FREIMÜLLER/OBEREDER/PILZ
RECHTSANWÄLT_INNEN GMBH

# Datenschutzgrundverordnung DSGVO – Was ist zu tun?

## Eine Übersicht in drei Kapiteln

Rechtsanwalt Mag. Michael Pilz
FREIMÜLLER/OBEREDER/PILZ Rechtsanwält_innen GmbH
michael.pilz@jus.at
1080, Alserstraße 21
Tel. 01/406 05 51
www.jus.at

**Frühjahr 2017**

# Kapitel I:

## Alles neu, macht der Mai

# Was ist die DSGVO?

- Die „Datenschutzgrundverordnung - DSGVO" ist **unmittelbar anwendbares Gemeinschaftsrecht** und ersetzt weitgehend alle bisherigen nationalen Datenschutzvorschriften
- Sie tritt am **25.05.2018** in Kraft
- Datenschutz wird zu dem wesentlichsten **Compliance-Thema**
- Datenschutz ist kein Orchideen-Thema mehr:
  Verstöße gegen die DSGVO können mit Geldstrafen von bis zu **20 Mio EUR oder 4 % des weltweiten Konzernjahresumsatzes** bestraft werden

# DSGVO: Welche Datenverarbeitungen sind erfasst?

**Sachlicher Anwendungsbereich:**

- DSGVO gilt für jede **Verarbeitung personenbezogener Daten** (= alle Informationen, die sich auf eine **identifizierte oder identifizierbare <u>natürliche</u> Person** beziehen)
- Bei der Beurteilung der Identifizierbarkeit sind auch **Möglichkeiten Dritter** einzubeziehen
- **Manuelle Daten** nur, wenn in strukturierter Sammlung gespeichert und zugänglich
- „**Haushaltsausnahme**": DSGVO gilt nicht für persönliche oder familiäre Tätigkeit, zB in Social Media

# Für wen gilt die DSGVO?

**Persönlicher Anwendungsbereich:**

- **Verantwortliche** (bisher: Auftraggeber)

natürliche oder juristische Person, die allein oder gemeinsam mit anderen über Datenverarbeitung entscheidet

- **Auftragsverarbeiter** (bisher: Dienstleister)

natürliche oder juristische Person, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

Auch für Auftragsverarbeiter gelten nach der DSGVO erhebliche regulatorische Pflichten!

# Wo gilt die DSGVO?

**Räumlicher Anwendungsbereich:**

- Verantwortliche und Auftragsverarbeiter mit **Sitz in der EU oder im EWR**
- Sitz außerhalb der EU/EWR, aber **Datenverarbeitung erfolgt im Rahmen der Tätigkeit einer Niederlassung**
- Sitz von Verantwortlichem oder Auftragsverarbeiter außerhalb EU/EWR, aber **Anbieten von Waren oder Dienstleistungen in EU/EWR**
- **Beobachtung von Verhalten**, zB Online Advertising Networks

# DSGVO: Datenschutzgrundsätze

- **Rechtmäßigkeit, Treu und Glauben, Transparenz:**
  Rechtsgrundlage muss vorhanden sein, Erfüllung von Informationspflichten
- **Zweckbindung:**
  Erhebung und Verarbeitung von Daten nur für vorab definierten Zweck
- **Datenminimierung:**
  Nur Verarbeitung von Daten im dem Zweck angemessenen, notwendigem Maß
- **Richtigkeit:**
  Daten müssen richtig sein, ggf.auf dem neuesten Stand
- **Speicherbegrenzung:**
  Daten dürfen nur für erforderliche Dauer des Verarbeitungszwecks gespeichert werden und sind danach zu löschen oder zu anonymisieren.
- **Integrität und Vertraulichkeit:**
  angemessene Datensicherheitsmaßnahmen
- **Rechenschaftspflicht:**
  Implementierung von Compliance-Maßnahmen

