DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Empfehlung zum Internet der Dinge

Herausgeber:

Datenschutzstelle
Kirchstrasse 8
Postfach 684
9490 Vaduz
Fürstentum Liechtenstein

T +423 236 60 90
info.dss@llv.li
www.dss.llv.li

Version 1.0 / Januar 2015

Inhaltsverzeichnis

1. Einleitung

„Smarte Dinge“ begegnen uns in zahlreichen Lebensbereichen, wie beispielsweise in unseren Häusern, Autos, im Arbeitsumfeld oder in der alltäglichen Kommunikation. Sie scheinen unser Leben zu vereinfachen. So können im Gesundheitsbereich oder im Bereich Energie vernetzte Geräte unser Verhalten im positiven Sinn verändern: wir leben gesünder und reduzieren unseren Energieverbrauch.[1]

Auf der anderen Seite dürfen die Auswirkungen auf die Privatsphäre der Betroffenen nicht unbeachtet bleiben. Durch den Einsatz „smarter Dinge“ entstehen immer grössere Datenmengen, die gespeichert und ausgewertet werden. Sei es, um „nur“ umgebungsspezifische Daten des Nutzers zu messen oder gezielt dessen Gewohnheiten zu beobachten und zu analysieren. Mit dem Internet der Dinge finden potenzielle Überwachungswerkzeuge Einzug in die intimsten Bereiche des privaten Lebens der Nutzer.

Das gegenständliche Dokument führt in das Thema Internet der Dinge ein. Der Fokus wird dabei auf die drei Bereiche Wearable Computing, Quantified Self und Heimautomatisierung gelegt. Dies vor allem, weil gerade in diesen Bereichen grosse Datenmengen über Nutzer bearbeitet werden und die entsprechenden Geräte bereits tatsächlich in Gebrauch sind.

2. Das Internet der Dinge

Hinter dem Internet der Dinge (IoT) wird im weitesten Sinn verstanden, dass Milliarden von Sensoren in alltägliche Geräte („Dinge“) eingebaut sind. Die Dinge bearbeiten Informationen und kommunizieren miteinander, ohne dass ein Mensch etwas dazutut. Sie sind darauf ausgelegt, völlig autonom und unauffällig zu kommunizieren. Das Internet der Dinge verbindet auf diese Weise die physische Welt mit der virtuellen.

2.1 Wearable Computing

Wearable Computing *(dt. tragbare Datenbearbeitung)* bezieht sich insbesondere auf Alltagsgegenstände, beispielsweise Armbanduhren oder Brillen sowie Kleidung, deren Funktionalität durch den Einbau von Sensoren erweitert wird. Mit den eingebetteten Sensoren wie Kameras, Mikrofone, Beschleunigungs- und Lagesensoren usw. können verschiedenste Daten erfasst und für beliebige Zwecke bearbeitet werden. Häufig stehen Programmierschnittstellen für Anwendungen zur Verfügung, über die Dritte Zugriff auf die gesammelten Daten bekommen können. Da die Dinge von gewöhnlichen oder vertrauten Gegenständen kaum zu unterscheiden sind, erfahren sie rasch eine gewisse Akzeptanz bei den Nutzern.

Beispiel: Armbanduhren, die laufend den Puls messen, Brillen mit Displays und Kameras oder auch Kleidungsstücke mit eingearbeiteten elektronischen Hilfsmitteln zur Kommunikation und Musikwiedergabe.

[1] 36. Internationale Datenschutzkonferenz, Mauritius Declaration über das Internet der Dinge, 14. Oktober 2014, http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf.

2.2 Quantified Self

Dinge und Softwarelösungen im Zusammenhang mit Quantified Self unterstützen die Nutzer bei der Aufzeichnung und Analyse der eigenen personenbezogenen Daten. Die Nutzer sind vor allem an einer Auswertung – meist über einen längeren Zeitraum – ihrer persönlichen, gesundheitlichen oder sportlichen Gewohnheiten interessiert.

