www.jusletter.ch

Floriane Zollinger-Löw / Anna Kuhn

Datenschutzrecht und Fernmelderecht im Internet of Things

Eine rechtliche Analyse der LoRaWAN-Technologie

Der vorliegende Beitrag untersucht die datenschutz- und fernmelderechtlichen Voraussetzungen und Rahmenbedingungen für die Einführung eines Internet of Things-Angebots basierend auf der LoRaWAN Technologie bei zwei Schweizer Hochschulen. Die Autorinnen kommen zum Schluss, dass der Einführung eines Service LoRaWAN aus datenschutz- und fernmelderechtlicher Sicht nichts Grundsätzliches entgegensteht, soweit beim Betrieb des Service LoRaWAN gewisse Vorkehrungen getroffen und wo nötig die Voraussetzungen hierfür geschaffen werden.

Beitragsart: Beiträge
Rechtsgebiete: Informatik und Recht

Zitiervorschlag: Floriane Zollinger-Löw / Anna Kuhn, Datenschutzrecht und Fernmelderecht im Internet of Things, in: Jusletter 2. Dezember 2019

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1. Einleitung

[1] Das Internet of Things («**IoT**») vernetzt verschiedene Gegenstände durch kleine Computer untereinander, um automatisierte Abläufe zu ermöglichen, also M2M-Kommunikation (Machine-to-Machine). Die Gegenstände (hier Sensoren) müssen befähigt sein, Informationen über deren Zustand an Applikationen zu kommunizieren. IoT-Sensoren verwenden in vielen Fällen ein spezifisches Netzwerk für die Übermittlung ihrer Rohdaten an die Gateways. Ein solches Netzwerk ist das Long Range Wide Area Network («**LoRaWAN**») mit einer Datenübertragungsrate von rund 0,3 – 5,4 kBit/s (Details unter Ziff. 3 unten). Weitere IoT-Zugangstechnologien sind z.B. Narrowband IoT (20 – 250 kBit/s), LTE-M (375 kBit/s – 1 Mbit/s), 3G- und 4G-Mobilfunk (10 Mbit/s) oder 5G (3 GBit/s).[1]

[2] Der vorliegende Beitrag untersucht die LoRaWAN Technologie unter fernmelde- und datenschutzrechtlichen Gesichtspunkten anhand eines konkreten Anwendungsfalles, dem geplanten Einsatz der Technologie an zwei Schweizer Hochschulen. Dazu werden nach einer kurzen Darstellung des Sachverhaltes in einem ersten Schritt die technischen Grundlagen von LoRaWAN erklärt.

[3] Anschliessend wird unter dem Titel «Fernmelderecht» geprüft, ob durch die Übertragung von Informationen unter Verwendung des LoRaWAN-Protokolls und des öffentlichen Internets für die Hochschulen als Betreiberinnen der Gateways gesetzliche Pflichten gemäss Fernmelderecht entstehen. Ebenfalls werden die Betreiber der Sensoren und Applikationen untersucht. Ob die übrigen involvierten Parteien (wie die Betreiberinnen der Application Server oder die Betreiber der Network Server) ebenfalls in eine der Kategorien von Mitwirkungspflichtigen nach FMG / BÜPF fallen, bildet nicht Gegenstand des vorliegenden Beitrags und wäre separat zu prüfen.

[4] Weiter wird im Kapitel «Datenschutzrecht» untersucht, ob bei einem Einsatz von LoRaWAN «Personendaten» oder sogar «besonders schützenswerte Personendaten» anfallen, welche datenschutzrechtlichen Rollen («*Verantwortliche*», «*Auftragsbearbeiter*», betroffene Person) die einzelnen IoT-Stakeholder haben und wie die allgemeinen datenschutzrechtlichen Bearbeitungsgrundsätze, das Recht auf Information sowie weitere ausgewählte datenschutzrechtliche Pflichten im vorliegenden Fall umgesetzt werden könnten. Geschlossen wird mit ergänzenden Überlegungen zur Datensicherheit bei LoRaWAN sowie zu weiteren relevanten Rechtsgebieten.

2. Sachverhalt

[5] Zwei Schweizer Hochschulen planen, den Forschenden ihrer Institutionen ein neues Netzwerkangebot im Bereich IoT zu offerieren (nachfolgend «**Service LoRaWAN**» oder «**IoT-Projekt**»). Während bislang der Einsatz von LoRaWAN nicht geregelt wurde, soll ein Service durch die Infor-

[1] Für weitere Technologien siehe z.B. Body of European Regulators for Electronic Communications (BEREC), Bericht «Internet of Things indicators», BoR (19) 25 vom 7. März 2019, Ziff. 3.

matikdienste der Hochschulen zentral verwaltet zur Verfügung gestellt und koordiniert werden. Die Leistungen der zentralen Informatik der Hochschulen sollen im Wesentlichen in der Beschaffung und dem Betrieb der Gateways liegen.

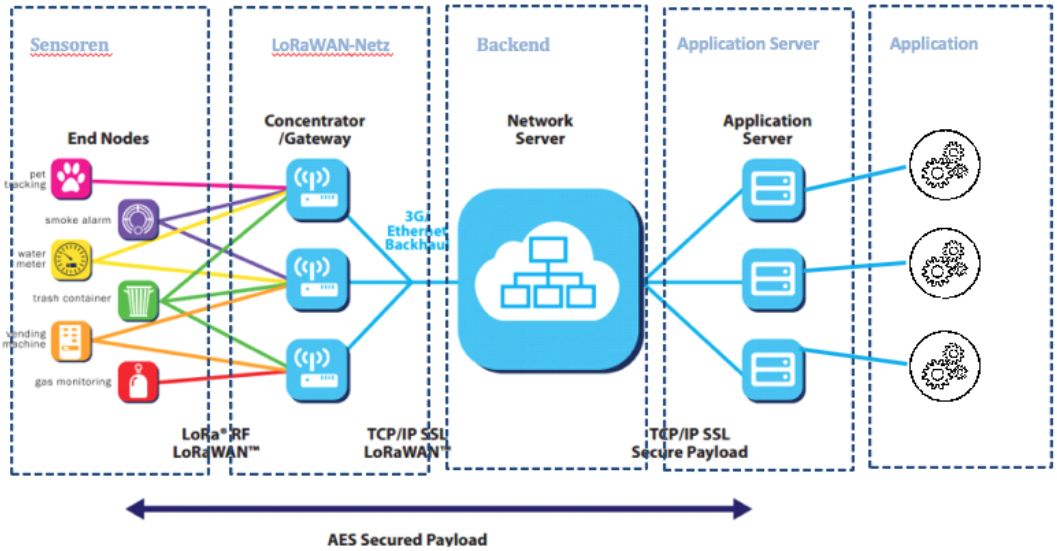
[6] Denkbare Anwendungsfälle wären zum Beispiel der Einsatz von Sensoren zur Messung von «Gesundheitsparametern» wie Herzrhythmus, Hirnströme, Blutzucker; Messungen der Raumnutzung (Bewegungssensoren) oder auch die Messung von Infrastrukturparametern (Feuchtigkeit von Pflanzen auf dem freien Feld, Stromverbrauch von Anlagen). Denkbar wäre auch, dass Sensoren in Räumen sowie in Abfalleimern oder Seifenspendern platziert werden, welche die Temperatur und den CO2-Gehalt in der Umgebung messen, um Erfahrungen zu sammeln, wie die Reinigung und das Lüftungsmanagement optimiert werden kann.

3. Technische Grundlagen der LoRaWAN-Technologie

3.1. Allgemeines

[7] LoRaWAN ist ein Low-Power-Wireless-Netzwerkprotokoll, das für die Kommunikation im Internet der Dinge entwickelt wurde. Die LoRaWAN-Spezifikation ist asymmetrisch auf Energieeffizienz der IoT-Geräte ausgerichtet. Das bedeutet in erster Linie eine hohe Reichweite (10km urban) mit geringer Bandbreite (125, 250, 500 kHz) für den Versand von Rohdaten der Sensoren an die Gateways. Die Datenübertragungsrate beträgt zwischen 292 Bit/s und 50 Kilobit/s mit Frequenz-Shifting.

[8] Die LoRaWAN-Umgebung besteht aus **Sensoren**, dem **LoRaWAN-Netz** (bestehend aus Gateways), einer **Backend-Infrastruktur** (bestehend aus dem Network Server) sowie den **Backend-Applikationen** (bestehend aus mehreren Application Server und / oder Applikationen).



Quelle: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf
(Stand 21. Oktober 2019).

3.2. Sensoren

[9] Ein Sensor ist immer einer bestimmten Applikation zugeordnet. Jeder Sensor enthält eine einmalige Sensor-ID. Die Sensor-ID ist aber nicht, wie bspw. eine IP-Adresse, einem weiten Personenkreis oder sogar öffentlich zugänglich, sondern wird immer nur für die Kommunikation zwischen einem Sensor und einer bestimmten Applikation verwendet. Der Hersteller oder «Besitzer» einer Applikation kauft die Sensoren, welche er für das Erheben der Daten braucht, in der Regel bei einem externen Dritten ein. Sensoren können in beliebiger Anzahl und von jedermann aufgestellt werden. Es wird vorliegend davon ausgegangen, dass die Sensoren der Hochschulen an den Institutionen zentral registriert werden.

3.3. LoRaWAN-Netz

[10] Wie oben aufgeführt messen **Sensoren** einen bestimmten Umstand (z.B. Blutzucker, Temperatur). Die Sensoren senden ihre Messdaten per Funk unter Verwendung des LoRaWAN-Protokolls verschlüsselt hinaus. Der nächstverfügbare **Gateway** empfängt das Signal. Jeder Sensor kann an jeden Gateway Daten schicken. Eine Einschränkung oder Kontrolle ist nicht möglich. Es ist also auch möglich, dass Sensoren, welche mit dem IoT-Projekt der Hochschulen nichts zu tun haben, Informationen an die Gateways der Hochschulen schicken. Solche Datenpakete werden dann aber vom Network Server im Backend verworfen.

[11] Der Gateway verfügt über die Information, um welche Uhrzeit von welchem Sensor resp. von welcher Sensor-ID ein bestimmter Messwert gesendet wurde. Was die Messwerte angeht, so sind diese beim Gateway verschlüsselt, d.h. die Gateway-Betreiberin sieht den Inhalt des Messwertes grundsätzlich nicht. Die Gateway-Betreiberin kann in Bezug auf die Daten von nicht registrierten Sensoren grundsätzlich auch keine Zuordnung machen, zu welcher Person eine Sensor-ID gehört, falls der Sensor in einem Gerät (Laptop, Handy, iPad etc.) oder in einem *Wearable* einer bestimmten Person eingebaut ist.

[12] Die Gateways werden von den Hochschulen bei einem Dritten eingekauft und einem bestimmten Nutzerkreis zur Verfügung gestellt. Es wird davon ausgegangen, dass die Betreiberinnen der Gateways in der Regel kein eigenes Interesse an den Daten haben, welche von den IoT-Geräten erhoben und verarbeitet werden.

3.4. Backend-Infrastruktur

[13] Alle Datenpakete werden vom Gateway verschlüsselt über das öffentliche Internet an den resp. die **Network Server** gesendet. Der Network Server nimmt nur diejenigen Datenpakete an, welche von registrierten Sensoren stammen. Der Betreiber der Network Server erhält nur die Information, um welche Uhrzeit von welchem Sensor aus ein bestimmter Messwert gesendet wurde. Da die Messwerte bei den Network Servern ebenfalls noch verschlüsselt sind, sieht der Betreiber der Network Server den Inhalt des Messwertes grundsätzlich ebenfalls nicht. Die Network Server leiten die Daten über das öffentliche Internet an den resp. die **Application Server** weiter.

3.5. Backend-Applikation

[14] Die Application Server entschlüsseln die Daten. Die Betreiberin der Application Server sieht damit den Inhalt der Messdaten. Die Application Server können intern bei den Hochschulen oder bei einem externen Anbieter betrieben werden. Die Application Server leiten die entschlüsselten Daten an die eigentlichen Applikationen weiter. Die Hersteller bzw. «Besitzer» der einzelnen **Applikation** erhalten und sehen die unverschlüsselten Messdaten, die von registrierten Sensoren stammen. Applikationen können, wie die zugehörigen Sensoren (siehe Ziff. 3.2 oben), theoretisch in beliebiger Anzahl und von jedermann hergestellt und in den Service LoRaWAN der Hochschulen integriert werden.

4. Fernmelderecht (BÜPF / VÜPF / FMG)

4.1. Rechtliches

4.1.1. Gesetzliche Grundlagen

[15] Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2018 («**BÜPF**») regelt die Überwachung des Post- und Fernmeldeverkehrs, die insbesondere im Rahmen von Strafverfahren angeordnet und durchgeführt wird. Die dazugehörigen Ausführungsbestimmungen finden sich in den entsprechenden Verordnungen, insbesondere der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017 («**VÜPF**»).

[16] Ebenfalls zu beachten ist das Fernmeldegesetz vom 30. April 1997 («**FMG**») sowie die dazu gehörige Verordnung über Fernmeldedienste vom 9. März 2017 («**FDV**»).

