bitkom

selbstregulierung informationswirtschaft e.V.

Privacy Icons

Konzeptionierung zur Erstellung sinnvoller Icons in Umsetzung von Art. 12 DS-GVO und Begleitdokument zum Bitkom Icon Set

Ein gemeinsames Projekt von Bitkom und dem SRIW

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
Tel.: 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Rebekka Weiß | Bitkom
T 030 27576-161 | r.weiss@bitkom.org

Verantwortliche Bitkom-Gremien
AK Datenschutz – AG Privacy Icons

Layout
Anna Stolz | Bitkom

Titelbild
© Warchi – iStock.com

Inhalt

1 Hintergrund

Die DS-GVO sieht in Art. 12 Abs. 7 vor, dass sich die verantwortliche Stelle zur Erfüllung ihrer Informationspflichten nach Art. 13 und 14 auch bestimmter Bildsymbole bedienen kann, die der betroffenen Person in Kombination mit den erforderlichen (textlichen) Informationen bereitgestellt werden. Dadurch soll der betroffenen Person in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form ein aussagekräftiger Überblick über die beabsichtigte Verarbeitung vermittelt werden.

Art. 12 Abs. 8 DS-GVO sieht die Möglichkeit eines delegierten Rechtsaktes vor. Hierüber kann die Kommission festlegen, welche Informationen durch Bildsymbole darzustellen sind und welche Verfahren dabei Anwendung finden.

Trotz mehrfachen Ersuchens hat die Kommission die Rechtsaktbefugnis bis jetzt nicht genutzt. Da der bitkom und seine Mitglieder den Ansatz – insbesondere vor dem Hintergrund von Datenverarbeitungen durch Geräte mit sehr kleinen oder gar ohne Displays – als sinnvoll und notwendig erachtet, hat die AG Privacy Icons des Bitkom AK Datenschutz proaktiv und eigenständig eine Umsetzung und Iconbeispiele erarbeitet und stellt diese zur Nutzung im Markt bereit. Das erarbeitete Icon-Set ist separat verfügbar und wird durch ein begleitendes Whitepaper ergänzt.

2 Allgemeine Überlegungen zu Icons

Icons (standardisierte Bildsymbole) sind nach der DS-GVO in zweierlei Hinsicht denkbar: einerseits ergänzend zu textlichen Informationen (Art. 12 Abs. 7 oder Art 12 Abs. 8) andererseits aber auch als ausschließliche Informationsquelle (Art. 12 Abs. 8).

2.1 Gesetzlich intendierter Zweck von Icons

Der Zweck solcher Icons ergibt sich im Grunde bereits qua Natur der Sache. »Ein Bild sagt mehr als tausend Worte« ist als Redewendung weithin bekannt. Soweit die darzustellenden Sachverhalte dazu geeignet sind, sollen Icons den Betroffenen einen schnellen, verständlichen Überblick über die geplanten Datenverarbeitungen geben.

Dies spiegelt sich auch in EWG 60 der DS-GVO wider. Dort heißt es, Informationen könnten »in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.«

Hierbei akzeptiert der europäische Gesetzgeber bereits eine in der Praxis zu erwartende Schwierigkeit. Bildsymbole gehen nahezu zwingend mit einer Vereinfachung der darzustellenden Sachverhalte einher. Mithin sind Icons allenfalls geeignet einen Überblick, nicht aber einen ebenso feingliedrigen und detaillierten Einblick in durch die verantwortliche Stelle intendierte Verarbeitungsvorgänge zu geben.

2.2 Praktische Konsequenzen aufgrund des Telos

Jede Entwicklung von Icons gleich durch welche Beteiligte ist am Zweck des Gesetzes auszurichten. Vereinfachte Erfassung der Transparenzvorgaben, bessere Navigierbarkeit durch Datenschutzbestimmungen und einheitlichere Darstellung von Datenschutzprozessen waren für die Arbeitsgruppe tragende Erwägungen bei der Erarbeitung. Die Arbeitsgruppe verfolgt vor allem den Zweck, mehr Akzeptanz für Icons und die übersichtliche Darstellung und Umsetzung der Transparenzvorgaben herzustellen.

2.2.1 Betroffene(-nverständnis) im Zentrum aller Entwicklung

Zunächst sind in das Zentrum jedweder Entwicklung der Icons die Betroffenen in den Mittelpunkt zu stellen. Ausdrücklicher Zweck von unseren Icons ist es, das Verständnis

der Betroffenen zu fördern. Mithin ist bei der Gestaltung neben juristischem und technischem Sachverstand insbesondere durch Integration entsprechender wissenschaftlicher Expertise sicherzustellen, dass Icons Betroffenen den gewünschten Mehrwert bieten.

