfüllt werden oder eine angemessene Datensicherheit gewährleistet wird.

[7] Auf der Grundlage dieser Überlegungen wurden 19 Privacy Icons erarbeitet, die sechs Themenfelder abdecken: Art der Personendaten (6 Privacy Icons), Quelle der Personendaten (3 Privacy Icons), Zweck der Bearbeitung (3 Privacy Icons), Besondere Bearbeitungen (2 Privacy Icons), Weitergabe an Dritte (2 Privacy Icons) und Ort der Bearbeitung (3 Privacy Icons). Alle Privacy Icons haben eine Bezeichnung (z.B. «allgemeine Personendaten» oder «erhaltene Daten») und ihre Bedeutung wird in einem Kurztext verbal umschrieben (z.B. «Wir bearbeiten ihre Standortdaten» oder «Wir nutzen ihre Personendaten für Marketing und Werbung»).

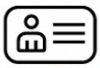
[8] Die Privacy Icons sind auf einer Webseite unter der Adresse https://privacy-icons.ch frei zugänglich. Sie können dort in einem gängigen Format heruntergeladen und anschliessend in die eigene Webseite oder App eingebunden oder auf Drucksachen abgebildet werden.

---

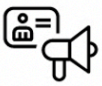
13 Siehe dazu: Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff., 7050; Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last revised and adopted on 11 April 2018, 19 f.; Boris P. Paal/Moritz Hennemann, in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018, DSGVO 12 N 31; Matthias Bäcker, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG Kommentar, 2. Aufl., München 2018, DSGVO 12 N 21.

14 Die DSGVO sieht ausdrücklich vor, dass die Informationen, welche den betroffenen Personen nach Art. 13 f. DSGVO zur Verfügung gestellt werden müssen, in Kombination mit standardisierten Bildsymbolen bereitgestellt werden können, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln (Art. 12 (7) DSGVO).

15 So Art. 3 Abs. 1 lit. a DSG (Personendaten) und Art. 3 Abs. 1 lit. c DSG (besonders schützenswerte Personendaten) bzw. Art. 4 (1) DSGVO (personenbezogene Daten) und Art. 9 DSGVO (besondere Kategorien von Personendaten).

	Icon	Bezeichnung und Kurztext	Erläuterung
Art der Personendaten		**Allgemeine Personendaten** Wir bearbeiten allgemeine Personendaten über Sie, z.B. Name und Kontaktdaten.	Darunter fallen allgemeine Daten mit Personenbezug, die sich nicht einer besonderen Kategorie zuordnen lassen. Beispiele sind Name, Adresse, Telefonnummer, E-Mail-Adresse, Benutzername oder Kundennummer.
		**Finanzdaten** Wir bearbeiten Ihre Finanzdaten.	Darunter fallen Daten über die Einkommens- und Vermögenssituation sowie persönliche Zahlungs- und Kontoangaben. Beispiele sind Kontostand, Einkommen oder Wertschriftenportfolio und -ertrag sowie vollständige Bankkonto- oder Kreditkartennummern. Nicht als Bearbeitung von Finanzdaten gelten hingegen die Speicherung gekürzter Kreditkartennummern und generelle Angaben zur Zahlungsart.
		**Gesundheitsdaten** Wir bearbeiten Ihre Gesundheitsdaten.	Darunter fallen Daten zur körperlichen oder geistigen Gesundheit. Beispiele sind Daten zu Krankheiten und Behinderungen, aber auch zu Allergien und Unverträglichkeiten, zu Seh- und Hörstärke oder zu Übergewicht. Als Gesundheitsdaten gelten auch die Tatsache einer Schwangerschaft sowie Daten, die erkennen lassen, dass eine Person bestimmte Gesundheitsdienstleistungen in Anspruch genommen hat. Nicht als Bearbeitung von Gesundheitsdaten gilt hingegen die Speicherung eines Fotos mit äusserlich erkennbarer Behinderung, sofern es nicht spezifisch hinsichtlich Gesundheitsinformationen bearbeitet oder ausgewertet wird.
		**Standortdaten** Wir bearbeiten Ihre Standortdaten.	Darunter fallen ortsbezogene Daten, die eine Aussage über den Standort einer Person zu einem bestimmten Zeitpunkt erlauben und mit diesem Fokus bearbeitet werden. Beispiele sind die Lokalisierung eines Nutzers über Mobilfunkdaten, Bluetooth, WLAN oder GPS, z.B. im Zusammenhang mit Navigationsdiensten oder sogenannten Location-based Services. Nicht als Bearbeitung von Standortdaten gilt hingegen die einmalige Erfassung eines Standorts, z.B. die Erfassung einer Wohnadresse.

