

# „Datenschutz(grund)verordnung“

## EU DS GVO

Ein Vortrag im Rahmen des  
Datenschutzaufklärungsabend 2018.8

# „Europäische Datenschutz Grundverordnung“

## *Allgemeines*

### Geltungszeitraum

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN  
PARLAMENTS UND DES RATES

vom 27. April 2016

# „Europäische Datenschutz Grundverordnung“

## *Allgemeines*

### Geltungszeitraum

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN  
PARLAMENTS UND DES RATES

vom 27. April 2016

Die Richtlinie 95/46/EG wird mit Wirkung vom **25. Mai 2018**  
aufgehoben.

# „Europäische Datenschutz Grundverordnung“

## *Allgemeines*

### Ziele der EU DS GVO

# „Europäische Datenschutz Grundverordnung“

## *Allgemeines*

### Ziele der EU DS GVO

Der Schutz der **Personenbezogenen Daten**  
einer *natürlichen Person*.

# „Europäische Datenschutz Grundverordnung“

## Artikel 1

- (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

# „Europäische Datenschutz Grundverordnung“

## *Allgemeines*

### Ziele der EU DS GVO

Der Schutz der Personenbezogenen Daten  
einer natürlichen Person.

Grundregeln für die Datenverarbeitung solcher Daten

# „Europäische Datenschutz Grundverordnung“

## Artikel 4

2. „**Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie **das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung**, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;



# „Europäische Datenschutz Grundverordnung“

## Artikel 24-43

Die Artikel 24-43 der EU DS GVO bestimmen u.a. die

„Verantwortung des Verantwortlichen“

„Wie Technik datenschutzfreundlich gestaltet sein muß“

„Was Auftragsdatenverarbeiter dürfen und müssen“

„Die Sicherheit der Verarbeitung“

„Die Stellung und Aufgaben eines Datenschutzbeauftragten“

# „Europäische Datenschutz Grundverordnung“

## *Allgemeines*

### Ziele der EU DS GVO

Der Schutz der Personenbezogenen Daten  
einer natürlichen Person.

Grundregeln für die Datenverarbeitung solcher Daten

Strafen für Datenschutzvergehen sicherstellen

# „Europäische Datenschutz Grundverordnung“

## Artikel 83

### Allgemeine Bedingungen für die Verhängung von Geldbußen

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

- a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
- b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

# „Europäische Datenschutz Grundverordnung“

## *Allgemeines*

### Ziele der EU DS GVO

Der Schutz der Personenbezogenen Daten  
einer natürlichen Person.

Grundregeln für die Datenverarbeitung solcher Daten

Strafen für Datenschutzvergehen sicherstellen

Die Zusammenarbeit auf europäischer Ebene regeln

# „Europäische Datenschutz Grundverordnung“

Wer muß sich eigentlich an die DSGVO halten ?

# „Europäische Datenschutz Grundverordnung“

## Artikel 2

(1) Diese Verordnung **gilt für** die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte **Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.**

(2) Diese Verordnung **findet keine Anwendung** auf die Verarbeitung personenbezogener Daten

...

c) **durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,**

d) **durch die zuständigen Behörden zum Zwecke** der Verhütung, Ermittlung, Aufdeckung oder **Verfolgung von Straftaten** oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 1:

**Sie schreiben den Namen Ihres Bruders für Ihre Schwester auf.**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 1:

Sie schreiben den Namen Ihres Bruders für Ihre Schwester auf.

**DS GVO gilt nicht.**



# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 2:

**Sie schreiben den Namen eines Anrufers in Ihren Terminkalender.**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 2:

Sie schreiben den Namen eines Anrufers in Ihren Terminkalender.

**DS GVO gilt, wenn der Termin nicht rein privat ist.**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 2:

Sie schreiben den Namen eines Anrufers in Ihren Terminkalender.

**DS GVO gilt, wenn der Termin nicht rein privat ist.**

**Kommt sogar noch schlimmer!**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 2:

Weil Sie den Namen in ein „Ordnungssystem“ abh. Kalender eintragen wollen, müssen Sie den Anrufer **vorher** darauf hinweisen, wie **Sie** seine Daten bei sich schützen.

Sie müssen ihm min. den Rechtsgrund, die Dauer und die Schutzmaßnahmen der Speicherung seiner Personenbezogenen Daten mitteilen.

Eine Folgeabschätzung, welchen Schaden er nimmt, wenn Ihr Kalender abhanden kommt, müßte auch von Ihnen durchgeführt werden.

