RheinlandPfalz

Ergebnispapier

WEARABLES – FITNESSARMBÄNDER & CO

Fünfter Verbraucherdialog

Handlungsempfehlungen für Anbieter zur verbraucher- und datenschutzfreundlichen Angebotsgestaltung

INHALT

I Abstrakt

Die vorliegenden Handlungsempfehlungen zum Verbraucher- und Datenschutz bei Wearables beziehen sich vorzugsweise auf Fitness- und Lifestylegeräte für den privaten Gebrauch. Sie wurden im fünften rheinland-pfälzischen Verbraucherdialog – einem Fachforum des Ministeriums für Familie, Frauen, Jugend, Integration und Verbraucherschutz, der Verbraucherzentrale Rheinland-Pfalz e.V. sowie dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz – mit Expertinnen und Experten der Wirtschaft und Wissenschaft, von Behörden, Institutionen und Organisationen erarbeitet.

Die Empfehlungen sollen Anbietern Kriterien zur verbraucher- und datenschutzfreundlichen Angebotsgestaltung an die Hand geben. Gleichzeitig können sie Impulse unter anderem für die Verbraucherpolitik und die Verbraucherinformationsarbeit liefern. Sie gliedern sich in 14 Schwerpunkte. Insbesondere sind anwendungs-, kosten-, datenschutz- und -sicherheitsrelevante Kriterien unter Berücksichtigung technisch-organisatorischer Maßnahmen, vertragsrechtlicher Bestimmungen sowie Maßnahmen zur Verbraucherinformation angesprochen.

Aus Verbraucherschutzsicht ist vor allem wichtig, dass die Einrichtung und Bedienung von Geräten und Diensten keine besonderen technischen Kenntnisse verlangt, Kosten und Vertragsbedingungen transparent dargestellt werden und dass Systeme möglichst über die gesamte Lebensdauer technisch unterstützt werden. Der Anwendungszweck der Geräte sollte klar erkennbar sein und zuverlässig erfüllt werden. Auf Datenverarbeitungen basierende Aussagen sollten für die Nutzerinnen und Nutzer verwertbar sein, was unter anderem transparente Informationen zur Auswertung und Interpretation der erhobenen Daten voraussetzt. Weiter sollten sich die Geräte vollständig ausschalten lassen und jegliche Teilfunktionen sollten selektiv aktivierbar sein.

Aus Sicht des Datenschutzes stehen im Zusammenhang mit Wearables vor allem Datenminimierung, Transparenz und Datensouveränität im Fokus. Es muss für die Nutzerinnen und Nutzer erkennbar sein, wann welche Daten, in welchem Umfang, in welcher Weise und zu welchem Zweck verarbeitet werden und welche Stellen auf diese zugreifen können. Nach Möglichkeit sollten Wearables eine pseudonyme beziehungsweise anonyme Verarbeitung personenbezogener Daten vorsehen. Sie sollten für die personenbezogene Datenverarbeitung von den Nutzerinnen und Nutzern aktiv zu wählende Optionen anbieten. Zur Wahrnehmung ihrer Rechte müssen die Nutzerinnen und Nutzer zudem über ausreichende Kontroll- und

Steuerungsmöglichkeiten verfügen. Neben den genannten Punkten ist die Datensicherheit unabdingbare Voraussetzung für die datenschutzkonforme Ausgestaltung. Hierbei sind insbesondere die Verschlüsselung und die Prinzipien "Privacy by design" und "Privacy by default" zu berücksichtigen.

II Grundlagen des fünften Verbraucherdialogs

1. Marktentwicklung und Herausforderungen

Derzeit entsteht in Deutschland ein Volumenmarkt für Wearables, das heißt körpernah tragbare vernetzte elektronische Geräte mit entsprechenden Diensten. Lifestylegeräte wie Fitnessarmbänder und Smartwatches, die zum Beispiel Schritte zählen, den Puls messen oder Schlafgewohnheiten überwachen können, sind zunehmend im Einzelhandel präsent und verzeichnen steigende Absatzzahlen. Weitere Wearables wie smarte Kopfhörer, aber auch smarte Kleidung und Schuhe, die zum Beispiel im Leistungssport bereits Vital- und Bewegungsdaten analysieren, sind auf dem Vormarsch.

Gleichwohl steht die Angebotsentwicklung für Verbraucherinnen und Verbraucher erst am Anfang. Marktforscher erwarten Impulse vor allem im Bereich Mobiler Gesundheitsanwendungen, unter anderem indem Fitness- und Lifestylegeräte um heute noch getrennte medizinische Anwendungen, beispielsweise Blutzuckermessungen, erweitert werden. Außerdem wird Wearables das Potenzial zugesprochen, sich zu einer „persönlichen Schnittstelle“ zu vernetzten Geräten und Anwendungen zu entwickeln.

Damit erreicht die Digitalisierung des Alltags eine neue Dimension. Über Wearables geht gewissermaßen auch der Mensch online. Gleichzeitig wird die in tragbaren Objekten integrierte Technologie immer leistungsfähiger und weniger sichtbar. Die Steuerung erfolgt zunehmend intuitiv, etwa über Sprache, Gestik und Mimik.

Dies birgt Chancen, aber auch Risiken. Neben einem Zugewinn an Unterstützung und Komfort liegen Chancen insbesondere im Bereich innovativer Gesundheitsversorgung und -prävention, wenn Vitaldaten qualitätsgesichert überwacht und an Ärzte übermittelt werden können. Gleichzeitig bestehen Risiken, wenn Messwerte nicht verlässlich sind, falsche Ratschläge und Annahmen getroffen werden oder unbefugte Datenzugriffe und -verwendungen nicht sicher ausgeschlossen sind. Auch mangelnde Anwendungskompetenzen sind zu bedenken.

Verbraucherinnen und Verbraucher stehen grundsätzlich vor der Herausforderung, mit der rasanten technologischen Entwicklung und neuen komplexen Angeboten Schritt

zu halten. Dabei sind Zugänge, Kenntnisse und Fertigkeiten im Bereich Digitales unter Verbraucherinnen und Verbrauchern individuell ausgeprägt.

