IOS
INSTITUT OSTERREICHISCHER
STEUERBERATER

**Informationsveranstaltung**
**Mittwoch, 14.02.2018**

# „Die EU-Datenschutzgrundverordnung für Steuerberater“

**Referent:**
**Nicolas Nagel, CIS DSB**

# Die Umsetzung der EU Datenschutz-Grundverordnung (DSGVO)


## WAS BIS 25.05.2018 ZU TUN IST

Nicolas Nagel – Senior Consultant Datenschutz

## Was ist „Datenschutz“ ?

2

## Was ist „Datenschutz" ?

- Unterschied zwischen Datenschutz und Datensicherheit !
- Datenschutz hat zum Ziel den Menschen und Informationen / Daten über diesen zu schützen (Informationelles Selbstbestimmungsrecht)
- Sichergestellt über Vorschriften in lokalen und internationalen Gesetzen
  - EU-Datenschutzgrundverordnung
  - Österreichisches Datenschutzgesetz
  - Telekommunikationsgesetz
- Datensicherheit hat zum Ziel Daten zu schützen (Teilaspekt des Datenschutzes)
  - Physische Sicherheit
  - Datensicherung
  - Schutz vor unberechtigten Zugriffen,…

3

## Datenschutz?

- **Datenschutzgesetz 1978**
- **EU Richtlinie 1995**
- **Datenschutzgesetz 2000**
- **EU-Datenschutzgrundverordnung 2018**


## Was gänzlich Neues?

4

# Überblick zur neuen Datenschutz-Grundverordnung (DSGVO)

5

## Überblick zur Datenschutzgrundverordnung

- 2012 Beginn der Verhandlungen zur Reform des Datenschutzrechts
- Nach Zustimmung des Europäischen Parlaments ist die DSGVO am 04. Mai 2016 im EU-Amtsblatt veröffentlicht worden und damit 20 Tage später am 25. Mai 2016 in Kraft getreten
- DSGVO entfaltet zwei Jahre nach dem Inkrafttreten der Verordnung ihre unmittelbare Wirkung, am **25.Mai 2018**
- Ist eine Neuregelung des Datenschutzes überhaupt notwendig?
- EU-Richtlinie und DSG 2000 werden aufgehoben
- DSGVO räumt den Mitgliedstaaten über sogenannte Öffnungsklauseln Umsetzungsspielräume ein

6

# Strafrahmen der DSGVO

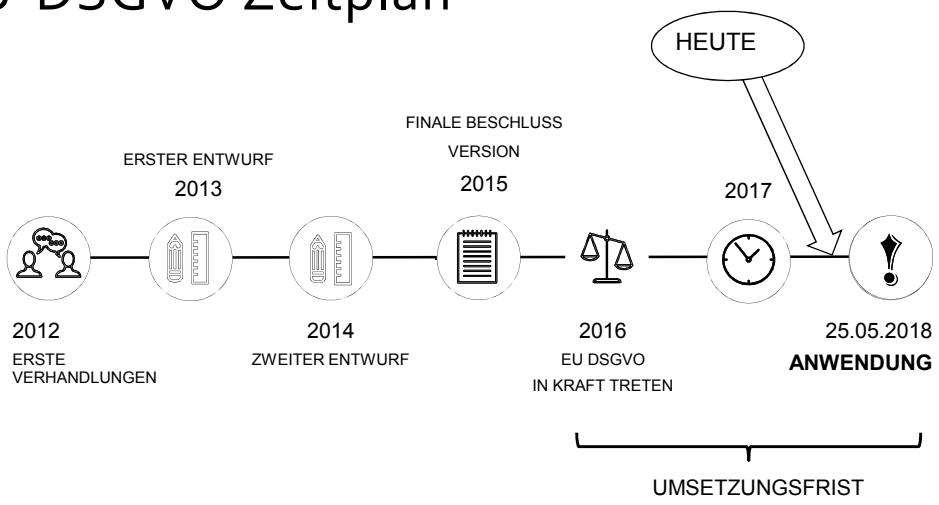
- Allgemein
  - Verhängung von Geldbußen für Verstöße gegen die DSGVO müssen im jeweiligen Einzelfall wirksam, verhältnismäßig und abschreckend sein
  - Werden zusätzlich zu oder anstelle von weiteren Maßnahmen verhängt
  - Relevante Faktoren für die Bemessung der Strafe sind etwa die Art, Schwere und Dauer des Verstoßes, die Anzahl betroffener Personen, die Sensibilität der Daten oder getroffene Schutzmaßnahmen
- Maximale Bußgelder
  - 2 Strafrahmenvarianten je nach Verstoß

bis zu **10 Mio. EUR** oder **2 %** des gesamten weltweit erzielten Jahresumsatzes

bis zu **20 Mio. EUR** oder **4 %** des gesamten weltweit erzielten Jahresumsatzes

