



ATLANTIC Hotel Kiel

08.09.2025

Internet of Things – Das Zusammenspiel von Data Act und DSGVO

- **Frederick Gaß (ULD)**
- **Harald Zwingelberg (ULD)**



Unboxing.IoT.Privacy

Gefördert durch:



Bundesministerium
für Forschung, Technologie
und Raumfahrt

Vertretene Auffassungen sind solche der Referenten.



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Struktur des Vortrags

- (1) Hintergrund und Anwendungsbereich der DSGVO und des Data Acts
- (2) Rollen und Entitäten des Data Acts und ihre Beziehungen
- (3) Ausgewählte Einzelaspekte für die Praxis
- (4) Key-Takeaways

Hintergrund – DSGVO

- Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf informationelle Selbstbestimmung
- Vereinheitlichung des Datenschutzstandards innerhalb der EU
- Pflichten der DSGVO treffen hauptsächlich den sog. Verantwortlichen
- Anwendungsbereich: Verarbeitung von personenbezogenen Daten
 - Jede Form der Verarbeitung von personenbezogenen Daten bedarf einer Rechtsgrundlage (Art. 6 DSGVO)

Hintergrund – Data Act

- Verbesserung der Zugänglichkeit und die Nutzung von Daten durch Bereitstellungspflichten für eine steigende Wettbewerbsfähigkeit und Innovation
- Schaffung eines „echten“ Binnenmarkts für Daten
- Keine Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten, allgemeiner Datenbegriff nach dem DA
(P) Ein Großteil der Daten ist personenbezogen, Beschränkungen der DSGVO sind zu beachten!
- Anwendungsbereich:
 - Bereitstellen und Nutzen von Daten aus vernetzten Produkten (IoT-Geräte) oder verbundenen Diensten

Hintergrund – Data Act Gliederung

- Kapitel I – Allgemeine Bestimmungen (Definitionen etc.)
- Kapitel II – Datenweitergabe B2C/B2B (Rechte & Pflichten)
 - Art. 3-7 DA
 - Insb. Rechte nach Art. 3 (1), (2) und Art. 4 (1) DA
- Kapitel III – Pflichten des Dateninhabers - B2B bei der Datenweitergabe
- Kapitel IV – Missbräuchliche Vertragsklauseln
- Kapitel V – Bereitstellung von Daten für öffentliche Stellen
- Kapitel VI – Wechsel zwischen Datenverarbeitungsdiensten
- Kapitel VII – XI – Unrechtmäßiger Zugang, Interoperabilität, Anwendung und Durchsetzung, Schutzrecht sowie die Schlussbestimmungen