2.2.2 Mehrwert durch Repetition

Der Wortlaut erlaubt per se auch mehrere parallele Standards.[1] Das ergibt sich nicht zuletzt auch daraus, dass die DS-GVO es versäumt, eine Zuständigkeit für die Entwicklung standardisierte Bildsymbole vorzusehen. Das Gesetz geht schlicht von der Existenz eben solcher Icons aus.

Die genutzten Icons sollten eine hohen Wiedererkennungswert und eine Darstellungsform haben, die aus sich selbst heraus spricht. Förderlich aus Sicht Betroffener sollte hierbei die ständige Repetition der Icons sein. Die gleiche beabsichtigte Verarbeitung sollte für den Betroffenen stets mit dem identischen Icon verknüpft werden. Gänzlich kontraproduktiv und unbedingt zu vermeiden wäre die Situation, in der mehrere Icon-Sets genutzt werden, wobei die jeweiligen Icons zudem eine Verwechslungsgefahr bzgl. konträrer Verarbeitungsszenarien aufweisen.

Diesem flexiblem Ansatz und der intendierte Repetition steht es nicht entgegen, dass sich aus bestimmten Verwendungskontexten (Geräteklassen, Branchen, etc.) spezielle, ergänzende Transparenzanforderungen ableiten lassen könnten. Ohne die grundsätzliche Freiwilligkeit von Icons in Frage zu stellen, sollten spezifische Icons sinnvollerweise in Ergänzung zu einem bestehenden, flächendeckenden Basis-Set treten.

2.2.3 flächendeckender Einsatz durch einfache Verständlichkeit ./. einfache Verständlichkeit durch flächendeckenden Einsatz

Dieses Dilemma könnte dem bekannten »Henne-Ei«-Problem ähneln. Eine Wechselbezüglichkeit beider Faktoren ist jedenfalls nicht in Abrede zu stellen. Je leichter verständlich entwickelte Icons sind, umso bereitwilliger wird deren Einsatz erfolgen. Je flächendeckender standardisierte Icons Verwendung finden und je häufiger sich Betroffene mit diesen konfrontiert sehen, umso eher werden auch nicht optimal eingängige Icons memoriert werden.

1 Dies ergibt sich arg. e. contr. Art. 12 Abs. 8 DS-GVO.

Dennoch ist dieses Dilemma im Wesentlichen aufzulösen: die Entwicklung standardisierter Bildsymbole kann (und sollte) sich zunächst darauf konzentrieren, eine leichte Verständlichkeit ohne besondere Sachkunde der Betroffenen aus sich heraus sicherzustellen. Dies scheint unmittelbar mit dem Grundsatz verbunden, Icons sukzessive von zentralen Verarbeitungsszenarien ausgehend zu entwickeln.

Soweit die Entwicklung fokussiert auf wenige, dafür aber für Betroffene – nachweislich – relevante Aspekte erfolgt, erscheint eine solche auch unter der Prämisse »leichte Verständlichkeit« realisierbar. Erfahrungswerte, die mit diesem Grundstock gesammelt werden, können in weitere Entwicklungsversionen einfließen. Diese wiesen neben Optimierungen des Bestands auch die konsequente Erweiterung auf neue Sachverhalte aus.

2.2.4 Anleihen bestehender Symbolik

Da eine starke Kombinatorik bestimmter Umstände zu erwarten ist, erscheint ein Ansatz ähnlich der »Wäschelabels« zielführend. Hierbei könnte für ein bestimmtes Cluster ein Übericon entwickelt werden, welches je nach Kontext um Subicons ergänzt wird.

Hierbei sollte beachtet werden, dass die Cluster sich einerseits thematisch, andererseits aus der Perspektive der Darstellungsfähigkeit bilden sollten. So könnte ein Cluster »Datenverarbeitung für Werbezwecke« gebildet werden mit den Unterrubriken »individualisiert«, »durch Werbenetzwerke«, »...«. Ebenso könnte ein Cluster »Datenverarbeitung durch Dritte« gebildet werden mit den Unterrubriken »Dienstleister«, »Werbenetzwerk«, »Analysedienst«, »...«.

Im Rahmen der weiteren Überlegungen sollte sich deshalb von ggf. aus der rein juristischen Diskussion bekannten Schemata verabschiedet werden und stattdessen offen und ggf. unter Hinzuziehung entsprechender (externer) Expertise über den Zweck der Icons dienliche Ansätze nachgedacht werden.