7

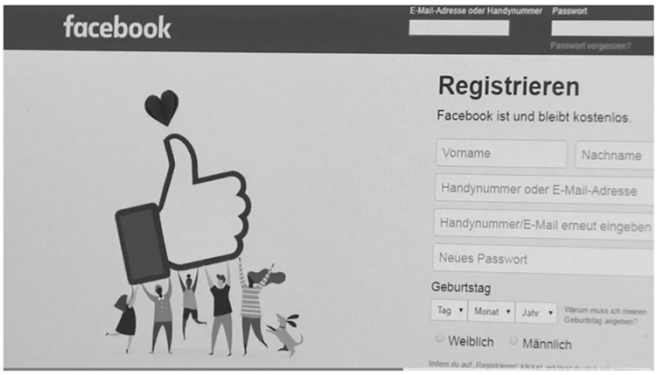
# EU-DSGVO Zeitplan



## Facebook muss 110 Millionen Euro Strafe zahlen

Die EU-Kommission hat Facebook mit einer Strafzahlung von mehr als 100 Millionen Dollar belegt. Grund sind falsche Angaben des US-Konzerns bei der Übernahme von WhatsApp.

18. Mai 2017, 7:52 Uhr / Aktualisiert am 18. Mai 2017, 9:08 Uhr / Quelle: ZEIT ONLINE, dpa, Reuters, spo, kg / 69 Kommentare




**Datenschutz - EU bestraft Facebook wegen falscher Angaben bei WhatsApp-Übernahme**

9

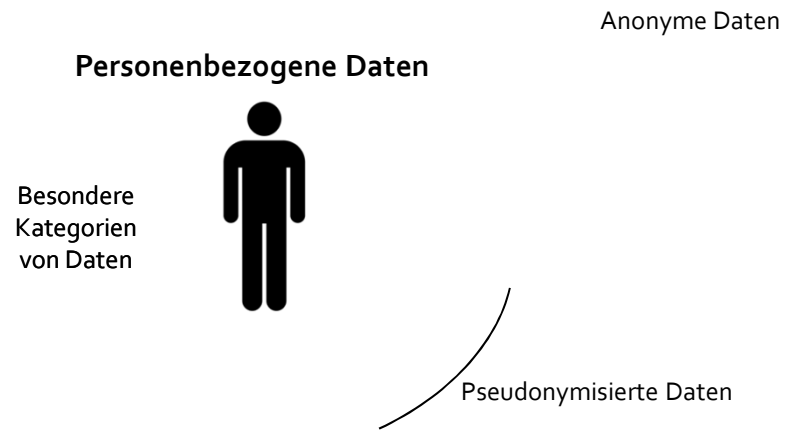
## Schön und gut, aber trifft mich das überhaupt als kleine Steuerberaterkanzlei?

10

# Grundbegriffe

11

## Grundbegriffe




12

# Definitionen

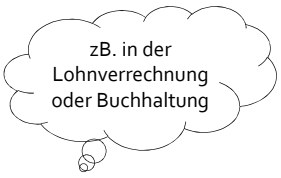
- Personenbezogene Daten:
  - alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (auch „betroffene Person") beziehen
  - als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden
- Anonyme Daten:
  - Kein Rückschluss auf eine individuelle Person mehr möglich
- Pseudonymisierte Daten:
  - Verarbeitung von Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können