Umso wichtiger ist daher, dass die Angebotsentwicklung digitaler Dienste und Produkte wie zum Beispiel Wearables nicht primär Geschäftsinteressen, sondern echten und nachweislichen Verbesserungen für die Allgemeinheit dient und sich an den Bedarfen der Nutzerinnen und Nutzer orientiert. Wearables und zugehörige Apps sollten so gestaltet sein, dass auch Verbraucherinnen und Verbraucher ohne besondere Vorkenntnisse in der Lage sind, individuell geeignete Angebote auszuwählen und sicher und kompetent zu nutzen.

Anbieter, die über das gesetzlich geforderte Maß hinaus Schutz- und Unterstützungsmaßnahmen vorsehen, tragen dazu bei, dass Verbraucherinnen und Verbraucher von Anfang an berechtigtes Vertrauen in neue Angebote haben und Mehrwerte erschließen können. Hierin liegt ein wesentlicher Schlüssel für erfolgreiche Geschäftsmodelle. Ein hohes Verbraucherschutz- und Datenschutzniveau kann somit als Qualitäts- und Wettbewerbskriterium gelten.

Gerade in der digitalen Welt gelingt Verbraucher- und Datenschutz nicht allein durch Regulierung, sondern auch durch verantwortungsbewusste Angebotsgestaltung, Transparenz und Information.

2. Der (fünfte) Verbraucherdialog

Beim Verbraucherdialog handelt es sich um ein interdisziplinäres Fachforum zu neuen verbraucherrelevanten Angeboten am digitalen Markt, das seit 2007 regelmäßig zu wechselnden Themenschwerpunkten ausgerichtet wird.

Veranstalter ist das Ministerium für Familie, Frauen, Jugend, Integration und Verbraucherschutz Rheinland-Pfalz (MFFJIV) in bewährter Kooperation mit:

- der Verbraucherzentrale Rheinland-Pfalz e.V. (VZ)
- sowie dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI).

Das Forum dient dem konstruktiven Austausch von Expertinnen und Experten des Verbraucher- und Datenschutzes, der Wirtschaft, Wissenschaft und Verwaltung im Interesse eines vorsorgenden Verbraucher- und Datenschutzes in der digitalen Welt. Ziel ist die gemeinsame Formulierung von Anforderungen an neue digitale Dienste und Produkte sowie von Hinweisen zu deren Gestaltung. In Form von Handlungsempfehlungen sollen der Wirtschaft ein Orientierungsrahmen und Anregungen für die Angebotsgestaltung an die Hand gegeben werden, die auch Anknüpfungspunkte für mögliche Selbst- oder Koregulierungen liefern können. Gleichzeitig soll der Verbraucherdialog Impulse für

politische Initiativen sowie öffentlich geförderte Maßnahmen zur Verbraucherbildung, -information und -beratung geben. Er ist ein wichtiges verbraucherpolitisches Instrument der rheinland-pfälzischen Landesregierung. Weitere Informationen sind unter www.verbraucherdialog.rlp.de erhältlich.

Der fünfte Verbraucherdialog fand von September 2017 bis April 2018 zum Thema „Wearables: Fitnessarmbänder und Co.“ in Mainz statt. Ziel war die Erarbeitung von anbieteradressierten Handlungsempfehlungen zur verbraucher- und datenschutzfreundlichen Angebotsgestaltung von Wearables und zugehörigen Apps, die in Form dieses Ergebnispapieres seit dem 12. April 2018 vorliegen.

Die Handlungsempfehlungen richten sich primär an Anbieter beziehungsweise Zusammenschlüsse von Anbietern. Unter „Anbieter“ werden im fünften Verbraucherdialog Hersteller von Geräten und Apps sowie Betreiber von Diensten gefasst.

Im Sinne des vorbeugenden Verbraucher- und Datenschutzes gehen die Handlungsempfehlungen über die bei Veröffentlichung geltenden Rechtsvorschriften sowie die Neuregelungen durch die EU-Datenschutz-Grundverordnung (DS-GVO) hinaus. Sie sind technikneutral gehalten.

Folgende Verbände, Unternehmen, Einrichtungen und Organisationen haben am fünften Verbraucherdialog teilgenommen und an der Entwicklung der Handlungsempfehlungen mitgewirkt:

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)
- Chaos Computer Club e.V. (CCC)
- Fraunhofer-Institut für Experimentelles Software Engineering (IESE)
- Hochschule Kaiserslautern, Prof. Hendrik Speck, Fachbereich Informatik und Mikrosystemtechnik
- MedienKompetenzNetzwerk (MKN) Mainz-Rheinhessen
- Medizinische Hochschule Hannover, Peter L. Reichertz Institut für Medizinische Informatik, Priv.-Doz. Dr. med. Urs-Vito Albrecht
- Ministerium für Soziales, Arbeit, Gesundheit und Demografie Rheinland-Pfalz (MSAGD)
- Technische Universität Kaiserslautern, Nachwuchsgruppe wearHEALTH, Fachbereich Informatik
- TÜV Rheinland AG
- VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

3. Wearables: Definition und Befassung im fünften Verbraucherdialog

Der fünfte Verbraucherdialog definiert Wearables wie folgt:

Unter Wearables (englisch: Wearable Computing Devices) werden am und im Körper tragbare vernetzte elektronische Geräte und entsprechende Dienste verstanden, die der Messung körperlicher Aktivitäten und Vorgänge sowie der Interaktion von Mensch und Computer dienen sollen.

Derzeit fallen hierunter beispielsweise Wearables, die als Accessoires und Hilfsmittel am Handgelenk (zum Beispiel Fitnessarmbänder, Smart Watches), im Sehbereich (zum Beispiel Datenbrillen, smarte Kontaktlinsen), Hörbereich (zum Beispiel smarte Kopfhörer) oder in Form von Bekleidung (zum Beispiel smarte Shirts, Schuhe) getragen werden können. Zudem gibt es Wearables, die auf und in der Haut applizierbar sind (zum Beispiel elektronische Pflaster, Tattoos).

Wearables werden unter anderem zur privaten Anwendung im Unterhaltungs-, Fitness- und Gesundheitssektor angeboten. Sie können sowohl als geschlossenes System als auch im Internet der Dinge genutzt werden.

Wearables verfügen über einen oder mehrere Sensoren zur Datenerhebung (zum Beispiel optische Sensoren, GPS oder Bewegungssensoren) und/ oder Aktoren zur Aussendung von Signalen (zum Beispiel Vibration) sowie über mindestens eine digitale Schnittstelle, über welche sie mit externen Geräten und Diensten kommunizieren (zum Beispiel via WLAN, Bluetooth oder NFC).