[17] Das BÜPF sieht verschiedene Kategorien von Mitwirkungspflichtigen vor, für die sich je nach Kategorie mehr oder weniger umfassende Mitwirkungspflichten ergeben. Art. 2 BÜPF sieht folgende Kategorien von Mitwirkungspflichtigen vor, die im Rahmen des IoT-Projekts relevant sein können:

- Anbieterinnen von Fernmeldediensten nach FMG (nachfolgend «**FDA**»);
- Anbieterinnen abgeleiteter Kommunikationsdienste (nachfolgend «**AAKD**»);
- Betreiberinnen von internen Fernmeldenetzen;
- Personen, die ihren Zugang zum öffentlichen Fernmeldenetz Dritten zur Verfügung stellen.

[18] Nachfolgend werden weitere Ausführungen zu den einzelnen Mitwirkungspflichtigen gemacht. Anschliessend wird untersucht, ob und falls ja in welche Kategorie von Mitwirkungspflichtigen die Betreiberinnen der Gateways sowie die Betreiber der Sensoren und Applikationen fallen.

4.1.2. Anbieterinnen von Fernmeldediensten

[19] Für die Definition des Begriffs Anbieterin von Fernmeldediensten müssen die beiden Elemente «*Fernmeldedienst*» und «*Erbringen*» kumulativ vorliegen. Als **Fernmeldedienst** gilt nach Art. 3 lit. b FMG die «*fernmeldetechnische Übertragung von Informationen für Dritte*», wofür wiederum drei Voraussetzungen vorliegen müssen: (1) Eine «*fernmeldetechnische Übertragung*», das

heisst ein elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk (Art. 3 lit. c FMG); (2) Die Übertragung von «*Informationen*», d.h. für Menschen, andere Lebewesen oder Maschinen bestimmte Zeichen, Signale, Schriftzeichen, Bilder, Laute oder Darstellungen jeder Art (Art. 3 lit. a FMG) und (3) «*Für Dritte*», d.h. nicht zum Eigengebrauch, sondern für andere juristische oder natürliche Personen, wobei eine Übertragung innerhalb eines Unternehmens, zwischen Mutter- und Tochtergesellschaften oder innerhalb einer Konzernstruktur kein Drittverhältnis darstellt.[2] Kein Fernmeldedienst besteht sodann in der Informationsübertragung innerhalb öffentlich-rechtlicher Körperschaften oder zwischen ihnen (Art. 2 lit. d FDV).

[20] Das **Erbringen** von Diensten beinhaltet eine wirtschaftliche und eine technische Komponente. In wirtschaftlicher Hinsicht setzt das Erbringen eines Fernmeldedienstes ein Kundenverhältnis zwischen Anbieter und Drittem voraus und in technischer Hinsicht eine angemessene Infrastruktur. Indem das Gesetz von Übertragung für Dritte spricht, impliziert es einen wirtschaftlich orientierten Dienstleistungsbegriff und setzt das Vorliegen einer Kundenbeziehung voraus. Als FDA gilt nach diesem Verständnis, wer gegenüber Kunden als Dienstleisterin auftritt, mit ihnen Verträge abschliesst, für die Dienstleistung – d.h. die Informationsübermittlung – Gewähr bietet und dafür Rechnung stellt.[3] Aus technischer Sicht wird für das «*Senden oder Empfangen von Informationen*» nicht explizit verlangt, dass die dafür notwendigen Sende- und Empfangsanlagen von der FDA selber betrieben werden müssen, weshalb auch das Outsourcing bzw. der Wiederverkauf von Diensten erfasst wird.[4] Das rechtfertigt sich auch dadurch, dass sich der Kunde primär einen Ansprechpartner wünscht, der Verantwortung für die Dienstleistung übernimmt, den gewünschten Service anbietet und für allfällige Mängel haftet (Prinzip des *One Stop Shopping*); wer die Übertragungsinfrastruktur effektiv aufbaut und betreibt, ist für ihn zweitrangig.[5]

[21] Soweit jemand als FDA zu betrachten ist, muss der gesamte Pflichtenkatalog des BÜPF erfüllt werden. Dazu gehört insbesondere Folgendes:

1. Lieferung von Auskünften über Fernmeldedienste (Art. 21 BÜPF);
2. Aufzeichnung der Randdaten des Fernmeldeverkehrs und Aufbewahrung während sechs Monaten (Art. 26 Abs. 5 BÜPF);
3. Lieferung des Inhalts und der Randdaten des Fernmeldeverkehrs von überwachten Personen auf Verlangen (Art. 26 Abs. 1 BÜPF);
4. Lieferung der für die Durchführung der Überwachung notwendigen Informationen, Duldung der Überwachung und Gewährung unverzüglichen Zugangs zu den eigenen Anlagen, Entfernung von angebrachten Verschlüsselungen (Art. 26 Abs. 2 lit. a–c BÜPF);
5. Bereitstellung definierter Schnittstellen für Echtzeitzugriffe (Art. 26 Abs. 4, Art. 31 Abs. 3 BÜPF);
6. Automatisierte Beantwortung von Auskunftsgesuchen (Art. 18 Abs. 2 VÜPF);
7. Nachweis, dass die FDA in der Lage ist, die standardisierten Auskünfte zu erteilen und die standardisierten Überwachungen durchzuführen (Art. 33 Abs. 1 VÜPF);

---

2 Leitfaden vom 1. Mai 2010 zum Meldeformular für das Erbringen von Fernmeldediensten, Bundesamt für Kommunikation BAKOM, Ziff. 1.2.1 und 1.2.2 (zit. Leitfaden BAKOM).

3 Leitfaden BAKOM (FN 2), Ziff. 1.2.1 und 1.2.2.

4 Leitfaden BAKOM (FN 2), Ziff. 1.2.1 und 1.2.2; Botschaft vom 10. Juni 1996 zum revidierten Fernmeldegesetz (FMG), BBl 1996 1405 ff. (zit. Botschaft revidiertes Fernmeldegesetz), 1425.

5 Leitfaden BAKOM (FN 2), Ziff. 1.2.1 und 1.2.2.

8. Bereitstellung eines Pikettdienstes (Art. 11 Abs. 1 und 2 VÜPF).

[22] Zusätzlich zu den Pflichten nach BÜPF gilt für FDA eine Meldepflicht beim Bundesamt für Kommunikation (BAKOM) nach Art. 4 Abs. 1 FMG.[6] Weiter unterliegen FDA dem Fernmeldegeheimnis nach Art. 43 FMG, und gemäss Art. 321ter StGB droht ihnen eine strafrechtliche Sanktionierung, falls sie Dritten unberechtigterweise Angaben über den Fernmeldeverkehr ihrer Kundschaft machen.

[23] Seit Inkrafttreten des revidierten BÜPF kann der Dienst Überwachung Post- und Fernmeldeverkehr («**Dienst ÜPF**») auf Gesuch einer FDA diese als **FDA mit reduzierten Überwachungspflichten** erklären, insbesondere wenn sie Dienstleistungen von geringer wirtschaftlicher Bedeutung anbietet oder wenn die Fernmeldedienste nur im Bereich der Bildung und Forschung angeboten werden (Art. 26 Abs. 6 BÜPF). Eine «*geringe wirtschaftliche Bedeutung*» i.S.v. Art. 26 Abs. 6 BÜPF liegt vor, wenn eine FDA weniger als zehn Überwachungsaufträge in den letzten 12 Monaten erhalten hat und wenn der Jahresumsatz in der Schweiz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten weniger als CHF 100 Mio. in zwei aufeinanderfolgenden Geschäftsjahren beträgt.[7]

[24] Eine FDA mit reduzierten Überwachungspflichten hat nach wie vor die ihr zur Verfügung stehenden Randdaten auf Verlangen zu liefern sowie die Pflichten nach Art. 26 Abs. 2 BÜPF zu erfüllen (siehe Ziff. 3 und 4 der obigen Aufzählung). Anders als bei regulären FDA handelt es sich dabei nur um passive Pflichten.

4.1.3. Anbieterinnen abgeleiteter Kommunikationsdienste

[25] Eine FDA ist insbesondere abzugrenzen von der AAKD nach Art. 2 lit. c BÜPF. Letztere stellt Dritten gegenüber bestimmte Kommunikationsdienste bereit, die nur in Verbindung mit der Tätigkeit einer Fernmeldedienstanbieterin (insb. einer Internetzugangsanbieterin) angeboten werden können.[8] AAKD oder Internetdienstanbieterinnen übertragen oder befördern keine Daten und können ihre Dienste nur durch Inanspruchnahme einer FDA anbieten, welche die Daten für sie überträgt. Erfasst werden Anbieter von Einweg- und Mehrwegkommunikation, wobei irrelevant ist, ob die Kommunikation synchron oder asynchron erfolgt. Typische Beispiele von AAKD sind Webhoster (Hosting-Provider), Anbieter von E-Mail-Speicherplatz, Cloud-Services oder Peer-to-Peer Internettelefonie.[9] Indem die Botschaft davon spricht, dass AAKD «*Dienste bereitstellen*», wird auch hier impliziert, dass von einem wirtschaftlich orientierten Dienstleistungsbegriff ausgegangen wird und dass das Vorliegen einer Kundenbeziehung vorausgesetzt ist. Diese Auffassung bestätigt auch das Merkblatt «FDA-AAKD» zur Abgrenzung von

6 Vgl. jedoch Art. 4 Abs. 1 des Entwurfes für ein revidiertes FMG, wonach die Meldepflicht nur noch eingeschränkt gelten wird. Konkret soll sie nur für FDA Bestand haben, welche vom ComCom oder dem BAKOM zugewiesene Funkfrequenzen und Adressierungselemente nutzen.

7 Art. 51 Abs. 1 lit. b VÜPF.

8 Botschaft vom 27. Februar 2013 zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), BBl 2013 2683 ff. (zit. Botschaft Überwachung Post- / Fernmeldeverkehr), 2707.

9 Botschaft Überwachung Post- / Fernmeldeverkehr (FN 8), 2708.

FDA und AAKD, welches der Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF) herausgegeben hat.[10]

[26] AAKD müssen nur über die ihnen vorliegenden Angaben Auskunft liefern (Art. 22 Abs. 3 BÜPF). Daneben unterliegen sie lediglich passiven Überwachungspflichten und müssen insb. auf Verlangen zur Verfügung stehende Randdaten des Fernmeldeverkehrs liefern, Zugang zu ihren Anlagen gewähren und für die Überwachung notwendige Auskünfte erteilen (Art. 27 BÜPF).

4.1.4. Betreiberinnen von internen Fernmeldenetzen

[27] Betreiberinnen interner Fernmeldenetze gem. Art. 2 lit. d BÜPF bieten den Dienst nicht Dritten, sondern nur einem beschränkten Kreis von Personen mit besonderer Eigenschaft an. Ein Beispiel ist eine öffentliche Einrichtung, die nur ihre Angestellten über ein solches Netz untereinander kommunizieren lässt, dieses mit anderen Worten nicht für alle zugänglich macht.[11]

[28] Als Folge unterliegt eine Betreiberin eines internen Fernmeldenetzes nur passiven Pflichten, wie insbesondere den Pflichten zur Lieferung der ihr zur Verfügung stehenden Randdaten des Fernmeldeverkehrs auf Verlangen, zur Duldung der Überwachung und Gewährung unverzüglichen Zugangs zu den Anlagen sowie zur Erteilung der für die Überwachung notwendigen Auskünfte (Art. 28 BÜPF).

4.1.5. Personen, die den Zugang zum öffentlichen Fernmeldenetz Dritten zur Verfügung stellen

[29] Art. 2 lit. e BÜPF erfasst Personen, die Dritten Zugang zu einem öffentlichen Fernmeldenetz zur Verfügung stellen. Typische Beispiele sind Hotels, Cafés oder Schulen, die ihren Internetzugang (WLAN, kabelgebunden oder andere Form) Dritten, insbesondere ihrer Kundschaft, verfügbar machen. Erfasst werden aber auch Private, deren Zugang Dritten absichtlich oder unabsichtlich offensteht. Solche Personen sind deshalb keine FDA, da die Übertragung von Informationen für Dritte nicht durch sie, sondern durch andere Anbieter übernommen wird (z.B. Swisscom).[12] Entscheidend ist jedoch, dass die Personen ihren eigenen Zugang Dritten zur Verfügung stellen und diesen selbst betreiben, der Zugang mithin nicht an professionelle Anbieter ausgelagert wird.[13] Die Pflichten von Personen, die Dritten Zugang zu einem öffentlichen Fernmeldenetz zur Verfügung stellen, sind in Art. 29 BÜPF festgehalten und decken sich mit denjenigen unter Ziff. 4.2.4 hiervor.

---

10 Merkblatt «FDA – AAKD», Abgrenzung zwischen Fernmeldedienstanbieterinnen (FDA) und Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) vom 16. April 2019, Ziff. 4.2. i.V.m. Ziff. 3.2.

11 Botschaft Überwachung Post- / Fernmeldeverkehr (FN 8), 2708.

12 Botschaft Überwachung Post- / Fernmeldeverkehr (FN 8), 2709.

13 Thomas Hansjakob, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF / VÜPF), N 1390, St. Gallen 2006 (zit. Komm BÜPF / VÜPF-VerfasserIn).