13

A1

# Definitionen

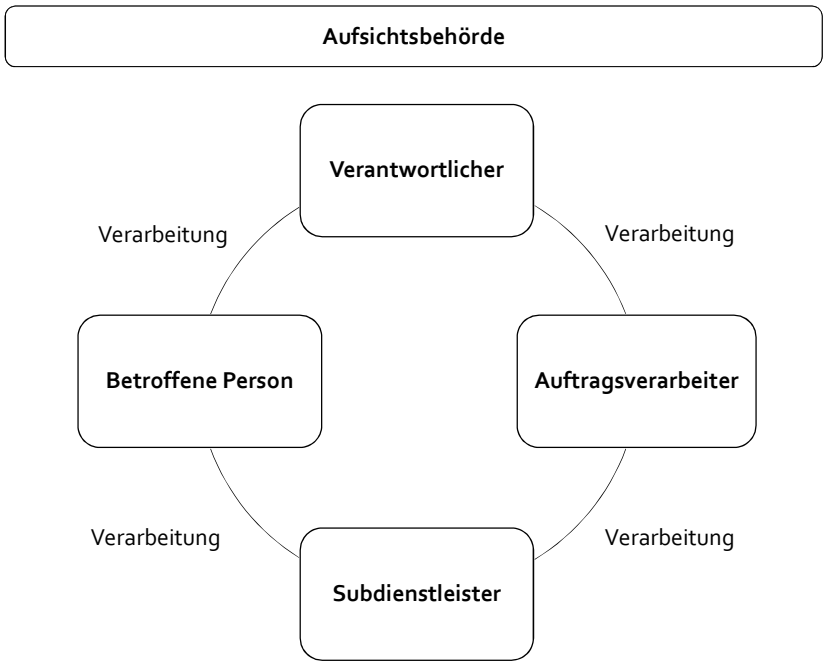
Besondere Kategorien personenbezogener Daten




**Besondere Kategorien von Daten**

- Taxative Auflistung
  - rassische und ethnische Herkunft
  - politische Meinungen
  - religiöse oder weltanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
  - genetischen Daten
  - biometrischen Daten
  - Gesundheitsdaten
  - Daten zum Sexualleben oder der sexuellen Orientierung
- Dürfen nur unter bestimmten Voraussetzungen verarbeitet werden, zB
  - Ausdrückliche Einwilligung
  - Gesetzliche Rechte und Pflichten
  - Zum Schutz lebenswichtiger Interessen

14




15

# Definitionen

- Verantwortlicher:
  - die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle
  - die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- Auftragsverarbeiter:
  - eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle
  - die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
- Betroffene Person:
  - Die natürliche Person deren personenbezogene Daten verarbeitet werden
- Verarbeiten von Daten:
  - jeder Vorgang der personenbezogene Daten betrifft
  - zB das Erheben, das Erfassen, das Ordnen, die Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, die Verwendung, die Offenlegung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, das Löschen oder die Vernichtung

16

# Datenschutzgrundsätze

**RECHTMÄßIGKEIT**

- Verarbeitung personenbezogener Daten generell verboten!
- Ausnahme: explizite Rechtsgrundlage (zB Einwilligung, gesetzliche Verpflichtung,…)
- Interessensabwägung zwischen Betroffenem und Verantwortlichen

**SPEICHER-BEGRENZUNG**

- Betroffene müssen zu jeder Zeit informiert sein, welche ihrer Daten zu welchen Zwecken verarbeitet werden, wo diese gespeichert werden, wer Zugriff hat,…
- Signifikante Ausweitung im Vergleich zu bestehender Rechtslage!

**ZWECKBINDUNG**

- Daten dürfen nur für im Vorhinein festgelegte Zwecke verarbeitet werden
- Neuer Zweck = neue Rechtsgrundlage
- Kompatibilitätsassessment notwendig

**DATENMINIMIERUNG**

- Nur die notwendigsten Daten dürfen verarbeitet werden
- Speicherfrist ist an gesetzliche Grundlage oder Zweckerfüllung gebunden
- Sicheres Löschverfahren oder Anonymisierung

**RICHTIGKEIT**

- Sicherstellung der Richtigkeit von personenbezogenen Daten zu jeder Zeit
- Unrichtige Daten müssen sofort gelöscht oder korrigiert werden
- Kommunikationspflichten gegenüber anderen Empfängern

**DATENSICHERHEIT**

- Angemessene technische und organisatorische Maßnahmen müssen zum Schutz der Daten ergriffen werden
- Unberechtigter Zugriff, Unrechtmäßige Verarbeitung, Verlust, Schaden und Zerstörung