2.3 E-Privacy Verordnung

Auch der Entwurf der ePrivacy-Verordnung (ePVO)[2] und der Entwurf zur Überarbeitung der ePrivacy-Verordnung vom Europäischen Parlament und dem Rat der Europäischen Union[3] sieht die Verwendung von Bildsymbolen vor, Art. 8 Abs. 3 f.[4] Hiernach können Informationen nach Art. 8 Abs. 2a in Kombination mit standardisierten Bildsymbolen bereitgestellt werden. Interessant ist, dass hierdurch kein Überblick über die Verarbeitung, sondern lediglich über die Erhebung gewährleistet werden soll.[5] Dies deckt sich jedoch zumindest vordergründig mit den Pflichten aus Art. 8 Abs. 2a . Hier soll nämlich über die Modalitäten der Erhebung, ihren Zweck, die dafür verantwortliche Person, die anderen nach Art. 13 DSGVO verlangten Informationen – soweit personenbezogene Daten betroffen sind – sowie letztlich über Möglichkeiten aufgeklärt werden, was ein Endnutzer gegen die Erhebung unternehmen kann um diese Erhebung gänzlich zu unterbinden oder jedenfalls auf ein Minimum zu reduzieren.

2.3.1 Erhebung vs. Verarbeitung sowie Informationen vs. Personenbezogene Daten

Weder die ePVO noch der Änderungsvorschlag verfügen über eine eigene Begriffsbestimmung für den Begriff Verarbeitung. Mithin muss auch davon ausgegangen werden, dass die Verarbeitung im Sinne der DS-GVO[6] das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung umfasst.

Art. 12 Abs. 7 DS-GVO hat ausdrücklich das Ziel, über die Verarbeitung aufzuklären. Der europäische Gesetzgeber wird voraussichtlich bewusst in der ePVO nur von Erhebung sprechen. Mithin wäre über die Verarbeitungsoptionen primär nicht aufzuklären.

Zugleich soll auch über den »Zweck« aufgeklärt werden. Ein Erhebungszweck impliziert eine weitere Verarbeitung, jedenfalls.[7]

2 Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) ↗ http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42678

3 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2022/58/EC (Regulation on Privacy and Electronic Communications: ↗ https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

4 Weitere Erwähnung in EWG 41 ePVO.

5 Art. 8 Abs. 3 a.E.

6 Art. 4 Nr. 2 DS-GVO.

7 Letztlich ist Art.8 Abs. 2 lit. b ePVO und der darin enthaltene (Art. 8 Abs. 2a) an dieser Stelle unglücklich formuliert. Aufzuklären ist übern »ihren Zweck«. »Ihren« kann sich dabei nur auf »die Informationen« beziehen, die erhoben werden. Ist hiermit jedoch nur der »Erhebungszweck« gemeint? Wenn ja, welche »Erhebungszwecke« sind denkbar, die keine weitergehende »Verarbeitung« bedeuten? Oder ist mit »Zweck« doch bereits die weitere Verarbeitung gemeint – was sprachlich naheliegt und hier zunächst vertreten wird.

Dass es sich um Informationen handelt, die nicht zwingend für die Erfüllung der bloßen Funktion eines Endgerätes erforderlich sind, ergibt sich als arg. e. contr. aus der letzten Informationspflicht – nämlich den Nutzer darüber aufzuklären, wie er die Erhebung unterbinden oder auf ein Minimum reduzieren kann.

Erklärbar wird dies ggf. dadurch, dass die ePVO von Informationen, die DS-GVO demgegenüber von personenbezogenen Daten ausgeht. So spricht Art. 8 Abs. 2 ePVO und Vorschlag Art. 8 Abs. 2a über die Informationen – nicht personenbezogenen Daten – aufzuklären, die von Endeinrichtungen ausgesendet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können. Auch die Informationspflichten nach Art. 13 DS-GVO, auf die Art. 8 Abs. 2 lit. B und Art. 8 Abs. 2a ePVO referenzieren, sind nur zu berücksichtigen, soweit diese Informationen ausnahmsweise auch personenbezogene Daten sind.

2.3.2 Vorläufiges Fazit für die Entwicklung von Privacy Icons

Für die Entwicklung von Privacy Icons in der Bitkom Arbeitsgruppe haben wir folgende Aspekte festgehalten:

- soweit ausnahmsweise personenbezogene Daten betroffen sind, gelten die Pflichten nach Art. 13 DS-GVO; mithin sollte im Sinne der Repetition[8] auf die gleichen Symbole zurückgegriffen werden;
- soweit es sich um Hinweise auf die Unterbindung / Einschränkung der Erhebung von Informationen gemäß ePVO handelt, besteht eine Lücke gegenüber den Symbolen nach DS-GVO;
- die Zwecke könnten sich wesentlich von denen nach der DS-GVO unterscheiden;
- es ist über die Modalitäten der Erhebung aufzuklären; dies adressiert höchstwahrscheinlich auch unterschiedliche technische Erhebungsszenarien sowie primär Unterscheidungen wie »automatisch im Hintergrund«, »aufgrund Nutzeraktion«, etc.[9]

Das Delta zwischen DS-GVO und ePVO erscheint nicht groß. Allerdings wirken die Umstände, die nicht von der DS-GVO bereits abgedeckt werden, äußerst speziell und technisch. Inwieweit sich derartige Icons für eine Iconset Version 1.0 anbieten, ist zu evaluieren.