		**Biometrische Daten** Wir bearbeiten Ihre biometrischen Daten.	Darunter fallen dauerhafte physische, physiologische oder verhaltenstypische Merkmale, die mittels spezieller technischer Verfahren erfasst werden und eine natürliche Person eindeutig identifizieren. Beispiele sind Fingerabdruck, Iris und Retina, Geometrie des Gesichts oder Stimmprofile. Nicht als Bearbeitung biometrischer Daten gelten hingegen die blosse Abbildung einer Person auf einem Foto oder in einem Video oder Stimmaufzeichnungen, die nicht mittels solcher Verfahren bearbeitet werden.
		**Privatsphäre** Wir bearbeiten Daten über Ihre Privat- und Intimsphäre.	Darunter fallen Daten, die den engsten Privat- und Intimbereich einer Person betreffen. Beispiele sind die sexuelle Ausrichtung, religiöse und weltanschauliche Überzeugungen sowie politische Meinungen. Nicht dazu gehören hingegen Fotos und Videos, Adresslisten sowie Korrespondenz, auch wenn diese privaten Charakter aufweisen. Ebenfalls nicht dazu gehören allgemeine Angaben zur Person wie Geschlecht, Geburtsdatum oder Zivilstand.
Quelle der Personendaten		**Überlassene Daten** Wir bearbeiten Personendaten, die Sie uns zur Verfügung stellen.	Darunter fallen Daten, die die betroffene Person selbst direkt oder indirekt zur Verfügung stellt. Beispiele sind die eigenständige Erfassung von Personendaten in einem Anmeldeformular, bei einer Wettbewerbsteilnahme oder bei der Erstellung eines Benutzerkontos. Ebenfalls dazu gehören Bilder, die bei der Nutzung eines Cloud-Speicherdienstes hochgeladen werden, vom Nutzer bei einem Streaming-Dienst erstellte Playlisten sowie bei der Nutzung eines Fitness Trackers erfasste Körperwerte oder zurückgelegte Strecken.
		**Erhobene Daten** Wir bearbeiten Personendaten, die wir über Sie erheben.	Darunter fallen Daten, die vom verantwortlichen Unternehmen ohne bewusstes Zutun der betroffenen Person selbst erhoben werden. Beispiele sind die Erfassung von Transaktionsdaten durch einen Zahlungsdienstleister oder einen Detailhändler oder die Erfassung von Verbindungsdaten durch ein Telekommunikationsunternehmen. Weitere Beispiele sind Webtracking mittels Cookies und anderen Tracking-Technologien.

