

# **ACHTUNG BEACHTEN SIE AB 25. Mai 2018 DIE NEUE DATENSCHUTZGRUNDVERORDNUNG 2016/679**

Kurzüberblick zum Thema Datenschutzgrundverordnung 2016/679.

**WARUM** verordneter Datenschutz?

Personenbezogene Daten sind persönliche Daten, die nur die Person selbst ermächtigt den Umfang als auch den Inhalt im außerbehördlichem Bereich weiterzugeben bzw. Ermächtigungen für die Weiterverarbeitung erteilen kann.

Daher wurde für den Schutz der personenbezogenen Daten eine europäische Datenschutzgrundverordnung geschaffen.

**WANN** tritt diese Verordnung in Kraft?

Mit 25.Mai 2018

**WER** muss diese Verordnung einhalten?

Die DSGVO müssen alle Unternehmen und öffentliche Stellen innerhalb der EU beachten, die personenbezogene Daten verarbeiten, sowie alle Unternehmen aus Drittstaaten, wenn diese Produkte und Leistungen in der EU anbieten.

**WAS** kann passieren, wenn diese Verordnung nicht eingehalten wird?

Der Strafraum bei Verletzungen bzw. Missachtung der DSGVO beträgt bis zu 20 Mio. Euro oder bis zu 4% des Gesamtumsatzes. (Je nach dem welcher Wert höher ist).

**WAS** bedeutet personenbezogene Daten?

Alle Daten die eine Person direkt oder indirekt identifizieren. (Name, Emailadresse, IP-Adresse, .....)

*„Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.*

*Hinzuzählen auch IP-Adressen (dynamisch als auch fix zugeordnete, Cookie-Kennungen, etc.)*

*Auch Informationen über die natürliche Person, die im Zuge der Anmeldung sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, ...“*

**WAS** bedeuten besondere Kategorien personenbezogener Daten?

Das sind personenbezogene Daten, aus denen die **rassische** und **ethnische** Herkunft, **politische** Meinungen, **religiöse** oder **weltanschauliche** Überzeugungen oder die **Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von **genetischen** Daten, **biometrischen** Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum **Sexualleben** oder der **sexuellen Orientierung** einer natürlichen Person.

Diese Daten zu verarbeiten ist **UNTERSAGT** die Verarbeitung ist nur unter bestimmten Voraussetzungen erlaubt.

Bei den Besuchen im Unternehmerumfeld und dem Hinweis auf die DSGVO 2016/679 sind einige Gerüchte bzw. Falschinterpretationen aufgetaucht.

Wie zum Beispiel folgende:

*„Unter 250 Mitarbeitern betrifft mich keine DSGVO“* **IST ein Gerücht.**

Unter 250 Mitarbeitern sollte es eine erleichterte Dokumentationspflicht geben, die Ausnahmen sind jedoch so formuliert, dass diese Ausnahmen so gut wie kein Unternehmen betreffen.

*„Warum sollte gerade mein Unternehmen geprüft werden?“* **ACHTUNG!**

Aufgrund der Meldepflicht an die Aufsichtsbehörde über eine Verletzung von personenbezogenen Daten beginnt ein Prozess der Überprüfung. Keine Meldung, also eine Meldepflichtverletzung kann eine Strafe von 20Mio. auslösen.

Eine Meldung an die Aufsichtsbehörde kann natürlich auch unabhängig des betroffenen Unternehmens, von jeder Person die eine Verletzung der Datenpflicht vermutet, erfolgen.

*„Ich habe nur mit Firmen zu tun“* **ACHTUNG!**

Einzelunternehmen fallen -auch wenn Sie im Firmenbuch eingetragen sind (e.U.) - unter personenbezogene Daten.

Ansprechpartner fallen unter personenbezogene Daten.

Mitarbeiter fallen unter personenbezogene Daten und unter **sensible** Daten.

Bewerber fallen unter personenbezogene Daten und wussten Sie, dass Sie Bewerbungsdaten 6 Monate nach Ablehnung bzw. Mitteilung über die Nichtanstellung löschen müssen?

Sollten Sie diesbezüglich Fragen haben, stehe ich Ihnen als „geprüfter Datenschutzexperte“ sehr gerne zur Verfügung.

Testen Sie Ihr DSGVO-Wissen unter

<http://www.chvaco.at/dsgvo-2016/679/>

(Der Test ist Anonym, wir speichern keine Ergebnisse)



Andreas Chvatlinsky, MBA, Dipl.-Bw  
Geprüfter DSGVO-Datenschutzexperte  
Unternehmens- und Organisationsberater  
Geschäftsführender Gesellschafter der  
Chvatlinsky & Co GmbH