Beispiel: Die Nutzer verwenden zur Erfassung der persönlichen Daten unter anderem Schlaf-Tracker, Aktivitätszähler zur Erfassung von Kalorienverbrauch, zurückgelegter Wegstrecke, Gewicht, Puls oder andere Körper- bzw. Gesundheitswerte, spezifische Smartphone-Apps usw.

Die Sensoren erfassen dabei häufig mehr Informationen als den Nutzern bewusst ist bzw. präsentiert werden. So könnte beispielsweise ein Beschleunigungssensor an einem Brustgurt die Bewegungen des Brustkorbs einer Person messen (Rohdaten), daraus Informationen über den Atemrhythmus extrahieren (aggregierte Daten oder extrahierte Information) und das Mass der körperlichen Belastung der betroffenen Person anzeigen (dargestellte/interpretierte Information). Es gibt Geräte, bei denen dem Nutzer nur die interpretierten Informationen zugänglich sind; Rohdaten und aggregierte Daten bleiben dem Nutzer verborgen.

2.3 Heimautomatisierung

Vernetzte Dinge finden sich auch in Büros oder zu Hause, wie z. B. mit dem Internet verbundene Glühbirnen, Thermostate, Rauchmelder, Wetterstationen, Waschmaschinen oder Backöfen, die teilweise gar die Möglichkeit des Fernzugriffs über das Internet bereitstellen. So erkennt die „intelligente“ Haustechnik mit Bewegungssensoren, wenn eine Person sich im Haus aufhält, erfasst deren Bewegungsmuster und kann bestimmte, vorab festgelegte Aktionen anstossen (z. B. das Einschalten der Beleuchtung oder das Ändern der Raumtemperatur). Zahlreiche Dinge im Umfeld der Heimautomatisierung sind ständig miteinander oder mit dem Internet verbunden und können auch Daten an die Hersteller senden.

Beispiel: Wohnhäuser können die Anwesenheit von Personen erkennen, messen die Temperatur innen und aussen, die Luftfeuchtigkeit und Beleuchtung in den Räumen, die Sonneneinstrahlung und vieles mehr. Diese Daten können in weiterer Folge zur Rollladen- und Heizungssteuerung verwendet werden. Moderne Geräte machen jedoch sehr viel mehr als nur die Temperatur zu regeln. Sie vernetzen sich mit ihrem Umfeld und tauschen sich mit anderen Dingen aus. So kann beispielsweise online der Wetterbericht abgerufen und falls notwendig Heizmaterial nachbestellt werden.

3. Risiken für die Privatsphäre

Wenn zukünftig die Geräte autonom agieren und selbstständig Daten austauschen, stellt dies den Schutz der Privatsphäre vor besondere Herausforderungen. Personenbezogene Daten sollten unter dem Grundsatz von Treu und Glauben bearbeitet werden. Dieses Erfordernis ist umso wichtiger, je weniger aufdringlich und offensichtlich die Dinge agieren. Gerade im Zusammenhang mit dem Schutz der Privatsphäre ergeben sich konkrete Fragen: Was wird an Daten erzeugt? Welche Daten werden weitergegeben? An wen werden diese weitergegeben? Wann

werden sie gelöscht? Wie wird die Datensicherheit in sämtlichen Bearbeitungsschritten sichergestellt? Wie kann eine betroffene Person dies kontrollieren? Wo kann eine betroffene Person ihre Rechte wahrnehmen? usw. Mit dem Einsatz der Geräte sind spezifische Risiken verbunden.

3.1 Informationspflichten und Einwilligung

Grundsätzlich sind die Nutzer im Vorfeld einer Datenbearbeitung zu informieren (Informationspflichten) und falls die Umstände der Datenbearbeitung dies verlangen, ist eine Einwilligung einzuholen. In der Praxis werden heute, so scheint es zumindest, die Dinge in der Regel so gestaltet, dass sie weder die Nutzer ausreichend informieren noch einen Mechanismus zur Einwilligung zur Verfügung stellen. Ein Mangel an Information stellt jedenfalls ein ernsthaftes Hindernis für eine gültige Einwilligung dar.

