FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Cloud Computing nach der EU-Datenschutz-Grundverordnung am Beispiel von Wearable Devices

Vortrag auf dem Forschungssymposium
des Instituts für wirtschafts- und
rechtswissenschaftliche Forschung Frankfurt
am 5. Mai 2017

Institut für wirtschafts- und
rechtswissenschaftliche Forschung
Frankfurt

Gliederung der Präsentation

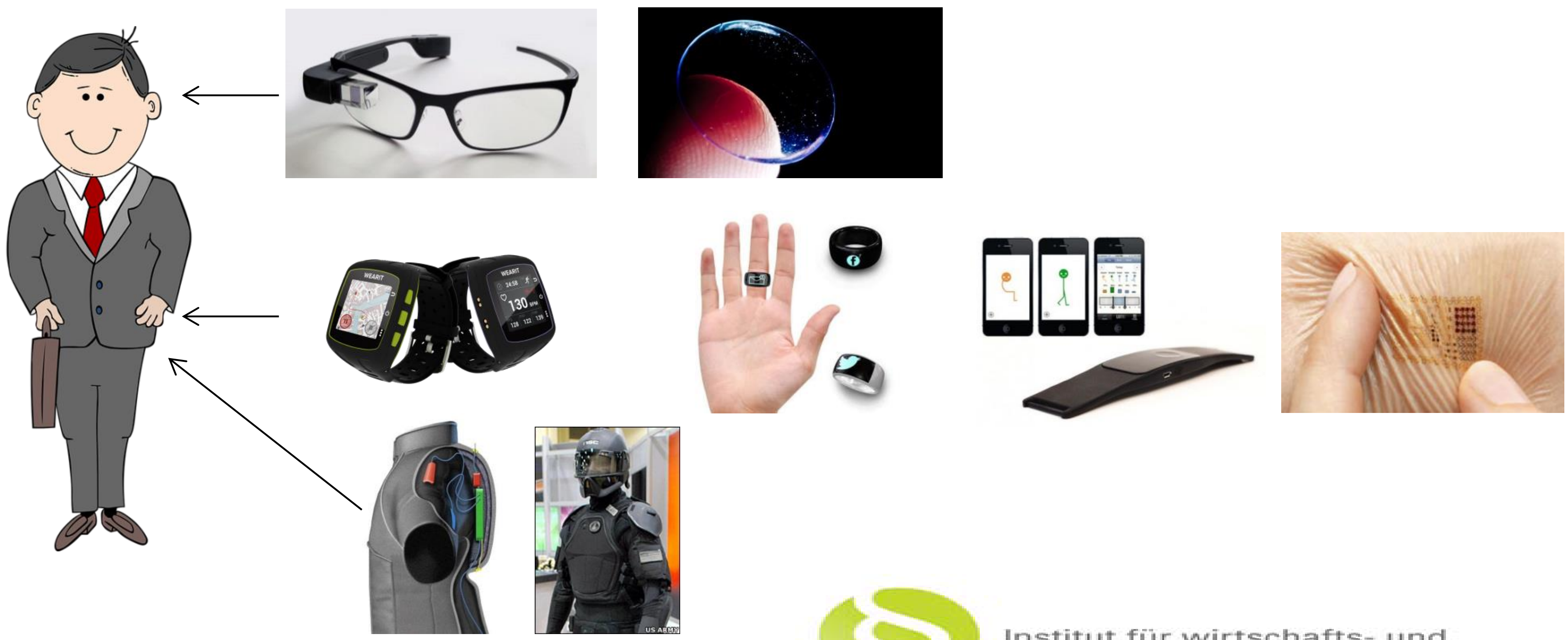
- Definitionen: Cloud Computing und Wearable Devices
- Datenschutzrisiken: Wearables und Cloud Computing
- Anwendung der Europäischen Datenschutzgrundverordnung (DS-GVO) auf Cloud Computing
- Cloud-Computing außerhalb der EU
- Auswirkungen für Anbieter von Wearables

Definition: Cloud Computing

- Cloud Computing beschreibt die Bereitstellung von IT-Infrastruktur und IT-Leistungen wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Service über das Internet.
- Nach der Organisationsform lassen sich unterscheiden:
  - Private Cloud: Bereitstellung aus einem unternehmenseigenen Rechenzentrum; Dienste sind nur für eine beschränkte Anzahl von Personen (z.B. Mitarbeiter und autorisierte Geschäftspartner) zugänglich.
  - Public Cloud: Bereitstellung aus einem öffentlich zugänglichen System durch einen externen IT-Dienstleister; kann von vielen Personen und Unternehmen über das Internet genutzt werden.

Definition: Wearable Devices

- Wearable Devices sind kleine Computer, die am oder im Körper getragen werden. Sie sind meist (unmittelbar oder mittelbar) mit dem Internet verbunden.
- Beispiele:



Definition: Wearable Devices

- Anwendungsbereiche (Beispiele):

Gesundheit	Sport / Fitness	Wellness	Lifestyle	Arbeit
Optimierte Diagnostik	Tracking	Monitoring: Gewicht, Haltung, Augenpflege	Alltagsorganisation	Sicherheit
Überwachung von Behandlungsabläufen	Coaching	Analyse des Schlafverhaltens	Interaktive Spiele	Wissenstransfer
Hausnotruf			Media- und Infotainment	Produktivität
Erweiterung der Körperfunktionalitäten				

Datenschutzrisiken von Wearables

- Die Nutzung von Wearbles macht ohne die gleichzeitige Nutzung von Cloud Services nur wenig Sinn, da die Funktionen – wenn überhaupt – nur eingeschränkt zur Verfügung stehen.
- Die von Wearables erfassten Daten sind oft sensibel:
  - Aufenthaltsort ⟹ Bewegungsmuster
  - Herzschlag
  - Atmung
  - Hautwiderstand

    ⟹ Fitness, Stress, Alkoholkonsum, Körperliche Aktivität, Rauchen, Gesundheitszustand (Fieber etc.)
  - Puls/Blutdruck
  - Blutzucker
  - EKG etc.

    ⟹ Gesundheitszustand
  - ...

Datenschutzrisiken von Wearables

- Wearable-Anbieter erhält personenbezogene, insbes. sensible Daten.
- Speicherung dieser Daten in einer Public Cloud stellt eine Weitergabe an Dritte dar.
- Weitergabe und Veröffentlichung der Daten zur Auswertung und Nutzung durch Dritte (→Zusammenführung mit anderen Daten zu Big Data-Analysen) ermöglichen die Erstellung von Persönlichkeitsprofilen und Verhaltensprognosen für Menschen und Gruppen, die für wirtschaftliche Zwecke genutzt werden können.
- Durch Einwilligung in Datenschutzerklärungen, die auch Cloud-Nutzung umfassen, wird die Hoheit über die eigenen Daten aus der Hand gegeben; oft fehlt es an Transparenz.

Datenschutzrisiken von Wearables

- Sicherheitslücken beim Datentransfer (nur Bruchteile des Transfers erfolgen über verschlüsselte Verbindungen).
- Eindeutige Netzwerk-ID (derzeit meist noch Standard) ermöglicht eine Langzeit-Überwachung des Nutzers.
- Wearables eignen sich als „Spionage-Tool" (Beispiele):
  - Unbemerkt können Fotos/Filmaufnahmen/Tonaufzeichnungen von der Umgebung gemacht werden;
  - Apps wie z.B. MoLe (Motion Leaks through Smartwatch Sensors) ermöglichen das Mitlesen von Texteingaben über die Computertastatur;
  - Hacker können auf Daten zugreifen, wenn die Kommunikationsschnittstelle nicht deaktiviert wurde/W-Lan-Router nicht ausreichend geschützt ist.
- Die Gefahr eines Fremdzugriffs (auch „Man in the Middle-Angriffe") oder einer Manipulation der Daten lässt sich nicht ganz ausschließen.
- ....

Datenschutzrisiken beim Cloud Computing (Beispiele)

- Cloud-Dienste nutzen oft nicht nur die Infrastruktur eines Anbieters, sondern zur effizienten Ressourcennutzung Infrastrukturen verschiedener Unterauftragnehmer in verschiedenen Ländern; bei Nutzung von Cloud-Diensten außerhalb von EU/EWR besteht evtl. ein abweichendes Datenschutzniveau.
- Cloudeigene Verschlüsselungsangebote ermöglichen Zugriff durch den Betreiber (und staatliche Stellen), da Datenverschlüsselung auf dem Server mit serverseitig generierten und gespeicherten Schlüsseln erfolgt.
- Vom Cloudanbieter zur Verfügung gestellte Verschlüsselungsmöglichkeiten für nutzerseitige Verschlüsselung bergen vergleichbare Risiken.
- Schwache Passwörter der Nutzer ermöglichen „hacking".

Anwendung der DS-GVO auf Cloud-Computing

- Bis zum 24.05.2018 gilt die aktuelle Rechtslage (BDSG/LDSG)
- Ab dem 25.05.2018 gilt DS-GVO unmittelbar in allen EU-Mitglieds-staaten sowie für Mitgliedsstaaten des EWR.
- Wenn Wearable-Anbieter Cloud-Computing-Dienste Dritter nutzen, liegt Auftragsdatenverarbeitung vor, die für private Unternehmen abschließend in Art. 28 DS-GVO geregelt ist.
  - **Neu:** Erlaubnistatbestand immer notwendig (streitig)
    Art. 6 Abs. 1 lit f) DS-GVO: „berechtigtes Interesse des Verantwortlichen“

  Problem: Weitergabe besonderer Kategorien personenbezogener Daten (u.a. auch **Gesundheitsdaten**) nicht umfasst, Art. 9 DS-GVO

  Daher **zukünftig** bei besonderen Kategorien personenbezogener Daten **immer Einwilligung** notwendig.

Anwendung der DS-GVO auf Cloud-Computing

- Die DS-GVO ist anwendbar, wenn entweder
  - der Cloud-Anbieter oder der Verarbeiter (Wearable-Anbieter) eine Niederlassung innerhalb der EU oder des EWR hat und personenbezogene Daten verarbeitet werden (unerheblich ist, wo die Verarbeitung tatsächlich stattfindet), oder
  - personenbezogene Daten einer natürlichen Person, die sich innerhalb der EU oder des EWR aufhält, verarbeitet werden.

- Außereuropäische Cloud-Anbieter, die sich an den europäischen Markt richten, müssen zukünftig aus eigener Verpflichtung die Einhaltung der europäischen Datenschutzvorschriften sicherstellen (bußgeldbewehrt).

Cloud-Computing außerhalb der EU

- Die Übermittlung der Daten in Drittstaaten setzt voraus, dass das Datenschutzniveau dem in der EU garantierten Datenschutzniveau gleichwertig ist.

  Alternativen der Feststellung sind:

  - Verbindliche Entscheidung der EU-Kommission
    - Sichere Drittstaaten: Andorra, Argentinien, Kanada (für Handelsorganisatio-nen), Schweiz, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neusee-land und Uruguay
    - USA: EU-Privacy Shield - Beschluss vom 12.07.2016 - angemessenes Datenschutzniveau für Datenübermittlungen in die USA, sofern ein vorge-gebener Selbstzertifizierungsmechanismus durch das Unternehmen ein-gehalten wird. Die Entscheidung der EU-Kommission bedeutet nicht, dass für die USA allgemein ein angemessenes Datenschutzniveau festgestellt wurde (Nichtigkeitsklagen vor dem Gericht der Europäischen Union sind anhängig) . Am 6. April 2017 - Kritische Resolution EU-Parlaments: EU-Kommission wird zur erneuten Überprüfung und Nachbesserung des Datenschutzniveaus aufgefordert; Anpassung an DS-GVO notwendig.

Cloud-Computing außerhalb der EU

- Bei allen anderen Staaten muss die Daten übermittelnde Stelle grundsätzlich selbst das Datenschutzniveau des Staates überprüfen und sicherstellen.

  Alternativen sind:

  - Abschluss der von der EU-Kommission bereitgestellten Standardvertragsklauseln
  - Binding Corporate Rules (z.B. innerhalb einer Unternehmensgruppe)
  - **Einwilligung des Betroffenen**

Auswirkungen für Anbieter von Wearables

- Anbieter von Wearables müssen sich auf die neue DS-GVO einstellen.
- Wenn Cloud Services Dritter genutzt werden, sind die Vorgaben zur Auftragsdatenverarbeitung gem. § 28 DS-GVO einzuhalten.
- Sollen besondere Kategorien personenbezogener Daten wie z.B. Gesundheitsdaten in der Cloud eines Dritten verarbeitet werden, ist gem. Art. 9 Abs. 2 a DS-GVO zukünftig immer eine ausdrückliche Einwilligung des Betroffenen in die Cloud-Nutzung notwendig, wenn – wie regelmäßig – die weiteren Ausnahmetatbestände des Art. 9 DS-GVO nicht vorliegen. Dto. bei berufsrechtlichen Geheimhaltungspflichten.
- Bei der Formulierung der Einwilligung in Datenschutzerklärungen sollte auf Transparenz geachtet werden, da die Einwilligung gem. Art. 7 DS-GVO in verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache zu erfolgen hat; sie muss von anderen Sachverhalten klar zu unterscheiden sein.

Vielen Dank für Ihre Aufmerksamkeit!

Ich stehe Ihnen gerne für Fragen zur Verfügung?