8 Vgl. 2.2.2.
9 Jedenfalls im Bereich »automatisch im Hintergrund« »durch Nutzeraktion« ist eine Parallele zur DS-GVO denkbar

3 Grundkonzept

Die Ausarbeitung soll leicht umzusetzen sein, praktische Relevanz und zugleich eine hohe Akzeptanz sowohl seitens der Unternehmen als auch seitens der Betroffenen erreichen. Denn nur so ist es überhaupt denklogisch möglich, dass Privacy Icons den intendierten Zweck – eine Förderung des informationellen Selbstbestimmungsrechts Betroffener durch kompakte, verständliche Information – erfüllen.

Die Arbeitsgruppe nutzte bestehende Arbeiten und Überlegungen der Beteiligten als Ausgangspunkt. Die Deutsche Telekom stellte eine Ausarbeitung denkbarer Icons auf dem AK Datenschutz bereits am 11. November 2016 in Berlin vor. Der SRIW war daneben über ein Gemeinschaftsprojekt mit der Quadriga Hochschule Berlin, mediaTest digital GmbH Hannover sowie dem Institut für Angewandte Informatik in Leipzig (PGuard) an einer Klassifizierung relevanter Informationen im App-Kontext beteiligt.

Beide Ansätze haben gemein, dass sie akzeptieren, nicht von Anfang an absolute Perfektion erreichen zu können: Es ist bereits unrealistisch, alle denkbaren Kombinationsmöglichkeiten aus Datenarten, Verarbeitungszwecken, Weitergaben, Zugriffen et al. in einer abschließenden Liste zusammenzustellen. Mithin ist es erst recht unmöglich, all diese unterschiedlichen Verarbeitungsszenarien in Bildsymbolen darzustellen, die dem in Art. 12 Abs. 7 DS-GVO dargelegten Zweck gerecht werden, den Betroffenen in verständlicher und klar nachvollziehbarer Form zu informieren. Zugleich steht hinter der von der DS-GVO vorgesehenen Verwendung von Bildsymbolen nicht die Erwartungshaltung, dass diese die textliche Information vollständig ersetzen. Bildsymbole sollen lediglich in Kombination mit textlicher Information zum Einsatz kommen und dem Betroffenen einen »aussagekräftigen Überblick« über die Datenverarbeitung vermitteln. Es ist somit zwar erstrebenswert, aber nicht zwingend und nicht von Anfang an erforderlich, jedes Verarbeitungsszenario in ein eindeutiges Bildsymbol zu überführen.

Die Icons-Vorschläge und dieser Leitfaden sollen sich daher dynamisch entwickeln können.

4 Konkretes

Informationspflichten treffen verantwortliche Stellen unabhängig von dem verwendeten Medium. Je nach Medium ergeben sich aus Sicht der Betroffenen abweichende Interessenlagen und Notwendigkeiten einer kompakten Darstellung durch Bildsymbole.

Informationen, die für Apps hilfreich sind, können in den meisten Fällen auch für Webseiten genutzt werden. Die denkbaren Verarbeitungsszenarien von Webseiten sind im Wesentlichen eine Teilmenge der denkbaren Verarbeitungsszenarien von Apps. Da sich das Display bei einem Wechsel von mobilem Device auf Laptop/Desktop in der Regel vergrößern wird, ist nicht mit veränderten Anforderungen für die Gestaltung zu rechnen.

4.1 Mobile Devices

Mobile Devices können thematisch aus der Perspektive »App« betrachtet werden. Mithin sind nachfolgende Aspekte für Betroffene relevant:

Einerseits ergibt sich eine potentielle Datenverarbeitung aus den der jeweiligen App eingeräumten Zugriffsrechten. Hierbei ist aber zu beachten:

- Zugriffsrechte werden einerseits vom Betriebssystem vorgegeben.
- Andererseits können diese bereits jetzt vor Installation in den App-Stores inklusive bestehender Symbole eingesehen werden.
- Insbesondere in jüngeren Betriebssystemversionen müssen diese bei der Nutzung der App im Falle des ersten Zugriffs explizit bestätigt werden.
- Letztlich bedeuten Zugriffsrechte der App nicht zugleich auch Verarbeitungen durch die verantwortliche Stelle (App-Anbieter), da die entsprechenden Daten das mobile Endgerät nicht verlassen müssen – weder in Reinform noch in irgendeiner anderen Form.