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 2:

Weil Sie den Namen in ein „Ordnungsregister“ eintragen wollen, müssen Sie den Auftraggeber auf die DSGVO hinweisen, wie Sie seine Daten verarbeiten werden.

Sie müssen ihm die Rechtsgrundlage, die Dauer und die Schutzmaßnahmen für die Verarbeitung seiner Personenbezogenen Daten mitteilen.

Die Risikoprüfung, welchen Schaden er nimmt, wenn Ihr Unternehmen mit seinen Daten umgeht, müsste auch von Ihnen durchgeführt werden.

**Datenschutzerklärung**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

**Artikel 13** definiert die Pflichten des Datenverarbeiters  
( in diesem Fall Sie ) u.A. mit :

**Absatz 1:** „Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgendes mit:

**Name des Verantwortlichen, Kontaktdaten, den Zweck, die berechtigten Interessen, alle Empfänger der Daten, die Rechte des Besitzers der gespeicherten Daten, usw. usw.**

„Europäische Datenschutz Grundverordnung“

Entspannen Sie sich wieder !

Keine Panik

„Europäische Datenschutz Grundverordnung“

„Artikel 32 ist Ihr Freund.“



# „Europäische Datenschutz Grundverordnung“

## Artikel 32

### Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 3:

Sie haben eine Webseite, die nur für Freunde und Verwandte ist.

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 3:

Sie haben eine Webseite, die nur für Freunde und Verwandte ist.

**DS GVO gilt nicht Sie.**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 4:

Sie haben eine Webseite, die für die Öffentlichkeit ist.

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 4:

Sie haben eine Webseite, die für die Öffentlichkeit ist.

**DS GVO gilt.**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 5:

Sie tragen die Nummer Ihrer Freunde bei Whats App ein.

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 5:

Sie tragen die Nummer Ihrer Freunde bei Whats App ein.

**DS GVO gilt.**

# „Europäische Datenschutz Grundverordnung“

## Beispiele – Wann gilt die GVO

### Beispiel 5:

Sie tragen die Nummer Ihrer Freunde bei Whats App ein.

**DS GVO gilt.**

**Und es kommt noch schlimmer!**



„Europäische Datenschutz Grundverordnung“

**WHATS APP ist ILLEGAL !**

„Europäische Datenschutz Grundverordnung“

## WHATS APP ist ILLEGAL !

Weil Sie Personenbezogene Daten von natürlichen Personen **ohne deren ausdrückliche Genehmigung** an Dritte (What's App) übermitteln,...

... und das auch noch ausgerechnet in die USA!

[http://www.lareda.hessenrecht.hessen.de/lexsoft/default/hessenrecht\\_lareda.html#docid:7860914](http://www.lareda.hessenrecht.hessen.de/lexsoft/default/hessenrecht_lareda.html#docid:7860914)

# „Europäische Datenschutz Grundverordnung“

Webseiten – Datenschutz was tun?

Einige Fälle aus der Praxis

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 1:

Sie haben Ihre Webseite in Panik gelöscht

und jetzt ist nur noch eine weiße Seite unter Ihrer Domain erreichbar.

**Sie nehmen an, daß Sie jetzt aus der DS Nummer raus sind.**

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 1:

Sie haben Ihre Webseite in Panik gelöscht

**Sie haben sich leider geirrt!**

# „Europäische Datenschutz Grundverordnung“

## Datenschutzerklärung

Webserver speichern den Aufruf der leeren Webseite in Ihrem Serverlogfile. Damit entsteht eine Verarbeitung und Speicherung von personenbezogenen Daten, da IP Adressen als personenbezogene Daten gelten.

**Sie brauchen für Ihre leere Webseite eine Datenschutzerklärung.**

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 2:

Sie haben auf Ihrer Webseite ein Kontaktformular.

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 2:

Sie haben auf Ihrer Webseite ein Kontaktformular.

Sie müssen die Webseite jetzt aufgrund von **Artikel 32** mit einem **SSL-Zertifikat** versehen und über **HTTPS** erreichbar machen.

Ferner müssen Sie sicherstellen, daß eine Datenübertragung per ungesicherter **HTTP** Verbindung nicht mehr möglich ist.