In vielen Fällen weiss ein Nutzer nichts von einer Datenbearbeitung. Es ist nicht immer offensichtlich, dass mit bestimmten Dingen überhaupt Daten erfasst oder anderweitig bearbeitet werden können. In diesem Zusammenhang drängt sich die Frage einer Kennzeichnung für Gegenstände des Internets der Dinge auf. Beispielsweise wäre es möglich, eine entsprechende Kennzeichnung einzuführen, die es den betroffenen Personen ermöglicht, einen Gegenstand als „smart“ zu erkennen.

3.2 Unkontrollierte Datenflüsse

Unkontrollierte Datenflüsse stellen eines der grössten Risiken im Zusammenhang mit dem Schutz der Privatsphäre der Betroffenen dar. Dies vor allem, wenn beispielsweise die Weitergabe der Daten in intransparenter Weise erfolgt. Aus den gesammelten Daten der Dinge lassen sich meist Nutzerprofile erstellen, die speziell Dritte interessieren könnten.

Nutzer werden verschiedentlich durch Unternehmen mit Gutscheinen oder Rabatten belohnt, wenn sie sich nach einem entsprechend vorgegebenem Verhalten richten. Auch wenn dies beispielsweise für einen gesunden Menschen verlockend klingt, sollte den Nutzern der damit verbundene Eingriff in die Privatsphäre bewusst sein. Mit Daten des täglichen Konsums oder auch Körper- sowie Trainingswerten können zusammen mit weiteren Daten umfassende Gesundheitsprofile erstellt und daraus Prognosen über zukünftige gesundheitliche Entwicklung abgeleitet werden. Unabhängig der Aussagekraft solcher Prognosen können sie dazu genutzt werden, künftige Risikozuschläge zu berechnen. Der Nutzer bezahlt somit plötzlich für dieselbe Leistung mehr oder wird von bestimmten Leistungen ausgeschlossen.

Beispiel: So gibt es Motorfahrzeugversicherungen, die den Versicherungsnehmern bei risikoarmer Fahrweise eine Prämienermässigung gewähren. Dazu werden folgende Daten erhoben: Angaben zur Fahrzeugposition (aktuell und historisch), Adressdaten der Start- und Zielpunkte von Fahrten, Datum und Uhrzeit, Fahrtdauer, Geschwindigkeit und Geschwindigkeitsübertretungen, Brems- und Beschleunigungsereignisse, zurückgelegte Kilometer sowie Fahrtrichtung und Strecke mit Bezug zu einer Landkarte. Alle diese Informationen werden ausgewertet und beeinflussen die Prämienhöhe.

3.3 Zweckbindung

Die gesammelten Daten könnten ohne grossen Aufwand für andere Zwecke verwendet werden, was in den meisten Fällen wohl nicht im Sinne des Nutzers sein wird. Aus diesem Grund ist es wichtig, dass auf jeder Ebene der Datenbearbeitung (Rohdaten, extrahiert und angezeigte Daten) der Zweck einer Datenbearbeitung mit dem ursprünglichen Zweck kompatibel ist. Eine zweckentfremdete Nutzung der Daten ist nur sehr eingeschränkt zulässig.

Beispiel: Gewisse Fahrzeuge haben serienmässig über 100 Sensoren verbaut, wie beispielsweise Ultraschallsensoren (Einparkhilfe), Regensensor, Raddrehzahlsensoren (ABS), Querbeschleunigungssensoren (ESP), Achslastsensoren, Füllstandssensoren (z. B. für Öl, Treibstoff, Scheibenwaschwasser), Fahrspurerkennung, Crash-Sensoren (Airbag), Temperatursensoren (z. B. für Innen-, Aussen-, Motortemperatur), GPS-Sensoren (Navigationsgeräte), Mikrofon (Freisprecheinrichtung) usw. Diese werden im Sinne der Sicherheit und des Fahrkomforts laufend ausgewertet. Die dabei generierten Daten könnten in weiterer Folge dazu verwendet werden, um andere Informationen in einem völlig anderen Zusammenhang und anderer Bedeutung (z. B das individuelle (sportliche) Fahrverhalten, Bewegungsprofile) abzuleiten.

