Die EU-DSGVO und die „anonymen Daten“

Kann man und wann kann man Daten nach der EU-DSGVO als „anonym“ ansehen?

23.05.2016

Gerald Spyra,
LL.M.
Kanzlei Spyra

gerald.spyra@kanzlei-spyra.de

Vorstellung meiner Person

Gerald Spyra, LL.M.

- **Rechtsanwalt**
- **Hohe Affinität für die Informationssicherheit**
- **Spezialisiert auf:**
  - **den Informations- / Datenschutz,**
  - **das Software-Medizinprodukterecht**
  - **die IT-Forensik**
- **Externer betrieblicher Datenschutzbeauftragter**

gerald.spyra@kanzlei-spyra.de

Vorbemerkung

- **Von vielen Seiten hört man, dass es mit Geltung der EU-Datenschutzgrundverordnung (VO) keine anonymen Daten mehr geben soll!?**

- **Dieses insbesondere deshalb, weil die „Anonymisierung“ bzw. der Begriff „anonym“ nicht mehr in den Regelungen der VO erwähnt ist.**

- **Kurz und bündig:**
  „Weil die „Anonymisierung“ nicht in den Regelungen enthalten ist, gibt es sie auch nicht mehr“!

- **Aber so leicht ist es wiederum auch nicht…**

gerald.spyra@kanzlei-spyra.de

Die Geltung der EU-DSGVO

- Die VO enthält in ihren Regelungen **nur Vorgaben** dazu, **wann** sie **Anwendung** findet.

- Sie **findet** immer dann **Anwendung**, wenn Daten verarbeitet werden (sollen), die einen **Personenbezug ermöglichen** bzw. eine Person mittels dieser Daten „**identifizierbar**“ ist / wird.

- Im **Umkehrschluss** muss dieses aber auch bedeuten, dass die **Regelungen** der VO **keine Anwendung** finden, wenn die **Daten keinen Personenbezug** (mehr) zulassen.

- In diesem Punkt ähneln die Regelungen der VO auch der **Datenschutz-Richtlinie 95/46/EG**.

gerald.spyra@kanzlei-spyra.de

Die Anonymität in der EU-DSGVO

- **Dass es aber weiterhin „anonyme“ Daten gibt / geben soll, sagt bspw. Erwägungsgrund (EG) 26.**

- **EG 26 ist der maßgebliche Erwägungsgrund u.a. zur Regelung von Artikel 4 Nr. 1 der VO, in dem „personenbezogene Daten“ definiert werden…**

- **N.B.: Leider ist dieser EG „nur“ ein Erwägungsgrund (Auslegungshinweis) und keine eigenständige Regelung im Verordnungstext!**

gerald.spyra@kanzlei-spyra.de

EG 26 (Teil 1)

- **So heißt es in EG 26:**

„Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten,

d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen,

ODER

personenbezogene Daten, die in einer Weise ANONYMISIERT worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“

- **Nach EG 26 existieren deshalb „zwei Möglichkeiten“ für anonyme Daten…**

gerald.spyra@kanzlei-spyra.de

EG 26 – die „zwei Möglichkeiten“

- EG 26 zeigt „zwei Möglichkeiten“ auf, wann Daten anonym sind / werden können.
  - 1. Daten sind von „Natur“ aus anonym
  - 2. Personenbezogene Daten werden so verarbeitet (Art. 4 Nr. 2 = Erlaubnistatbestand notwendig), dass sie „anonym“ werden und bleiben…

- Das bedeutet mithin, dass wann immer eine Person (für wen auch immer) mittels entsprechender Informationen identifizierbar ist, die Daten nicht mehr anonym sein können.

- Und wann eine Person (re-) identifizierbar ist bzw. (re-) identifiziert werden kann, sagt uns auch EG 26…

gerald.spyra@kanzlei-spyra.de

Erwägungsgrund 26 – (Re-)Identifizierbarkeit

- ***„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“.***

- **1. Voraussetzung:**
- **Der Verantwortliche oder (jede) andere Person = KEINER darf mehr in der Lage sein, eine Person mittels der Daten zu (re-) identifizieren.**

- **2. Voraussetzung:**
- **Es gilt ferner alle zur Verfügung stehenden Mittel zu berücksichtigen (und ihre „Kombination“), die nach allgemeinen Ermessen, wahrscheinlich genutzt werden (können), um eine Person zu identifizieren….**

gerald.spyra@kanzlei-spyra.de

Erwägungsgrund 26 – Mittel

- ***„Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“***

- **Alle objektiven Faktoren müssen deshalb herangezogen werden, wozu bspw. die zu Verfügung stehenden Ressourcen wie:**
  - **Kosten / Zeit oder**
  - **technologische Entwicklungen (zum Zeitpunkt der Verarbeitung) gehören.**

- **Damit lässt sich nun auch das Verhältnis „anonymer“ zu „pseudonymer“ Daten darstellen…**

gerald.spyra@kanzlei-spyra.de

Verhältnis anonymer vs. pseudonymer Daten

- **Pseudonyme Daten können niemals anonyme Daten sein (siehe auch WP 216 der Art. 29 Gruppe)!**
- **Diese, von der Art. 29 Datenschutzgruppe vertretene Ansicht, wird höchstwahrscheinlich auch beim EU-Datenschutzausschuss, der die Art. 29 Gruppe ersetzt (und gleich besetzt sein wird) fortbestehen.**
- **Sobald deshalb (bei wem auch immer) eine Zuordnungsregelung existiert, fehlt es an der „Anonymität" von Daten (Vgl. Art. 4 Nr. 5).**
- **Die „faktische Anonymität" dürfte es damit nicht mehr geben.**
- **Daher lassen sich folgende Schlüsse ziehen....**

gerald.spyra@kanzlei-spyra.de

Zusammenfassung – „Anonyme Daten“

- Es gibt auch **mit Geltung** der **VO** weiterhin noch **anonyme Daten**.
- Anonyme Daten zeichnet aus, dass **KEINER** mehr aus ihnen eine **Identifizierung** einer Person (mit seinen Mitteln) vornehmen kann.
- Ferner zeichnet anonyme Daten aus, dass sie entweder
  - von „**Natur**“ aus anonym sind oder
  - durch eine **entsprechende Verarbeitung** anonym werden (und bleiben).
- Daten aus dem **medizinischen Umfeld** und die zur **Verfügung stehenden Identifizierungsmöglichkeiten**, lassen die **erste Alternative** (von „Natur“ aus anonym) jedoch immer **weniger wahrscheinlich** werden…

gerald.spyra@kanzlei-spyra.de

Begebenheiten, die die „Anonymität“ von Daten in Frage stellen können… (1)

- Viele der im Gesundheitsbereich verwendeten Daten sind so „verdichtet“, dass sie oftmals von sich aus eine (Re-) Identifizierung ermöglichen.

- Ferner gilt es folgende Aspekte zu berücksichtigen:
  - Einzelne atypische Vorkommnisse lassen eine Person, direkt identifizierbar werden (z. B. der Mann mit Brustkrebs).
  - Moderne Technik gewinnt aus vermeintlich als anonym angesehenen Daten personenbeziehbare Informationen (z. B. Möglichkeit der 3D- Konstruktion eines Gesichts aus Röntgenbildern).
  - Immer mehr „smarte“ Geräte des Alltags „tracken“ Nutzer und ihre Tätigkeiten (Metadaten)
  - „BigData“ eröffnet Möglichkeit, Daten praktisch „unendlich“ miteinander bzw. anderen Daten zu kombinieren;

gerald.spyra@kanzlei-spyra.de

Begebenheiten, die die „Anonymität“ von Daten in Frage stellen können… (2)

- Und noch mehr:
  - Der „genetische Fingerabdruck“ (70 SNPs reichen meistens aus – oftmals auch weniger);
  - Der Aufbau öffentlicher / privater Gen- / Biobanken, ihre Vernetzung und der Austausch von Daten / gemeinsame Verarbeitungsmöglichkeiten ermöglichen (Re-) Identifizierbarkeit;
  - Die steigende „Mitteilungsbedürftigkeit“ über „social networks“ ermöglicht, die preisgegeben Daten mit medizinischen Daten in Kontext zu setzen;
  - …

- Aufgrund der vielen Unsicherheitsfaktoren bei „anonymen“ Daten sollte man deshalb prüfen, ob man die Daten nicht entsprechend der zweiten Alternative „bearbeiten“ kann, um sie „anonym“ nutzen zu können.

gerald.spyra@kanzlei-spyra.de

„Anonymisierung“ als Verarbeitung

- Die „Anonymisierung“ / „Pseudonymisierung“ von Daten stellt wie bisher einen Verarbeitungsvorgang (Art. 4 Nr. 2) dar.

- Daraus folgt, dass auch zur „Anonymisierung“ ein Ermächtigungsgrund dem Verantwortlichen zur Verfügung stehen muss.

- Dem Verbot mit Erlaubnisvorbehalt folgend, kann dieser entweder eine (wirksame) Einwilligung des Betroffenen oder eine gesetzliche Regelung sein.

gerald.spyra@kanzlei-spyra.de

Legitimation durch VO / Rechtsvorschrift

- Die Regelungen der VO sind abschließend (VO geht deutschen Regelungen vor / verdrängt sie).
- Es existiert kein expliziter Legitimationstatbestand für die „Anonymisierung“ in der VO.
- Jedoch existieren „Nationale Öffnungsklauseln“ für die Verarbeitung von Gesundheitsdaten.
- Damit ist der bzw. die deutschen Gesetzgeber gefordert, neue Regelungen zu schaffen bzw. vorhandene Regelungen wie § 28 Abs. 6, Abs. 7 BDSG beizubehalten.
- Ansonsten existiert die Möglichkeit der Einwilligung des Betroffenen, die jedoch auch nicht ohne Probleme ist…

gerald.spyra@kanzlei-spyra.de

Legitimation durch Einwilligung

- Weiterhin besteht die Möglichkeit, die Einwilligung des Betroffenen in die „Verarbeitung“ seiner Daten einzuholen.

- Diese muss jedoch den Anforderungen der VO nach insbesondere informiert, freiwillig sein und sich auf einen bzw. mehrere festgelegte Zwecke beziehen.

- Daher besteht ein Problem der Einwilligung beim „broad consent“ (wann ist es noch „bestimmt“ genug?).

- Ein weiteres Problem existiert bei der Einwilligung bei der Verarbeitung bestimmter Daten....

gerald.spyra@kanzlei-spyra.de

Herausforderung bei der Einwilligung bei „besonderen“ Daten

- Soll die **Einwilligung** in die Verarbeitung von Daten gegeben werden, die **nicht nur den Einwilligenden betreffen**, treten naturgemäß weitere Fragestellungen auf.

- Kann der **Betroffene** etwa in die Verarbeitung dieser Daten **einwilligen**, wenn sie bspw. auch **seine Vorfahren**, **Nachfahren**, **Familienangehörigen** betreffen?

- Lässt sich hierfür eine **gesetzliche Legitimation** schaffen (**Nationale Öffnungsklausel für genetische Daten**)?

- Und selbst wenn man eine Legitimation hat, muss man sich dann noch mit der **Frage** auseinandersetzen, welchen **Wert** als „**anonymisiert anzusehende Daten**“ für die **moderne Forschung** überhaupt noch haben können?

gerald.spyra@kanzlei-spyra.de

Nutzen von „anonymisierten“ Daten

- **Selbst wenn man Daten rechtskonform „anonymisiert“ hat, bleibt stets die Frage, ob sich die „anonymisierten“ Daten dann noch für die mit der jeweiligen Forschung beabsichtigten Zwecke überhaupt eignen.**

- **Die zu ergreifenden technischen und organisatorischen Maßnahmen, um einen Personenbezug auszuschließen, dürften die Nutzbarkeit von „anonymisierten Daten“ deutlich limitieren / reduzieren.**

- **Und daher gibt es viel zu diskutieren…**

gerald.spyra@kanzlei-spyra.de

Gibt es noch Fragen?

Gerald Spyra, LL.M.
Rechtsanwalt,
externer Datenschutzbeauftragter

www.recht-technisch.de

gerald.spyra@kanzlei-spyra.de

Kanzlei Spyra
Kaiserstr. 7
51688 Wipperfürth

Vielen Dank für Ihr Interesse!

gerald.spyra@kanzlei-spyra.de