# „Europäische Datenschutz Grundverordnung“

## Artikel 32

### Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

# „Europäische Datenschutz Grundverordnung“

## *Bundesdatenschutzgesetz §64 Abs. 3 Ziff. 1-14*

### Anforderungen an die Sicherheit der Datenverarbeitung

(3) 2. **Verhinderung des unbefugten Lesens**, Kopierens, Veränderens oder Löschens von Datenträgern (Datenträgerkontrolle),

(3) 8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie **beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden** (Transportkontrolle),

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 3:

Sie schicken und empfangen Emails über einen Emailserver

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 3:

Sie schicken und empfangen Emails über einen Emailserver

Sie müssen den Mailserver so betreiben, daß er nur noch TLS 1.2 verschlüsselte Übertragungen akzeptiert und durchführt,

außer der Server dient **ausschliesslich** der Kommunikation mit Ihren Freunden und Familienangehörigen.

# „Europäische Datenschutz Grundverordnung“

## Referat 23 des *Bundesbeauftragten für den Datenschutz...*

Sehr geehrter Herr S.,

wie ich Ihnen bereits am 22.05.2018 mitgeteilt habe,..., gleichwohl **stimme ich Ihnen zu, dass die Verwendung der Protokolle TLS 1.0 und 1.1 nicht sicher ist.** Damit **liegt ein Datenschutzverstoß gemäß DSGVO Art. 32 Abs. 1 lit a. nahe.**

Wie genau in dieser Angelegenheit in Ihrem Fall zu verfahren ist, müssen Sie bitte mit dem LDI Niedersachsen klären. **Die Angelegenheit selbst bedarf der weiteren Abstimmung mit Datenschutzstellen in Deutschland und auf europäischer Ebene, die ich nunmehr einleiten werden.** Die Abstimmungen werden einiges an Zeit benötigen, ich bitte Sie daher um Geduld.

Ich werde Sie zu gegebener Zeit über den Stand informieren.

--

Im Auftrag  
mit freundlichen Grüßen

Referat 23 bei der  
Bundesbeauftragten für  
den Datenschutz und  
die Informationsfreiheit  
Husarenstr. 30  
D 53117 Bonn

# „Europäische Datenschutz Grundverordnung“

Webseiten – Datenschutz was tun?

Fall 4:

Thema Fotos

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 4:

#### Thema Fotos

Beim Thema Fotos streiten sich die Geister, da es in Deutschland ein spezielles Gesetz gibt, daß Fotoaufnahmen regelt.

Spezialgesetze haben Vorrang vor Allgemeinen Gesetzen und Verordnungen wie der DS GVO.

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Fall 4:

#### Thema Fotos

Jetzt ist die DS GVO eine Grundverordnung im Range eines Gesetzes, gedacht wie ein Grundgesetz in unserer Verfassung.

Grundgesetze kann man nicht aushebeln.



# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Abmahnungen:

Als Unternehmen können Sie kostenpflichtig abgemahnt werden, wenn Sie sich einen unlauteren Vorteil verschaffen.

z.b. wenn **KEINE** Datenschutzerklärung auf der Webseite ist

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Abmahnungen:

Sie können aber nicht abgemahnt werden,  
wenn die Datenschutzerklärung kleine Fehler enthält.

Strafen verhängen, darf nur die Datenschutzbehörde,  
und die ist gehalten, den Fall genau abzuwägen.

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Abmahnungen:

Als Unternehmen können Sie kostenpflichtig abgemahnt werden, wenn Sie Emails auf dem Transportweg unverschlüsselt annehmen, versenden

oder Daten aus Kontaktformulare nicht per HTTPS gesendet werden.

# „Europäische Datenschutz Grundverordnung“

## Webseiten – Datenschutz was tun?

### Abmahnungen:

**Merke:** Die unlautere Vorteilsnahme ist abmahnfähig,  
nicht der Verstoß an sich.

# „Europäische Datenschutz Grundverordnung“

Welche Rechte haben Sie einem Datenverarbeiter gegenüber?

# „Europäische Datenschutz Grundverordnung“

Welche Rechte haben Sie einem Datenverarbeiter gegenüber?

Sie können Einsicht in die gespeichert Daten, die Löschung und Korrektur falscher Daten verlangen und unberechtigte Datensammlung löschen lassen.

Sie dürfen auch eine maschinenlesbare Kopie der Daten zum Zwecke der Übertragung an Konkurrenzunternehmen verlangen.

Letzteres ist allerdings so schwammig formuliert worden, daß es praktisch nicht sinnvoll umsetzbar ist.

# „Europäische Datenschutz Grundverordnung“

Was passiert, wenn was passiert ist ?

# „Europäische Datenschutz Grundverordnung“

## Artikel 82

### Haftung

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.



# „Europäische Datenschutz Grundverordnung“

## *Artikel 999*

Danke für Ihre Aufmerksamkeit.