In der Regel werden die Daten über die Schnittstelle an eine ein- oder mehrstufige Verarbeitungskette, typischerweise an ein Smartphone übertragen, auf dem eine spezifische Anwendung (zum Beispiel Fitness- und/oder Gesundheits-App) zur Aggregation und Aufbereitung der Daten lokal und/oder mithilfe von Diensten aus dem Internet installiert ist.

Kennzeichnend für Wearables und Apps ist die Kommunikation mit Nutzerinnen und Nutzern, Anbietern und gegebenenfalls weiteren beteiligten Stellen.

Der fünfte Verbraucherdialog hat sich schwerpunktmäßig mit Wearables aus dem Fitness- und Lifestylesegment befasst, die heute und in näherer Zukunft freiverkäuflich am Volumenmarkt erhältlich sind beziehungsweise sein könnten. Dies schließt neben smarten Accessoires und Hilfsmitteln erwartungsgemäß auch smarte Kleidung ein.

Ausgangspunkt der Betrachtung war die bestimmungsgemäße private Verwendung dieser Geräte zu Unterhaltungs- und Selbstmonitoringzwecken in Freizeit und Sport. Gleichwohl wurden auch nicht-bestimmungsgemäße Verwendungsszenarien, beispielsweise infolge falscher Erwartungshaltungen der Nutzerinnen und Nutzer, bei der Erarbeitung der Handlungsempfehlungen erwogen.

Von Fitness- und Lifestyle-Wearables prinzipiell zu unterscheiden sind Wearables, die nach dem Medizinproduktegesetz (MPG) als Medizinprodukt eingestuft werden. Die Abgrenzung erfolgt anhand des vom Hersteller festgelegten Verwendungszwecks eines Gerätes. Im Allgemeinen gelten Wearables als Medizinprodukt im Sinne des Medizinproduktegesetzes, wenn sie in ihrer Kennzeichnung, der Gebrauchsanweisung oder den Werbematerialien nach den Angaben des Herstellers zu medizinisch-therapeutischen Verwendungszwecken bestimmt sind. Näheres ergibt sich aus § 3 Nr. 1 und 10 MPG.

Wearables, die Medizinprodukte im Sinne des Medizinproduktegesetzes sind, waren nicht Gegenstand des fünften Verbraucherdialogs.

Nicht gesondert berücksichtigt wurden auch Wearables wie zum Beispiel smarte Datenbrillen, die computergesteuert eine „erweiterte Realität“ oder „virtuelle Realität“ („Augmented Reality“/ „Virtual Reality“) erzeugen können.

Ferner waren Fitness- und Gesundheitsapps auf Smartphones und Tablets, die eigenständig ohne weitere Zusatzgeräte nutzbar sind, per Definition nicht Gegenstand des fünften Verbraucherdialogs.

4. Regulierung und Koregulierung

Rechtsgrundlagen

Die Einhaltung und Anwendung der geltenden Rechtsvorschriften wird vorausgesetzt.

Wichtige Rechtsgrundlagen sind zum Beispiel die Regelungen aus dem Bürgerlichen Gesetzbuch (BGB) sowie der EU-Datenschutz-Grundverordnung (DS-GVO), die ab dem 25. Mai 2018 EU-weit anwendbar ist. Perspektivisch von Bedeutung ist die Reform des EU-Vertragsrechts für den Warenhandel und für digitale Inhalte.

Je nach Ausgestaltung des Wearables sind zudem spezialgesetzliche Rechtsgrundlagen in den Blick zu nehmen. Hierzu gehören insbesondere das Telemediengesetz (TMG), das Medizinproduktegesetz (MPG) sowie die Vorschriften zur allgemeinen Produktsicherheit (Produktsicherheitsgesetz (ProdSG)) und dem allgemeinen (Produkt-)Haftungsrecht. Gemäß dem Koalitionsvertrag zwischen CDU, CSU und SPD auf Bundesebene vom 14. März 2018 soll zwecks Erhöhung der IT-Sicherheit in verbrauchernahen Produkten eine Novellierung des Produktsicherheitsrechts und unter anderem Anpassung des Produkthaftungsrechts erfolgen.

Außerdem gelten gesetzliche Vorschriften zur Einhaltung und Kennzeichnung technischer Sicherheitsnormen.

Freiwillige Zertifizierungen

Darüber hinaus können freiwillige Zertifizierungsmöglichkeiten beispielsweise nach ISO 2700x, ISO 27018 oder BSI-IT-Grundschutz herangezogen werden.

Weiter kommen zum Beispiel das Europäische Datenschutz-Gütesiegel (EuroPriSe), das Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), das Prüfzeichen „IoT – Protected Privacy“ des TÜV Rheinland oder das Prüfzeichen „Wearable Technologies“ des TÜV SÜD in Betracht.

Im Rahmen der Cyber-Sicherheitsstrategie für Deutschland des Bundesministeriums des Innern (BMI) arbeitet das Bundesamt für Sicherheit in der Informationstechnik (BSI) außerdem an einem Gütesiegel für IT-Sicherheit.

Selbst- und Koregulierung

Daneben bestehen Initiativen in Politik und Wirtschaft zur Ergänzung und Konkretisierung des Rechtsrahmens durch freiwillige Ko- beziehungsweise Selbstregulierung.

Gesundheits-Apps betreffend, steht auf Initiative der Europäischen Union eine Selbstverpflichtung der Hersteller von Gesundheits-Apps zur Einhaltung der Datenschutzbestimmungen (Code of Conduct on Privacy for Mobile Health Applications) kurz vor dem Abschluss. Sie soll App-Entwicklern Unterstützung bei der Anwendung der geltenden Bestimmungen bieten.

Auf nationaler Ebene wird im Rahmen der E-Health-Initiative des Bundesministeriums für Gesundheit (BMG) ein Metakatalog von Kriterien zur Bewertung von Gesundheits-Apps entwickelt, der Akteurinnen und Akteuren im Gesundheitswesen die Beschreibung oder Bewertung von Apps erleichtern soll.

Wearables betreffend, befasst sich der Verein Deutscher Ingenieure e.V. (VDI) seit 2017 in Richtlinienausschüssen zur Erarbeitung technischer Regelwerke mit der Verwendung und Standardisierung von Wearables.