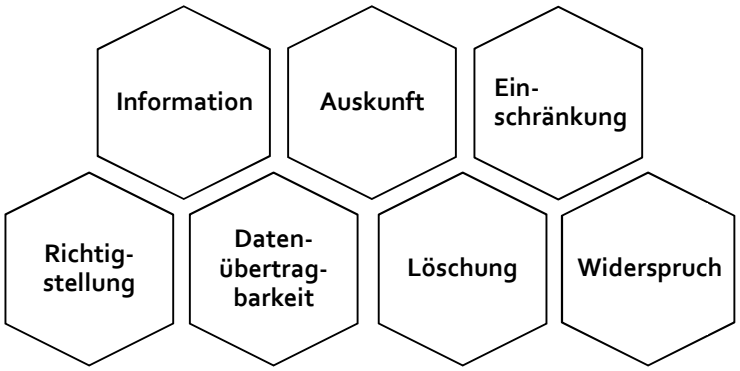
# Rechtsgrundlagen

18

## Rechtmäßigkeit der Datenverarbeitung und Weiterverarbeitung

- Rechtfertigungsgründe zur Datenverarbeitung
  - Einwilligung der betroffenen Person zur Datenverarbeitung für einen oder mehrere Zwecke
  - Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist
  - Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt
    - EU Recht oder nationale Gesetzgebung
  - Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, überwiegen
  - Erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen
    - zB Überwachung von Epidemien oder Katastrophenhilfe
  - Für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde

19




# Rechte von Individuen

20

# Was muss ich tun und was mein Klient?

21

## Rechte von Individuen

**Achtung!**
Gesetzliche Verschwiegenheitspflicht

- Auskunftsrecht
  - Recht auf Auskunft der vom Verantwortlichen verarbeiteten pb Daten der betroffenen Person und Bereitstellung einer Kopie
  - Unverzüglich, spätestens aber innerhalb eines Monats zu beantworten
  - Ein sicheres Onlinesystem, welches der betroffenen Person direkten Zugriff auf die bereitgestellten Informationen bietet, wird empfohlen
- Informationspflichten
  - Verantwortliche müssen betroffene Personen über die Verarbeitung ihrer pb Daten zu informieren
  - Umfang und Inhalt sehr umfangreich
  - In präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln

22

# Rechte von Individuen

- Richtigstellung
  - Betroffenenrecht die Berichtigung oder Vervollständigung unrichtiger personenbezogener Daten zu verlangen
- Datenübertragbarkeit
  - Recht bereitgestellte pb Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, zu übermitteln
  - Auch dass Daten direkt von einem Verantwortlichen zu einem anderen Verantwortlichen übermittelt werden
- Löschung
  - „Recht auf Vergessenwerden"
  - Veröffentlichte Daten: Der Verantwortliche ist verpflichtet, angemessene Maßnahmen zu treffen um andere Verantwortliche über das Löschungsbegehren zu informieren

23

# Rechte von Individuen

- Widerspruchsrecht
  - Direktmarketingzwecke (absolutes Recht)
  - Verarbeitung für wissenschaftliche oder historische Forschungszwecke oder zu statistischen Zwecken
  - Verarbeitung aufgrund „berechtigter Interessen" oder „öffentlichem Interesse"

Aus Gründen, die sich aus der besonderen Situation des Betroffenen ergeben

- Einschränkung
  - „Eingeschränkte" Daten darf der Verantwortliche nur mehr speichern
  - Die Daten dürfen nicht mehr weiterverarbeitet werden (mit Ausnahmen)
  - Der Verantwortliche muss allen Empfängern von pb Daten jede Einschränkung anzeigen

24

# Pflichten für Unternehmen und Mitarbeiter

25

## Pflichten

**Organisationen müssen ihre DSGVO Compliance jederzeit nachweisen können!**

- Generelle Regelung
  - Verantwortliche müssen geeignete technische und organisatorische Maßnahmen ergreifen um die Inhalte der GDPR umzusetzen und den Nachweis darüber jederzeit erbringen können
- Privacy by Design
  - Unter Berücksichtigung des Stands der Technik müssen geeignete technische und organisatorische Maßnahmen die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen, implementiert werden
- Privacy by Default
  - Gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit
  - Daten dürfen durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von Personen zugänglich gemacht werden

26

# Muss ich als Steuerberater ein Verarbeitungsverzeichnis führen?

Da gabs doch etwas mit 250 Mitarbeitern?

27

## Pflichten

Verarbeitungsverzeichnis

- Unternehmen die weniger als 250 Mitarbeiter beschäftigen, müssen kein Verzeichnis führen wenn
  - die Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt,
  - die Verarbeitung nur gelegentlich erfolgt und
  - nicht die Verarbeitung besonderer Datenkategorien bzw. von Daten über strafrechtliche Verurteilungen und Straftaten einschließt
- Jeder Verantwortliche hat ein Verzeichnis aller Verarbeitungstätigkeiten zu führen
- Jeder Auftragsverarbeiter hat ebenso ein Verzeichnis zu allen von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, zu führen
- Das Verzeichnis ist schriftlich zu führen (zB in einem elektronischen Format – Excel genügt dieser Anforderung)
- Der Aufsichtsbehörde ist das Verzeichnis auf Anfrage zur Verfügung zu stellen. Achten Sie auf keine Selbstbelastungen!