Es erscheint daher sinnvoll, Zugriffsrechte zunächst nicht in Privacy Icons zu übersetzen! Hinzu kommt, dass sich die Informationspflichten der Art. 13 und 14 DSVGO – mithin auch eine etwaige Pflicht zur bildlichen Darstellung gem. Art. 12 DS-GVO – nicht auf bloße Zugriffsrechte erstreckt, sondern sich allein auf die Datenverarbeitung bezieht.

Folglich sollte grundsätzlich darauf abgestellt werden, welche Daten tatsächlich verarbeitet werden und zu welchen Zwecken. Hierbei ist ebenfalls zu berücksichtigen, dass eine losgelöste bildhafte Darstellung einzelner Datenarten Betroffenen keinen informationellen Mehrwert bieten wird.

Sinnvoll erscheinen vielmehr nur Icons, die aus einer Kombination aus Datum/Datenkategorie und Verwendungszweck[10] oder Datum/Datenkategorie und Erlaubnistatbestand bestehen.

Letzteres erscheint indessen redundant. Die Icons sollten sowohl in Datenschutzerklärungen als auch Einwilligungstexten verwendet werden können. Denn beide Anwendungsszenarien sind aus Sicht der Betroffenen identisch: anstelle endlose textliche Informationen zu lesen, soll durch Symbole leicht verständlich erfasst werden können, ob überhaupt Verarbeitungen von gesondertem Nutzer(lese)interesse beabsichtigt sind. Sieht man davon ab[11], die einzelnen gesetzlichen Erlaubnistatbestände mit einzelnen Symbolen zu versehen (z. B. Vertrag/gesetzliche Pflicht, Interessenabwägung, »öffentliche Aufgaben/Interessen«, etc.) bliebe lediglich die Information übrig, dass eine konkrete Verarbeitung auf Grundlage einer Einwilligung oder eines gesetzlichen Erlaubnistatbestands erfolgen wird. Spätestens das Symbol »Datenverarbeitung wird auf Einwilligung gestützt« in eine Einwilligung zu integrieren, wäre insoweit tautologisch.

Zu bevorzugen ist somit eine Verbindung mit Verarbeitungszwecken.

Hiervon können wiederum besonders sensible Datenarten eine Ausnahme darstellen, was im Einzelfall zu prüfen sein wird. Denkbar erscheinen zum Beispiel die Verarbeitung von Daten der individuellen Kontakte oder auch Gesundheitsdaten.

Ebenso von Interesse für Nutzer könnten bestimmte Verarbeitungsarten sein, z. B. Integration von Drittanbietern, Weitergabe (aggregierter) Daten im Konzern respektive in einem Partnernetzwerk, Rückgriff auf externe Dienstleister (Auftragsverarbeiter), etc.

Da diese Verarbeitungsarten indessen in fast jedem Falle auftreten, wird zu überlegen sein – zur Vermeidung eines Abstumpfungseffekts – ob diese Informationen erst bei Überschreiten bestimmter Grenzwerte piktographisch dargestellt werden sollten. Diese Frage tangiert jedoch die Gestaltung der Icons an sich nicht, sondern würde allenfalls zu entwickelnde Vorgaben bzgl. des Verfahrens der Verwendung der Icons betreffen, vorgreiflich und entsprechend Art. 12 Abs. 8 letzter HS DS-GVO.

10 Wie zuvor erläutert: mobile Betriebssysteme und App-Stores bilden bereits jetzt Zugriffsrechte ab. Dies sollte eine Beschäftigung auch mit diesem Thema für die Arbeitsgruppe nicht per se ausschließen – zumal durchaus Kritik an den gewählten Berechtigungsbündeln besteht. Dennoch scheint eine durch Betroffene verstandene Symbolik zu bestehen. Anstelle das Rad gänzlich neu zu erfinden, könnte und sollte sich zunächst in diesem Bereich auf eine Bestandsaufnahme und Konsolidierung des Bestands konzentriert werden.

11 Es erscheint zwar nicht gänzlich ausgeschlossen, dass Nutzer an dem konkreten Erlaubnistatbestand ein ausweisliches Interesse haben – nicht umsonst ist die Angabe der Rechtsgrundlage unter der DS-GVO in die Informationspflichten aufgenommen worden. Ob der konkrete Erlaubnistatbestand (Norm) aber von solch übergeordnetem Interesse ist, dass dieser bereits in der ersten Version in ein Icon überführt werden muss, erscheint zumindest fraglich. Auf Dauer ist hier neben den ETB der DS-GVO zudem an alle weiteren ETB der noch an die DS-GVO anzupassenden Spezialgesetze zu denken.