III Handlungsempfehlungen für Anbieter zum Verbraucher- und Datenschutz bei Wearables

Der fünfte Verbraucherdialog gibt folgende Hinweise und Empfehlungen:

1. Gute Verbraucherinformation

Geräte- und App-Hersteller sowie Betreiber von Diensten, im Folgenden Anbieter genannt, sollten auf Produktverpackungen und in öffentlich gut zugänglichen Produktbeschreibungen umfassende und leicht verständliche Verbraucherinformationen vorhalten.

Eine leichte Verständlichkeit ist vor allem durch klare und einfache Sprache zu gewährleisten. Die Informationen sollten leicht zugänglich sein und in gut strukturierter Form, unterstützt durch visuelle Darstellungen und mehrstufige Informationsebenen, erfolgen, ohne dass darunter die Vollständigkeit und Eindeutigkeit leiden. Hierbei ist die durchschnittliche Informationsverarbeitungsfähigkeit der jeweiligen Zielgruppe (zum Beispiel ältere Menschen, Minderjährige) zu berücksichtigen.

Eine leichte Zugänglichkeit kann neben der Information durch das geschulte Verkaufspersonal oder anhand von ausgedruckten Produktbeschreibungen zum Beispiel auch unter Verwendung von interaktiven Bildschirmen im Geschäft oder von QR-Codes auf der Produktverpackung realisiert werden, über welche die Informationen abgerufen werden können. Hierbei ist die durchschnittliche technische Erfahrung der jeweiligen Zielgruppe zu berücksichtigen.

2. Vorvertragliche Informationen

Insbesondere sollten Anbieter darüber informieren, welchen Anwendungszweck die Produkte haben. Nutzerinnen und Nutzer sollten anhand einer Produktkennzeichnung klar erkennen können, dass ein Produkt nicht für medizinische Anwendungen bestimmt ist.

Zudem sollte kenntlich sein, welche Betriebssysteme, Versionen von Betriebssystemen und Schnittstellen unterstützt werden. Nach Möglichkeit sollte ein Mindestdatum angegeben werden, bis zu dem für bestimmte Systeme technische Unterstützung sowie Sicherheits- und Funktions-Updates nach dem Stand der Technik be-

reitgehalten werden. Auf jeden Fall sollte das Produktionsdatum des Wearables angegeben werden.

Nutzerinnen und Nutzer sollten vor dem Kauf durch eine Angabe auf der Verpackung darauf hingewiesen werden, ob und welche Daten gesammelt, ausgewertet und übermittelt werden. Weiter sollte eine umfassende und leicht verständliche Information (beispielsweise durch Informationstexte im Internet) über die gesammelten Daten und deren Auswertung (zum Beispiel in Form von Aussagen zum persönlichen Verhalten), deren Weitergabe oder Verknüpfung mit Daten aus anderen Quellen erfolgen.

Hierzu gehören vor allem die folgenden Angaben:

- Der konkrete Zweck der jeweiligen Datenverarbeitung, insbesondere bei Datenübermittlung an weitere Stellen
- Falls Datenverarbeitungen über die primären und sekundären Zwecke des Wearables hinausgehen (zum Beispiel zwecks Marktforschung, Profilbildung, Produktverbesserung oder Werbung), auch Informationen darüber, welche Daten oder Datenarten verwendet werden (zum Beispiel Name, Adresse, E-Mail, Messdaten). Weiterhin aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person
- Beteiligte oder Kategorien von Beteiligten
- Die jeweils für die Datenverarbeitung rechtlich Verantwortlichen
- Missbrauchsgefahren und Risiken, insbesondere
  - bei der Verarbeitung besonderer Kategorien personenbezogener Daten (hier Gesundheitsdaten oder biometrische Daten nach Art. 4 Nr. 14 und 15 DS-GVO), insbesondere bei der Erstellung von Profilen,
  - sowie bei der Verknüpfung von Daten in sozialen Medien, insbesondere bei der Preisgabe von personenbezogenen Daten besonderer Kategorien
- Möglichkeiten der Anpassung von Datenschutzeinstellungen durch die Nutzerinnen und Nutzer
- Löschfristen des Anbieters und der beteiligten Stellen
- Hinweis, wenn bestimmte Funktionen des Wearables ausschließlich mithilfe eines Online-Dienstes genutzt werden können
- Hinweis, ob Daten außerhalb der Europäischen Union verarbeitet werden und wenn ja, nach Möglichkeit wo.

Ebenfalls sind das rechtliche Instrument nach Kapitel V der DS-GVO, auf dessen

Grundlage die Verarbeitung erfolgt, und die Möglichkeit der Kenntnisnahme des jeweiligen Inhalts des rechtlichen Instruments zu benennen.

Eine optische Hervorhebung sollte insbesondere erfolgen, wenn

- besondere Kategorien personenbezogener Daten verarbeitet werden
- Daten zur Marktforschung, Profilbildung oder Werbung verwendet werden können
- mit der Datenverarbeitung datenschutzrechtliche Risiken einhergehen.

Weiter sollten Nutzerinnen und Nutzer in allgemeiner Form insbesondere über das Vorhandensein jeglicher Sensoren und Aktoren sowie über die Art der messbaren Größen (zum Beispiel Körperfunktionen oder Bewegungen) in Kenntnis gesetzt werden. Außerdem sollten sie eine allgemeine Information darüber erhalten, welche Aussagen (zum Beispiel über die Fitness) die Auswertung der gesammelten Daten zulässt.

Die Anbieter sollten Nutzerinnen und Nutzer über die technisch sichere und bestimmungsgemäße Anwendung der Produkte informieren. Dazu zählen auch Angaben, die ein grundlegendes technisches Verständnis, vor allem über die konkrete Art der Datenerfassung und -nutzung (zum Beispiel mittels Sensoren), ermöglichen.

Über etwaige Kosten (zum Beispiel für Abonnements und Zusatzfunktionen) ist klar und verständlich vor dem Kauf zu informieren.

Anbieter sollten in der Lage sein, Nutzerinnen und Nutzern auf Rückfrage präzise und kostenlos Auskunft über diese Punkte zu geben.

3. Bedienfreundlichkeit und Support

Die Bedienung von Geräten, Apps und Diensten sollte für Nutzerinnen und Nutzer grundsätzlich schnell erlernbar und einfach sein. Bedienungsanleitungen sollten allgemein verständlich verfasst sein und alle Funktionen hinreichend beschreiben.