3.4 Anonyme Nutzung

Durch gerätespezifische Merkmale oder eindeutige Gerätekennungen *(engl. device identifier)* können in vielen Fällen die Geräte jeweils einer bestimmten Person (Nutzer) zugeordnet werden. Diese Gerätekennungen können in verschiedensten Anwendungsszenarien – einschliesslich der Standortanalyse oder der Analyse von Bewegungsmustern von Menschenmassen und einzelnen Personen – verwendet werden. Im Zusammenhang mit dem Internet der Dinge scheint gerade wegen der möglichen eindeutigen Zuordnung der Geräte zu bestimmten Personen die anonyme Nutzung erschwert.

3.5 Datensicherheit

Vor allem sind die entsprechenden Massnahmen der Datensicherheit wie beispielsweise sichere Kommunikation, Löschfristen, Vergabe von Zugriffsrechten, zur Verfügung stellen von Kontroll- und Steuerungsmöglichkeiten usw. zu berücksichtigen. Die „PC-Welt“ hat über die Jahre Möglichkeiten entwickelt, den Gefahren aus dem Internet zu begegnen; z. B. durch Einsatz von Virenscannern, automatisches Einspielen von Sicherheitsupdates oder anderer Sicherheitssoftware. Durch das Internet der Dinge entstehen zahlreiche neue Angriffsflächen, wobei die zuvor genannten „klassischen“ Sicherheitsmassnahmen nicht einfach anwendbar sind. Es besteht hier dringender Handlungsbedarf vor allem seitens der Hersteller und Entwickler, welche die mit dem Internet verbundenen Dinge angemessen sichern müssen.

Beispiel: Eine fest im Fahrzeug verbaute SIM-Karte ermöglicht beispielsweise die Nutzung internetbasierter Dienste wie News, Wetter, Online-Suche, Office-Funktionen, E-Mail usw. Durch die Vernetzung kann das Fahrzeug über das Internet angegriffen und schlussendlich auch mit Schadsoftware infiziert werden. Ein Angreifer könnte beispielsweise den Fahrzeuginnenraum abhören (Mikrofon der Freisprecheinrichtung), das Fahrzeug durch Zugriff auf das Navigationsgerät orten oder durch Beobachtung über einen längeren Zeitraum ein Bewegungsprofil erstellen.

3.6 Änderung von Verhalten und Gewohnheiten

Die Artikel-29-Datenschutzgruppe geht in Ihrer Stellungnahme zum Internet der Dinge[2] davon aus, dass durch die Verwendung von vernetzten Geräten das soziale Verhalten der Nutzer langfristig verändert wird. Dies in gleicher Weise, wie die intensive Verwendung von Videoüberwachungen das Verhalten von betroffenen Personen im öffentlichen Raum geprägt hat. Die Verhaltensänderung wird jedoch nicht auf den öffentlichen Raum beschränkt bleiben, da mit dem Internet der Dinge mögliche potenzielle Überwachungswerkzeuge Einzug in die intimsten Bereiche des privaten Lebens finden.