28

# Benötige ich als Steuerberater jetzt einen Datenschutzbeauftragten?

29

Die Bestellung eines (internen oder externen) **Datenschutzbeauftragten** ist u.a. dann verpflichtend vorgesehen, wenn der Geschäftszweck in der Verarbeitung personenbezogener Daten besteht (zB ein Steuerberater, der für Klienten die Lohnverrechnung durchführt). Der **Datenschutzbeauftragte ist an die Datenschutzbehörde zu melden.**

[redacted] bietet Planung, Lösungsvorschläge und Umsetzungen im General Business. Unsere Schwerpunkte liegen in der **Steuerberatung**, im **Finanz- und Rechnungswesen**, in der **Lohn- und Gehaltverrechnung** sowie in der **Personalrechtsberatung**.

# Achten Sie darauf woher Sie Ihre Informationen bekommen!

30

# Pflichten

- Datenschutzbeauftragter verpflichtend, wenn
  - Verarbeitung durch Behörde oder öffentliche Stelle
  - Kerntätigkeit:
    - in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (relevant für Steuerberater)
    - in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von strafrechtliche Verurteilungen und Straftaten besteht
  - Lokale Gesetzgebung diesen vorsieht (in Ö keine Regelung)
- Fachwissen und Praxis auf dem Gebiet des Datenschutzrechts wird vorausgesetzt
- Auch externe Bestellung eines Datenschutzbeauftragten möglich
- Unabhängig von einer Bestellpflicht muss sich jemand im Unternehmen um die Datenschutzbelange kümmern!

31

# Pflichten

- Datenschutz Folgenabschätzung
  - Verfahren zur Identifikation und Minimierung von Non-Compliance Risiken
  - Rechtliche und technisch-organisatorische Bewertung von Datenverarbeitungsvorgängen
  - Durchzuführen wenn eine Verarbeitung von pb Daten aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat
- Datenschutzverletzungen
  - Verschiedenste Meldepflichten
  - Internes Datenschutzverletzungs-Register zu führen
    - dokumentiert Verletzungen einschließlich aller Fakten, deren Auswirkungen und der Abhilfemaßnahmen
    - Die Aufsichtsbehörde kann den „Data Breach Notification" Prozess beim Verantwortlichen jederzeit auditieren

32

# Benötige ich spezielle Verträge mit meinen Klienten oder Dienstleistern?


33

## Pflichten

- Verwendung von Auftragsverarbeitern
  - DSGVO stellt hohe Anforderungen an die Auswahl von Auftragsverarbeitern
  - Auftragsverarbeiter müssen hinreichend Garantien dafür bieten, dass die Datenverarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt
  - Unterschiedliche Pflichten zum Abschluss von Verträgen
    - Auftragsverarbeitervertrag (AVV)
    - „Spiegelverträge" zu Subdienstleistern (zB ausgelagerte Funktionen, Hosting Provider, IT Dienstleister,...)
    - EU-Standardvertragsklauseln
  - In aller Regel empfiehlt es sich umfassende Muster zu erstellen, die auch technische und organisatorische Maßnahmenlisten beinhalten

34

# Internationaler Datenverkehr

35

## Datentransfer personenbezogener Daten

- Innerhalb der EU grundsätzlich erlaubt
- Übermittlung pb Daten in Drittstaaten ist nur erlaubt wenn der Empfänger bzw. der Empfängerstaat ein angemessenes Datenschutzniveau bieten
- Vorteil gegenüber alter Rechtslage
  - Keine Genehmigung der Datenschutzbehörde eines internationalen Datentransfers mehr notwendig
- EU Kommission kann bestimmten Ländern, Branchen oder internationalen Organisationen ein geeignetes Datenschutzniveau attestieren
- Herstellung eines angemessenen Datenschutzes möglich, mittels

| Standardvertrags-klauseln der EU (EUMC) | Binding Corporate Rules (BCR) | Privacy Shield Framework | CoC oder Zertifizierung |
|---|---|---|---|

36

# Danke für Ihre Aufmerksamkeit!


## NICOLAS NAGEL

SENIOR CONSULTANT FÜR DATENSCHUTZ

ZERTIFIZIERTER DATENSCHUTZBEAUFTRAGTER

NICOLAS.NAGEL@GMX.AT

TEL.: 0677 / 616 252 70