4.2. Qualifikation der Gateway-Betreiberinnen

4.2.1. Keine Fernmeldedienstanbieterinnen

[30] Indem der Gateway Messdaten per Funk erhält und durch seine Netzwerkanbindung via öffentliches Internet an den Backend Server weiterleitet, ist die Voraussetzung einer «*fernmeldetechnischen Übertragung*» erfüllt. Was das Kriterium der Übertragung für «*Dritte*» angeht, so dürften die Institutionsangehörigen keine «*Dritten*» darstellen. Dies ergibt sich einerseits aus Art. 2 lit. d FDV (vgl. Ziff. 4.1.2 oben). Zudem wird im BÜPF eine Abgrenzung gemacht zwischen «*Dritten*» (der Öffentlichkeit) und einem «beschränkten Kreis von Personen mit einer besonderen Eigenschaft»[14]. Wer einem beschränkten Personenkreis Dienste anbietet (z.B. eine öffentliche Einrichtung, die ihren Mitarbeitern ein Fernmeldenetz für die Kommunikation untereinander zur Verfügung stellt), gilt, jedenfalls unter dem BÜPF, als Betreiberin von internen Fernmeldenetzen und nicht als Fernmeldedienstanbieterin[15]. Das IoT-Netzwerk mit den aufgestellten Gateways kann nun aber nicht nur von den Institutionsangehörigen, sondern theoretisch von jedermann als Übertragungsinfrastruktur verwendet werden (siehe Ziff. 3.3 oben). Die Gateways können bekanntlich nicht steuern, welche Datenpakete sie empfangen und weiterleiten. Damit erfolgt die Übertragung durch die Gateways faktisch für beliebige «*Dritte*» bzw. für sämtliche Betreiber von Sensoren, die sich in ihrer Reichweite befinden. Demnach ist die Voraussetzung der Übertragung für «*Dritte*» erfüllt.

[31] Auch die dritte Voraussetzung, wonach «*Informationen*» i.S.v. Art. 3 lit. a FMG vorliegen müssen, ist vorliegend erfüllt. Wie unter Ziff. 4.2.2 oben aufgeführt, gelten als «*Informationen*» i.S.v. Art. 3 lit. a FMG alle für Menschen, andere Lebewesen oder Maschinen bestimmten Zeichen, Signale, Schriftzeichen, Bilder, Laute oder Darstellungen jeder Art (siehe Ziff. 4.2.2 oben). Man könnte sich zwar die Frage stellen, ob von dieser Definition auch die für das IoT kennzeichnenden maschinengenierten Informationen erfasst werden. Die Botschaft zum FMG aus dem Jahre 1996 gibt dazu keine Antwort.[16] In der Lehre wurde bereits die Frage diskutiert, ob der gesamte Internetverkehr oder nur (zweiseitige) Kommunikationsvorgänge unter das FMG und BÜPF fallen. Unter dem «*gesamten Internetverkehr*» wären auch normale Internet-Sessionen erfasst, bei welchen der Internet-Benutzer nur einseitig auf einem Server gespeicherte Daten herunterlädt, ohne dass eine Kommunikation mit einem Partner stattfindet.[17] Zu dieser Frage wird die Auffassung vertreten, dass auch einseitiger Internetverkehr mit Datenbanken dem BÜPF und FMG unterstellt werden kann.[18] Im IoT präsentiert sich die Sachlage aber insofern anders, als auch das Abrufen der Informationen nicht durch einen Menschen erfolgt, sondern an «beiden Enden» der Informationsübertragung eine Maschine steht.

[32] Die Legaldefinition von «*Informationen*» in Art. 3 lit. b FMG, auf welche sich das BÜPF bezieht, schliesst die IoT-Daten aus unserer Sicht jedenfalls nicht aus. Es ist deshalb davon auszugehen, dass die IoT-Daten in den Anwendungsbereich des BÜPF fallen und als Informationen nach Art. 3 lit. a FMG gelten, sodass deren fernmeldetechnische Übertragung als Fernmeldedienst nach Art. 3 lit. b FMG zu qualifizieren ist.

14 Botschaft Überwachung Post- / Fernmeldeverkehr (FN 8), 2708.

15 Botschaft Überwachung Post- / Fernmeldeverkehr (FN 8), 2708.

16 Botschaft revidiertes Fernmeldegesetz (FN 4), 1405 ff.

17 Botschaft Überwachung Post- / Fernmeldeverkehr (FN 8), 2704.

18 Komm BÜPF / VÜPF-Hansjakob, N 1323 ff.

[33] Im vorliegenden Fall scheitert die Qualifikation der Gateway-Betreiberinnen als Fernmeldedienstanbieterinnen allerdings daran, dass sie keinen Dienst «erbringen» (siehe Ziff. 4.2.2 oben). Die Gateway-Betreiberinnen und die «*Dritten*» (siehe oben) stehen im hier zu untersuchenden Fall nicht in einem Kundenverhältnis. Dies ergibt sich einerseits daraus, dass die Hochschulen gar nicht in allen Fällen wissen, wer ihre Infrastruktur benutzt. Da die Hochschulen den Datenverkehr nicht steuern können, ist ihnen nicht bekannt, welche bzw. wessen Messdaten effektiv über ihre Gateways versandt werden. Die Betreiberinnen der Gateways können andererseits nicht beeinflussen, welcher Gateway ein bestimmtes Signal empfängt und weiterleitet; darüber entscheidet der Zufall bzw. die geografische Reichweite eines Gateways. Auch die Funktion einer Ansprechperson gegenüber potentiellen Drittbenutzern der Gateways können die Hochschulen folglich nicht wahrnehmen. Weiter ist der Betrieb von Gateways für Dritte auch nicht beabsichtigt: Die Absicht von Hochschulen ist lediglich die Zurverfügungstellung von Gateways für Forschende und andere Hochschulangestellte innerhalb der eigenen Institution. Die theoretisch mögliche Nutzung der Infrastruktur durch Dritte ist durch Verwendung des LoRaWAN-Netzwerkprotokolls rein technisch bedingt. Die Hochschulen treten also nicht als Anbieter gegenüber Dritten auf. Gegen das Erbringen einer Dienstleistung für Dritte spricht umso mehr, dass das im konkreten Sachverhalt verwendete LoRaWAN-Protokoll per Definition unentgeltlich zur Verfügung gestellt werden muss. Weiter ist davon auszugehen, dass die Hochschulen keine Gewähr für die korrekte Informationsübertragung bieten, da das LoRaWAN-Protokoll für eine lückenlose und garantierte Übertragung technisch gar nicht geeignet ist, und auch sonst keine Verantwortung für die angebotenen Dienste übernehmen. Durch den Betrieb der Gateways ergänzen die Hochschulen lediglich ein bestehendes IoT-Netzwerksystem und tragen zu einer besseren Netzabdeckung bei. Aus alldem ist zu schliessen, dass die Hochschulen mit dem Betrieb der Gateways keinen Fernmeldedienst für Dritte im Sinne der Gesetzgebung erbringen und eine Qualifikation der Hochschulen als FDA ausser Betracht fällt. Falls der Dienst ÜPF die Betreiberinnen von Gateways in einer IoT-LoRaWAN-Netzwerkinfrastruktur wider Erwarten als FDA qualifizieren würde, könnten sich Hochschulen als weitere Massnahme auf die Ausnahmebestimmung nach Art. 51 Abs. 1 lit. a VÜPF berufen und geltend machen, dass die Schwellenwerte nicht erreicht werden oder das Angebot nur im Bereich Bildung und Forschung besteht.

4.2.2. Qualifikation als sonstige Mitwirkungspflichtige

[34] Zu prüfen ist, ob die Betreiberinnen der Gateways als **AAKD** gelten. Hierzu wäre erforderlich, dass es sich bei dem Service LoRaWAN um einen Dienst handelt, welcher sich auf Fernmeldedienste stützt und eine Einweg- oder Mehrwegkommunikation ermöglicht. Bei dem Service LoRaWAN handelt es sich kaum um einen «Dienst» im Sinne von Art. 2 lit. c BÜPF. Auch das Kriterium «Anbieten» dürfte nicht erfüllt sein. Das «Anbieten» eines Dienstes i.S.v. Art. 2 lit. c BÜPF setzt wie auch bei den FDA eine Kundenbeziehung voraus (siehe Ziff. 4.2.3 oben). Eine solche ist vorliegend nicht ersichtlich (siehe Ziff. 4.3.1 oben). Zudem nehmen die Betreiberinnen der Gateways die Übertragung der Informationen selber vor – sie lassen diese nicht durch eine FDA übertragen. Aus diesen Gründen handelt es sich bei den Gateway-Betreiberinnen nicht um AAKD.

[35] Als weitere Kategorie von Meldepflichtigen kommt für die Betreiberinnen der Gateways **Art. 2 lit. e BÜPF** (Person, die Dritten Zugang zu einem öffentlichen Fernmeldenetz zur Verfügung stellt) in Frage. Voraussetzung hierfür wäre, dass es sich bei dem IoT-Netzwerksystem um

ein öffentliches Fernmeldenetz handelt, dass die Hochschulen den Zugang zu diesem Netz selber betreiben und dass sie den Zugang Dritten zur Verfügung stellen. Wie bereits unter Ziff. 4.2.5 oben ausgeführt, betreiben die Personen nach Art. 2 lit. e BÜPF nur den Zugang zum Netz und übertragen selber keine Informationen. Diese Funktion kommt den FDA zu. Im vorliegenden Fall werden die Informationen aber durch die Betreiberinnen der Gateways (und die Betreiber der Network Server und Application Server) selber übertragen und nicht durch eine dritte, «professionelle», Anbieterin. Damit handelt es sich bei den Betreiberinnen der Gateways nicht um Personen, die Dritten ihren Zugang zu einem öffentlichen Fernmeldenetz zur Verfügung stellen.

[36] Bei den Betreiberinnen der Gateways dürfte es sich hingegen um **Betreiberinnen eines internen Fernmeldenetzes** i.S.v. Art. 2 lit. d BÜPF handeln, da der Service LoRaWAN nur den Forschern und Hochschulangestellten der Hochschulen und somit einem beschränkten Personenkreis angeboten wird. In diesem Fall unterliegen die Hochschulen aber nur passiven Pflichten wie insbesondere den Pflichten zur Lieferung der ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs auf Verlangen, zur Duldung der Überwachung und Gewährung unverzüglichen Zugangs zu den Anlagen sowie zur Erteilung der für die Überwachung notwendigen Auskünfte (Art. 28 BÜPF).

4.2.3. Betreiber der Sensoren und Applikationen

[37] Die Forschenden der Hochschulen und die weiteren Betreiber von Sensoren und Applikationen im IoT-Projekt sind lediglich Anwender des Services LoRaWAN. Sie setzen Sensoren und Applikationen für von ihnen gewünschte Messungen und für eigens definierte Zwecke ein. Die Betreiber der Sensoren und Applikationen übertragen selber keine Informationen, weder für Dritte noch hochschulintern – vielmehr nutzen sie für die Übertragung ihrer Daten die Netzwerkumgebung, welche ihnen von der Institution zur Verfügung gestellt wird. Die Betreiber von Sensoren und Applikationen gelten damit weder als FDA noch als AAKD und fallen auch in keine andere Kategorie von Mitwirkungspflichtigen unter dem BÜPF.

4.3. Fazit

[38] Es lässt sich gut argumentieren, dass die Hochschulen als Betreiberinnen der Gateways im IoT-Projekt nicht als FDA und auch nicht als AAKD gemäss FMG und BÜPF zu qualifizieren sind. Zwar handelt es sich bei der Übertragung der Informationen um einen Fernmeldedienst – die Qualifikation als FDA oder als AAKD scheitert aber an der Voraussetzung der Dienstleistungserbringung. Die Hochschulen haben keine Kundenbeziehung mit den «*Dritten*», fungieren nicht als deren Ansprechperson und übernehmen keine Gewähr für die korrekte Informationsübertragung. Die Betreiberinnen der Gateways sind auch nicht als Personen, die Dritten ihren Zugang zum öffentlichen Fernmeldenetz zur Verfügung stellen (Art. 2 lit. e BÜPF), zu qualifizieren, da sie die Informationen selber übertragen. Die Hochschulen als Betreiberinnen der Gateways sind hingegen wohl als Betreiberinnen eines internen Fernmeldenetzes zu qualifizieren. Als solche haben sie indessen nur passive Pflichten wie insbesondere die Pflichten zur Lieferung der ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs auf Verlangen, zur Duldung der Überwachung und zur Gewährung unverzüglichen Zugangs zu den Anlagen sowie Erteilung der für die Überwachung notwendigen Auskünfte (Art. 28 BÜPF).

5. Datenschutzrecht

5.1. Rechtsgrundlagen

5.2. Kantonales Datenschutzrecht

[39] Bei kantonalen Hochschulen sind die jeweils für Behörden geltenden kantonalen Datenschutzgesetze zu beachten. Vorliegend werden die Ausführungen auf die für den Kanton Zürich bzw. Zürcher Hochschulen anwendbaren Datenschutzgesetze beschränkt. Dabei handelt es sich um das Gesetz über die Information und den Datenschutz vom 12. Februar 2007 («**IDG**») und die Verordnung über die Information und den Datenschutz vom 28. Mai 2008 («**IDV**»). Weiter gilt für die Hochschulen des Kantons Zürich unter gewissen Voraussetzungen die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung; «**DSGVO**»).

[40] Im Kanton Zürich besteht überdies das Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999.

5.3. Schweizer Datenschutzrecht

[41] Für Schweizer Behörden und somit auch Schweizer Hochschulen finden sich die anwendbaren Datenschutzbestimmungen im Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Datenschutzgesetz; «**DSG**») sowie den entsprechenden Verordnungen, insbesondere der Verordnung zum Bundesgesetz über den Datenschutz vom 16. Juni 1993 (Datenschutzverordnung; «**VDSG**»). Ebenfalls kann für eine Schweizer Hochschule unter gewissen Voraussetzungen die DSGVO zur Anwendung gelangen. Schliesslich wird die Schweizer Hochschule die Bestimmungen des revidierten Schweizer Datenschutzgesetzes beachten müssen. Der vorliegende Beitrag berücksichtigt deshalb wo angebracht auch den Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz («**E-DSG**»).

5.4. Anwendbarkeit des Datenschutzrechts

[42] Damit das Datenschutzrecht auf eine Datenverarbeitung im Rahmen des IoT-Projekts der Hochschulen anwendbar ist, müssen Daten von natürlichen oder juristischen[19] Personen bearbeitet werden. Das IDG enthält auch Bestimmungen, welche für die Bearbeitung von «*Informationen*» gelten, und ist somit nicht auf Personendaten beschränkt, sondern erfasst vielmehr auch Sachdaten. Es handelt sich dabei aber primär um Bestimmungen zur Informationssicherheit (zur Informationssicherheit vgl. Ausführungen unter Ziff. 6 unten). Die Ausführungen, welche in diesem Kapitel zum Datenschutz gemacht werden, gelten auch unter dem IDG nur für Personendaten und nicht allgemein für Informationen.

[19] Die juristischen Personen sind gemäss dem geltenden DSG und IDG geschützt (Art. 3 lit. b DSG, § 3 lDG, vgl. PK-Rudin, § 3 N 16, in: Bruno Baeriswyl / Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich IDG, Zürich / Basel 2012 (zit. PK-Verfasser). Gemäss DSGVO und E-DSG werden nur natürliche Personen geschützt (vgl. Art. 4 Abs. 1 DSGVO; Art. 4 lit. a E-DSG).

5.5. Bearbeiten

[43] Der Begriff des «*Bearbeitens*» von Personendaten ist weit auszulegen; er erfasst jeden Umgang mit Personendaten, unabhängig der angewandten Mittel und Verfahren, und umfasst insbesondere das Beschaffen, Aufbewahren, Verwenden Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 lit. e DSG, Art. 4 lit. d E-DSG, Art. 4 Ziff. 2 DSGVO, § 3 IDG). Die Erfassung oder der Versand von Personendaten sowie auch das reine Speichern von Personendaten in einer Cloud stellen also bereits eine Bearbeitung im Sinne der Datenschutzgesetze dar.[20]

5.6. Personendaten

[44] Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG, § 3 IDG, vgl. auch Art. 4 Ziff. 1 DSGVO).

[45] Der Bestimmbarkeit liegt ein relativer Ansatz zugrunde. Die Bestimmbarkeit ist gegeben, wenn nach der allgemeinen Lebenserfahrung damit gerechnet werden muss, dass ein Interessent den Aufwand auf sich nehmen wird, um die Person zu bestimmen, wobei der Stand der Technik und die technischen Entwicklungsmöglichkeiten zu berücksichtigen sind.[21] Dabei ist grundsätzlich auf die Perspektive des jeweiligen Datenbearbeiters abzustellen. Es sind aber die Interessen, Zusatzinformationen und Informationsmöglichkeiten eines Dritten zu berücksichtigen, wenn diese dem die Daten übermittelnden Bearbeiter bekannt waren oder hätten bekannt sein müssen[22] oder wenn der die Daten übermittelnde Bearbeiter indirekt auf diese Mittel zugreifen kann. Ein Bearbeiter, welcher Daten übermittelt, untersteht daher selbst dann dem Datenschutzrecht, wenn er aus den Daten selbst keine Personen identifizieren kann, die Daten aber an einen Bearbeiter übermittelt, der über diese Möglichkeit verfügt und an einer Identifizierung auch interessiert ist.[23]

[46] Nicht mehr bestimmbar ist eine Person, wenn die Daten anonymisiert sind, d.h. wenn der Personenbezug irreversibel so aufgehoben wurde, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr möglich sind.[24] Bei einer Anonymisierung ist auch der Inhaber der Daten nicht mehr in der Lage, einen Personenbezug herzustellen.[25] Die Anonymisierung kommt aus praktischen Gründen nur in wenigen Fällen in Frage, z.B. wenn statistische Daten in der Cloud bearbeitet werden.[26] Im Falle einer Anonymisierung ist der Personenbezug aufgehoben und die Bestimmungen, welche für Personendaten gelten, sind nicht anwendbar.

---

20 Vgl. auch David Schwanninger / Stephanie S. Lattmann, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter 11. März 2013, N 6.

21 BGE 136 II 508, 513 f. E. 3.2; BGer 4A_365/2017 vom 26. Februar 2018, E. 5; Urteil des EuGH C-582/14 vom 19. Oktober 2016, Breyer, N 46 f.; DSGVO, Erwgr. 26.

22 PK-Rudin, § 3 N 26.

23 Vgl. BGE 136 III 508, 515 E. 3.4.

24 SHK DSG-Rudin, Art. 3 N 13, in: Bruno Baeriswyl / Kurt Pärli (Hrsg.), Datenschutzgesetz (DSG), Stämpflis Handkommentar, Bern 2015 (zit. SHK DSG-Verfasser); BSK DSG-Blechta, Art. 3 N 13, in: Urs Maurer-Lambrou / Gabor-Paul Brechta (Hrsg.), Datenschutzgesetz (DSG) / Öffentlichkeitsgesetz (BGÖ), Basler Kommentar, 3. A., Basel 2014 (zit. BSK DSG-Verfasser); vgl. auch Philippe Fuchs, Cloud Computing – eine datenschutzrechtliche Betrachtung, in: Jusletter IT 6. Juni 2012, N 1.

25 Ursula Widmer, Gesundheitsdaten in der Cloud, DACH Security 2011, 177.

26 Widmer, (FN 25), 177

[47] Bei einer Pseudonymisierung werden die personenbezogenen Merkmale durch Platzhalter ersetzt, z.B. Namen durch eine Kennziffer, so dass für Dritte, welche nicht über eine Referenzliste für Identitäten und ihre Pseudonyme verfügen, kein Rückschluss auf eine bestimmte Person mehr möglich ist. Problematisch bei der Pseudonymisierung ist, dass die Aufhebung des Personenbezugs häufig nicht absolut möglich ist. Werden z.B. Patientendaten durch eine Nummer ersetzt, so reicht dies zu einem Ausschluss des Personenbezuges nicht aus, wenn aufgrund anderer individualisierender Merkmale eine personenbezogene Zuordnung nach wie vor möglich ist, was häufig der Fall ist.[27] Die Verschlüsselung stellt eine umfassende Art der Pseudonymisierung dar.

[48] Bei der Pseudonymisierung wird der Personenbezug aufgehoben, aber nur reversibel: Der Schlüssel zur Re-Identifizierung der Information bleibt erhalten. Pseudonymisierte Daten stellen für alle, die Zugang zum Schlüssel bzw. der Zuordnungsregel haben, weiterhin Personendaten dar. Für Aussenstehende, welche nicht über einen Schlüssel verfügen und auch keinen Zugang zum Schlüssel haben, sind pseudonymisierte Personendaten nicht mehr Personendaten.[28]

[49] Die Daten, welche im Rahmen des IoT-Projekts gesammelt und bearbeitet werden, können sehr unterschiedlich sein und von simplen Sensordaten wie bspw. Temperaturangaben bis hin zu kompletten Bewegungsprofilen variieren. Ob es sich bei den einzelnen Messdaten um Personendaten handelt, muss pro IoT-Anwendungsfall geprüft werden. Nach dem Gesagten ist dabei grundsätzlich immer auf die Perspektive des einzelnen Datenbearbeiters abzustellen. Ein Personenbezug ist beispielsweise möglich, wenn der Datenbearbeiter – z.B. ein Applikationsbetreiber – nicht nur über einen bestimmten Messwert (wie bspw. einen Blutzuckerwert) und die Sensor-ID des Sensors verfügt, von welchem aus der Messwert gesendet wurde, sondern über zusätzliche Informationen, welche es ihm erlauben, den Messwert einer bestimmten natürlichen Person zuzuordnen. Solche zusätzlichen Informationen könnten Personalien sein, welche das Datensubjekt (die betroffene Person) bspw. im Zeitpunkt der Installation oder der Nutzung einer Applikation bekanntgegeben hat. Ebenso kann es im IoT-Projekt zu einem Personenbezug kommen, wenn ein IoT-Stakeholder[29] grosse Mengen an Daten analysiert («Big Data-Analyse») und aus den Daten Profile bilden und Muster herauslesen kann, welche ihm eine Identifikation einer einzelnen Person erlauben.[30] Was die Betreiberinnen der Gateways angeht, so kann festgehalten werden, dass die Messdaten bei den Gateways verschlüsselt sind und dass die Betreiberinnen keinen Zugriff auf den Schlüssel haben. In der Folge darf davon ausgegangen werden, dass Messdaten im aktuellen Stadium aus isolierter Sicht der Betreiberinnen der Gateways keine Personendaten darstellen. Wie unter Ziff. 5.8.1 ausgeführt wird, bedeutet dies jedoch noch nicht, dass die Hochschulen im Rahmen des IoT-Projekts keine Pflichten in Bezug auf den Datenschutz und die Datensicherheit übernehmen müssen.

27 Widmer, (FN 25), 176 f.

28 SHK DSG-Rudin, Art. 3 N 14.

29 Die verschiedenen IoT-Stakeholder werden in Ziff. 5.8 unten aufgeführt.

30 Vgl. dazu auch Dominic N. Staiger, Data Protection Challenges in the Internet of Things, in: Jusletter IT 7. Juni 2018, N 14; auch gem. Art. 29 Arbeitsgruppe, Opinion 8/2014 on the Recent Developments on the Internet of Things, vom 16. September 2014, 4 ff. sowie 10 f., handelt es sich bei den Daten, welche im Rahmen von IoT bearbeitet werden, um Personendaten i.S.d. DSGVO.

5.7. Besonders schützenswerte Personendaten / Persönlichkeitsprofile

[50] Besondere Regeln gelten für sog. «*besonders schützenswerte Personendaten*» gem. Art. 3 lit. c DSG, Art. 9 Ziff. 1 DSGVO (dort benannt als «*besondere Kategorien personenbezogener Daten*») und § 3 IDG (dort benannt als «*besondere Personendaten*»). Darunter fallen Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen oder Sanktionen. Gemäss DSGVO und E-DSG gelten zudem Daten über die Zugehörigkeit zu einer Ethnie, genetische Daten und biometrische Daten, die eine natürliche Person eindeutig identifizieren, als besonders schützenswert. Es kann nicht ausgeschlossen werden, dass im Rahmen des IoT-Projekts solche Daten erhoben werden und dass diese im Laufe der Zeit einer natürlichen Person zugeordnet werden können, selbst wenn die Zuordnung im Zeitpunkt der Erhebung der Daten nicht beabsichtigt gewesen sein sollte.

[51] Ebenso gelten besondere Regeln für den Umgang mit «*Persönlichkeitsprofilen*» gem. Art. 3 lit. d DSG und § 3 IDG. Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.[31] In Art. 4 Ziff. 4 DSGVO und in Art. 4 lit. f E-DSG findet sich anstelle des Persönlichkeitsprofils der Begriff des «*Profiling*». Das Profiling weist eine Ähnlichkeit zum Persönlichkeitsprofil auf, die Begriffe sind aber nicht deckungsgleich.[32] Die Daten, welche im Rahmen des IoT-Projekts bearbeitet werden, können Persönlichkeitsprofile darstellen, wenn die Zusammenstellung der Daten eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, selbst wenn eine solche Zusammenstellung oder Beurteilung im Zeitpunkt der Erhebung der Daten nicht beabsichtigt gewesen sein sollte.

[52] Ebenso kann ein Profiling i.S. der DSGVO vorliegen, wenn die IoT-Geräte eingesetzt werden, um bewusst das Verhalten einzelner Personen zu beobachten bzw. um bestimmte persönliche Aspekte einer natürlichen Person zu bewerten (z.B. mittels Tracking oder Geolokalisierung).

[53] Unter dem DSG bedarf die Bearbeitung von besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen durch Bundesorgane einer gesetzlichen Grundlage im formellen Sinn oder ausnahmsweise einer Einwilligung der betroffenen Person im Einzelfall (Art. 17 Abs. 2 DSG).[33] Dies im Gegensatz zu gewöhnlichen Personendaten, bei welchen bereits eine Gesetzesgrundlage auf Verordnungsstufe reicht.[34]

[54] Unter dem IDG bedarf die Bearbeitung von besonderen Personendaten einer hinreichend bestimmten Regelung in einem formellen Gesetz (§ 8 Abs. 2 IDG). Aufträge an Dritte zum Bearbeiten von besonderen Personendaten müssen von der vorgesetzten Stelle bewilligt werden (§ 25 Abs. 3 IDV). Falls Informatiksysteme und Anwendungen mit strategischer Bedeutung für die kantonale Verwaltung betroffen sind, muss die Auslagerung vom Regierungsrat bewilligt werden (§ 1 Abs. 2 Gesetz über die Auslagerung von Informatikdienstleistungen).

---

31 Art. 3 lit. d DSG; § 3 IDG.

32 Für Details zum «Profiling» siehe Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderungen weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff., 7021.

33 Wobei das allfällige Vorliegen einer Einwilligung unseres Erachtens aber nicht von dem Erfordernis einer hinreichenden gesetzlichen Grundlage befreit.

34 Art. 17 Abs. 1 DSG; § 8 Abs. 1 IDG.

5.8. Rollen der einzelnen IoT-Stakeholder

5.8.1. Einleitung

[55] Im Internet of Things gibt es verschiedene Stakeholder. Im Bereich der Sensoren gibt es die Benutzer, welche Sensoren betreiben und für ihre Zwecke einsetzen (z.B. Forschende) sowie die Hersteller der Sensoren. Im Bereich der Gateways gibt es die Betreiberinnen der Gateways (Informatikdienste der Hochschulen) sowie die Hersteller der Gateways. Im Bereich des Backend gibt es die Betreiber der Network Server sowie die Betreiberinnen der Application Server. Im Bereich der Applikationen gibt es schliesslich die Hersteller der Software einer Applikation sowie diejenigen Personen, welche eine Software eingekauft bzw. lizenziert haben und den Nutzen aus einer Applikation ziehen. Letztere Personen können identisch sein mit den Herstellern der Software der Applikation, wenn z.B. ein Forscher eine eigene Software für die Auswertung der von ihm gemessenen Daten entwickelt, dies ist aber nicht zwingend. Schliesslich gibt es diejenigen Personen, deren Daten im Rahmen des IoT-Projekts erhoben und bearbeitet werden.

[56] Nachfolgend wird geprüft, welche datenschutzrechtliche Rolle den einzelnen IoT-Stakeholdern zukommt. Dies ist relevant, weil die einzelnen Rollen mit unterschiedlichen datenschutzbezogenen Rechten und Pflichten verbunden sind. Insbesondere ist zu prüfen, ob die einzelnen IoT-Stakeholder als «*Verantwortliche*» (engl. «*controller*»), als «*Auftragsbearbeiter*» (engl. «*processor*») oder als «*betroffene Personen*» (engl. «*data subjects*») im Sinne des Datenschutzrechts gelten.

[57] «*Verantwortlicher*» ist dabei jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[35] Datenschutzrechtlich «*verantwortliche*» Personen haben diverse datenschutzrechtliche Verpflichtungen wie bspw. eine umfassende Informationspflicht gegenüber den betroffenen Personen, sowie die Pflicht zur Wahrung der übrigen Betroffenenrechte wie bspw. das Recht auf Auskunft, Berichtigung unrichtiger Personendaten oder das Recht auf Datenübertragbarkeit. Die «*Verantwortlichen*» können im Falle einer Verletzung ihrer datenschutzrechtlichen Verpflichtungen gebüsst werden. Praxisgemäss sind es stets natürliche Personen, die Daten bearbeiten. Es gilt deshalb zu ermitteln, ob das Handeln der natürlichen Person selbst oder einer juristischen Person / Organisation zuzurechnen ist, für die sie tätig wird. In letzterem Fall wird die Auffassung vertreten, dass jeweils die gesamte juristische Person / Organisation als *Verantwortliche* zu betrachten ist und nicht einzelne Abteilungen, Dezernate etc., die der Organisationseinheit angehören.[36]

[58] Als «*Auftragsbearbeiter*» gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des *Verantwortlichen* verarbeitet.[37] «*Auftragsbearbeiter*» treffen ebenfalls gewisse datenschutzrechtliche Verpflichtungen und sie können im Falle einer Verletzung dieser Pflichten gebüsst werden.

---

35 Art. 4 Ziff. 7 DSGVO; ähnlich Art. 4 lit. i E-DSG. Das DSG spricht vom «*Inhaber der Datensammlung*» (Art. 3 lit. i DSG).

36 DSGVO Komm-Hartung, Art. 4 Nr. 9 N 5 ff., in: Jürgen Kühling / Benedikt Buchner (Hrsg.), Kommentar Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, 2. A., München 2018 (zit. DSGVO Komm-Verfasser).

37 Vgl. Art. 4 Ziff. 8 DSGVO (dort benannt als «*Auftragsverarbeiter*»); ähnlich Art. 4 lit. j E-DSG.

[59] Als «*betroffene Personen*» gelten alle natürlichen oder juristischen Personen, über die Daten bearbeitet werden.[38] Betroffene Personen haben verschiedene Rechte gegenüber den verantwortlichen Personen (siehe Ausführungen zu den Betroffenenrechten unter Ziff. 5.11 unten).

5.8.2. Betroffene Personen

[60] «*Als betroffene Personen*» gelten diejenigen Personen, deren Daten im Rahmen einer IoT-Anwendung erhoben werden. Denkbar sind z.B. Forschungsprojekte, bei welchen Gesundheitsdaten erhoben werden. Die Personen, deren Gesundheitsdaten erhoben und bearbeitet werden, gelten als betroffene Personen. Ebenso ist es denkbar, dass die Institution die Auslastung von Räumen messen möchte und zu diesem Zweck Standortdaten von Personen erheben und auswerten möchte. In diesem Fall gelten diejenigen Personen, deren Standortdaten untersucht werden, als betroffene Personen. Weiter gibt es Personen, welche den IoT-Service der Hochschulen für eigene Zwecke nutzen möchten (bspw. für die Reservation eines Sitzplatzes in einer Bibliothek) und hierfür eine Applikation auf ihren Geräten installieren. In diesem Fall gilt die Person, welche die Applikation auf ihrem Gerät installiert und deren Daten in der Folge bearbeitet werden, als betroffene Person.[39]

5.8.3. Hersteller der Sensoren

[61] Die Hersteller der Sensoren entscheiden zwar, welche Art von Daten in welcher Frequenz mit ihren Geräten gesammelt werden können und welche übrigen Funktionalitäten die Geräte haben sollen. Sie entscheiden aber nicht, für welche Zwecke die gesammelten Daten eingesetzt werden bzw. was mit den gesammelten Daten passieren soll. Vielmehr entscheidet i.d.R. der Betreiber des Sensors und / oder der Betreiber der dazugehörigen Applikation, was mit den gesammelten Daten geschehen soll resp. zu welchen Zwecken die Daten erhoben werden. Sensor-Hersteller sind also grundsätzlich nicht als «*Verantwortliche*» im Sinne der Datenschutzgesetzgebung zu qualifizieren.[40]

[62] Anders kann der Fall liegen, wenn sich ein Sensor-Hersteller den Zugang zu den Daten sichert. Zwar stellt der Zugang zu Daten keine begriffliche Voraussetzung eines «*Verantwortlichen*» dar[41]. Wenn sich ein Sensor-Hersteller aber den Zugang zu den Daten sichert, ist dies zumindest ein Indiz dafür, dass er ein eigenes Interesse an den Daten hat bzw. die Daten für seine eigenen Zwecke verwenden möchte. In solch einem Fall sind weitere Abklärungen zu tätigen und es kann nicht ausgeschlossen werden, dass der Hersteller des Sensors ebenfalls als «*Verantwortlicher*» im Sinne der Datenschutzgesetzgebung zu qualifizieren ist.[42] Falls es sich in diesem Fall beim Sensor-Hersteller um einen Institutions-Angehörigen oder einen Auftragnehmer der Hoch-

38 Vgl. auch Ausführungen unter Ziff. 5.4 oben: Die juristischen Personen sind gemäss dem geltenden DSG und IDG geschützt. Gemäss DSGVO und E-DSG werden nur natürliche Personen geschützt (vgl. Art. 4 Abs. 1 DSGVO; Art. 4 lit. a E-DSG).

39 Vgl. auch Art. 29 Arbeitsgruppe (FN 30), 13.

40 Kritischer indes Art. 29 Arbeitsgruppe (FN 30), 11, wonach «*device manufacturers*» grundsätzlich als «*data controllers*» gelten.

41 David Rosenthal, Controller oder Processor: Die Datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Ziff. 8.e.

42 Auch gem. Art. 29 Arbeitsgruppe (FN 30), 11, gelten «*device manufacturers*» als «*data controllers under EU law*».

schulen handelt, gilt als datenschutzrechtlich «*Verantwortlicher*» aber nicht der einzelne Sensor-Hersteller, sondern die Hochschule als übergeordnete Institution (siehe hierzu auch Ziff. 5.8.1 oben).

5.8.4. Betreiber der Sensoren

[63] Die Benutzer des Service LoRaWAN bzw. Betreiber der Sensoren, welche Sensoren für ihre Zwecke einkaufen, konfigurieren und aufstellen, entscheiden, wann, wo und für welche Zwecke die Sensoren zum Einsatz kommen. Sie haben die volle Kontrolle darüber, wann und wo ihre Sensoren die vorgesehenen Daten erfassen und sie entscheiden grundsätzlich auch, was mit den erfassten Daten passieren soll. Solange ein Sensor-Betreiber die Daten allerdings innerhalb seines Tätigkeitsbereichs und unter der möglichen Kontrolle seiner Institution erhebt und bearbeitet, gelten als datenschutzrechtlich «*Verantwortliche*» nicht die einzelnen Sensor-Inhaber, sondern die Hochschulen.[43] Dies trifft zumindest in denjenigen Fällen zu, wo die Hochschulen als Arbeitgeberin oder Auftraggeberin des Sensor-Betreibers ein eigenes Interesse an den Datenbearbeitungen hat, was im IoT-Projekt auf die meisten Fälle zutreffen dürfte. So werden Forschungsvorhaben grundsätzlich im öffentlichen Auftrag der Institution durchgeführt.

5.8.5. Hersteller der Gateways

[64] Die Hersteller der Gateways haben eine relativ geringe Entscheidungsbefugnis und -macht, was die Datenbearbeitungen ihrer Geräte angeht. Die Hersteller der Gateways haben keinen Einfluss darauf, welche Daten zu welchen Zwecken über ihre Gateways geschickt werden. Gateways sind relativ «dumm». Sie machen im Grunde nichts anderes, als empfangene Daten weiterzuleiten. Für andere Zwecke können Gateways kaum eingesetzt werden. Die Hersteller der Gateways haben auch nicht die Möglichkeit, auf die Daten bei den Gateways zuzugreifen und die Daten für eigene Zwecke zu verwenden. Die Gateway-Hersteller gelten damit nicht als «*Verantwortliche*». Mangels Auftrags, Daten für andere IoT-Stakeholder zu bearbeiten, handelt es sich bei den Gateway-Herstellern auch nicht um «*Auftragsbearbeiter*».

5.8.6. Betreiberinnen der Gateways

[65] Die Betreiberinnen der Gateways entscheiden zwar, wo welche Gateways aufgestellt werden und wann sie in Betrieb gesetzt werden. Sie haben aber keine Kontrolle darüber, welche Daten ihre Gateways empfangen. Die Betreiberinnen der Gateways sehen die unverschlüsselten Daten nicht und haben – jedenfalls im vorliegenden Fall – kein eigenes Interesse an den Daten. Die Gateway-Betreiberinnen entscheiden nicht, für welche Zwecke die Daten erhoben und verwendet werden, welche über ihre Gateways verschickt werden. Die Betreiberinnen der Gateways gelten damit nicht als «*Verantwortliche*». Sie sind auch keine «*Auftragsbearbeiter*».

43 Vgl. dazu Ausführungen in DSGVO Komm-Hartung, Art. 4 Nr. 9 N 6 f.; DSGVO Komm-Gola, Art. 4 N 48; DSGVO Komm-Sydow-Raschauer, Art. 4 N 125.

5.8.7. Betreiber der Network Server

[66] Der Betreiber der Network Server hat relativ eingeschränkte Möglichkeiten, auf die Datenverarbeitungen in dem IoT-Projekt der Hochschulen Einfluss zu nehmen. Wie unter Ziff. 3.4 oben ausgeführt, sieht der Betreiber der Network-Server den Inhalt der Messdaten nicht. Er verwendet die anfallenden Daten nicht für seine eigenen Zwecke. Der Betreiber der Network-Server ist vielmehr den Weisungen seines Auftraggebers (Hochschulen) unterstellt. Er hat von den Hochschulen den Auftrag, Datenpakete von registrierten Sensoren an die Application Server weiterzuleiten und Datenpakete von nicht registrierten Sensoren zu verwerfen. Zudem hat er den Auftrag, die verschlüsselten Messdaten auf seiner Cloud-Infrastruktur (zumindest zwischen-) zu speichern. Der Betreiber der Network Server entscheidet nicht selber, für welche Zwecke die Daten erhoben und verwendet werden. Er ist folglich weder «*Verantwortlicher*» noch «*Auftragsbearbeiter*».

5.8.8. Betreiberin der Application Server

[67] Die Betreiberin der Application Server hat den Auftrag, die entschlüsselten Daten an die richtige Applikation zu senden. Sie entscheidet nicht, welche Daten bei ihr eingehen und von ihr bearbeitet werden. Auch wenn die Betreiberin der Application Server den Inhalt der Messdaten sieht, so fehlt ihr die Kompetenz, darüber zu entscheiden, für welche Zwecke die Daten erhoben werden und was mit den empfangenen Daten passieren soll. Sie darf die empfangenen Daten nicht für eigene Zwecke verwenden. Die Betreiberin der Application Server ist damit keine «*Verantwortliche*». Da sie den Weisungen der Hochschule unterworfen ist und die Daten in deren Auftrag bearbeitet, ist sie allenfalls als «*Auftragsbearbeiterin*» zu qualifizieren».

5.8.9. Betreiber der Applikationen

[68] Die Betreiber der Applikationen können identisch sein mit den Betreibern der Sensoren, das ist aber nicht zwingend. Ein Student bspw., welcher eine Applikation auf einem seiner Geräte installiert, um auf einen bestimmten Service zuzugreifen (z.B. Reservation einen Sitzplatzes in einer Bibliothek), gilt als «betroffene Person» (vgl. Ziff. 5.8.2 oben). Der Student ist in diesem Fall nicht Inhaber des zugehörigen Sensors. Anders liegt der Fall, wenn bspw. ein Forscher Gesundheitsdaten messen möchte und zu diesem Zweck einen Sensor einkauft sowie eine dazu passende Software (Applikation) erwirbt, welche die vom Sensor gemessenen Daten auswerten kann. In diesem Fall gilt das, was oben für den Betreiber eines Sensors aufgeführt wurde: Der Betreiber der Applikation hat hier die volle Kontrolle darüber, wann und wo seine Sensoren die vorgesehenen Daten erfassen und entscheidet – im Rahmen der Möglichkeiten, welche der Softwarehersteller der Applikation vorgegeben hat – auf welche Art und Weise, in welchem Umfang und zu welchen Zwecken die Messdaten verwendet werden. Der Betreiber der Applikation sieht die unverschlüsselten Messdaten und zieht den direkten Nutzen aus ihnen. Er verwendet die Daten für seine eigenen Zwecke bzw. diejenigen seiner Institution. Der Inhaber der Applikation bzw. die Hochschulen gelten in diesem Fall als datenschutzrechtlich «*Verantwortliche*» (siehe hierzu auch Ziff. 5.8.4 oben).

5.8.10. Hersteller der Software einer Applikation

[69] Hersteller der Software einer Applikation kann ein externer Dritter sein, welcher im Auftrag der Hochschulen eine Software entwickelt, die für eine bestimmte Anwendung im IoT-Projekt eingesetzt wird. Es ist aber auch denkbar, dass ein Forscher selber eine Software programmiert, welche er für seine IoT-Anwendung benötigt.

[70] Falls es sich beim Software-Hersteller um eine externe Person handelt, kommt es für die Qualifikation darauf an, ob er die Daten für seine eigenen Zwecke verwendet.[44] Die Sicherstellung des Zugangs zu den Messdaten wäre ein Indiz hierfür, zwingend nötig ist das aber nicht. Falls der Software-Hersteller die Daten für seine eigenen Zwecke verwendet, ist er als «*Verantwortlicher*» zu qualifizieren.[45]

[71] Falls es sich beim Software-Hersteller nicht um eine externe Person handelt, sondern um einen Forscher, welcher bei der Hochschulen angestellt ist, und falls der Forscher im Rahmen seines Tätigkeitsbereichs und unter der theoretischen Kontrolle der Institution über die Zwecke und die Mittel der Datenverarbeitungen entscheidet, die mit der Software vorgenommen werden sollen, so gelten die Hochschulen als datenschutzrechtlich «*Verantwortliche*».

5.9. Rechtsgrundlage für die Verarbeitung

[72] Unter dem DSG und dem IDG dürfen Hochschulen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht.[46] Die DSGVO sieht nebst der gesetzlichen Grundlage bzw. «*rechtlichen Verpflichtung*»[47] zwar noch andere Tatbestände vor, welche eine Datenverarbeitung erlauben (Einwilligung, Erforderlichkeit für die Erfüllung eines Vertrages, überwiegendes Interesse etc.); dies ändert aber nichts daran, dass sich staatliches Handeln grundsätzlich auf eine gesetzliche Grundlage stützen muss. Die Hochschulen benötigen also eine gesetzliche Grundlage, wenn sie Personendaten bearbeiten. Ob eine hinreichende gesetzliche Grundlage vorliegt, muss im Einzelfall geprüft werden. Dazu muss für jede Datenverarbeitung, also insbesondere für jede Anwendung (Applikation) im IoT-Projekt, gesondert geprüft werden, ob Personendaten oder sogar besonders schützenswerte Personendaten bearbeitet werden.

[73] Soweit im Einzelfall, z.B. im Rahmen einer bestimmten IoT-Anwendung, besonders schützenswerte Personendaten oder Persönlichkeitsprofile betroffen sind – was vorliegend nicht ausgeschlossen werden kann (siehe hierzu Ziff. 5.7 oben) – bedarf es wie unter Ziff. 5.7 oben ausgeführt eines Gesetzes im formellen Sinn.

[74] Dabei ist nicht für jede einzelne Datenbearbeitung eine explizite Rechtsgrundlage erforderlich; die Aufgabenumschreibung im Gesetz muss aber klar sein und für die betroffenen Personen die notwendige Transparenz schaffen.[48] Die gesetzlich umschriebenen Aufgaben der Hoch-

---

44 Vgl. dazu auch Art. 29 Arbeitsgruppe (FN 30), 12 f., wonach «*other third parties*» als «*data controllers*» gelten, wenn sie Daten, welche von IoT-Geräten generiert werden, für eigene Zwecke verwenden – auch wenn sie keine Kontrolle darüber haben, welche Daten von den verschiedenen IoT-Geräten gesammelt und verarbeitet werden.

45 Vgl. dazu auch Art. 29 Arbeitsgruppe (FN 30), 12, welche die «*third party application developers*» als «*controller*» qualifizieren, soweit sie die von IoT-Geräten generierten Daten für eigens definierte Zwecke erheben und speichern.

46 Art. 17 Abs. 1 DSG; § 8 Abs. 1 IDG.

47 Vgl. Art. 6 Abs. 1 lit. c DSGVO.

48 PK-Baeriswyl, § 8 N 3 f.

schulen befinden sich in Gesetzen, Verordnungen, Reglementen, Studien- oder Fachhochschulordnungen oder Weisungen.[49] Was den blossen Betrieb des Services LoRaWAN – losgelöst vom konkreten IoT-Anwendungsfall – angeht, so kann davon ausgegangen werden, dass sich dieser wohl für die meisten Hochschulen unter die bestehenden gesetzlichen Grundlagen subsumieren lässt. So sehen verschiedene Hochschulgesetze vor, dass die Hochschulen für die langfristige Qualitätssicherung von Lehre, Forschung und Dienstleistung verantwortlich sind. Zudem steht in verschiedenen Hochschulgesetzen, dass die Hochschule zur Erfüllung ihrer gesetzlichen Aufgaben Personendaten und auch besonders schützenswerte Personendaten bearbeiten darf. Auch finden sich teilweise gesetzliche Bestimmungen, wonach die Hochschulen im Rahmen von Forschungsprojekten Personendaten, einschliesslich besonders schützenswerter Personendaten sowie Persönlichkeitsprofilen bearbeiten dürfen, soweit dies für das entsprechende Forschungsprojekt erforderlich ist.

[75] Es kann mit guten Gründen argumentiert werden, dass eine moderne Infrastruktur und die Verwendung und Förderung neuer Technologien wie LoRaWAN als Massnahmen für eine langfristige Qualitätssicherung der Lehre und Forschung an den Hochschulen notwendig sind. Es sollte aber zusätzlich für jeden einzelnen IoT-Anwendungsfall geprüft werden, ob sich die konkrete Datenverarbeitung ebenfalls unter die bestehenden gesetzlichen Grundlagen der Institution subsumieren lässt.

5.10. Bearbeitungsgrundsätze

5.10.1. Allgemeines

[76] Personenbezogene Daten müssen auf rechtmässige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden («Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz»).[50] Personendaten dürfen ferner nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist («Zweckbindung»).[51] Personendaten müssen zudem verhältnismässig bearbeitet werden, d.h. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Mass beschränkt («Datenminimierung»).[52] Weiter müssen Personendaten sachlich richtig und erforderlichenfalls auf dem neusten Stand sein, wobei alle angemessenen Massnahmen zu treffen sind, damit personenbezogene Daten, die unrichtig sind, unverzüglich gelöscht oder berichtigt werden («Richtigkeit»).[53] Personendaten müssen sodann grundsätzlich in einer Form gespeichert werden, welche die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich

49 Vgl. z.B. im Kanton Zürich das Universitätsgesetz (UniG) vom 15. März 1998 (LS 415.11), das Gesetz über die Pädagogische Hochschule vom 25. Oktober 1999 (LS 414.41), das Fachhochschulgesetz vom 2. April 2007 (LS 414.10), die allgemeine Studienordnung der Zürcher Hochschule der Künste vom 18. Dezember 2007 (LS 414.262), die Hochschulordnung der Zürcher Hochschule für Angewandte Wissenschaften vom 25. Januar 2008 (LS 414.251) und die Verordnung über Datenbearbeitung im Bildungsbereich (Bildungsdatenverordnung) vom 21. Juli 1999 (LS 410.7).

50 Art. 5 Abs. 1 lit. a DSGVO; Art. 4 Abs. 1, 2 und 4 DSG; §§ 4 und 12 IDG.

51 Art. 5 Abs. 1 lit. b DSGVO; Art. 4 Abs. 3 DSG; ähnlich § 9 IDG.

52 Art. 5 Abs. 1 lit. c DSGVO; vgl. auch Art. 4 Abs. 2 DSG und § 11 Abs. 1 und 2 IDG.

53 Art. 5 Abs. 1 lit. d DSGVO; ähnlich Art. 5 DSG und § 7 Abs. 2 lit. b IDG.

ist («Speicherbegrenzung»).[54] Schliesslich müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden («Datensicherheit», «Integrität und Vertraulichkeit»).[55]

[77] Nachfolgend werden die wichtigsten Pflichten im Kontext des IoT-Projekts weiter untersucht und konkrete Lösungsvorschläge dazu gemacht, wie diese Pflichten umgesetzt werden könnten.

5.10.2. Treu und Glauben, Transparenz

[78] Die Grundsätze von Treu und Glauben und der Transparenz[56] verlangen, dass Personendaten niemals gesammelt und bearbeitet werden sollen, ohne dass die betroffene Person davon Kenntnis hat.[57] Dieses Erfordernis erlangt im IoT-Kontext eine besondere Bedeutung, da Sensoren häufig unauffällig oder sogar unsichtbar sind. IoT-Stakeholders, welche als «*Verantwortliche*» gelten, sollten aufgrund des Transparenzprinzips die betroffenen Personen in der geographischen oder digitalen Nähe von Sensoren und Gateways darüber informieren, dass Daten über sie oder ihr Umfeld erfasst werden.[58] Zudem sollten die Hochschulen aufgrund ihrer umfassenden Informationspflichten z.B. auf ihrer Webseite an einem leicht zugänglichen Ort Informationen zum IoT-Projekt und den einzelnen Anwendungsfällen aufschalten – hierauf wird unter Ziff. 5.11.2 unten näher eingegangen.

5.10.3. Zweckbindung

[79] Der Zweckbindungsgrundsatz[59] verlangt, dass Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Zwecke, zu denen die Erhebung und die beabsichtigte Verarbeitung erfolgen sollen, müssen schon zum Zeitpunkt der Datenerhebung festgelegt sein.[60] Eine Zweckänderung[61] ist nur zulässig, wenn kumulativ zwei Voraussetzungen erfüllt sind: Die Weiterverarbeitung zu dem neuen Zweck darf nicht mit dem bei der Datenerhebung festgelegten Zweck unvereinbar sein (Erfordernis der Zweckvereinbarkeit) und für die Weiterverarbeitung zu dem neuen Zweck muss eine ausreichende Rechtsgrundlage vorhanden sein. Das zweite Kriterium bedeutet bspw., dass, wenn die Verarbeitung auf einer Einwilligung beruht, vor einer Zweckänderung diese neu eingeholt werden muss.[62]

[80] Art. 5 Abs. 1 lit. b DSGVO regelt nicht, in welcher Form die Zweckfestlegung erfolgen muss. Da der «*Verantwortliche*» aber gemäss Art. 5 Abs. 2 DSGVO die Einhaltung von Art. 5 Abs. 1 DSGVO und damit auch die Einhaltung des Zweckbindungsgrundsatzes nachweisen können

54 Art. 5 Abs. 1 lit. e DSGVO.

55 Art. 7 DSG; ähnlich Art. 5 Abs. 1 lit. f DSGVO und § 7 Abs. 2 lit. a IDG.

56 Art. 5 Abs. 1 lit. a DSGVO; Art. 4 Abs. 1, 2 und 4 DSG; §§ 4 und 12 IDG.

57 Art. 29 Arbeitsgruppe (FN 30), 16 f.

58 Art. 29 Arbeitsgruppe (FN 30), 16 f.

59 Art. 5 Abs. 1 lit. b DSGVO; Art. 4 Abs. 3 DSG; ähnlich § 9 Abs. 1 IDG.

60 DSGVO Komm-Herbst, Art. 5 N 31.

61 Die DSGVO spricht in Art. 5 Abs. 1 lit. b von «*Weiterverarbeitung*».

62 Vgl. DSGVO Komm-Herbst, Art. 5 N 49.

muss, empfiehlt sich die Dokumentation der Verarbeitungszwecke in Schriftform.[63] Die Mitteilung der Verarbeitungszwecke an die betroffene Person gem. Art. 13 Abs. 1 lit. c oder Art. 14 Abs. 1 lit. c DSGVO (siehe hierzu Ziff. 5.11.2 unten) kann zugleich die nach Art. 5 Abs. 1 lit. b DSGVO erforderliche Zweckfestlegung darstellen.

[81] Im Kontext des IoT-Projekts bedeutet der Zweckbindungsgrundsatz, dass sich alle «*Verantwortlichen*» vorgängig (d.h. bevor Daten erhoben werden) überlegen müssen und schriftlich festhalten sollten, zu welchen Zwecken die Daten erhoben werden sollen und dass die anfallenden Daten dann auch nur für diese Zwecke verwendet werden

5.10.4. Datensparsamkeit

[82] Nach Art. 5 Abs. 1 lit. c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Mass beschränkt sein.[64] Im Rahmen des IoT-Projekts bedeutet dies, dass Daten, welche für den Betrieb eines bestimmten Dienstes nicht nötig sind, entweder gar nicht erst erhoben werden sollten oder – wenn das nicht möglich ist – dass unnötige Daten so rasch wie möglich wieder gelöscht werden. Es ist nicht zulässig, Daten, welche für den vorgesehenen Zweck unnötig sind, aufzubewahren für den Fall, dass sie später einmal nützlich sein könnten.[65] So ist es beispielsweise ganz im Sinne des Grundsatzes der Datensparsamkeit, dass Datenpakete von nicht registrierten Sensoren von den Network Servern im Backend verworfen werden, ohne dass eine Kopie dieser Daten behalten wird.

[83] Wenn eine Löschung von unnötigen Daten nicht möglich ist, sollten die entsprechenden Daten anonymisiert oder, wenn auch das nicht möglich ist, zumindest der Zugriff darauf so weit wie möglich beschränkt werden.

5.10.5. Speicherbegrenzung

[84] Nach Art. 5 Abs. 1 lit. e DSGVO darf bei der Speicherung personenbezogener Daten die Identifizierung der betroffenen Personen nur so lange möglich sein, wie es für die Verarbeitungszwecke erforderlich ist. Mit diesem Grundsatz der Speicherbegrenzung wird eine zeitliche Grenze der Verarbeitung personenbezogener Daten festgelegt: Die Speicherung personenbezogener Daten muss beendet werden, sobald sie für die Zwecke der Verarbeitung nicht mehr erforderlich ist.

[85] Für die Hochschulen bedeutet dies Folgendes: Zunächst sollten die verschiedenen IoT-Stakeholder der Institutionen sicherstellen, dass sie Daten löschen, sobald sie für den vorgesehenen Zweck nicht mehr benötigt werden. Zudem gilt für die Betreiberinnen der Application Server, welche die Datenpakte entschlüsseln, dass sie Daten dann, wenn sie für den vorgesehenen Zweck, also die Weiterleitung an die richtige Applikation, nicht mehr benötigt werden, löschen müssen, ohne eine Kopie davon zu behalten. Weiter gilt auch für die Betreiber / Inhaber von Applikationen, dass sie die Daten löschen müssen – und zwar grundsätzlich sowohl die originalen

63 Art. 29 Arbeitsgruppe (FN 30), 18.

64 Vgl. auch Art. 4 Abs. 2 DSG und § 11 Abs. 1 und 2 IDG.

65 Art. 29 Arbeitsgruppe (FN 30), 16 f.

Messdaten als auch die Auswertungsergebnisse – wenn diese Daten für die vorgesehen Zwecke (also bspw. ein bestimmtes Forschungsprojekt) nicht mehr benötigt werden.

5.11. Betroffenenrechte

5.11.1. Allgemeines

[86] Unter der DSGVO, aber auch unter dem DSG, dem E-DSG und dem IDG haben die betroffenen Personen weitgehende Rechte. Zu den Rechten der betroffenen Personen gehören das Recht auf eine transparente Information durch den «*Verantwortlichen*»,[66] auf Auskunft,[67] auf Berichtigung unrichtiger Personendaten,[68] auf Löschung von personenbezogenen Daten («Recht auf Vergessenwerden»),[69] auf Einschränkung der Verarbeitung,[70] auf Datenübertragbarkeit[71] sowie das Widerspruchsrecht.[72] Auf die im IoT-Projekt wichtigsten Betroffenenrechte wird nachfolgend eingegangen.

5.11.2. Recht auf eine transparente Information und Kommunikation

[87] Einen datenschutzrechtlich «*Verantwortlichen*» treffen umfangreiche Informationspflichten.[73] Gemäss Art. 13 Abs. 1 DSGVO[74] muss der «*Verantwortliche*» den betroffenen Personen zum Zeitpunkt der Erhebung der Daten diverse Informationen mitteilen, wie beispielsweise der Zweck, für welchen die Daten bearbeitet werden.

[88] Diese Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden.[75] Art. 12 Abs. 1 Satz 2 DSGVO schreibt dabei keine bestimmte Form vor. Die Informationen können bspw. in elektronischer Form, z.B. per E-Mail bereitgestellt werden.[76] Auch eine Bereitstellung der Informationen über eine Webseite kommt in Frage, wenn die Webseite für die Öffentlichkeit bestimmt ist.[77] Der Abruf der Informationen muss dabei ohne Zugangshindernisse oder Beschränkungen (z.B. Passwort) erfolgen.[78]

[89] Was das IoT-Projekt angeht, so steht es der Hochschulen grundsätzlich frei, auf welche Art und Weise sie die betroffenen Personen informieren wollen. Die verschiedenen Kategorien von betroffenen Personen können auch über unterschiedliche Kanäle informiert werden. Zu beachten

66 Art. 12 ff. DSGVO; Art. 18a Abs. 2 DSG; § 14 IDG.

67 Art. 15 DSGVO; Art. 8 DSG; § 20 IDG.

68 Art. 16 DSGVO; Art. 5 Abs. 2 DSG; § 21 lit. a IDG.

69 Art. 17 DSGVO; das Löschungsrecht ergibt sich auch unter dem DSG implizit aus dem Verhältnismässigkeitsgrundsatz von Art. 4 Abs. 2 DSG und unter dem IDG aus § 11 Abs. 2 IDG.

70 Art. 18 DSGVO; unter dem DSG ableitbar aus dem Verhältnismässigkeitsgrundsatz von Art. 4 Abs. 2 DSG.

71 Art. 20 DSGVO.

72 Art. 21 DSGVO.

73 Art. 12 ff. DSGVO; Art. 18a DSG; § 14 IDG.

74 Etwas weniger umfangreich aber grundsätzlich ähnlich Art. 18a Abs. 2 DSG; relativ rudimentär § 14 IDG.

75 Art. 12 Abs. 1 DSGVO.

76 DSGVO Komm-Sydrow / Greve, Art. 12 N 16.

77 DSGVO, E. 58.

78 DSGVO Komm-Sydrow / Greve, Art. 12 N 18.

ist dabei, dass das Zurverfügungstellen einer generellen Datenschutzerklärung mit allgemeinen Informationen über das IoT-Projekt nicht ausreichend ist, sondern, dass die Betroffenen jeweils in Bezug auf jeden IoT-Anwendungsfall, welcher sie betrifft, informiert werden müssen.

[90] Zur Umsetzung dieser Informationspflichten ist es beispielsweise denkbar, dass die Hochschulen auf ihrer Webseite an einem gut zugänglichen Ort präzise, transparente und verständliche Informationen zum IoT-Projekt und zu den einzelnen Anwendungsfällen aufschalten. Zusätzlich kann denjenigen Betroffenen, welche Applikationen auf ihren Geräten installieren, um auf einen bestimmten Service zuzugreifen, im Rahmen des Installations- bzw. Registrationsprozesses eine Datenschutzerklärung zur Kenntnis gebracht werden. Weiter können Informationsschilder in der Nähe von Sensoren und Gateways aufgestellt werden mit Hinweisen mit weiteren Informationen zum Service LoRaWAN resp. den einzelnen Anwendungsfällen; dies wird aus Transparenzgründen ohnehin empfohlen (siehe Ziff. 5.10.2 oben).

5.12. Weitere ausgewählte Pflichten

5.12.1. Privacy by design

[91] Der Grundsatz von «privacy by design» («Datenschutz durch Technikgestaltung»), welcher in Art. 25 Abs. 1 DSGVO erwähnt wird, bezweckt, dass der Datenschutz zu einem möglichst frühen Zeitpunkt bei der Auswahl, Festlegung und Einrichtung der Systeme für eine Datenverarbeitung berücksichtigt wird.[79] Dies bedeutet, dass bereits bei der Programmierung, Architektur und Konzeption von Systemen und Programmen und beim Einkauf entsprechender Systeme und Leistungen von Dritten die entsprechenden datenschutzfreundlichen Aspekte zu berücksichtigen sind und der Datenschutz in die Technik einzubinden ist.[80]

[92] Die Pflicht des «*Verantwortlichen*» aus Art. 25 Abs. 1 DSGVO ist es, frühzeitig angemessene technische und organisatorische Massnahmen («**TOMs**») zu treffen. Insofern handelt es sich um die gleichen technisch-organisatorischen Massnahmen, die der «*Verantwortliche*» bereits nach Art. 24 sowie Art. 32 DSGVO (Datensicherheit)[81] zu treffen hat. Als konkrete Beispiele für TOMs nennt Art. 25 Abs. 1 DSGVO lediglich die Pseudonymisierung. Da aber wie ausgeführt ein enger Zusammenhang zu Art. 24 und 32 DSGVO besteht, sind auch die dort genannten Beispiele wie etwa Verschlüsselung, Zugangs- und Zutrittskontrollen zu nennen. Auch ohne spezielle Erwähnung ist die Anonymisierung von Daten eine geeignete Methode.[82]

[93] Für das IoT-Projekt bedeutet der Grundsatz, dass alle IoT-Stakeholder versuchen müssen, die datenschutzrechtlichen Grundsätze bereits frühzeitig in ihren Geräten und Prozessen zu integrieren. Z.B. sollten die Sensoren und Gateways so konfiguriert werden, dass sie nicht mehr Daten erfassen als nötig oder dass sie unnötige Daten automatisch löschen. Zudem sollten die involvierten Geräte und Server (also auch die Network Server, Application Server und weitere Server, auf welchen Rohdaten und bearbeitete IoT-Daten liegen) so konfiguriert werden, dass unnötige Daten automatisch gelöscht werden oder zumindest möglichst einfach manuell gelöscht

79 DSGVO Komm-Hartung, Art. 25 N 11.

80 DSGVO Komm-Hartung, Art. 25 N 11 m.w.H.

81 Vgl. auch Art. 7 Abs. 1; § 7 IDG.

82 DSGVO Komm-Hartung, Art. 25 N 16.

werden können. Zudem muss der physische und elektronische Zugriff auf die Geräte so weit wie möglich eingeschränkt werden.

5.12.2. Privacy by default

[94] Der Grundsatz von «privacy by default» («Datenschutz durch datenschutzfreundliche Voreinstellungen») bedeutet, dass ein Produkt oder eine Dienstleistung für den Nutzer ohne weiteres Zutun beim ersten Einschalten bzw. ersten Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten aufweisen soll.[83] Umgekehrt bedeutet dies, dass alle Massnahmen, welche zu weniger Datenschutz und mehr Datenbearbeitungen führen, vom Nutzer einzuschalten und zu aktivieren sind.[84] Damit sollen insbesondere die Nutzer geschützt werden, die weniger technikaffin sind und z.B. deswegen nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen.

[95] Konkret verlangt Art. 25 Abs. 2 DSGVO, dass der «*Verantwortliche*» geeignete TOMs trifft, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

[96] Für das IoT-Projekt bedeutet der Grundsatz, dass die Applikationen, welche die Betroffenen auf ihren Geräten installieren, standardmässig datenschutzfreundlich eingestellt sein müssen. Für die Sensoren und Gateways gilt das Gleiche: Auch sie müssen so konfiguriert werden, dass sie standardmässig datenschutzfreundliche Voreinstellungen aufweisen.

