

The background is a digital illustration of a server room. It features rows of server racks on both sides of a central aisle, receding into the distance. The scene is bathed in a deep blue light. Floating throughout the space are various lines of computer code in a lighter blue, monospaced font, creating a sense of data flow and digital environment.

# Nutzungsbedingungen für Datenräume (DSGVO-Anforderungen)

Ted Kroke

# Überblick

**Ausgangslage:** Im Rahmen von Manufacturing-X sollen maschinengenerierte Sensordaten zur Optimierung von Maschinenbetrieb, Wartung und Serviceleistungen in Datenräumen geteilt werden.

**Allerdings** haben derartige Daten häufig einen DSGVO-relevanten Personenbezug, obwohl dieser für die eigentlichen Verarbeitungszwecke irrelevant ist.

**Das bedeutet,** dass beim Teilen von maschinengenerierten Sensordaten in Datenräumen die weitreichenden Beschränkungen der DSGVO eingehalten werden müssen. <sup>1</sup>

## **Dieses Dokument erläutert:**

- wann maschinengenerierte Sensordaten der DSGVO unterfallen;
- wie für einen Datenraum durch Nutzungsbedingungen die Beschränkungen der DSGVO wesentlich begrenzt werden können.

<sup>1</sup> Natürlich könnte man auch die Anforderungen der DSGVO ignorieren, da das Risiko der Verfolgung durch Behörden sicherlich geringer sein wird als in vielen anderen Fällen von DSGVO-Verstößen. Dennoch muss man wissen, dass dann weder die Bereitstellung der Daten noch deren Nutzung im Datenraum zulässig wäre. Das würde voraussichtlich viele Unternehmen von der Nutzung des betreffenden Datenraumes abhalten.

# 1. Der Personenbezug von maschinengenerierten Daten

Für einen Personenbezug reicht es aus, dass sich Daten auf eine identifizierbare Person beziehen (Art. 4 Nr. 1 DSGVO). Die Person muss nicht bereits identifiziert sein – es genügt, dass die Zuordnung mit Hilfe weiterer Informationen möglich ist.

## Beispiele:

- Maschinensteuerung / Bedienzeitpunkte: **personenbezogen**, da Rückschlüsse auf das Verhalten der Bedienperson möglich sind (Bedienfehler, Pausenverhalten, Effizienz); allein ist zwar meistens keine Zuordnung möglich – aber mit Schichtplan und Zeitstempel – also "weiteren Informationen" – sind diese Daten einer Person zuordenbar.
- Umgebungsdaten (z.B. Temperatursensor für Umgebungstemperatur): **nicht personenbezogen**, wenn sie nur Rückschlüsse über die allgemeinen Umstände zulassen, denen eine Person ausgesetzt ist.

## Aber: Der Personenbezug ist relativ!

Die Frage, ob Daten personenbezogen sind, wird für jeden Teilnehmer an einem Datenraum getrennt gestellt. Können Teilnehmer an einem Datenraum faktisch und rechtlich nicht auf die zur Identifizierung der betroffenen Person erforderlichen weiteren Informationen (im Beispiel Schichtplan und Zeitstempel) zugreifen, sind die maschinengenerierte Sensordaten für sie nicht personenbezogen.

## 2. Relevanz für die Nutzungsbedingungen eines Datenraumes

Die Nutzungsbedingungen des Datenraumes müssen sicherstellen, dass die im Datenraum bereitgestellten Daten für die Datennutzer nicht personenbezogen sind. Nur dann können die Datennutzer diese Daten ohne DSGVO-Beschränkungen nutzen.

### Was muss dafür geregelt werden?

- Der Bereitsteller der betreffenden Daten sollte durch die Nutzungsbedingungen verpflichtet werden, nur pseudonymisierte Daten bereitzustellen.
- Die Nutzungsbedingungen sollten sicherstellen, dass Daten erst dann in den Datenraum gelangen, wenn ein "Gatekeeper" bestätigt hat, dass die Daten tatsächlich pseudonymisiert sind.

### Verständnisfrage: Warum sollen die Daten durch den Bereitsteller der Daten nur pseudonymisiert und nicht direkt anonymisiert werden?

- Tatsächlich würde eine Anonymisierung i.S.d. DSGVO den Personenbezug der betreffenden Daten für jeden, also auch für den Bereitsteller der Daten entfernen. Allerdings ist eine Anonymisierung unter Aufrechterhaltung der Nutzbarkeit der Daten derzeit rechtlich nicht verlässlich möglich.
- Demgegenüber bleiben bei der Pseudonymisierung die inhaltlichen Informationen (z. B. Maschinenmetriken, Verhaltensmuster, Zeitreihen) unangetastet; die Identitätsinformationen werden lediglich abgetrennt, verlagert und gesondert kontrolliert, aber eben nicht vernichtet.

# Exkurs: Anonymisierung ↔ Pseudonymisierung

**Kernunterschied i.S.d. DSGVO:** Anonymisierung beseitigt den Personenbezug für alle – Pseudonymisierung nur für Dritte, nicht aber für denjenigen, der für die Pseudonymisierung verantwortlich ist.

| Anonymisierung |                                                                                                          | Pseudonymisierung |                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ergebnis       | Daten, die durch niemanden mehr einer Person zugeordnet werden können                                    | Ergebnis          | Identifikatoren werden durch einen Schlüssel ersetzt;<br>→ <b>nur</b> derjenige, der für die Pseudonymisierung verantwortlich ist, kann noch re-identifizieren |
| Schlüssel      | Kein Schlüssel<br>Re-Identifizierung ist nicht mehr möglich (auch nicht für den Bereitsteller der Daten) | Schlüssel         | Schlüssel existiert und verbleibt beim Bereitsteller                                                                                                           |
| Folge          | DSGVO gilt nicht mehr<br>(kein Personenbezug für alle)                                                   | Folge             | DSGVO gilt nicht für diejenigen, die pseudonymisierte Daten erhalten (gilt aber weiterhin für denjenigen, der für die Pseudonymisierung verantwortlich ist)    |
| Praxis         | Kaum erreichbar bei gleichzeitiger Nutzbarkeit der Daten                                                 | Praxis            | <b>Praktisch umsetzbar</b>                                                                                                                                     |

### 3. Erläuterung

#### **Verständnisfrage: Warum sollen die Daten durch den Bereitsteller der Daten überhaupt pseudonymisiert werden?**

Natürlich kann man behaupten, dass ein Datennutzer von Daten in einem Datenraum nie Zugriff auf Zusatzinformationen wie einen Schichtplan (siehe Beispiel auf Folie 3) aus dem Unternehmen des Datenbereitstellers hat. Allerdings können Sensordaten auch direkt identifizierende Informationen (z.B. Klarname-Login) beinhalten, insoweit müsste der Datenbereitsteller immer pseudonymisieren. Statt in Bezug auf jeden Datensatz eine Einzelfallprüfung vorzunehmen, könnte durch eine allgemeine Pflicht zur Pseudonymisierung ein erhöhtes Vertrauen in die Nutzbarkeit der Daten im Datenraum geschaffen werden.

#### **Verständnisfrage: Warum ist ein Gatekeeper erforderlich (siehe Folie 4)?**

Ein Gatekeeper ist aus rechtlicher Sicht nicht erforderlich. Verstößt aber ein Datenbereitsteller gegen die in den Nutzungsbedingungen geregelte Pflicht zur Pseudonymisierung, gelangen Daten, die dann auch für alle Datennutzer personenbezogen sind, in den Datenraum. Dann unterliegen alle Datennutzer den umfänglichen Anforderungen der DSGVO. Durch einen Gatekeeper, der die Mittel hat, Daten in Bezug auf eine erfolgreiche Pseudonymisierung zu prüfen, würde eine weitere Absicherung geschaffen und das Vertrauen der Datennutzer in die Nutzbarkeit der Daten im Datenraum erhöht.



### 3. Erläuterung

#### **Verständnisfrage: Lässt eine Pseudonymisierung durch den Datenbereitsteller den Personenbezug für Datennutzer immer entfallen?**

Eine Pseudonymisierung lässt den Personenbezug für den Datennutzer nur dann entfallen, wenn die Maßnahmen tatsächlich geeignet sind, eine Zuordnung auch mittels sonstiger verfügbarer Identifizierungsmittel – etwa durch Datenabgleich – zu verhindern. Ist der Datennutzer trotz (formaler) Pseudonymisierung durch den Datenbereitsteller in der Lage, die Daten über andere Mittel einer Person zuzuordnen, bleibt der Personenbezug für ihn bestehen.

**Beispiel:** Beim Datennutzer handelt es sich um den Maschinenhersteller, dem bekannt ist, welcher Mitarbeiter des Datenbereitstellers die konkrete Maschine bedient. Dann sind die betreffenden Sensordaten für den Maschinenhersteller trotz formaler Pseudonymisierung unverändert personenbezogen.