# Kapitel II:

## Sieben Schätze bis Mai 2018

# Die sieben wichtigsten Compliance-Schritte bis 28.5.2018

1) Implementierung eines **Datenschutz-Compliance-Programms**
2) (eventuell) Bestellung eines **Datenschutzbeauftragten**
3) **Verzeichnis** der Verarbeitungstätigkeiten
4) Prüfung der **Rechtsgrundlage der existierenden Datenverarbeitungen** im Unternehmen
5) Schaffung **DSGVO-konformer Datenschutzerklärungen**
6) Prüfung der **Rechtsgrundlage für internationale Datenübermittlungen**
7) Abschluss neuer Vereinbarungen mit **Auftragsdatenverarbeitern**

# 1. Datenschutz Compliance Programm

Ein Datenschutz Compliance Programm ist bis Mai 2018 von jedem Verantwortlichen zu erstellen!

- **Organisatorische Maßnahmen:**
  - Entwicklung von Datenschutzstrategien („Data Protection Policy"): Ziele, Verantwortlichkeiten, Organisationsstruktur, Details

- **Technische Maßnahmen:**
  - Datenschutz durch Technik („**Privacy by Design**") Umsetzung der Datenschutzgrundsätze in der IT
  - Datenschutz durch Voreinstellungen („**Privacy by Default**") Voreinstellungen für den jeweiligen Verarbeitungszweck; insbesondere sind Daten defaultmäßig nicht ohne Eingreifen des Betroffenen zu veröffentlichen

# 2. Datenschutzbeauftragter

- **Verpflichtende Bestellung erforderlich, wenn**
  - nationales Recht dies verlangt (in Ö: Nein), **oder**
  - es sich beim Verantwortlichen oder Auftragsdatenverarbeiter um eine öffentliche Stelle handelt, **oder**
  - Kerntätigkeit der Verarbeitung eine umfangreiche regelmäßige und systematische Überwachung (zB Online-Werbenetzwerke)ist, **oder**
  - Kerntätigkeit eine umfangreiche Verarbeitung sensibler Daten ist.
- **Stellung des Datenschutzbeauftragten:**
  - weisungsfrei und genießt Kündigungsschutz
  - berichtet unmittelbar an das Management
  - Einbindung in alle datenschutzrechtlichen Fragen
  - Ausstattung mit den notwendigen Ressourcen erforderlich
  - hat Zugang zu personenbezogenen Daten und Verarbeitungen
  - Anlaufstelle für betroffene Personen
  - ist zur Verschwiegenheit verpflichtet
  - berät das Management und überwacht die Einhaltung der DSGVO

# 3. Verzeichnis der Verarbeitungen

- in **schriftlicher oder elektronischer Form** zu führen,
- der **Aufsichtsbehörde** auf Anfrage zur Verfügung zu stellen
- **Einsichtsrecht** für betroffene Personen
- **Inhalt des Verzeichnisses** des Verantwortlichen:
  - Kontaktdaten des Verantwortlichen u. ggf. des Datenschutzbeauftragten
  - Verarbeitungszwecke
  - Beschreibung der Kategorien der Betroffenen, der Daten, der Empfänger
  - Speicherdauer der Datenkategorien
  - Beschreibung der Datensicherheitsmaßnahmen
  - Datenübermittlung in Drittländer: Drittland, Risikobeurteilung, Garantien
- **Inhalt des Verzeichnisses** des Auftragsverarbeiters:
  - Kontaktdaten des Auftragsverarbeiters u. ggf. des Datenschutzbeauftragten
  - Kontaktdaten des Verantwortlichen
  - Kategorien der Verarbeitung im Auftrag des Verantwortlichen
  - Beschreibung der Datensicherheitsmaßnahmen
  - Datenübermittlung in Drittländer: Drittland, Risikobeurteilung, Garantien

# 4. Rechtsgrundlage der Verarbeitung

**Nicht-sensible Daten:**

- schlüssige oder ausdrückliche **Einwilligung** der betroffenen Person
- Erfüllung eines **Vertrages** mit der betroffenen Person
- Erfüllung einer **gesetzlichen Verpflichtung** des Verantwortlichen
- **lebenswichtige Interessen** der betroffenen Person oder eines Dritten
- **überwiegende Interessen** des Verantwortlichen
- **Aufgabe im öffentlichen Interesse**