4.1.1 Besonders relevante Datenverarbeitungen bei Apps[12]

Einige Datenverarbeitungen bei Apps sind aus Betroffenensicht besonders relevant/interessant und eignen sich, zumindest zum Teil, auch für die bildliche Darstellung. Die Arbeitsgruppe hat folgende Überlegungen als Ausgangspunkt genommen und hieraus das Iconset entwickelt. Nicht alle Kategorien sind bereits im ersten Icon-Set dargestellt, können aber Anlass für weitere Versionen sein und sind hier der Vollständigkeit halber umfassend dargestellt.

- App verarbeitet Kontaktinformationen
  - Einzahl, also nur die Informationen des Nutzers
- App verarbeitet Kontaktinformationen von Kontakten
  - Mehrzahl = untechnisch »liest Adressbuch aus«
- App verarbeitet Standortdaten
- App verarbeitet Geräteinformationen zur Identifikation Ihres Endgeräts
  - App verarbeitet statistische Gerätekennungen
- App integriert Drittanbieter
  - App integriert Werbenetzwerke
- App verarbeitet Daten im Ausland (also außerhalb EU/EWR)
- Daten werden »weitergegeben«
  - Daten werden durch Dienstleister verarbeitet
  - Daten werden in der Unternehmensgruppe geteilt
  - Daten werden in Partnernetzwerk geteilt
- Es erfolgt eine Profilbildung
- Profile werden durch Informationen aus Drittquellen angereichert
- Daten werden für individualisierte Werbung genutzt
  - »von Anbieter«
  - »von Dritten«
  - »von Partnern«
- Daten werden verschlüsselt verarbeitet
- Daten werden aggregiert verarbeitet
- Daten werden nur als Hashwerte verarbeitet
- Änderungsvorbehalte

12 Diese Liste wurde den Forschungen des Projekts PGuard entnommen und stellt auch dort noch eine dynamische Arbeitsgrundlage dar.

4.1.2 Verknüpfung mit Informationspflichten DS-GVO[13]

Pflicht	Umsetzbarkeit	Sinnhaftigkeit
vollständige Kontaktdaten	(-)	(-)
(Kategorien) von Empfängern Andere verantwortliche Stellen ■ Zahlungsdienstleister ■ Auskunfteien ■ Werbenetzwerke ■ Logistiker ■ Auftragsverarbeiter ■ Infrastructure ■ Software ■ Analyse ■ Maintenance	(+/-)	(+/-)
Betroffenenrechte (ergänzende Darstellung per Icon von Auskunft, Löschung, Portabilität, etc.)	(+)	(-)
Beschwerderecht bei DPA	(-)	(-)
Rechtsgrundlage (jedenfalls Gesetz / Einwilligung)	(+)	(+/-)
Automatisierte Entscheidungsfindung	(+)	(+/-)
Profiling	(+)	(+)
Entscheidungslogik	(-)	(-)
Tragweite der denkbaren Auswirkungen	(-)	(-)
Verarbeitungszwecke ■ Werbung ■ Vertragsabwicklung ■ Optimierung des Services ■ Gewährleistung der Sicherheit und Erreichbarkeit des Service ■ Individualisierung ■ (Markt-)Forschung ■ eigene Profile / Profile Dritter ■ Vorbehalt zur Weiterverarbeitung	(+/-)	(+)

13 Diese Tabelle ist schon eine Konsolidierung der im Text aufgekommenen Themen; diese ist keine abschließende Darstellung aller denkbaren Icons. Vielmehr eine Vorstufe zur Reduzierung der Themen für ein erstes Icon-Set.

Pflicht	Umsetzbarkeit	Sinnhaftigkeit
Kategorien / Art der personenbezogenen Daten[14]	(+)	(+)
■ Persönliche Daten (Namen, Adresse, Geburtsdatum, Beruf, etc.) ■ Kontaktdaten (Adresse, Telefon, IM, etc.) ■ Kontakte (also Adressbuch etc.) ■ Finanzdaten (Konto, Kreditkarten, Zahlungshistorien) ■ Protokolldaten (IP, OS, Zugriffszeitpunkte, etc.) ■ Social Media Daten (Beiträge, Likes, etc.) ■ Benutzerdaten (Nutzername, PW, etc.) ■ Lokale Daten (Dokumente, Medien, Kalender, etc.) ■ Daten in Drittservices / Cloud ■ Kommunikationsdaten ■ Verbindungsdaten ■ Inhaltsdaten ■ etc. ■ Standortdaten (GPS, W-Lan, Beacons, approximiert, exakt, etc.)		
Übermittlung in Drittland ■ innerhalb EU / EWR ■ außerhalb EU / EWR	(+)	(+)
Speicherdauer ■ soweit konkrete Dauer (+)	(+)	(+/-)
Löschprinzipien ■ Löschung von Einzeldaten durch Nutzer selbst möglich ■ Löschung des Accounts und aller Daten durch Nutzer selbst möglich	(+/-)	(+/-)
Datenquelle	(+/-)	(+/-)
Nutzereingabe	(+)	(+)
Automatisiert	(+)	(+)
Dritte	(+)	(+)
Konkrete Quelle	(-)	(-)
Anonymisierte Weiterverarbeitung		

14 Hier wird für die Gruppierung auf Erkenntnisse des Forschungsprojekts PGuard zurückgegriffen. Das dortige Schema ist insbesondere auf zweiter Ebene deutlich differenzierter; es wird allerdings davon ausgegangen, dass die zweite Ebene nicht durch individuelle Icons realisiert werden kann. B

4.2 IoT / Devices ohne bzw. mit sehr kleinem Display

Derartige Devices haben drei Anwendungsszenarien:

1. Darstellung der Icons auf der Verpackung / in der Produktbeschreibung
2. Darstellung der Icons auf dem bzw. durch das Gerät
3. Darstellung der Icons auf einem Drittgerät mit hinreichend großem Display

Zudem hätte hier der IT-Sicherheitsaspekt unabhängig datenschutzrechtlicher Pflichten Informationswert für den Nutzer. Datenschutzrechtlich ist zunächst nur über diejenigen Datenverarbeitungen der verantwortlichen Stelle aufzuklären. Eine datenschutzrechtliche Störerhaftung ist der DS-GVO nicht zu entnehmen.

Dennoch greifen mediale Berichte immer wieder Probleme der IT-Sicherheit unter dem Gesichtspunkt des Daten- respektive Verbraucherschutzes auf. Hintergrund sind meist unverschlüsselte Datenübertragungen im (Heim-)Netzwerk oder ähnliche Umstände.[15] Gerade bei optischen Sensoren kann eine unverschlüsselte Übertragung für Nutzer unangenehme Folgen haben. Der unberechtigte Zugriff auf das Bildmaterial durch Dritte wird erleichtert und die damit verbundenen Risiken des Missbrauchs werden erhöht.

Es erscheint denkbar und in sich stimmig, auch derartige Themen im Rahmen der Entwicklung von Icons zu berücksichtigen. Entsprechend eines Icons, welches über die verschlüsselte Kommunikation mit und / oder einer verschlüsselten Speicherung bei einer verantwortlichen Stelle aufklärt, könnte z. B. ein Icon erstellt werden, welches über die verschlüsselte Kommunikation von IoT untereinander, mit dem und respektive oder über das Heim-Netzwerk aufklärt.

15 Unverschlüsselte Bluetooth Übertragung zwischen Tastatur und Dongle. Eingaben (u. a. Zugangsdaten) können sodann »leicht« von Dritten mitgeschnitten werden.

4.2.1 Darstellung der Icons auf der Verpackung / in der Produktbeschreibung

Die Darstellung dieser Icons ähnelt dem Zweck der Icons bei Datenschutzerklärungen für Apps/Webseiten. Der Kunde wird vor/bei der Kaufentscheidung darüber aufgeklärt, welche Datenverarbeitungen bei Nutzung des Produktes stattfinden könnten. Ergänzend erscheinen nachstehende Szenarien für piktographische Darstellungen tauglich und sinnvoll:

- werden Daten zwingend im Intranet oder Internet synchronisiert oder ist auch eine offline Nutzung möglich
  - hier ggf. noch eine Unterscheidung, ob nur durch das Gerät selbst erhobene/ generierte Daten betroffen sind oder ob auch von anderen im Heimnetzwerk integrierten Geräten die von diesen erhobenen/generierten Daten betroffen sind
- Daten werden verschlüsselt übertragen
- Übertragungsweg (WLan, Bluetooth, RFID, etc.)
- Synchronisierungsfunktionen

Abweichend von den Überlegungen im Kontext von Apps und Webseiten, erscheint es bei dieser Art von Devices hilfreich, auch Icons für Zugriffsrechte zu veranschaulichen. Zwar wird es auch hier keine gesetzliche Pflicht geben, mithin der Anwendungsbereich von Art. 12 Abs. 7 und 8 DS-GVO nicht gegeben sein. Allerdings fehlt für diese Devices der bei Apps bereits vorhandene, zentrale Vertriebskanal.

Sinnvolle und für Betroffene relevante Zugriffsrechte zur Darstellung durch Icons sind:

- Ermittlung und Kategorisierung weiterer Devices im Netzwerk
- (autonome) Steuerung sensibler Devices im Netzwerk (etwa (Tür-)Schlösser)
- Zahlungsdienste
- Lokale oder cloud-basierte Speicher mit Lese/Schreibrechten
- Berechtigung, Daten an Empfänger außerhalb des Netzwerks zu teilen
- ...

Ebenso denkbar erscheint die bildliche Darstellung integrierter »Sensoren«, bspw.