4. Empfehlungen

4.1 Allgemeine Empfehlungen

- Alle Anspruchsgruppen sollten sich an die Grundsätze von Privacy by Design[3] und Privacy by Default[4] halten.
- Die Informationspflichten, die Einholung einer Einwilligung oder die Umsetzung des Widerspruchsrechts sollten so benutzerfreundlich wie möglich gestaltet und insbesondere *für Anwender* verständlich sein. Im Zusammenhang mit den Informationspflichten könnte beispielsweise neben einer vollständigen Datenschutzerklärung mit einem kurzen und übersichtlichen Datenschutzhinweis informiert werden.
- Eine Einwilligung für die Bearbeitung der Daten muss freiwillig sein. Die Nutzer sollten keine Nachteile dadurch erhalten, dass sie dem Gerät Zugang zu bestimmten Daten verweigern oder bestimmte Funktionen des Geräts nicht verwenden.
- Die Nutzer sollten die Möglichkeit haben, insbesondere die Datenflüsse eines Geräts selbst zu steuern oder einzuschränken. Dies insbesondere, wenn die Daten im Zusammenhang mit einem Vertragsverhältnis bearbeitet werden (z. B. Hotel, Krankenversicherung oder Automiete).
- Die Datenbearbeitung muss so gestaltet sein, dass betroffene Personen jederzeit in der Lage sind, deren Rechte (Auskunfts-, Lösch-, Berichtigungsrecht usw.) auszuüben.
- Für Nutzer oder betroffene Dritte sollte erkennbar sein, wenn Geräte eingeschaltet (aktiv) sind, z. B. durch Senden eines spezifischen Signals auf einem Funkkanal oder andere Indikatoren.
- In vielen Fällen besteht keine Notwendigkeit, Rohdaten auf den Geräten zu speichern. Die Rohdaten müssen gelöscht werden, sobald sie für die Datenbearbeitung nicht mehr erforderlich sind.

[2] Artikel-29-Datenschutzgruppe, Opinion 8/2014 on the on Recent Developments on the Internet of Things, angenommen am 16. September 2014 (WP 223), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[3] Privacy by Design: Funktionen zur Gewährleistung des Datenschutzes sind bereits bei der Systemauslegung spezifiziert, so dass die Wahrung der Privatsphäre proaktiv bereits bei der Entwicklung der eigentlichen Technologie berücksichtigt wird.

[4] Privacy by Default: Eine Datenbearbeitung ist standardmässig datenschutzfreundlich konfiguriert (datenschutzfreundliche Voreinstellungen).

4.2 Gerätehersteller

- Gerätehersteller müssen die Nutzer über Art und Umfang der von den Sensoren gesammelten und bearbeiteten Daten informieren.
- Gerätehersteller sollten in der Lage sein, alle an einer Datenbearbeitung Beteiligten darüber zu informieren, dass ein Nutzer einer zuvor erteilten Einwilligung widerspricht oder diese einschränkt.
- Ähnlich wie bei der „Bitte nicht stören"-Funktion auf Smartphones sollten die Dinge die Option „keine Daten sammeln" zur Verfügung stellen. Die Sensoren sollten unmittelbar und einfach deaktiviert werden können.
- Um das Verfolgen einzelner Personen *(engl. tracking)* zu erschweren, sollten Gerätehersteller die Möglichkeit des einfachen Auslesens einer eindeutigen Gerätekennung verhindern; beispielsweise durch Deaktivieren der Funkschnittstellen, wenn diese nicht benutzt werden.
- Gerätehersteller sollten entsprechend fein abgestufte Einstellungsmöglichkeiten anbieten, um den Zugriff auf die erfassten Daten durch Anwendungen (Apps) einzuschränken. Diese sollten nicht nur die Kategorie der gesammelten Daten sondern auch die Zeit und die Häufigkeit des erlaubten Zugriffs umfassen.
- Gerätehersteller sollten den Nutzern Werkzeuge zur Verfügung stellen, damit diese die erfassten Daten vor einer Datenübermittlung einsehen, verändern oder zurückhalten können.
- Gerätehersteller sollten *lokale* Kontrollmöglichkeiten anbieten *(engl. privacy proxy).* Nutzer sollten Daten einsehen können, die von verwendeten Dingen gesammelt, lokal gespeichert und bearbeitet werden; dies ohne dass die Daten zuvor an den Gerätehersteller oder Dritte übertragen werden müssen.
- Es sollten Werkzeuge zur Verfügung stehen, mit welchen die Betroffenen die sie betreffenden und auf dem Gerät gespeicherten Daten in einer strukturierten Form und in einem allgemein verwendeten Format exportieren können. Der Export sollte über eine dokumentierte Schnittstelle möglich sein, und sowohl gespeicherte aggregierte Daten als auch die gespeicherten Rohdaten beinhalten.
- Gerätehersteller sollten für bestehende Sicherheitslücken der Dinge zeitnah Sicherheits-Updates zur Verfügung stellen. Die Nutzer sollten über bereitgestellte Software-Updates benachrichtigt werden. Falls ein Gerät veraltet ist und vom Hersteller nicht mehr aktualisiert wird, sollten die Nutzer auf diesen Umstand hingewiesen werden.
- Zur Reduktion von Datenflüssen sollte, wo zweckmässig, die Datenbearbeitung auf dem Gerät erfolgen (beispielsweise die Umwandlung von Rohdaten in aggregierte Daten).
- Wo eine Nutzung von „smarten" Dingen durch verschiedene Personen erfolgt, sollte durch entsprechende Einstellungsmöglichkeiten (z. B. Vergabe von Zugriffsrechten, Benutzerprofile) sichergestellt werden können, dass die Personen nicht auf die erfassten Daten des jeweiligen anderen zugreifen können.
- Gerätehersteller sollten mit Normungsgremien und Datenplattformen zusammenarbeiten und ein standardisiertes Protokoll für den gegenseitigen Austausch von Präferenzen in Bezug auf die Datenerhebung und Bearbeitung erarbeiten. Ein Nutzer könnte auf diese Weise seine Präferenzen gegenüber *einem* Gerät zum Ausdruck bringen, welches dann diese Präferenzen unmittelbar an andere verwendete Dinge weitergibt.