Nach Möglichkeit sollten Geräte, Apps und Dienste barrierefrei ausgestaltet sein. Benutzeroberflächen sollten individuell anpassbar sein. Auf komplexe, verschachtelte Menüstrukturen sollte verzichtet werden.

Die Menüs zu den Datenschutzeinstellungen sollten übersichtlich gestaltet sein und die Einstellungsmöglichkeiten vollständig abbilden.

Für eine erhöhte Transparenz sollten Datenflüsse an Dritte auf einen Blick erkennbar sein (beispielsweise mit Hilfe von Piktogrammen).

Bei der Entwicklung von neuartigen Benutzerschnittstellen (zum Beispiel mittels Sprache, Datenbrillen oder als Teil von Kleidung) sollten Möglichkeiten der einfachen und sicheren Bedienung im Vordergrund stehen.

Nutzerinnen und Nutzer sollten von den Anbietern technische Unterstützung kurzfristig und auf leichte Weise erhalten können [zum Beispiel telefonisch, persönlich, über E-Mail, per Web-Chat, Fernwartung, Video-Tutorials oder in Form von Hilfetexten (sog. FAQs)].

Die Anbieter sollten auf ihrer Internetseite die Ansprechpartnerinnen und -partner für technische Unterstützung oder Fragen zu Vertragsbedingungen sowie deren Kontaktdaten aufführen.

4. Nutzung und Umfang der Datenverarbeitung

Die Einrichtung und bestimmungsgemäße Nutzung von Geräten, Apps und Diensten sollte weitgehend anonym oder zumindest pseudonym möglich sein.

Die Datenverarbeitung zur Erfüllung des primären Zwecks des Wearables (zum Beispiel Sammlung der Messdaten, Aufbereitung und Auswertung dieser Daten, Anzeige des Ergebnisses) sollte nur im unverzichtbaren Umfang erfolgen (zum Beispiel die Erhebung von personenbezogenen Daten und Standortangaben).

Die Datenverarbeitung zu sekundären Zwecken (zum Beispiel Überwachung der Batterieleistung, Erkennung von Messfehlern, Analyse von möglichen Fehlbedienungen oder Fehlfunktionen) sollte von den Nutzerinnen und Nutzern in den Einstellungsoptionen selbst angepasst werden können („Opt-out“).

Die Datenverarbeitung zu darüber hinausgehenden Zwecken (zum Beispiel Produktverbesserung, Marktforschung, Profiling, Werbung, aber auch Preisgabe von Daten in sozialen Netzwerken oder gegenüber anderen Dritten) sollte erst dann erfolgen, wenn die Nutzerinnen und Nutzer diese am Gerät selbst ausdrücklich aktivieren („Opt-in“).

Eine Verarbeitung für einen anderen Zweck als ursprünglich vereinbart sollte nicht erfolgen.

Anfallende Daten sollten – soweit dies funktionsbedingt möglich ist – unabhängig von Cloud-Diensten lokal im Wearable oder im Mittlergerät auf Nutzerseite verarbeitet und gespeichert werden. Die Nutzung des grundlegenden Funktionsumfangs eines Wearables sollte dauerhaft ohne eine Übertragung personenbezogener Daten ins Internet möglich sein. Sollte eine Übertragung der Daten ins Internet optionaler Bestandteil des Dienstes sein, so sollte dies den Nutzerinnen und Nutzern angezeigt und durch diese gesteuert werden können.

Die Geräte sollten sich durch Nutzerinnen und Nutzer vollständig ausschalten lassen können. Darüber hinaus sollten Teilfunktionen (beispielsweise Funkverbindungen, Schlafüberwachung und Schrittzähler) selektiv aktivierbar sein.

Die Geräte sollten nach Möglichkeit auch offline nutzbar sein.

5. Zuverlässigkeit der Datenerfassung

Sowohl die in Wearables verbauten Sensoren als auch die Systeme, die im Datenverarbeitungsprozess nachgelagert sind, sollten den angegebenen Anwendungszweck zuverlässig erfüllen sowie valide und reproduzierbare Ergebnisse liefern. Die Auswertungen sollten im Alltag und bei sportlicher Aktivität in gleicher Weise verlässlich sein. Auf mögliche Ungenauigkeiten der Ergebnisse sollte hingewiesen werden.

Nutzerinnen und Nutzer sollten über die Ursachen möglicher Mess- und Anwendungsfehler informiert werden.

Die Messgenauigkeit sollte – soweit vorhanden – technischen Normen entsprechen und mit einschlägigen Zertifizierungen belegt werden. Eine Erläuterung der Arbeitsweise der Sensoren sollte Nutzerinnen und Nutzern zur Verfügung gestellt werden.

6. Datenauswertung und ihre Aussagekraft

Die im Rahmen der Nutzung von Wearables durch Datenverarbeitung getroffenen Aussagen (zum Beispiel zur Lebensführung oder zur Fitness) sollten für die Nutzerinnen und Nutzer verwertbar sein. Sie sollten die gemessenen Zustände oder Entwicklungen realistisch wiedergeben.

Nutzerinnen und Nutzer sollten Informationen zur begrenzten gesundheitlichen Aussagekraft der Auswertungsergebnisse erhalten. Daneben sollten sie eine Interpretationshilfe für gemessene Werte (zum Beispiel bezogen auf die Pulswerte) erhalten.

Informationen zur Auswertung und Interpretation auf Basis der erhobenen Daten sollten einfach und in transparenter Form zugänglich sein. Dabei sollten die dafür genutzten Datenarten benannt und die Gewichtung der Daten in allgemein verständlicher Form beschrieben werden.

7. Haftung und Sorgfaltspflichten

Anbieter sollten Nutzerinnen und Nutzer klar über die bestehenden gesetzlichen und vertraglichen Haftungsgrenzen informieren, sowohl bezüglich der Datenerhebung, -speicherung und -verarbeitung als auch bezüglich der Validität der Aussagen.

Die Nutzerinnen und Nutzer treffen bei der Bedienung der Produkte allgemeine Sorgfaltspflichten. Darüber hinaus sollte ihnen jedoch nicht mehr auferlegt werden als die Pflicht zur Pflege und grundlegenden Absicherung eines Benutzerkontos und zur Durchführung von Sicherheitsupdates. Die Nutzerinnen und Nutzer sollten über diese Obliegenheiten ausdrücklich, nicht nur im Rahmen der Nutzungsbestimmungen, in Kenntnis gesetzt werden.

Die Anbieter sollten über das Vorhandensein von Updates sowie die wesentlichen Änderungen von Sicherheit und Funktion aktiv informieren.

8. Haltbarkeit

Anbieter sollten für Produkte und Dienste technische Unterstützung sowie Sicherheits- und Funktions-Updates möglichst über die gesamte Lebensdauer, mindestens aber für einen Zeitraum von drei Jahren nach dem angegebenen Produktionsdatum bereitstellen. Ein einmal erreichter Funktionsumfang von Produkten sollte nicht durch Updates verringert werden. Es sei denn, nur hierdurch können Anwendungsmöglichkeiten verbessert oder erweitert werden.

Bei Updates von Funktionalitäten sollte die Kompatibilität mit Vorversionen (Abwärtskompatibilität) – soweit wirtschaftlich und technisch vertretbar – beachtet werden.

Nach Möglichkeit sollten Geräte reparierbar sein. Dafür sollten Ersatzteile über lange Zeit vorrätig gehalten werden.

Informationen zur energiebedingten Laufzeit von Geräten sollten auf realistischen Anwendungsszenarien beruhen. Diese Angaben sollten Nutzerinnen und Nutzern bereits in Produktbeschreibungen und auf Verpackungen genannt werden.

Die Geräte sollten einen geringen Stromverbrauch und eine lange energiebedingte Laufzeit haben.

Anbieter sollten Hinweise zur sachgerechten Pflege von Geräten geben. Bei Geräten, die ein Teil von Kleidung darstellen, sollte die maximal mögliche Anzahl von Waschzyklen angegeben werden (beispielsweise in Produktbeschreibungen und auf Verpackungen).

9. Kosten

Kosten für Zusatzdienste, insbesondere für Abonnements und Kundendienste, sollten transparent angegeben werden. Kostenpflichtige Zusatzdienste sollten in unterschiedlichen Tarifen angeboten werden, darunter in Tarifen, die keine oder kurze Mindestvertragslaufzeiten voraussetzen.

Für die technische Unterstützung sollte entweder kein Entgelt oder nur ein Entgelt verlangt werden, das in einem angemes-

senen Verhältnis zum tatsächlichen Aufwand steht.

Updates, die Fehler beheben oder die Sicherheit erhöhen, müssen für Nutzerinnen und Nutzer kostenfrei erhältlich sein. Die Verwendung von Clouds oder sonstiger internetbasierter Dienste sollte kostenfrei möglich sein, wenn der bestimmungsgemäße Gebrauch aller Funktionen nur mit dieser Anbindung an das Internet möglich ist.

Für die Nutzung der grundlegenden Funktionen von Geräten und Diensten sollten keine Folgekosten (beispielsweise in Form von Abonnements) verlangt werden.

Anbieter kostenloser wie kostenpflichtiger Apps sollten – soweit zutreffend – transparent über die Finanzierung der App mittels eines datenbasierten Geschäftsmodells informieren.

Wenn eine Monetarisierung der Daten von Nutzerinnen und Nutzern erfolgt (beispielsweise für Zwecke der Werbung oder der Forschung), sollten sie darüber ausdrücklich informiert werden.

Die Produkte sollten in ihrem vollen Funktionsumfang verwendbar sein, ohne dass Nutzerinnen und Nutzer zuvor eine datenschutzrechtliche Einwilligung in eine Datenverarbeitung für Zwecke zu geben haben, die über den bestimmungsgemäßen Gebrauch hinausgehen.

10. Rechtmäßigkeit der Datenverarbeitung und Einwilligung

Anbieter von Wearables haben zu berücksichtigen, dass es sich bei den anfallenden Daten in der Regel um personenbezogene, jedenfalls personenbeziehbare Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO) handelt. Diese können zudem einer besonderen Kategorie im Sinne der Datenschutz-Grundverordnung – hier biometrische Daten oder Gesundheitsdaten (Art. 4 Nr. 14 und 15 DS-GVO) – angehören, an deren Verarbeitung das Datenschutzrecht aufgrund der hohen Sensitivität besondere Anforderungen stellt. Soweit bei Daten (zum Beispiel bei Sensorwerten) durch Verknüpfung mit weiteren Informationen (beispielsweise einer Geräte-ID) ein Bezug zum jeweiligen Nutzer beziehungsweise Vertragspartner hergestellt werden kann, ergibt sich auch hier ein Personenbezug. Dieser Personenbezug besteht dabei unabhängig von der gegebenenfalls unterschiedlichen Sensitivität einzelner Datenkategorien.

Die Verwendung personenbezogener Daten ist nur zulässig, soweit dies eine Rechtsvorschrift erlaubt oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt). Abweichende Regelungen in Allgemeinen Geschäftsbedingungen ersetzen keine Einwilligung.

Als gesetzliche Erlaubnisvorschrift kommt insbesondere Art. 6 Abs. 1 lit. b) DS-GVO in Betracht. Danach ist die Verarbeitung rechtmäßig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Bei der Verarbeitung von besonderen Kategorien personenbezogener Daten müssen darüber hinaus die Voraussetzungen nach Art. 9 Abs. 2 DS-GVO erfüllt sein, insbesondere ist eine ausdrückliche Einwilligung erforderlich. Die Einholung einer ausdrücklichen Einwilligungserklärung kann für die Übermittlung von Daten jedweder Kategorie in Staaten außerhalb der Europäischen Union erforderlich sein, wenn für diese kein Beschluss der Europäischen Kommission über die Angemessenheit des Datenschutzniveaus in diesem Staat vorliegt und auch keine sogenannte „geeignete Garantie“ besteht (Art. 49 Abs. 1 S. 1 lit. a) DS-GVO).

Eine Einwilligung ist an den Vorgaben der Art. 6 Abs. 1 lit. a), Art. 7, Art. 8, Art. 9 DS-GVO und der zugehörigen Erwägungsgründe (EG) in der Datenschutz-Grundverordnung, unter anderen EG 32, 42 und 43, zu messen. Sie dient als Erlaubnistatbestand vor allem für Datenverarbeitungen, die außerhalb dessen stattfinden, was zur Erfüllung eines Vertrags erforderlich ist. Sie muss insbesondere freiwillig, eindeutig und informiert erfolgen und ist grundsätzlich an einen oder mehrere konkret benannte Zwecke gebunden.

Die Erfüllung des Vertrags, welcher mit dem Kauf des Wearables geschlossen wird, einschließlich der Erbringung einer Dienstleistung im Zusammenhang mit dem Vertrag, darf nicht von der Einwilligung zu einer Datenverarbeitung abhängig gemacht werden, die für die Erfüllung des Vertrags nicht erforderlich ist. Insbesondere sollte die Einwilligung in die Verwendung von personenbezogenen Daten besonderer Kategorien nicht von materiellen Vorteilen abhängig gemacht werden, die über den eigentlichen Vertragszweck hinausgehen.

Bei Einholung der Einwilligungserklärung der Nutzerinnen und Nutzer zur Verarbeitung der genannten Daten sollte erneut mindestens die gleiche umfassende, leicht verständliche und leicht zugängliche Information erfolgen wie vor Vertragsschluss. Sie sollte in der konkreten Situation verfügbar sein. Ein Verweis auf das Internet oder andere nicht unmittelbar verfügbare Medien ist dann in der Regel nicht mehr ausreichend.

Spätestens bei der Einholung der Einwilligungserklärung sollten die Nutzerinnen und Nutzer darüber hinaus alle weiteren im Zusammenhang mit dem Datenschutz relevanten Informationen erhalten, insbesondere zu den folgenden Punkten:

- Rechtsgrundlage der jeweiligen Datenverarbeitung, insbesondere bei Datenübermittlung an weitere Stellen
- Recht auf Widerruf der Einwilligung
- Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung, Widerspruch gegen die Verarbeitung, Datenübertragbarkeit
- Möglichkeiten der Geltendmachung der Rechte, einschließlich der Kontaktdaten der Ansprechpartnerinnen und -partner
- Name und Kontaktdaten der verantwortlichen Stelle im Sinne der Datenschutz-Grundverordnung
- Beschwerderecht bei einer Aufsichtsbehörde

Wenn die Datenverarbeitung nicht auf Basis einer Einwilligungserklärung erfolgt, sondern zum Beispiel auf einer gesetzlichen Grundlage, gilt die Informationspflicht zum Zeitpunkt der Datenerhebung.

Die Rechtsvorschriften adressieren stets den Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO. Neben den Anbietern können dies zum Beispiel Hersteller, aber auch weitere eingebundene Dienstleister sein.

11. Datensouveränität

Für Nutzerinnen und Nutzer eines Wearables sollte vollständige Datensouveränität bestehen. Das heißt, sie sollten jederzeit die umfassende Kontrolle und Steuerung über die Datenerhebung, -verarbeitung und -nutzung haben.

Nutzerinnen und Nutzer sollten alle Daten gegebenenfalls in einer vorverarbeiteten Form selbst leicht einsehen können, gegebenenfalls mithilfe eines Mittlergeräts.

Nutzerinnen und Nutzer sollten die Möglichkeit haben, Backups der Daten und Einstellungen anlegen zu können.

Nutzerinnen und Nutzer sollten außerdem die Möglichkeit haben, einzelne oder alle Daten, einschließlich Nutzerkonten, vollständig selbst zu berichtigen oder zu löschen – auch endgültig, soweit keine gesetzlichen Aufbewahrungspflichten oder Zwecke der Vertragsabwicklung entgegenstehen. Bevor die Daten geändert oder gelöscht werden können, müssen die Nutzerinnen und Nutzer darüber informiert werden, welche Folgen dies gegebenenfalls für die weitere Nutzung des Wearables haben kann.

Für Nutzerinnen und Nutzer sollte klar erkennbar sein, ob die Daten endgültig gelöscht wurden und wenn nicht, an welche Empfänger der Verantwortliche die Daten gegeben hat.

Die Rücksetzung des Geräts in den Werkszustand sollte durch die Nutzerinnen und Nutzer jederzeit leicht möglich sein. Ein Hinweis hierauf sollte an geeigneter Stelle erfolgen.

Die Geltendmachung der Datenschutzrechte gegenüber dem Anbieter sollte den Nutzerinnen und Nutzern auf einfache und effektive Weise ermöglicht werden. Die Ausführung der Rechtsansprüche (Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung, Recht auf Vergessenwerden, Widerspruch gegen die Verarbeitung, Datenübertragbarkeit) sollte durch den Anbieter unverzüglich erfolgen. Der Anbieter sollte sicherstellen, dass die Rechtsansprüche auch bei Auftragsverarbeitern oder Dritten unverzüglich erfüllt werden.

12. Datenübertragbarkeit und Interoperabilität

Nutzerinnen und Nutzer sollten die Möglichkeit haben, mindestens die gesammelten oder ermittelten Daten aus Wearables vollständig und kostenfrei in einem standardisierten elektronischen Datenformat zu erhalten.

Die selbstbestimmte Datenübertragung auf andere Geräte und an andere Anbieter sollte ohne großen zeitlichen und organisatorischen Aufwand möglich sein. Die Anbieter sollten entsprechend gestaltete Funktionen vorsehen.

Um eine möglichst breite Anwendbarkeit sicherzustellen, sollten Geräte, Apps und Dienste auf der Grundlage von offenen Standards und Schnittstellen miteinander kommunizieren können. Dabei sollten die Datensicherheit und der Schutz der privaten Daten nicht beeinträchtigt werden.

Die Anbieter sollten darüber informieren, welche Produkte miteinander interoperabel sind.

13. Technisch-organisatorische Maßnahmen zum Schutz der Daten

Gemäß Art. 32 und (EG) 83 DS-GVO sollte der Anbieter eine Risikoanalyse durchführen, welche die Folgen der Datenverarbeitung (bei Nutzerinnen und Nutzern, beim Anbieter, bei Dritten) für die betroffenen Personen ermittelt. Es ist zu prüfen, ob die Durchführung einer Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO geboten und ein Datenschutzkonzept zu erstellen ist, das die Risikoanalyse und gegebenenfalls die Datenschutzfolgenabschätzung als Grundlage hat.