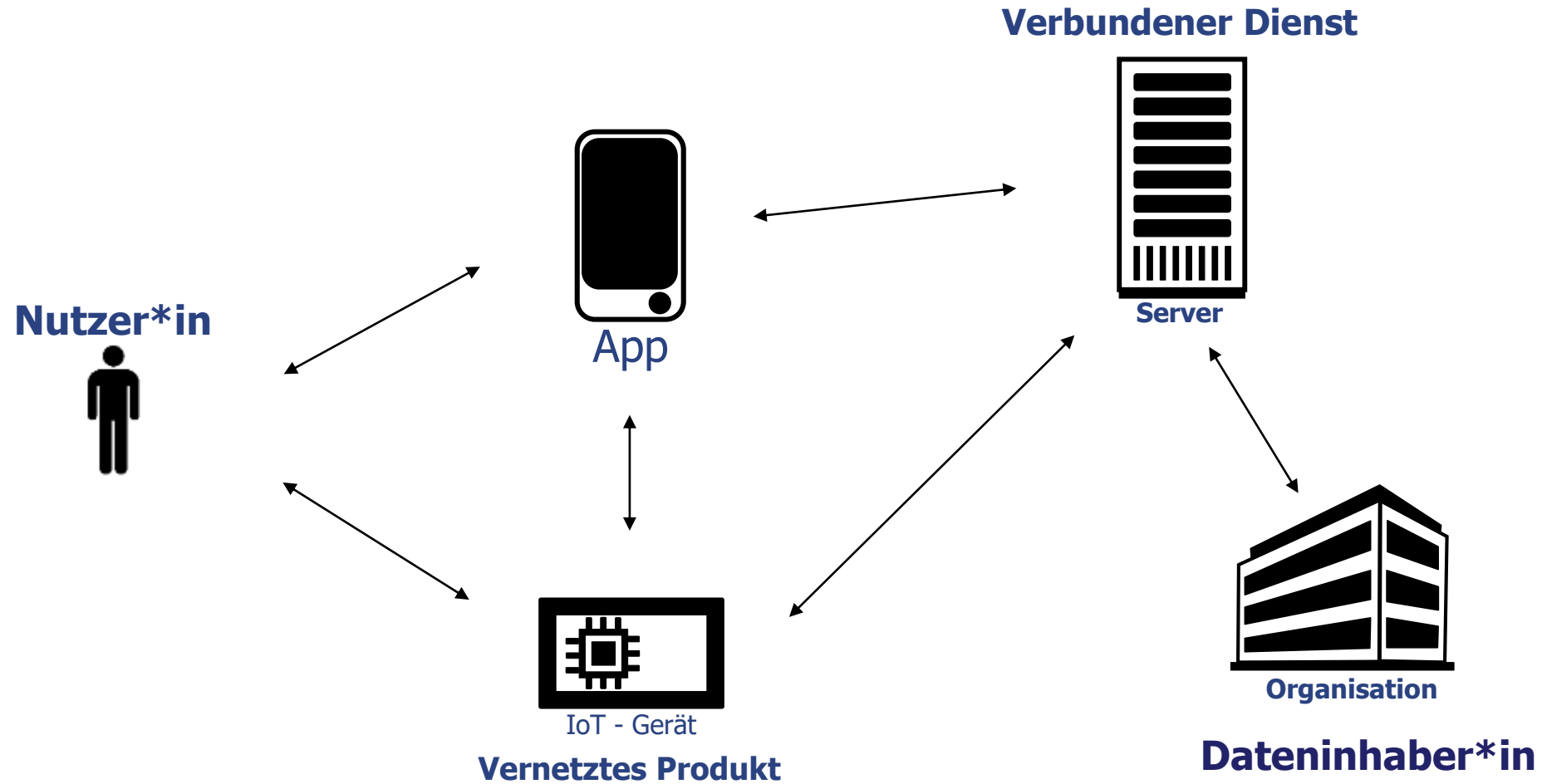
Anwendungsbereich (1) – Data Act

- Vernetztes Produkt (Art. 2 Abs. 5 DA)
 - „einen Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung im Namen einer anderen Partei außer dem Nutzer ist.“
- Daten (Art. 2 Abs. 1 DA)
 - „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material.“

Anwendungsbereich (2) – Data Act

- Metadaten (Art. 2 Abs. 2 DA)
 - Intention der Definition ist das Versichern, dass diese (einheitlich) nutzbar gemacht werden können, insb. in Kombination mit anderen Daten.
 - **Beachte:** Hieraus durch zusätzliches Investieren gewonnene Informationen fallen nicht unter den DA!
- Produktdaten (Art. 2 Abs. 15 DA) / verbundene Dienstdaten (Art. 2 Abs. 16 DA)
 - Durch den Gebrauch des Produkts oder Diensts generierte Daten.
- Ohne weiteres Verfügbare Daten (Art. 2 Abs. 17 DA)
 - Produktdaten und verbundene Dienstdaten, die ohne unverhältnismäßigen Aufwand rechtmäßig erhalten werden können.
- Geschäftsgeheimnis (Art. 2 Abs. 18 DA)
- Exportierbare Daten (Art. 2 Abs. 38 DA)

Rollen und Entitäten – Data Act



Nutzer*in – Data Act

- Nach Art. 2 Abs. 12 DA „eine natürliche oder juristische Person, die ein vernetztes Produkt **besitzt** oder der vertraglich zeitweilige **Rechte für die Nutzung** des vernetzten Produkts übertragen wurden oder **die verbundenen Dienste in Anspruch nimmt.**“
 - „**Besitz**“ meint hier (aufgrund des Vergleichs mit anderen Sprachfassungen) die Eigentümerstellung iSd § 903 BGB!
 - **Nutzer (-)** bei rein tatsächlichen Nutzungen (bspw. Beistehende) oder Gefälligkeitsverhältnisse (bspw. Leihe unter Freunden).
 - Hauptrolle im DA, Rechte nach Art. 3-7 DA. Beachte **Verbot** von Verhaltensweisen wie z.B. die Verwendung von Daten für Konkurrenzprodukte etc. (Art. 4 Abs. 10 DA).