		**Erhaltene Daten** Wir bearbeiten Personendaten über Sie, die wir von Dritten erhalten.	Darunter fallen Daten, die das verantwortliche Unternehmen von Dritten zur eigenen, nicht weisungsgebundenen Verwendung erhält. Beispiele sind Daten, die ein Unternehmen im Rahmen einer Kooperation erhält, Bonitätsauskünfte von Wirtschaftsauskunfteien oder der Adress- und Datenkauf von Adress- und Informationshändlern.
Zweck der Bearbeitung		**Marketing** Wir nutzen Ihre Personendaten für Marketing und Werbung.	Darunter fällt jede Nutzung von Personendaten für Marketing- und Werbezwecke, d.h. für die Förderung des Absatzes von Produkten und Dienstleistungen, generell für die vorteilhafte Darstellung von Angeboten sowie für die Förderung der Kundengewinnung und Kundenbindung. Beispiele sind der Versand von Werbung und Newslettern, Rabattaktionen oder das Anzeigen von Onlinewerbung. Erfasst wird auch die mittelbare Absatzförderung, z.B. Umfragen zur Kundenzufriedenheit oder die Aufforderung zur Abgabe einer Bewertung auf Online-Vergleichsdiensten.
		**Produktentwicklung** Wir nutzen Ihre Personendaten für die Entwicklung und Verbesserung von Produkten und Dienstleistungen.	Darunter fällt jede Nutzung von Personendaten, die darauf abzielt, Produkte und Dienstleistungen zu entwickeln oder zu verbessern, insbesondere um sie besser auf die Kundenbedürfnisse auszurichten, um die Kundenzufriedenheit zu erhöhen oder um die Kosteneffizienz zu steigern. Beispiele sind die Optimierung der Sortiments- und Preisgestaltung, die Verbesserung der „Customer Journey“ und der „Usability“ bei einem Webshop, die Verbesserung von Produktempfehlungsalgorithmen, das Training eines Sprachassistenten oder die Optimierung der Routenplanung eines Lieferdienstes.
		**Weitere Zwecke** Wir nutzen Ihre Personendaten für weitere, nicht mit der Kernleistung zusammenhängende Zwecke.	Darunter fällt jede Nutzung von Personendaten, die keinen engen sachlichen Zusammenhang mit der Kernleistung aufweist und mit der die betroffenen Personen nicht ohne weiteres rechnen. Beispiele sind die Nutzung von aggregierten Mobilfunk-Verbindungsdaten für Verkehrsprognosen und Stauwarnungen, die Nutzung von Daten aus einem Bonus- oder Treueprogramm für Bonitätsprüfungen, die Nutzung von Transaktions- und Browsing-Daten zum Festsetzen individualisierter Preise oder die Weitergabe von Personendaten an einen Adressaktualisierungsverbund.

Besondere Bearbeitungen		**Automatische Entscheide** Wir treffen wesentliche Entscheide vollautomatisch.	Gekennzeichnet werden damit eine bestimmte Person betreffende Entscheide, die ohne menschliche Mitwirkung vollautomatisch getroffen werden und in ihren Auswirkungen eine gewisse Tragweite haben. Beispiele sind Entscheide über die Gewährung eines Kredits, eine Stellenbewerbung oder die Kündigung eines Arbeitsvertrages. Nicht erfasst wird mangels Tragweite hingegen der Entscheid, ob in einem Webshop Kauf auf Rechnung angeboten wird oder ob ein Kunde volljährig ist und Alkohol bestellen darf.
		**Profiling** Wir analysieren Ihr Verhalten und treffen Annahmen über Ihre Interessen und Präferenzen.	Gekennzeichnet wird damit die automatisierte Bearbeitung von Personendaten, um persönliche Aspekte zu analysieren oder vorherzusagen. Beispiele sind die Analyse des Einkaufsverhaltens, der Nutzung von Webseiten und Apps oder anderer Transaktions- und Verhaltensmuster, um gestützt darauf Annahmen über persönliche Interessen, Präferenzen, Affinitäten und Gewohnheiten zu treffen. Profiling erfolgt häufig in Zusammenhang mit der Personalisierung von Angeboten oder Direktmarketingmassnahmen oder im Kontext von Kundenbindungsprogrammen.
Weitergabe an Dritte		**Datenweitergabe** Wir geben Ihre Personendaten an andere Unternehmen weiter, die selber entscheiden können, wie sie die Daten nutzen.	Darunter fällt jede Weitergabe von Daten an einen Empfänger, der die Daten als Verantwortlicher für eigene Zwecke nutzen kann (Controller-to-Controller Transfer). Erfasst wird sowohl die Weitergabe an konzernfremde Unternehmen als auch die Weitergabe an konzernmässig verbundene Unternehmen. Nicht erfasst wird die Auftragsbearbeitung, also die Weitergabe von Personendaten an weisungsgebundene Dienstleister (Controller-to-Processor Transfer).