5.12.3. Datenschutzfolgenabschätzung

[97] Gemäss Art. 35 Abs. 1 DSGVO muss der «*Verantwortliche*» vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

[98] Was das IoT-Projekt angeht, so ist für jeden IoT-Anwendungsfall gesondert zu prüfen, ob eine Datenschutzfolgenabschätzung vorgenommen werden muss. Dem Service LoRaWAN liegt eine relativ neue Technologie zugrunde. Dies allein dürfte aber noch nicht ausreichen, damit von einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen ausgegangen werden muss. Die Notwendigkeit zur Durchführung einer Folgenabschätzung besteht aber allenfalls dort, wo im Rahmen einer bestimmten IoT-Anwendung besonders schützenswerte Personendaten untersucht werden (z.B. Gesundheitsdaten).[85] Bei einer Erhebung von Daten von Heizanlagen oder bei einer Überwachung von Pflanzen auf dem freien Feld werden dagegen

83 DSGVO Komm-Hartung, Art. 25 N 24.

84 DSGVO Komm-Hartung, Art. 25 N 24.

85 Auch Art. 29 Arbeitsgruppe, Drei Guidelines zur DSGVO vom 8. Januar 2017, 10, hält folgendes fest: «*For example, certain «Internet of Things» applications could have a significant impact on individuals» daily lives and privacy and therefore require a DPIA.*» Die Art. 29 Arbeitsgruppe empfiehlt auch, wo angezeigt, die Folgenabschätzung zu veröffentlichen; vgl. Art. 29 Arbeitsgruppe (FN 30), 21.

keine besonders schützenswerten Personendaten bearbeitet, weshalb sich in solchen eine Datenschutzfolgenabschätzung erübrigt.

5.13. Fazit

[99] Aus datenschutzrechtlicher Sicht steht der Einführung eines Services LoRaWAN grundsätzlich nichts entgegen. Zu beachten ist aber, dass die Hochschulen Personendaten nur bearbeiten dürfen, wenn dafür eine hinreichende gesetzliche Grundlage besteht, wobei für die Bearbeitung von besonders schützenswerten Personendaten ein Gesetz im formellen Sinn erforderlich ist. Es ist für jede IoT-Anwendung separat zu prüfen, ob Personendaten oder sogar besonders schützenswerte Personendaten bearbeitet werden und ob sich die entsprechenden Datenbearbeitungen unter die bestehenden gesetzlichen Grundlagen subsumieren lassen oder ob eine neue gesetzliche Grundlage geschaffen werden muss.

[100] Die Hochschulen treffen als datenschutzrechtlich «*Verantwortliche*» verschiedene datenschutzrechtliche Pflichten. Insbesondere müssen sie die betroffenen Personen hinreichend über den Service LoRaWAN und die einzelnen IoT-Anwendungsfälle informieren und die Wahrung der übrigen Betroffenenrechte (wie das Recht auf Auskunft, Berichtigung oder Datenübertragbarkeit) sicherstellen. Zudem müssen sie eine Datenschutzfolgenabschätzung vornehmen, wenn im Rahmen einer bestimmten IoT-Anwendung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen besteht.

6. Datensicherheit

[101] Mögliche Bedrohungen aus dem Internet der Dinge für die Sicherheit und Privatsphäre sind unbestritten. Gemäss Schätzungen geht man bis 2020 von gegen 21 Milliarden vernetzten IoT-Geräten aus, wodurch die Sicherheitsrisiken kontinuierlich steigen werden.[86] Es ist insofern unabdingbar, in einem IoT-Netzwerksystem Massnahmen für die Datensicherheit zu treffen. Die gesetzlich verankerte Daten- und Informationssicherheit verpflichtet Bearbeiter von Personen- und teilweise auch Sachdaten denn auch, diese durch angemessene technische und organisatorische Massnahmen zu schützen.[87] Dabei ist kein absoluter Schutz erforderlich und als Faustregel gilt: Je vertraulicher und schützenswerter die Daten, umso höher das Mass an gebotener Sorgfalt.[88]

[102] In einer LoRaWAN-Netzwerkinfrastruktur sind die häufig mit schlechten Sicherheitsstandards ausgestatteten IoT-Geräte, die Übermittlung der Daten über teilweise ungesicherte Netzwerke (insb. durch Funk) sowie die generellen Angriffsmöglichkeiten durch unberechtigte Dritte (z.B. durch IoT-Botnets[89]) in der digitalen Welt zu nennen. Die Risiken für die Datensicher-

86 Mark Hung, Leading the IoT, Gartner Insights on How to Lead in a Connected World, 2017, abrufbar unter: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (Stand: 21. Oktober 2019).

87 Art. 7 Abs. 1 DSG, § 7 Abs. 1 IDG, Art. 5 Abs. 1 lit. f und Art. 32 DSGVO sowie Art. 7 Abs. 1 E-DSG.

88 SHK DSG-Baeriswyl, Art.7 N 23.

89 Ein prominentes Beispiel war IoT-Botnet «Mirai», der 2016 durch eine DDoS-Attacke Webseiten wie Twitter, The Guardian oder Netflix unerreichbar machte; vgl. dazu Nicky Woolf, DDoS attack that disrupted internet was largest of its kind in history, experts say, The Guardian vom 26. Oktober 2016, abrufbar unter: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet (Stand: 13. Oktober 2019).

heit werden in den eingangs erwähnten potentiellen IoT-Anwendungsfällen der Hochschulen als nicht sehr hoch eingestuft, da es sich um nicht sehr sensitive Daten handelt. Für die bleibenden Sicherheitsrisiken, die sich je nach zukünftigem Einsatz des LoRaWAN-Dienstes auch verstärken können, sind gewisse technische und organisatorische Massnahmen zwecks Datensicherheit aber erforderlich. Mit den beim LoRaWAN-Protokoll bereits implementierten Sicherheitsmassnahmen, wie der verschlüsselten Datenübertragung zwischen Sensor und Application Server oder der Validierung der Datenpakete, besteht ein gewisser Schutz.[90] Weiter verfügen Hochschulen häufig über ein Information and Security Management System (ISMS), dessen Massnahmen auf IoT-Projekte adaptiert werden können. Als zusätzliche Massnahmen können Anwender von IoT-Systemen Geräte von im Bereich IoT/Datensicherheit zertifizierten Anbieter wählen[91] oder sich bei der Implementierung von Sicherheitsmassnahmen an Best Practices und unverbindlichen Standards orientieren.[92]

7. Weitere relevante Rechtsgebiete

[103] In einer IoT-Netzwerkinfrastruktur werden neben dem Datenschutz- und Fernmelderecht diverse weitere Rechtsgebiete tangiert. So sind beim Betrieb oder der Nutzung eines LoRaWAN-Systems verschiedene Konstellationen denkbar, in welchen es z.B. durch Fehlfunktion von Software und IoT-Geräten oder durch Datendiebstahl zu einem Schaden und damit zu **Haftungsfragen** kommen kann. Nebst den gewöhnlichen Bestimmungen zum vertraglichen- und ausservertraglichen Haftungsrecht[93] ist im Falle von fehlerhaften Produkten – z.B. aufgrund Sicherheitslücken bei Applikationen oder Geräten – auch das Produkthaftpflichtgesetz zu berücksichtigen. Unter dem Titel des **geistigen Eigentums** stellt sich sodann die Frage, wer in einer IoT-Netzwerkinfrastruktur welche Nutzungsrechte an welchen Daten hat bzw. wie man sich diese Rechte zusichern kann (Stichwort Daten als «Ol des 21. Jahrhunderts»). Da es de lege lata kein Dateneigentum gibt und die im eingangs umschriebenen Sachverhalt generierten IoT-Daten wohl keinen Schutz unter dem Immaterialgüterrecht geniessen (z.B. als Werk oder Erfindung), ist den Hochschulen empfohlen, sich die notwendigen Nutzungsrechte an den Daten vertraglich vorzubehalten. Zudem stellen sich den Hochschulen im Rahmen des LoRaWAN-Projekts auch bei der Vertragsgestaltung einige weitere Herausforderungen; einerseits aufgrund der Vielzahl von involvierten Parteien und andererseits, da die traditionellen vertragsrechtlichen Prinzipien nicht durchgehend sinnvoll angewendet werden können.

90 The Things Network, LoRaWAN Security, abrufbar unter: https://www.thethingsnetwork.org/docs/lorawan/security.html (Stand: 21. Oktober 2019).

91 Z.B. hat die *International Standard Organization* (ISO) 2018 eine Norm veröffentlicht, welche die Sicherheit von Systemen spezifisch im Internet der Dinge gewährleisten soll; vgl. https://www.iso.org/standard/65695.html (Stand: 21. Oktober 2019).

92 Verbindliche Regulierungen bestehen bis dato nicht; vgl. aber bspw. die *European Union Agency for Network and Information Security* (ENISA), die einen Bericht zu Good Practices für das Internet der Dinge und intelligente Infrastrukturen erstellt hat: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool (Stand: 13. Oktober 2019).

93 Nebst den Haftungsregeln nach Art. 41 OR (unerlaubte Handlung), Art. 55 OR (Geschäftsherrenhaftung), Art. 55 ZGB (Organhaftung) sowie den vertraglichen Haftungsbestimmungen (insbes. Art. 97 ff. OR) ist bei Hochschulen auch die Staatshaftung zu beachten.

8. Fazit

[104] Der Beitrag gelangt zum Ergebnis, dass der Einführung eines Service LoRaWAN aus datenschutz- und fernmelderechtlicher Sicht nichts Grundsätzliches entgegensteht, soweit die Hochschulen gewisse Vorkehrungen treffen und wo nötig die Voraussetzungen hierfür schaffen. Im Bereich des **Fernmelderechts** handelt es sich bei den Betreiberinnen der Gateways nicht um FDA und auch nicht um AAKD oder um «Personen, die Dritten ihren Zugang zu einem öffentlichen Fernmeldenetz zur Verfügung stellen» i.S. der Fernmelde- und Überwachungsgesetzgebung. In Frage kommt lediglich eine Qualifikation als «Betreiberinnen eines internen Fernmeldenetzes». In diesem Fall unterliegen die Hochschulen aber nur passiven Pflichten wie insbesondere der Pflicht zur Lieferung der ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs auf Verlangen, zur Duldung der Überwachung und Gewährung unverzüglichen Zugangs zu den Anlagen sowie zur Erteilung der für die Überwachung notwendigen Auskünfte. Die Betreiber von Sensoren und Applikationen gelten weder als FDA noch als AAKD und fallen auch in keine andere Kategorie von Mitwirkungspflichtigen.

[105] Aus **datenschutzrechtlicher Sicht** handelt es sich bei den Daten, welche im Rahmen des IoT-Projekts bearbeitet werden, je nach Anwendung um Sachdaten, Personendaten oder sogar besonders schützenswerte Personendaten. Als datenschutzrechtlich verantwortliche Personen gelten die Betreiberinnen der Sensoren und Applikationen. Sofern es sich bei diesen Personen um Angestellte einer Institution handelt, gilt dabei nicht die einzelne handelnde Person, sondern die Institution als datenschutzrechtlich «*Verantwortliche*». In dieser Funktion unterliegt die Institution diversen datenschutzrechtlichen Pflichten. Insbesondere hat sie die betroffenen Personen über den Service LoRaWAN sowie die einzelnen IoT-Anwendungsfälle hinreichend zu informieren und die Wahrung der übrigen Betroffenenrechte wie des Rechts auf Auskunft, Datenberichtigung oder Datenübertragbarkeit sicherzustellen. Zu beachten ist ferner, dass sich jede staatliche Datenbearbeitung auf eine gesetzliche Grundlage stützen muss.

[106] Als hauptsächliche Risiken für die **Datensicherheit** im IoT-Projekt sind die häufig mit schlechten Sicherheitsstandards ausgestatteten IoT-Geräte, die Übermittlung der Daten (insb. durch Funk) sowie die generellen Angriffsmöglichkeiten durch unberechtigte Dritte in der digitalen Welt zu nennen. Die bestehenden Sicherheitsrisiken können sich je nach zukünftigen Einsätzen des Services LoRaWAN zusätzlich verstärken. Hinreichende technische und organisatorische Massnahmen zwecks Datensicherheit sind unabdingbar. Mit den beim LoRaWAN-Protokoll bereits implizierten Sicherheitsmassnahmen (insb. Verschlüsselungen) und dem Grundschutz an Datensicherheit durch die jeweiligen ISMS der Hochschulen bestehen bereits einige für das IoT-Projekt relevante Sicherheitsmassnahmen.

[107] Weitere tangierte Rechtsgebiete bei einem Einsatz von LoRaWAN resp. einem bestimmten IoT-Anwendungsfall sind insbesondere das **Haftungsrecht** sowie das **Immaterialgüterrecht**.

Floriane Zollinger-Löw, lic. iur., Rechtsanwältin bei Schellenberg Wittmer AG in Zürich.

Anna Kuhn, MLaw, Rechtsanwältin, General Counsel bei SWITCH.

Der Beitrag ist im Wesentlichen die Kurzfassung von zwei Kapiteln eines Rechtsgutachtens, das die Autorinnen im Frühling 2019 für zwei Schweizer Hochschulen erstellt haben.