Dateninhaber*in – Data Act

„eine natürliche oder juristische Person, die nach dieser Verordnung [...] berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat.“

- **(P)** Zirkulär – Verpflichtungen aus Art. 4-7 DA sollen den Dateninhaber eigentlich definieren, setzen ihn aber voraus.

Beachte Ausnahmeregelung: Art. 7 (1) DA -> Für Kleinst- und Kleinunternehmen & mittlere Unternehmen.

Pflicht nach Art. 3 Abs. 1 – Data Act

- Zugangsverschaffungspflicht **Art. 3 Abs. 1 DA** *(ab 09/2026)*
 - Standardmäßige und direkte Zugänglichkeit der Daten für den User bei vernetzten Produkten („**by Design**“)
 - Was? Produktdaten, verbundene Dienstdaten und erforderliche und relevante Metadaten.
 - Wie? Einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format.
 - Beschränkungen: Soweit technisch möglich und durchführbar.

Pflicht nach Art. 3 Abs. 2 – Data Act

- (Vorvertragliche) Transparenzpflichten nach **Art. 3 Abs. 2 DA**
 - Bei Verkäufer, Vermieter, Leasinggeber bzw. Hersteller – vorvertraglich sowie Veränderungen innerhalb der Nutzungen der Produkte.
 - Was? Alle Informationen bezüglich der Produktdaten, die das Produkt generieren kann (Art, Format und Umfang)

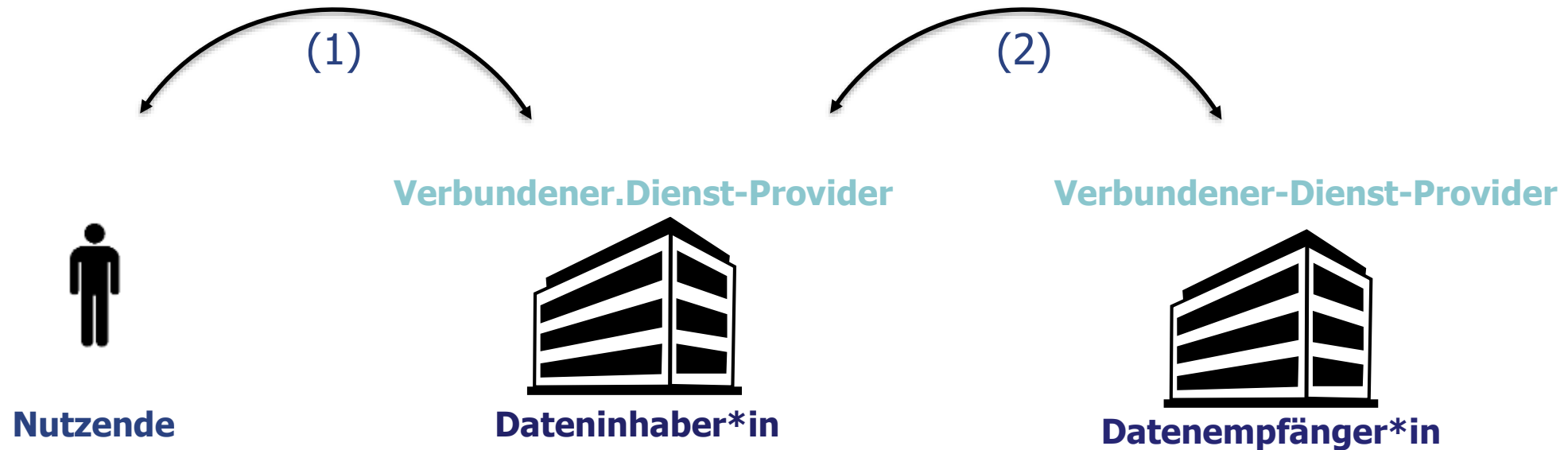
Pflicht nach Art. 3 Abs. 3 – Data Act

- (Vorvertragliche) Transparenzpflichten nach **Art. 3 Abs. 3** DA
 - Vor Abschluss eines Vertrags für verbundene Dienste mit dem Provider.
 - Was? Alle Informationen bezüglich der Speicherung, Zugang etc., Abruf durch den Provider (kontinuierlich, in Echtzeit etc.).
 - Insb. Umfang, Art und Häufigkeit der Erhebung durch den Provider sowie Speicherung und Aufbewahrung.
 - Die Verwendung durch den Provider, den Zweck der Verwendung und welche Weiterleitungen an Dritte vorliegen.
 - Identität der Dateninhaber*innen
 - Modalitäten für Abruf durch für Nutzer, Art, Umfang, Echtzeit etc.

Recht nach Art. 4 Abs. 1 – Data Act

- Bereitstellungverlangen Art. 4 (1) DA (*untergeordneter Anspruch*)
 - Wenn nicht direkt zugänglich (bspw. aus techn. Gründen), dann Verpflichtung, ohne Weiteres **verfügbare Daten** einfach, sicher und unentgeltlich (etc.) bereitzustellen.
 - Wie? Ohne unangemessene Erschwerung (Gestaltung, Funktionsweise etc.)
 - Beschränkungen: Nach Art. 4 Abs. 2, Abs. 13 DA durch Vertrag, aus Sicherheitsgründen, unlauterer Wettbewerb sowie bei Geschäftsgeheimnissen nach Art. 4 Abs. 6.

Datenempfänger*in – Data Act

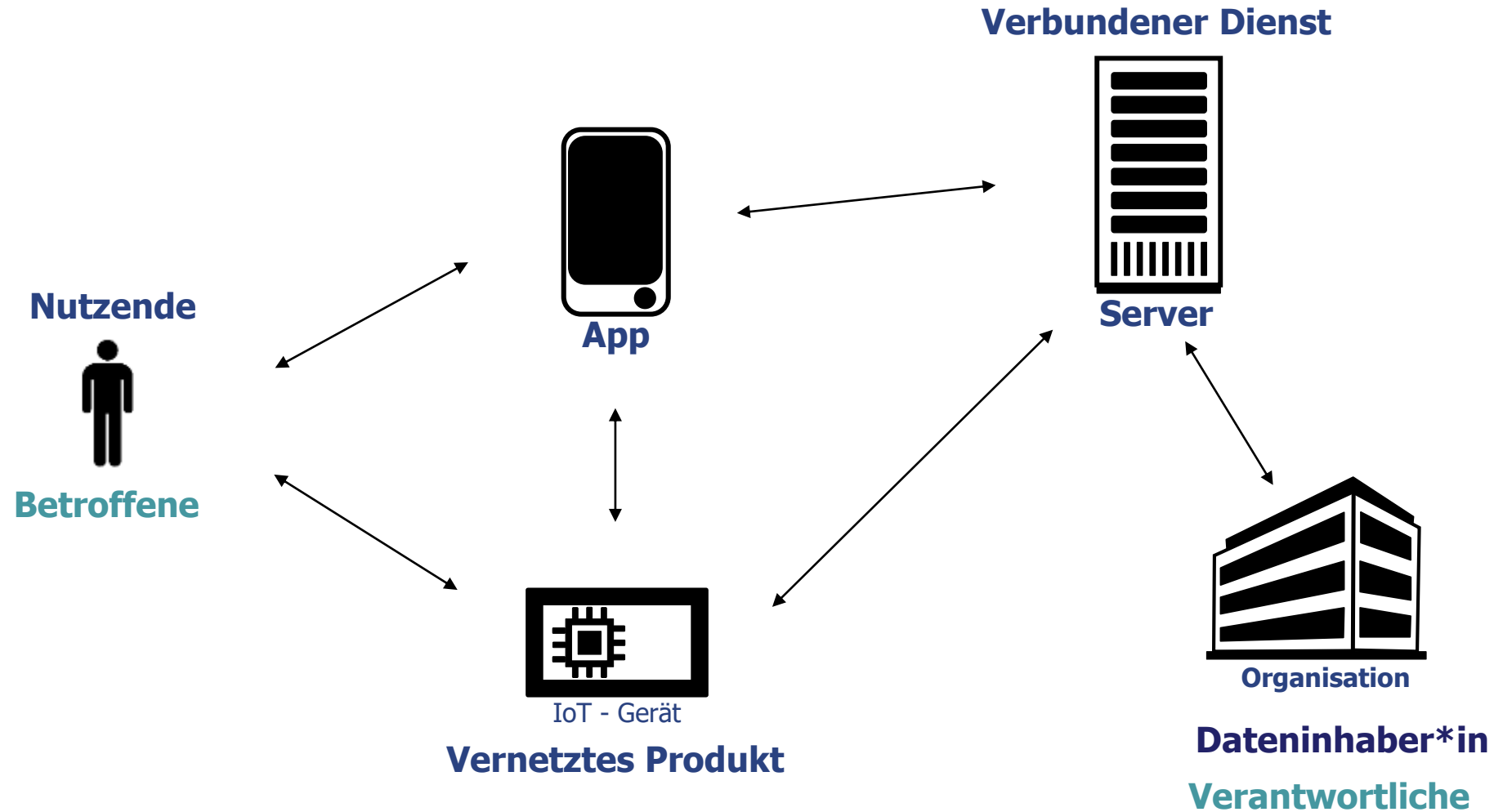


- Anspruch auf Weiterleitung von Daten an Dritte (Art. 5 Abs. 1 DA)
- Weiterleitung der Daten nur im Umfang dessen, wie es mit dem Nutzer vereinbart ist und unter Beachtung von Einschränkungen durch Geschäftsgeheimnissen o. unlautere Ziele Art. 6 Abs. 2 DA.

Recht nach Art. 5 Abs. 1 – Data Act

- Recht auf Weitergabe von Daten an Dritte
 - Was? Alle verfügbaren Daten sowie die für die Auslegung und Nutzung dieser Daten erforderlichen Metadaten
 - Wie? Unentgeltlich, unverzüglich, einfach, sicher in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, kontinuierlich und in Echtzeit.
 - Beschränkungen: Sog. Torwächter (Gatekeeper) gem. Art. 3 VO EU 2022/1925 sind nicht zugelassene Dritte
 - Beachte: Pflichten für Dritte, die auf Verlangen des Nutzer Daten erhalten finden sich in Art. 6 DA.

Rollen und Entitäten – Data Act & DSGVO



Ausgewählte Einzelaspekte und Hinweise für die Praxis

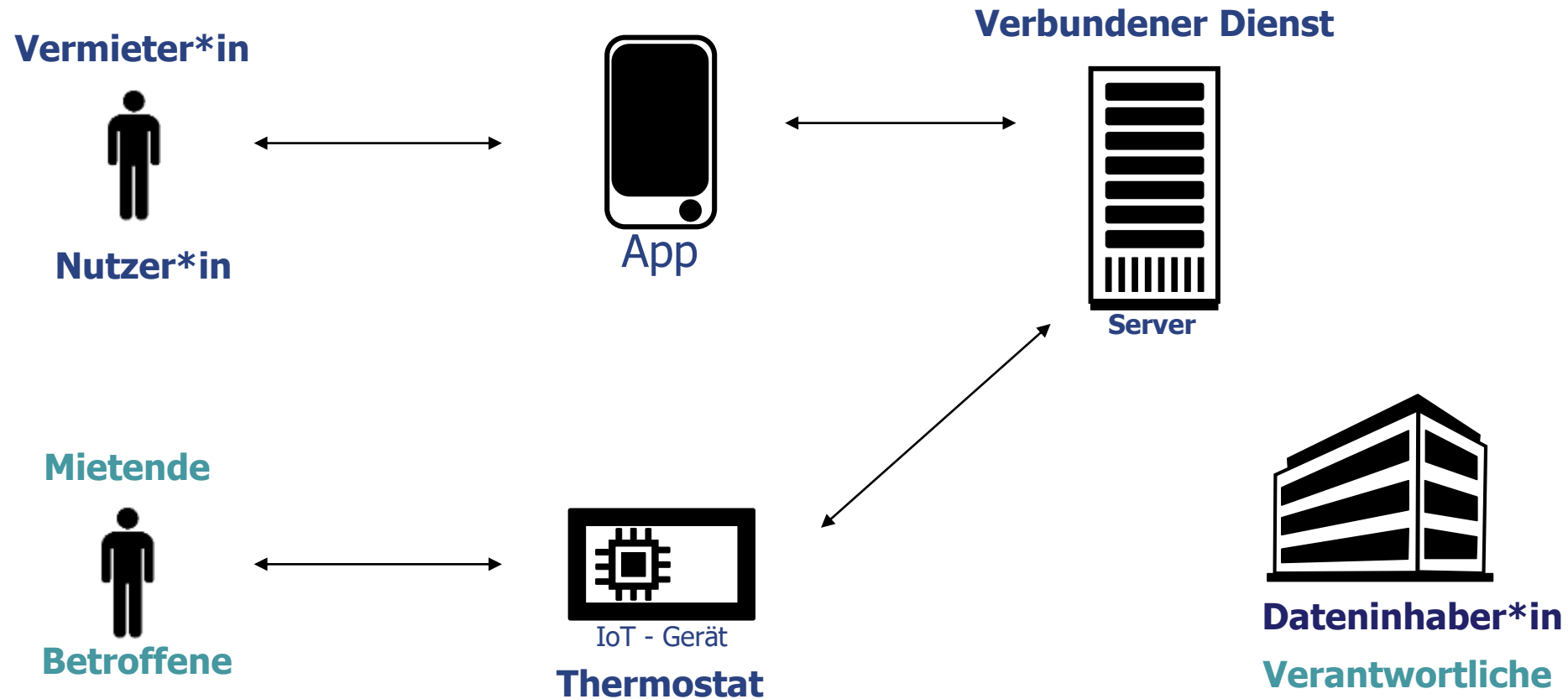
Berührungspunkte

Datenschutz und Data Act



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

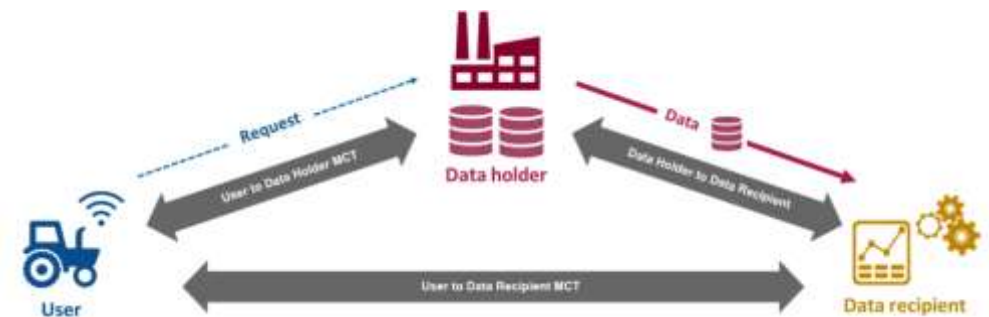
Personenverschiedenheit – Betroffener & User



Verträge

- Ab 12. Sep. 2025 ist ein Vertrag zur Datennutzung erforderlich, wenn Dateninhaber (Hersteller, Dienstanbieter,...) Produktdaten nutzen wollen
- Art. 4 Abs. 13 DA: Dateninhaber darf (nicht personenbezogene) Daten nicht ohne Vertrag mit dem Nutzer nutzen
- Wichtige Vertragsbeziehungen nach Data Act

▪ Nutzer	↔	Dateninhaber
▪ Dateninhaber	↔	Datenempfänger
▪ Nutzer	↔	Datenempfänger



Verträge

- Mustervertragsklauseln wurden im Auftrag der Kommission erstellt, aber Kritik des EDSA*):
 - Nicht alle Datenschutzaspekte erfasst, nicht immer sauber zwischen Daten mit und ohne Personenbezug differenziert
 - Vorrang der DSGVO vor dem Data Act als Richtschnur für die Anwendung, vergl. Art. 1 Abs. 5 DA
 - Datenschutz-Rollen und DA-Rollen müssen sauberer differenziert werden. Nur Nutzer*, die allein betroffene Person sind, haben Datenzugang, andere brauchen RGL im Verhältnis zu den Betroffenen

*) EDPB, [Statement 4/2025](#), 8.7.2025,

Verträge

- In der Praxis bei Verfahren mit Einsatz verbundener Geräte / IoT:
 - Personenbezug der verarbeiteten Daten? Wenn ja...
 - Rollen nach Datenschutzrecht und Data Act für konkret geplante Implementierung bestimmen
 - Rechtsgrundlage für alle Verarbeitungen ermitteln
 - Verträge nach Datenschutzrecht: Auftragsverarbeitung bzw. zwischen gemeinsam Verantwortlichen
 - Verträge nach Data Act wegen der Datennutzung

Rückwirkung

- Problem: Dateninhaber brauchen Datenlizenzvertrag für Weiternutzung von in der Vergangenheit erhobenen Daten.
Hindernisse:
 - Kontakt zum Nutzer vorhanden?
 - Wer war zum Erhebungszeitpunkt Nutzer?
- Bestand schon damals eine wirksame informierte datenschutzrechtliche Einwilligung aller Betroffenen (=Nutzer) unter klarer Bestimmung, dass der IoT-Dienstanbieter die personenbezogenen Daten auch zu benannten eigenen Zwecke verwenden wird, könnte Anforderungen an Datennutzungsvertrag entsprechen, wenn auch Bestimmungen zu Vergütung etc. fehlen.

Gestaltung durch Datenschutz

- Gestaltung von Verfahren unter Erwägung des Datenschutzes
 - Frühe Anonymisierung
Erfolgreiche Anonymisierung senkt Risiko des Verantwortlichen.
Einwände der Nutzer gegen eine frühe Anonymisierung greifen wohl eher nicht, da DSGVO-Konformität und Risikomanagement erlaubt sein müssen.
Es kann aber der eigene Nutzen an den Daten verloren gehen.
 - Rechtsgrundlage bei mehreren betroffenen Personen
Zugänglichmachung bedarf einer RGL für alle betroffenen Personen.
Nachweis durch Nutzer, der Daten verlangt. Im Regelfall bleibt Einwilligung als mögliche RGL.

Vergl. Bomhard/Zdanowiecki, RDi 2025, 419ff.

Unterstützung bei Transparenz

IoT-Datenflüsse ⇔ DSGVO-Transparenzpflichten

- Verantwortlicher muss Transparenzpflichten erfüllen
- Hersteller, Importeure, Händler nach DSGVO nicht verpflichtet
- Data Act als Hilfeleistung bei der Transparenzgewährung?
 - Art. 3 Abs. 2 Data Act: Pflicht für Verkäufer / Vermieter / Leasinggeber zu Informationsbereitstellung vor Verkauf über:
 - Art, Format, Umfang der generierten Produktdaten,
 - Verfügbarkeit in Echtzeit,
 - Speicherung lokal/remote, Speicherdauer

Unterstützung bei Transparenz

IoT-Datenflüsse ↔ DSGVO-Transparenzpflichten

- Data Act als Hilfeleistung bei der Transparenzgewährung?
 - Art. 3 Abs. 3 Data Act: Pflicht für Dienstanbieter zu Informationsbereitstellung vor Vertragsschluss über:
 - Art, Format, Umfang der erhobenen Produktdaten und erzeugten Dienstdaten
 - Modalitäten für Zugriff auf Produkt- und Dienstdaten für Nutzer
 - Absicht zur eigenen Verwertung oder Nutzung durch Dritte und ggf. Zwecke
 - Identität des potentiellen Dateninhabers + Adresse
- ⇒ Data Act kann Instrumentarium für Datenschützer werden, um bisher schwer verfügbare Informationen über die DV bei IoT-Geräten zu erhalten

Zu IoT & Transparenz: Hansen/Lo Iacono/Reinhardt/Zwingelberg, DuD 2025, 425.

Key-Takeaways

- Analyse aller Entitäten und Rollen (Map)
 - Beachtung aller tatsächlichen und rechtlichen Umstände
 - Transparenz gegenüber allen betroffenen Personen beachten
- Verträge künftig nach Datenschutzrecht und Data Act erforderlich
- Bei mehreren betroffenen Personen: Rechtsgrundlagen für alle Verarbeitungen erforderlich, Verantwortliche sind zu identifizieren und alle Verantwortlichkeiten konkret zugewiesen werden
- Bei Konflikten: Vorrang des Datenschutzrechts nach Art. 1 Abs. 5 DA

Haben sie den europäischen Computerführerschein?



Sag' ich nicht



OK, den Datenschutztest haben Sie auch bestanden



Fragen? Anregungen?

Kontakt

Frederick Gaß, uld65@datenschutzzentrum.de

Harald Zwingelberg, uld6@datenschutzzentrum.de

Gefördert im Projekt Unboxing.IoT.Privacy



Gefördert durch:



Bundesministerium
für Forschung, Technologie
und Raumfahrt

<https://www.datenschutzzentrum.de/projekte/unboxingiot/>