Bei der Erstellung des Datenschutzkonzeptes sind die Grundsätze „Privacy by design“ und „Privacy by default“ gemäß Art. 25 DS-GVO zu beachten. Den Nutzerinnen und Nutzern sollten Funktionen zur Verfügung gestellt werden, mit deren Hilfe sie die Verarbeitung ihrer Daten nachvollziehen und steuern können. Diese Funk-

tionen sollten verständlich erläutert und leicht zu bedienen sein. Nutzerinnen und Nutzer sollten bei Einstellungsänderungen über mögliche funktionale Einschränkungen oder damit verbundene Datenlöschungen vorab informiert werden.

Bei der Produktkonzeption sind die Grundsätze „Security by design“ und „Security by default“ zu beachten. Anbieter sollten ein Sicherheitskonzept erstellen, das den zuverlässigen Betrieb des Wearables und die Durchsetzung des Datenschutzkonzeptes gewährleistet sowie auf etablierten aktuellen Standards aufbaut. Der Hersteller sollte schon im Entwicklungsprozess des Wearables Missbrauchsszenarien identifizieren und geeignete Gegenmaßnahmen entwickeln und implementieren. Sicherheitsrelevante Anweisungen (zum Beispiel die Wahl eines Passworts oder die Aufforderung zum Pairing) sollten verständlich und nutzerfreundlich gestaltet sein.

Die verwendeten Sicherheitstechniken sollten dem Stand der Technik entsprechen und so nutzerfreundlich wie möglich sein, ohne das ermittelte Sicherheitsniveau zu unterschreiten. Die Software sollte einer ständigen Qualitätssicherung unterliegen, die gängige Fehler in der Softwareentwicklung verhindert.

Der Hersteller sollte über eine geeignete Update-Infrastruktur sicherstellen, dass bekanntgewordene Sicherheitslücken (zum Beispiel in Wearables, Mittlergeräten oder Apps) zeitnah [(zum Beispiel unter Orientierung am Risikobewertungsstandard CVSS (Common Vulnerability Scoring System)] und automatisiert geschlossen werden. Updates sollten inhaltlich erläutert, möglichst einfach und unter Kontrolle der Nutzerinnen und Nutzer eingespielt werden. Bei bereitgestellten Updates sollte die Vertrauenswürdigkeit vor der Installation anhand geeigneter Mechanismen (zum Beispiel der Digitalen Signatur) überprüft werden. Im Rahmen des angegebenen Haltbarkeitszeitraums sollte bei Updates gegebenenfalls auf eine Abwärtskompatibilität verzichtet werden, insofern diese dem Beheben von Sicherheitsrisiken entgegensteht. Etwaige Nutzereinstellungen und -daten sollten von einem Update unberührt bleiben.

Für die Außerbetriebnahme oder Weitergabe des Wearables sollte ein Rücksetzungsmechanismus implementiert werden, der alle Nutzerdaten – insbesondere die Schlüssel, die zu einem Entschlüsseln vergangener Verbindungen genutzt werden könnten – unwiederbringlich löscht.

Bei Entwicklung und Betrieb von Wearables und Diensten ist der Stand der Technik zu berücksichtigen. Hierzu zählen anerkannte aktuelle Standards der IT-Sicherheit und des Datenschutzes [zum Beispiel ISO 2700x, ISO 27018, BSI IT-Grundschutz, Standard Datenschutz Modell (SDM)]. Dies sollte durch eine entspre-

chende Zertifizierung nachgewiesen werden.

Um präventiv und reaktiv auf sicherheitsrelevante Vorfälle reagieren zu können, sollten Anbieter mit entsprechenden Informationsplattformen [zum Beispiel den Computer Emergency Response Teams (CERT)] kooperieren.

14. Sicherheit bei Datenspeicherung, -übertragung und -zugriff

Bei der Gestaltung von Wearables ist darauf zu achten, dass alle Datenübertragungen nur über verschlüsselte Verbindungen mit authentisierten Kommunikationspartnern und Mittlergeräten nach dem Stand der Technik erfolgen. Generell sollten Daten nur unter Verwendung von kryptographischen Methoden nach dem Stand der Technik gespeichert und vor unberechtigtem Zugriff geschützt werden. Dies gilt sowohl für das Wearable als auch für zugehörige Systeme eines Dienstanbieters beziehungsweise eines berechtigten Dritten sowie für deren Kommunikation.

Der Zugriff auf die Daten über ein Mittlergerät sollte sich zusätzlich (innerhalb der App) absichern lassen (zum Beispiel mittels Code oder Fingerabdruck). Bei der Nutzung von Online-Diensten sollte eine Zwei-Faktor-Authentifizierung genutzt werden (zum Beispiel SMS-Authorisierungscode, Transaktionsnummer, Zertifikate, Geräte-Token). Abgewiesene Authentifizierungsversuche der genannten Fälle sind zu protokollieren und den Nutzerinnen und Nutzern in einfacher Weise anzuzeigen.

Bei der Einrichtung eines Wearables sollte ein Kommunikationsweg (zum Beispiel E-Mail, SMS, Push-Mitteilung) vereinbart werden, über den Nutzerinnen und Nutzer zeitnah mit Informationen versorgt werden, die für den ordnungsgemäßen Betrieb des Produktes notwendig sind (zum Beispiel Informationen über Sicherheitsvorfälle, Updates).

Soweit Cloud-Dienste Bestandteil einer Wearable-Lösung sind, sollte nur auf solche Dienste zurückgegriffen werden, bei denen die Speicherung und Verarbeitung der Daten von Anbietern und in Rechenzentren in der Europäischen Union erfolgt und eine Weitergabe von Daten an Stellen außerhalb dieses Bereichs verlässlich ausgeschlossen werden kann. Über die Einbindung von Cloud-Diensten in die jeweilige Lösung sind die Nutzerinnen und Nutzer zu informieren.

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

verbraucherzentrale
Rheinland-Pfalz

RheinlandPfalz
MINISTERIUM FÜR FAMILIE,
FRAUEN, JUGEND, INTEGRATION
UND VERBRAUCHERSCHUTZ

Impressum

Ministerium für Familie, Frauen, Jugend,
Integration und Verbraucherschutz (Hrsg.)
Kaiser-Friedrich-Straße 5a
55116 Mainz
verbraucherschutz@mffjiv.rlp.de
www.mffjiv.rlp.de
Redaktion: Iris Feid
Bildnachweis: Titelbild „REDPIXEL – Fotolia.com“