**Sensible Daten:**

- **Ausdrückliche Einwilligung** der betroffenen Person
- Ausübung von Rechten aus **Arbeits- und Sozialrecht**
- Schutz **lebenswichtiger Interessen** des Betroffenen oder Dritter, wenn Betroffener **nicht zustimmen kann**
- **Mitgliederdatenverwaltung** durch Tendenzorganisation ohne Gewinnerzielungsabsicht
- wurden von **betroffener Person öffentlich** gemacht
- Notwendig zur **Ausübung von Rechtsansprüchen**
- **Gesundheitswesen, Archive, Statistik, Forschung**

# Exkurs:
# Die Einwilligung: Was ist notwendig?

- Die Einwilligung muss **freiwillig**, **für den bestimmten Fall** und **in informierter Weise** erfolgen
- Stillschweigen, vorausgefüllte Felder („**opt-out**") oder Untätigkeit sind **keine Einwilligung**
- Einwilligung für mehrere Verarbeitungsvorgänge muss **gesondert erteilt** werden können
- Einwilligung muss in **klarer, einfacher Sprache** erbeten werden
- **Trennung der Einwilligung von anderen Erklärungen** (zB AGB's)
- **Koppelungsverbot**: Vertragserfüllung darf nicht von nicht sachlich erforderlicher Einwilligung abhängig sein
- Erfüllung der **Informationspflichten**
- Information über das **Widerrufsrecht**
- Beachtung der **Altersgrenzen** bei Online-Diensten: 16 J.
- Beweislast für Einwilligung trägt der Auftraggeber
- Einwilligungen, die **vor dem 25.5.2018** erteilt wurden, **sind nur dann weiter gültig, wenn sie den Erfordernissen der DSGVO entsprochen haben!**

# 5. Die Datenschutzerklärung

**Aktive Information der betroffenen Personen!**

- **Zeitpunkt:**
  - Bei der Datenerhebung, wenn direkt beim Betroffenen Daten erhoben werden
  - Sonst im Zeitpunkt der erstmaligen Kommunikation mit dem Betroffenen oder erstmaliger Weitergabe der Daten, spätestens aber ein Monat nach Erhalt der Daten

- **Ausnahmen:**
  - Betroffene Person hat die Informationen bereits
  - Verarbeitung ist durch Rechtsvorschriften geregelt
  - Informationserteilung ist unmöglich oder erfordert unverhältnismäßigen Aufwand

# Inhalt der Datenschutzerklärung

- **Inhalt der Datenschutzerklärung:**
  - Namen und Kontaktdaten des Verantwortlichen
  - ggf. Kontaktdaten des Datenschutzbeauftragten
  - Verarbeitungszweck und Rechtsgrundlagen der Verarbeitung
  - wenn berechtigte Interessen Grundlage der Verarbeitung sind: Benennung der berechtigten Interessen
  - Empfänger einer Datenübermittlung
  - Wenn Übermittlung in ein Drittland beabsichtigt: Information darüber, sowie ob Angemessenheitsbeschluss der EU-Kommission vorliegt.
  - Dauer der Datenspeicherung
  - Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch)
  - Möglichkeit des Widerrufs der Einwilligung
  - Beschwerdemöglichkeit bei der Aufsichtsstelle
  - Ob Bereitstellung der Daten gesetzlich oder vertraglich vorgesehen oder für den Vertragsabschluss erforderlich ist
  - ggf. Bestehen automatisierter Entscheidungsfindungen („Profiling")
  - Wenn Weiterverarbeitung für anderen Zweck: Informationen darüber
  - Wenn die Erhebung nicht direkt beim Betroffenen erfolgt: Quelle der Daten

# Form der Datenschutzerklärung

- Mündliche oder schriftliche Information
- Bei Online-Diensten:
  Datenschutzerklärung, die über Link abrufbar ist
- **Praxistipp:**
  Layered Privacy Notice:

  Layer 1: Kurzhinweis mit Link für nähere Infos
  Layer 2: Zusammenfassung, mit Link auf vollständige Erklärung
  Layer 3: Datenschutzerklärung

# 6. Internationale Datenübermittlung

- Übermittlungen in **EU/EWR Staat** sind **zulässig**
- **Drittländer:**
  - **Keine Beschränkung:** (Beispiele)
    - Angemessenheitsbeschluss der EU-Kommission liegt vor (dzt. zB Schweiz, Israel, USA [wenn Empfänger selbstzertifiziert nach dem Privacy Shield]), oder
    - Übermittlung mit Standardvertragsklauseln der EU-Kommission
    - Konzerninterne Datenübermittlung unter von Aufsichtsbehörde genehmigten „Binding Corporate Rules"
    - Einwilligung der betroffenen Person
    - Übermittlung ist für Abschluss oder Erfüllung eines Vertrages erforderlich
    - Übermittlung erfolgt aus einem öffentlichen Register
  - **Meldepflichtige Übermittlung**
    - Keine wiederholte Übermittlung, Zahl der Betroffenen ist begrenzt
    - Übermittlung zur Wahrung zwingender berechtigter Interessen des Verantwortlichen
    - Geeignete Datenschutzgarantien werden vorgesehen
  - **Genehmigungspflichtige Übermittlung**
    - Alle anderen Übermittlungen

# 7. Auftragsdatenverarbeitervereinbarung

Mit dem Auftragsdatenverarbeiter ist zwingend eine **Vereinbarung vor Beginn des Auftrags** zu schließen

(schriftlich oder elektronisch):

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien der betroffenen Personen
- Pflichten und Rechte der Vertragspartner
  - Verarbeitung nur nach Weisung des Verantwortlichen
  - Datenschutzrechtliche Warnpflicht des Auftragsdatenverarbeiters
  - Verschwiegenheitsverpflichtung aller beteiligten Personen
  - Ergreifen aller erforderlichen Datensicherheitsmaßnahmen
  - Subunternehmer nur nach Genehmigung des Verantwortlichen
  - Unterstützung des Verantwortlichen bei der Erfüllung von Rechten Betroffener, bei Datensicherheitsmaßnahmen, Data Breach Notification
  - Löschung oder Rückgabe aller Daten nach Leistungserbringung

# Exkurs: Compliance-Schritte für Auftragsdatenverarbeiter

1. (eventuell) Bestellung eines **Datenschutzbeauftragten**
2. **Verzeichnis** von Verarbeitungstätigkeiten
3. Implementierung angemessener **Sicherheitsmaßnahmen**
4. Beiziehung von **Subauftragsverarbeitern nur mit schriftlicher Zustimmung** des Verantwortlichen
5. Einhaltung der **Vorschriften für internationale Datenübermittlungen**

# Kapitel III:

## Go-Live!

# Ab Mai 2018

1. Vor Neuaufnahme einer Datenverarbeitung ist **Risikoabschätzung** erforderlich („Privacy Impact Assessment")
2. Umfassende **Betroffenenrechte**
3. Beschränkungen für „**Profiling**"
4. Hohe Anforderungen an **Datensicherheitsmaßnahmen**
5. Bei Sicherheitsverletzungen: **Data Breach Notifications**
6. Betroffene können **gerichtliche Klagen** einbringen
7. Hohe **Strafen** möglich

# 1. Privacy Impact Assessment

- **Vor Neuaufnahme** einer Datenverarbeitung zu erstellen wenn die Datenverarbeitung „voraussichtlich ein hohes **Risiko für Rechte und Freiheiten** natürlicher Personen zur Folge hat".

  Jedenfalls aber dann, wenn
  - Profiling als Grundlage für Entscheidungen mit Rechtswirkungen oÄ
  - Umfangreiche Verarbeitung sensibler Daten
  - Systematische, umfangreiche Überwachung öffentlicher Bereiche
  - Art der Verarbeitung ist auf „schwarzer Liste" der Aufsichtsbehörde

- **Inhalt** des Assessment:
  - Stellungnahme des Datenschutzbeauftragten
  - Beschreibung und Zweck der Verarbeitung
  - Bewertung von Notwendigkeit und Verhältnismäßigkeit
  - Bewertung der Risiken für Rechte und Freiheiten der Betroffenen

- **Konsultationsverfahren** mit der Aufsichtsbehörde erforderlich, wenn Risiko hoch bewertet wird.

# 2. Betroffenenrechte

- Recht auf **Auskunft**: Achtung, Frist: ein Monat.
- Recht auf **Datenübertragbarkeit** in strukturierter Form
- Recht auf **Berichtigung**
- Recht auf **Löschung**
- „**Recht auf Vergessen werden**": Wurden Daten öffentlich gemacht, hat der Verantwortliche Dritte über den Löschungswunsch zu benachrichtigen
- Recht auf (vorläufige) **Einschränkung der Verarbeitung**
- Recht auf **Widerspruch**, wenn kein überwiegendes Interesse oder bei Direktmarketing, Forschung, Statistik

# 3. Profiling?

- **Definition**: Automatisierte Verarbeitung von personenbezogenen Daten um bestimmte persönliche Aspekte zu bewerten, zu analysieren oder vorherzusagen.
- **Automatisierte Einzelentscheidungen** (auch unter Zuhilfenahme von Profiling-Technologie) mit rechtlicher Wirkung (ZB Vertragsablehnung) **nur zulässig, wenn**
  - Vorabinformation der betroffenen Person
  - Ausdrückliche Einwilligung oder gesetzliche Grundlage
  - Recht auf Erwirkung des Eingreifens einer Person
  - Keine sensiblen Daten werden verwendet

# 4. Datensicherheitsmaßnahmen

- **Angemessenes Schutzniveau** ist einzuhalten, um Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten
  - Pseudonymisierung und Verschlüsselung
  - Sicherung der IT-Systeme
  - Incident-Response Systeme
  - Regelmäßige Überprüfung der Maßnahmen

- **Internationale Standards** als Richtschnur
  - ISO/IEC 27001 Informationssicherheit Managementsystem
  - ISO/IEC 27002 Katalog von Sicherheitsmaßnahmen

# 5.
# Data Breach Notification!

Im Falle einer Sicherheitsverletzung sind zu informieren:

- die **Aufsichtsbehörde**: unverzüglich, längstens binnen 72 Stunden, außer es ist kein Risiko für Rechte und Freiheiten natürlicher Personen gegeben
- die **betroffenen Personen**: Wenn hohes Risiko für deren Rechte und Freiheiten besteht
- der **Verantwortliche:** Wenn Sicherheitsverletzung bei einem Auftragsdatenverarbeiter erfolgte:.

- Jede Sicherheitsverletzung ist zu **dokumentieren**.

# 6. Zivilrechtliche Ansprüche

- Rechte des Betroffenen können mit **zivilrechtlicher Klage** gegen den Verantwortlichen oder gegen den Auftragsdatenverarbeiter durchgesetzt werden
- Schadenersatzansprüche für **materielle** und **immaterielle Schäden**
- Klagslegitimation auch für **Datenschutzorganisationen** ohne Gewinnabsicht im Namen von Betroffenen
  (vgl. § 17 ö Datenschutz-Anpassungsgesetz)

# 7. Verwaltungsstrafen drohen

- **Aufsichtsbehörden** erhalten umfassendere Befugnisse als derzeit
- Insbesondere ist (praktisch) jede Verletzung von gesetzlichen Verpflichtungen mit **Strafe** sanktioniert
- Strafen betragen bis zu **EUR 20 Millionen** oder bis zu **4 % des Konzernumsatzes** jenes Konzerns, dem das bestrafte Unternehmen angehört; zudem besteht eine **Haftung** der Konzernmutter.

# Vielen Dank für Ihre Aufmerksamkeit!

FREIMÜLLER/OBEREDER/PILZ
RECHTSANWÄLT_INNEN GMBH

**Mag. Michael Pilz**
**Rechtsanwalt**

**A-1080 Wien, Alser Straße 21**
**T: +43/1/406 05 51 • F: +43/1/406 96 01**

**michael.pilz@jus.at • www.jus.at**