

# IOT UND DATENSCHUTZ – HERAUSFORDERUNG UND CHANCE

Datenschutz in der digitalen Geschäftswelt

Das «Internet of Things» (IoT) ist zwar in aller Munde, jedoch finden sich verschiedene Definitionen des Begriffs. Es geht um die Vernetzung von Objekten über das Internet wie automatisierte Fahrzeuge, vernetzte Ampeln und intelligente Kühlschränke. Dadurch wird der Privatbereich vermehrt zu einem Teil des Internets, was datenschutzrechtliche Fragen aufwirft. Das Datenschutzrecht sollte dabei nicht bloss als regulative Hürde betrachtet, sondern als potenzieller Wettbewerbsvorteil genutzt werden.

Autor\*in: Dr. Andrea Schütz und Dr. Christian Schönfeld



IoT verändert die Anforderungen an den Datenschutz rasant.

**H**äufig wird unter «Internet of Things» (IoT) das Wirken beziehungsweise Handeln von «intelligenten Gegenständen» verstanden – was so viel heisst wie computerisierte, mit Sensorik und internetfähiger Kommunikation ausgestattete Objekte. Oftmals bedürfen computerisierte Vorgänge im Rahmen des IoT keiner physischen Eingaben durch Menschen mehr. Stattdessen können IoT-Objekte Informationen selbst erheben und bearbeiten.

Das IoT ist in unserem Alltag angekommen und für die Zukunft rechnet man mit einem starken Wachstum: So wird prognostiziert, dass bis 2050 fast alle Alltagsgegenstände, rund 24 Milliarden Objekte, vernetzt sein werden. Das IoT wird sämtliche Bereiche der Gesellschaft betreffen und stellt daher ein gewaltiges Wirtschaftspotenzial für Unternehmen aller Branchen dar. Gleichzeitig macht diese Vernetzung der Infrastruktur aber auch den

Privatbereich zu einem Teil des Internets. Dinge aus unserem Alltag sammeln, verschicken und werten Daten über unsere Gesundheit, unser Verhalten und unsere Gewohnheiten in sämtlichen Lebensbereichen aus. Neben all den Erleichterungen und Vorteilen, die das IoT der Allgemeinheit bietet, wirft es auch datenschutzrechtliche Fragen auf.

## RECHTE UND PFLICHTEN IM DATENSCHUTZRECHT

Das IoT fällt in den Anwendungsbereich des Datenschutzrechts, sobald Personendaten bearbeitet werden. Das sind jegliche Angaben, die sich auf eine bestimmte oder bestimmbar Person beziehen. Dies ist insbesondere der Fall, wenn Daten nicht anonymisiert bearbeitet werden. Unter den Begriff des «Bearbeitens» fällt jeder Umgang mit Personendaten, vom Beschaffen und Aufbewahren über das Verwenden, Bekanntgeben oder Archivieren bis hin zum Vernichten. In der Schweiz kommt bei einer Bearbeitung von Personendaten durch Privatpersonen das Bundesgesetz über den Datenschutz (DSG) zur Anwendung, während in der EU die Datenschutz-Grundverordnung (GDPR) einschlägig ist.

Im IoT bewegen sich verschiedenste Akteur\*innen, von den Hersteller\*innen von Sensoren über die Betreiber\*innen von Gateways und Servern sowie die Hersteller\*innen der Software bis zu den betroffenen Personen, deren Daten bearbeitet werden. Dabei nehmen diese Akteur\*innen unterschiedliche datenschutzrechtliche Rollen ein. Sogenannte Verantwortliche (auch Controller genannt), welche die Zwecke und Mittel der Datenbearbeitung festlegen, sowie Auftragsbearbeiter (auch Processors genannt), welche Datenbearbeitungen für Controller vornehmen, treffen bei der Bearbeitung von Personendaten datenschutzrechtliche Pflichten, deren Verletzung zu Bussen und anderen Ansprüchen führen kann. Demgegenüber stehen den betroffenen Personen diverse Rechte zu, etwa auf transparente Information, Auskunft, Berichtigung fehlerhafter Daten, auf Einschränkung der Bearbeitung sowie (in Zukunft) auf Datenübertragbarkeit. Allfällige Einwilligungen können jederzeit widerrufen werden.

## NACH TREU UND GLAUBEN

Zu den zentralen Grundsätzen, welche Controller und Processors bei der Bearbeitung von Personendaten einzuhalten haben, zählt, dass die Bearbeitung rechtmässig erfolgen muss. Gegebenenfalls setzt dies das Vorliegen eines Rechtfertigungsgrundes ▶



in Form der Einwilligung der betroffenen Person, eines überwiegenden Interesses oder einer gesetzlichen Grundlage voraus.

Die Bearbeitung muss nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise erfolgen. Ferner darf sie nur zu dem Zweck erfolgen, der bei der Beschaffung der Daten angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Zudem muss die Bearbeitung verhältnismässig sein, das heisst namentlich, dass sie auf das für den Zweck der Bearbeitung notwendige Mass beschränkt sein muss. Schliesslich ist sicherzustellen, dass Personendaten sachlich richtig sind und dass unrichtige Personendaten gelöscht oder berichtigt werden sowie dass sie durch angemessene technische und organisatorische Massnahmen (TOM) geschützt sind.

## UNNÖTIGE DATENSAMMLUNGEN AUF VORRAT

Diese Anforderungen werden (auch) im IoT augenscheinlich nicht immer erfüllt. Viele IoT-Anwendungen bearbeiten Personendaten, ohne die betroffenen Personen hierüber transparent zu informieren oder vorgängig, wo nötig, deren Einwilligung einzuholen. Viele IoT-Geräte erlauben es ihren Nutzern nicht, einzelne Datenbearbeitungen zu unterbinden, obwohl die grundsätzliche Entscheidung über die Bearbeitung von Personendaten als Ausprägung des Rechts auf Selbstbestimmung bei den Anwendern verbleiben sollte. Oftmals werden Personendaten auf Vorrat erhoben oder über einen Zeitraum gespeichert, der das notwendige Mass überschreitet, wodurch «Datensammlungen auf Vorrat» entstehen.

Die damit verbundenen Risiken werden dadurch verschärft, dass viele IoT-Geräte nur unzureichend geschützt sind, obwohl IoT-Geräte oder -Sensoren Einfallstore für Cyberattacken bieten können. (Das Küchengerät mit nichtdeklariertem Mikrophon mag als Beispiel dienen.) Dies führt nicht nur zu einem Risiko für die betroffenen Personen, sondern auch zu Reputations- und Haftungsrisiken für die bearbeitenden Controller und Processors.

## RISIKEN VERMEIDEN

Die Vermeidung solcher Risiken ist für alle Akteur\*innen von Vorteil und lässt sich auch im IoT mittels technischer und juristischer Massnahmen realisieren. Unverhältnismässige Datensammlungen lassen sich durch Gateways verhindern, welche die

Daten nicht registrierter oder entsprechend gekennzeichnete Endgeräte automatisch aussondern oder anonymisieren. Die transparente Information der betroffenen Personen über die beabsichtigten Datenbearbeitungen und deren Zwecke gibt diesen die geforderte Selbstbestimmung und steigert gleichzeitig deren Vertrauen in die Datenbearbeiter\*innen.

Entscheidend für eine reibungslose Umsetzung ist, dass Datenbearbeiter\*innen den Anforderungen des Datenschutzrechts von Beginn an die nötige Beachtung schenken. Dies ermöglicht ihnen, ihre Produkte und Dienstleistungen so zu konzipieren und zu entwickeln, dass diese den datenschutzrechtlichen Anforderungen genügen. So verstandenes «privacy by design» erlaubt es den Bearbeiter\*innen, die Anforderungen ihres Geschäftsmodells am besten mit den legitimen Interessen der betroffenen Personen auf Datenschutz in Einklang zu bringen.

Datenschutzrecht sollte dabei nicht bloss als regulative Hürde, sondern auch als potenzieller Wettbewerbsvorteil betrachtet werden. In einer Welt, in der die datenschutzrechtliche Mündigkeit der betroffenen Personen konstant wächst, heben sich diejenigen von der Konkurrenz ab, die als IoT-Unternehmen von Beginn an einen hohen Datenschutz gewährleisten. So kann etwa konsequent das Prinzip «privacy by default» verfolgt werden. Dieses besagt, dass Produkte oder Dienstleistungen für Nutzer\*innen ohne weiteres Zutun standardmässig die datenschutzfreundlichsten Einstellungen aufweisen. Der Ruf, den man sich mit einem solchen Auftreten auf dem Markt erarbeiten kann, könnte sich so auch zu einem entscheidenden Konkurrenzvorteil entwickeln. ■

---

**i** Dr. Andrea Schütz ist Rechtsanwältin bei der Prager Dreifuss AG.

---

**i** Dr. Christian Schönfeld ist Rechtsanwalt bei der Prager Dreifuss AG.

[www.prager-dreifuss.com](http://www.prager-dreifuss.com)