- Mikrofon
- Kamera
- unter Umständen auch spezielle Formen dessen, wie z. B. Tageslicht-, Restlicht- oder Nachtsichtfähigkeit, Wärmebildfunktion, etc.
- Ortungsfunktionen
- andere Sensorik (z. B. Bewegung)

Die häufig sehr kleine Fläche auf Verpackungen sollte Berücksichtigung finden. Hier ist ein Layered-Approach denkbar. So könnte auf der Verpackung lediglich eine Darstellung »Datenverarbeitung in Drittstaaten« erfolgen, eine detaillierte(re) Darstellung indessen erst in der Bedienungsanleitung; hier sollte auch über eine entsprechende Darstellung im Rahmen der Webpräsenz des Herstellers nachgedacht werden sowie eine Integration eines Verweises auf diese Webpräsenz auf der Verpackung, z. B. mittels QR-Code.

4.2.2 Darstellung der Icons auf dem bzw. durch das Gerät

Derartige Devices verarbeiten einen Großteil der Daten im Hintergrund.

Trotz fehlendem Display erscheint es zielführend, bestimmte Datenverarbeitungen / Verarbeitungsaktivitäten auf dem Endgerät darzustellen, z. B.

- in-/aktives Mikrofon
- in-/aktive Kamera
- in-/aktive Ortung
- in-/aktive Synchronisation
- in-/aktive weitere Sensorik (z. B. Bewegung)
- ...

4.2.3 Darstellung der Icons durch ein Drittgerät mit hinreichend großem Display

Es ist zudem zu unterscheiden, ob ein IoT über eine Anbindung an eine App oder sonstiges Browserportal verfügt.

Soweit ein IoT über eine Bedienung / Konfiguration via App bzw. Browserportal verfügt, eröffnen sich weitere Möglichkeiten für die transparente Darstellung von Datenverarbeitungen sowie der jeweils aktiven Sensoren.

4.2.3.1 (Grund-)Konfiguration via App / Browserportal

Soweit eine Konfiguration via App / Browserportal möglich erscheint, wäre streng genommen zu unterscheiden, ob bereits ohne eine solche Konfiguration Daten (durch die verantwortliche Stelle) verarbeitet werden. Soweit dies der Fall ist, unterlägen diese Datenverarbeitungen den Transparenzüberlegungen nach 4.2.1 bzw. 4.2.2. Hier sind insbesondere Fälle zu betrachten in denen eine Konfiguration auf dem Endgerät erfolgen kann und erst später eine Verbindung mit App / Browserportal und dann einer Synchronisation der Daten erfolgt.

Soweit eine Datenverarbeitung erst erfolgt, wenn und soweit diese via App bzw. Browserportal aktiviert wird, kann auf die Überlegungen nach 4.1 zurückgegriffen werden.

4.2.3.2 Bedienung via App / Browserportal

Hierbei kann auf die Überlegungen nach 4.1 zurückgegriffen werden. Allerdings sollte auf die besonderen Transparenzanforderungen für IoT Rücksicht genommen werden. Mithin sollten in diesen Fällen jedenfalls in der App aktivierte Sensoren für Nutzer leicht erkenntlich sein.

Zur Ermittlung sinnvollerweise darzustellender Sensoren oder sonstigen Datenerhebungen, kann voraussichtlich auf die Überlegungen unter 4.2.1 und 4.2.2 zurückgegriffen werden.

5 Datenschutz-Icons

Persönliche Daten

Kontaktdaten

Standortdaten

Finanzdaten

Kommunikationsdaten

Protokolldaten

Vertragsabwicklung

Integrität / Sicherheit

Optimierung

in der EU / EWR
außerhalb der
EU / EWR / EEA

Löschungsprinzip

Weitergabe an
Dritte

Werbung-
Weitergabe an Dritte

Weitergabe an
Behörden

Verarbeitungsstandort

Verarbeitungsstandort
nur mit EU

V1

Auftragsverarbeiter

V2

V3

V1

Verantwortlicher

V2

V1

gemeinsam Verantwortliche

V2

V1

Marktforschung

V2

V1

Profiling

V2

V3

V1

Marketing - Eigene Werbung

V2

V3

V1

Löschung (konkrete Speicherdauer)

V2

Kann offline genutzt werden

erfordert zwingend Internetzugriff

V1

Artikel 9

V2

V3

V4

V1

gemeinsame Verantwortung

V2

V3

Datenweitergabe außerhalb der EU

Datenweitergabe außerhalb der EU per Kommissionsbeschluss

Datenweitergabe außerhalb der EU per genehmigte Verhaltensregeln

Datenweitergabe außerhalb der EU per verbindliche interne Datenschutz Vorschriften

Datenweitergabe außerhalb der EU per Standard Datenschutzklauseln

Datenweitergabe in den Nicht-EU-Bereich

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom