**Wirtschaftsrat der CDU e.V.**
Luisenstr. 44, 10117 Berlin
Telefon: 0 30 / 240 87 - 216
Telefax: 0 30 / 240 87 - 205
E-Mail: t.koppitz@wirtschaftsrat.de

# Anwendungsfelder und Auswirkungen der EU-Datenschutzgrundverordnung auf den Bereich Digital Health!

***In den vergangenen 20 Jahren wurde unser Leben durch kaum etwas so stark verändert wie durch das Internet und die Verbreitung digitaler Technologien. Das trifft auch auf das Gesundheitswesen zu.***

***Die Datenpolitik ist ein Schlüsselelement der Standortpolitik in Zeiten der Digitalisierung. Gerade im Bereich digitaler Gesundheitsanwendungen basieren Geschäftsmodelle vielfach auf der Sammlung und Auswertung aller erdenklichen Daten. Big Data kann völlig neue Diagnosen, Gesundheitsanwendungen und Therapien ermöglichen. Dafür benötigen wir einen europäischen Rechtsrahmen, der es erlaubt, personenbezogene Daten anonymisiert bzw. pseudonymisiert zu erheben und zu nutzen. Da sich der Wert der Daten oftmals erst nach dem Zeitpunkt ihrer Erhebung ergibt, ist ein flexibles Gerüst erforderlich, das auch deren Nutzung erlaubt.***

***Dazu bedarf es dringend der Überprüfung und Anpassung des nationalen und internationalen Rechtsrahmens hinsichtlich der Datenspeicherung, -übertragung und -nutzung.***

Umstritten und weiterhin klärungsbedürftig in den fortschreitenden Verhandlungen um die **EU-Datenschutzgrundverordnung** sind die folgenden Punkte:

## 1. Definition des Schutzbedürfnisses unterschiedlicher Daten

Personenbezogene Daten gehören grundsätzlich den Personen selbst. Eine Verarbeitung solcher Daten kann grundsätzlich nur mit Einverständnis des Betroffenen erfolgen. Verschlüsselte, anonymisierte wie auch sichere pseudonymisierte Daten sind keine personenbezogenen Daten. Aus Gründen der Sicherheit vor Diebstahl und Missbrauch dürfen im Netz und in der Cloud keine personenbezogenen Daten transportiert bzw. gespeichert werden, d.h. sie müssen verschlüsselt, anonymisiert oder sicher pseudonymisiert sein und dürfen erst auf dem Benutzergerät (Client) im Klartext mit Personenbezug verwendet werden.

Pseudonymisierte Daten gelten nur dann als sicher, wenn sie nicht durch Dritte zurück verfolgbar sind, also der entsprechenden Person wieder zugeordnet werden können.
Wenn pseudonymisierte Daten technisch nur mit dem individuellen Schlüssel der betroffenen Person dieser wieder

zugeordnet werden können, entfällt die Schutzbedürftigkeit der Daten im Hinblick auf die weitere Verwendbarkeit der Daten (z.B. Forschung etc.).

Der Entfall der Schutzbedürftigkeit gilt auch für vollständig anonymisierte Daten.

Nicht schutzbedürftige Daten sollten einem Opt-Out Verfahren, schutzbedürftige Daten einem Opt-In Verfahren hinsichtlich der wissenschaftlichen und kommerziellen Verwertung unterliegen.

**2. Einwilligung**

Nach dem derzeitigen Verordnungsentwurf würde die Verarbeitung von Gesundheitsdaten für statistische und wissenschaftliche Zwecke eine Einwilligung voraussetzen. Auch wenn das Parlament hier einen Ausnahmetatbestand vorschlägt, bleiben dessen Voraussetzungen weiterhin unklar. Ausnahmen soll es danach geben bei einem „hohen öffentlichen Interesse“ und wenn die Forschung „nicht anders ausgeführt werden kann“. Diese Unklarheiten sollten in der weiteren Diskussion ausgeräumt werden. Dabei sollte für Daten mit Schutzbedürfnis der Verbotsvorbehalt Vorrang vor dem Erlaubnisvorbehlat haben.

**3. Big Data / Erlaubnis, Gesundheitsdaten zu pseudonymisieren oder anonymisieren**

Grundsätzlich sind in Deutschland die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (vgl. § 4 BDSG).

Bei der Verarbeitung sind die Daten in der Regel der Zweckbindung unterworfen, d.h. sie dürfen nur zu dem Zweck verwendet werden, zu dem sie ursprünglich erhoben wurden. Eine Zweckänderung liegt dementsprechend vor, wenn die Verarbeitung der Daten zu einem anderen Zweck, als dem ursprünglichen, erfolgen soll. Gerade vor dem Hintergrund der zunehmenden und vielversprechenden Big Data Anwendungen ist diese Einschränkung hinderlich. Zudem wird die Verwertbarkeit von Daten durch das Gebot der Datensparsamkeit behindert. Die Datenschutzgrundverordnung sollte innovative Big Data Anwendungen fördern, anstatt diese zu bremsen.

Zudem besteht das Risiko, dass Artikel 9 des Verordnungsentwurfes dahingehend ausgelegt werden kann, dass die Herstellung von pseudonymen oder anonymen Daten verboten ist. Die Verordnung sollte Pseudonymisierung und Anonymisierung aber gerade ermutigen und nicht beschränken. Der Akt des Herstellens pseudonymer oder

anonymer Daten stellt eine Form der Datenverarbeitung dar. Während bei „normalen“ Daten hier eine Rechtfertigung unter dem Gesichtspunkt des legitimen Interesses gegeben sein wird, gibt es für sensible Daten (z.B. Gesundheitsdaten) keine ausdrückliche Erlaubnis dafür. Um eine allzu strikte Auslegung der Verordnung, wonach die Anonymisierung oder Pseudonymisierung verboten ist, zu vermeiden, sollte eine generelle Erlaubnis dafür in den Verordnungstext eingeführt werden. Alternativ könnte eine Anonymisierung oder Pseudonymisierung auch als vom Verordnungszweck umfasst angesehen werden. Sollte in besonders sensiblen Bereichen, wie beispielsweise der Gesundheitsforschung, die Anonymisierung generell ausscheiden, um eine Rückverfolgbarkeit der Daten sicherzustellen, sollte ebenfalls die Pseudonymisierung ermöglicht werden. Wichtig ist, dass auf Seiten der Anwender Rechtsicherheit hergestellt wird.

**4. Keine Ausnahmen**

Ziel der Datenschutzgrundverordnung ist es, einheitliche Regeln in Europa zu formulieren und die Verwirklichung gleicher Standards in der gesamten EU. Vereinzelte Tendenzen, den Mitgliedsstaaten Ausnahmen für teilweise strengere Regeln zu ermöglichen, laufen diesem Verordnungszweck zuwider. Ausnahmetatbestände sollten daher auf ein absolutes Minimum reduziert werden. Wo entsprechende Regeln unbedingt erforderlich erscheinen, sollte deren Regelung klar definiert und abschließend in der Verordnung erfolgen.

Berlin, im August 2015