		**Datenverkauf** Wir verkaufen Ihre Personendaten.	Darunter fällt jede Weitergabe von Personendaten gegen Entgelt. Kein Datenverkauf liegt insbesondere bei Kooperationen vor, bei denen zwar auch Daten involviert sind, diese aber für den gemeinsamen Zweck der Kooperation bearbeitet und weitergegeben werden. Nicht als Datenverkauf gilt mangels Personendaten auch die Monetarisierung von aggregierten oder auf andere Weise anonymisierten Daten, sofern gewährleistet ist, dass die Daten keinen Personenbezug mehr aufweisen und dieser mit vernünftigem Aufwand auch nicht wiederhergestellt werden kann.
Ort der Bearbeitung		**Schweiz** Wir bearbeiten Ihre Personendaten nur in der Schweiz.	Aus der Reihe «Ort der Bearbeitung» ist immer nur ein Privacy Icon zu verwenden. Entscheidend ist, ob die Personendaten vom verantwortlichen Unternehmen (oder von einem anderen Unternehmen, das die Daten in dessen Auftrag bearbeitet) (1) ausschliesslich in der Schweiz, (2) neben der Schweiz auch (aber nur) in Staaten der EU, oder (3) neben der Schweiz und/oder der EU auch in weiteren Staaten bearbeitet werden. Unerheblich ist, ob der Empfängerstaat als Staat mit angemessenem Datenschutzniveau anerkannt ist. So ist bspw. bei einer Übermittlung von Daten nach Kanada oder Israel das Icon «weltweit» zu verwenden.
		**Europa** Wir bearbeiten Ihre Personendaten nur in der Schweiz und in der EU.	
		**Weltweit** Wir bearbeiten Ihre Personendaten auch ausserhalb der Schweiz und der EU.	

[9] Bei ersten Anwendungen der Privacy Icons hat sich gezeigt, dass Unternehmen zum Teil auch zum Ausdruck bringen möchten, dass sie bestimmte Arten von Daten (bspw. biometrische Daten oder Standortdaten) nicht bearbeiten oder bestimmte Arten von Bearbeitungen (bspw. Verkauf an Dritte) nicht vornehmen. Die Privacy Icons können deshalb sowohl in einer bejahenden Fassung (Privacy Icon) als auch in einer verneinenden Fassung (durchgestrichenes Privacy Icon) verwendet werden.

Bejahend	**Verneinend**	**Bejahend**	**Verneinend**
			
Marketing Wir nutzen Ihre Personendaten für Marketing und Werbung.	**Kein Marketing** Wir nutzen Ihre Personendaten nicht für Marketing und Werbung.	**Datenverkauf** Wir verkaufen Ihre Personendaten.	**Kein Datenverkauf** Wir verkaufen Ihre Personendaten nicht.

4. Verwendung der Privacy Icons

[10] Die Privacy Icons können kostenlos von jedem Unternehmen verwendet werden, um die vom Unternehmen selbst vorgenommenen und in der eigenen Datenschutzerklärung erläuterten Bearbeitungen von Personendaten darzustellen. Die Unternehmen müssen dabei gewisse Vorgaben einhalten, die in der Lizenz zur Nutzung der Privacy Icons[16] und in einem dazugehörigen «Style Guide»[17] festgelegt sind. Mit diesen Vorgaben wird sichergestellt, dass die Privacy Icons von den Unternehmen einheitlich genutzt und nicht verändert werden. Denn nur so können die Privacy Icons Transparenz herstellen, Vertrauen schaffen und sich als faktischer Standard etablieren.
[11] Der Lizenzenzvertrag wird mit der Nutzung der Privacy Icons durch die Unternehmen abgeschlossen. Lizenzgeber ist der Verein Privacy Icons, der als Rechtsnachfolger der Projektgruppe die Rechte an den Icons hält und die Einhaltung der Lizenzbestimmungen überwacht. Dies ist allerdings nur möglich, wenn der Verein weiss, welche Unternehmen die Privacy Icons verwenden. Die Unternehmen müssen dem Verein die Verwendung der Icons deshalb über ein Formular auf der Webseite melden[18].
[12] Mit der Lizenz werden die Unternehmen verpflichtet, die Privacy Icons nur für diejenigen Aussagen zu verwenden, die im Kurztext zum jeweiligen Icon genannt werden. Die Unternehmen müssen dabei immer alle auf ihre Datenbearbeitungen zutreffenden Privacy Icons verwenden, es dürfen also weder inhaltlich zutreffende Icons weggelassen noch unzutreffende Icons abgebildet werden. Dabei steht es den Unternehmen frei, nur diejenigen Privacy Icons zu verwenden, die darüber informieren, welche Datenbearbeitungen vorgenommen werden (bejahende Icons) oder auch diejenigen, die zum Ausdruck bringen, dass bestimmte Bearbeitungen nicht vorgenommen werden (verneinende Icons). Anders als bei den bejahenden Icons besteht bei den verneinenden Icons keine Pflicht, alle inhaltlich zutreffenden Icons zu verwenden, also mithilfe der verneinenden Icons umfassend darzustellen, welche Datenbearbeitungen nicht vorgenommen werden. Die Bezeichnung der Privacy Icons und die Kurztexte können von den Unternehmen zusammen mit den Icons verwendet werden, die Privacy Icons können aber auch ohne diese verwendet werden.
[13] Wie bei klassischen Datenschutzerklärungen liegt die Verantwortung für die wahrheitsgetreue Information über die Datenbearbeitungen auch bei der Verwendung der Privacy Icons allein bei den Unternehmen. Der Verein Privacy Icons kann die wahrheitsgetreue Verwendung der Icons nicht überprüfen und er kann auch nicht zusichern, dass die Verwendung der Privacy Icons von den zuständigen Behörden oder Gerichten als zulässiges und hinreichendes Mittel zur Gewährleistung der Transparenz der Bearbeitung von Personendaten qualifiziert wird. Immerhin hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), Dr. Adrian Lobsiger, im Rahmen der Lancierung der Privacy Icons öffentlich festgehalten, dass die Privacy Icons aus seiner Sicht ein geeignetes Mittel sind, um die Transparenz von Datenbearbeitungen zu erhöhen und den von ihm propagierten «*layered approach*» in der Kommunikation zu unterstützen[19]. Dabei hat er auch klargestellt, dass sich Unternehmen auf den mit Privacy Icons gemachten Aussagen behaften lassen müssen, dass ihnen also falsche Angaben entgegengehalten werden kön-

16 Privacy Icons Lizenz, https://privacy-icons.ch/lizenz.

17 Privacy Icons Style-Guide, https://privacy-icons.ch/style-guide.

18 Privacy Icons Kontakt, https://privacy-icons.ch/kontakt.

19 Medienmitteilung vom 30. November 2020; abrufbar unter https://privacy-icons.ch/news.

nen, unabhängig davon, ob sie in klassischen Datenschutzerklärungen oder mithilfe von Privacy Icons gemacht werden.

5. «Go Live»

[14] Die Privacy Icons wurden am 30. November 2020 lanciert[20]. Mit der Lancierung haben mehrere grosse Schweizer Unternehmen begonnen, die Privacy Icons zu verwenden, so namentlich Swisscom, Migros, SBB und Credit Suisse; in den nächsten Monaten werden BKW und Zurich Versicherung folgen. Ziel ist es, dass sich viele weitere grosse, mittlere und kleine Unternehmen anschliessen und die Verwendung von Privacy Icons in der Schweiz schon bald zum Standard wird. Wir laden deshalb alle Schweizer Unternehmen ein, die Privacy Icons zur Darstellung ihrer Bearbeitung von Personendaten zu nutzen und dem Verein Privacy Icons gegebenenfalls über das Kontaktformular mitzuteilen, wie die Privacy Icons weiter verbessert werden können. Damit kann es gelingen, den unbefriedigenden Zustand einer bloss formalen Transparenz von Datenbearbeitungen zu überwinden und sicherzustellen, dass die betroffenen Personen tatsächlich Kenntnis von der Bearbeitung ihrer Personendaten erlangen.

Florent Thouvenin, Prof. Dr., Rechtsanwalt, Inhaber des Lehrstuhls für Informations- und Kommunikationsrecht, Vorsitzender des Leitungsausschusses des Center for Information Technology, Society, and Law (ITSL) und Direktor der Digital Society Initiative (DSI) der Universität Zürich.

Matthias Glatthaar, Dr. iur., LL.M., Rechtsanwalt, Leiter Datenschutz und Digitalisierung, Migros-Genossenschafts-Bund.

Juliette Hotz, MLaw, Senior Counsel Data Governance, Swisscom.

Claudius Ettlinger, Lic. iur., LL.M., Rechtsanwalt, Datenschutzbeauftragter, SBB.

Michael Tschudin, Dr. iur., Rechtsanwalt, Zürich.

[20] Für Näheres dazu siehe: https://privacy-icons.ch.