4.3 App-Entwickler

- Generell sollte der „Privacy by Design"-Ansatz gewählt und der Umfang der gesammelten Daten auf das für den jeweiligen Zweck erforderliche Mass minimiert werden.
- Entwickler sollten die Nutzer regelmässig auf aktive Sensoren hinweisen.
- Die Software der Dinge (Apps) müssen die Betroffenenrechte wie beispielsweise das Auskunftsrecht, Änderungsrecht, Löschrecht usw. berücksichtigen.
- Entwickler sollten Werkzeuge zur Verfügung stellen, so dass die auf dem Gerät gespeicherten Roh- als auch aggregierte Daten in einem Standardformat exportiert werden können.
- Entwickler sollten bei der Wahl der Schutzmassnahmen insbesondere die Kategorien der bearbeiteten Daten berücksichtigen. Unter Umständen kann durch Verknüpfung mit anderen Datenquellen auf besonders schützenswerte Informationen geschlossen werden.

4.4 Nutzer

- Nutzer sollten die von den Herstellern und Entwicklern bereitgestellten Datenschutzerklärungen und Informationen lesen.
- Nutzer sollten einen möglicherweise kurzfristigen Vorteil bei der Nutzung von Dingen mit den langfristigen Gefahren bewusst abwägen.
- Nutzer sollten betroffene dritte Personen informieren, wenn deren Daten durch die Nutzung eines Geräts erfasst oder anderweitig bearbeitet werden. Die Entscheidung der betroffenen Personen sollte respektiert werden, falls diese eine Datenbearbeitung nicht wünschen bzw. einer solchen widersprechen.
- Nutzer sollten die (Privatsphären-) Einstellungen regelmässig überprüfen und bei Bedarf anpassen.
- Nutzer sollten, falls möglich, die Dinge unter einem Pseudonym nutzen.

5. Weitere Informationen

Weitere Informationen zum Thema Internet der Dinge finden sich in verschiedenen Stellungnahmen der Artikel-29-Datenschutzgruppe: beispielsweise in der Stellungnahme zum Internet der Dinge[5], der Stellungnahme zu Apps auf intelligenten Endgeräten *(engl. smart devices)*[6] sowie der Stellungnahme zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten[7].

[5] Artikel-29-Datenschutzgruppe, Opinion 8/2014 on the on Recent Developments on the Internet of Things, angenommen am 16. September 2014 (WP 223), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[6] Artikel-29-Datenschutzgruppe, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, angenommen am 27. Februar 2013 (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf.

[7] Artikel-29-Datenschutzgruppe, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, angenommen am 16. Mai 2011 (WP 185), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf.