

SEC4YOU

Advanced IT-Audit Services

Datenschutzgrundverordnung

Betroffenenrechte gemäß Artikel 12 – 22 und 34

Manfred Scholz / 12.12.2017

Einführung



Betrachtung der Anforderungen der DSGVO
aus fachlicher Sicht

Einführung

- **Was** ist zu tun?
- **Wie** ist es zu tun?
- **Wo** ist es zu tun?
- **Wer** muss es tun?

Begriffsdefinitionen

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder **identifizierbare** natürliche Person beziehen (betroffene Person)

(Artikel 4 Abs. 1)

Begriffsdefinitionen

Besondere Kategorien personenbezogener Daten

- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- die Gewerkschaftszugehörigkeit
- das Sexualleben oder die sexuelle Orientierung
- Gesundheitsdaten
- **genetische und biometrische Daten**

(Artikel 9 Abs. 1)

Begriffsdefinitionen

Der Verantwortliche

Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
die allein oder gemeinsam mit anderen
über die Zwecke und Mittel der Verarbeitung entscheidet.



(Artikel 4 Abs. 7)

Begriffsdefinitionen

Der Auftragsverarbeiter

Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
die personenbezogene Daten
im **Auftrag des Verantwortlichen** verarbeitet.



(Artikel 4 Abs. 8)

Rechte der Betroffenen



Die Rechte der Betroffenen wurden **wesentlich** gestärkt

Rechte der Betroffenen



Erhöhtes Risikopotenzial bei Verstößen gegen Betroffenenrechte!!!

Der Anspruch trifft den Verantwortlichen



Der Verantwortliche muss der betroffenen Person die Ausübung ihrer Rechte **erleichtern** und **kostenlos** erbringen.

Rechte der Betroffenen

- Recht auf Information (Art. 13 und 14)
- Recht auf Auskunft (Art. 15)
- Recht auf Berichtigung (Art. 16)
- Recht auf Löschung (Art. 17)
- Recht auf Einschränkung der Verarbeitung (Art. 18)
- Recht auf Datenübertragbarkeit (Art. 20)
- Recht auf Widerspruch (Art. 21)
- Recht, nicht auf einer ausschließlich automatisierten Entscheidung unterworfen zu werden (Art. 22)

Rechte der Betroffenen

Recht auf Benachrichtigung

Grundsätzlich müssen Datenschutzvorfälle die zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen vom Verantwortlichen gemeldet werden.

1. Aufsichtsbehörde: unverzüglich jedoch möglichst innerhalb von 72 Stunden (Art. 33)
2. Betroffene: Bei einem **hohem Risiko für die Betroffenen** sind diese unverzüglich zu verständigen (Art. 34)

Recht auf Information

- Name und Kontaktdaten des Verantwortlichen
- Ggfls. Kontaktdaten des Datenschutzbeauftragten (z.B. funktionale Emailadresse)
- Zweck der Verarbeitung und Rechtsgrundlage
- Empfänger bzw. Kategorien von Empfängern
- Geplante Übermittlung in ein Drittland und welche Garantien zum Schutz der Daten existieren
- Speicherdauer
- Hinweis auf Betroffenenrechte (Auskunft, Berichtigung, Löschung, etc.)
- Hinweis auf das Recht auf Beschwerde bei der Aufsichtsbehörde
- Existenz automatisierter Entscheidungen (Profiling)

(Art 13 und 14)

Recht auf Information

Wenn die personenbezogenen Daten nicht bei der Person selbst erhoben wurden hat der Betroffene das Recht zu erfahren aus welcher Quelle diese Daten stammen und ggfls. ob sie aus öffentlichen Quellen stammen.

(Art 14 Abs 2 lit. f)

Anforderungen an die Kommunikation

Informationen und Mitteilungen müssen in präziser, transparenter, verständlicher und **leicht zugänglicher Form** und in einer **klaren und einfachen Sprache** übermittelt werden.

Implementierung als „Layered Privacy Notice“



Recht auf Auskunft

- Verarbeitungszweck und Kategorien der Daten
- Empfänger oder Kategorien der Empfänger denen die Daten offengelegt werden
- Speicherdauer (Kriterien für die Dauer)
- Rechte (Löschung, Berichtigung, etc.)
- Herkunft der Daten
- Existenz automatisierter Entscheidungen (Profiling)
- Garantien bei Übermittlung in Drittland
- **Kopie der Daten !!!**

Recht auf Berichtigung



Halten Sie Ihre persönlichen Daten auf dem neuesten Stand

Recht auf Löschung

- Wegfall des Zwecks
- Wegfall der Rechtsgrundlage
- Widerruf der Einwilligung
- Unrechtmäßige Verarbeitung
- Andere rechtliche Verpflichtung

→ DIN 66398 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten

<http://www.din-66398.de/inhalt/index.html>

Das Recht auf Löschung ...

erfordert ein Löschkonzept

- Beschreibung der Vorgangsweise
- Dokumentationsstruktur (Weitere Dokumente)
- Löschregeln
- Umsetzungsvorgaben
- Verantwortlichkeiten

Aufbewahrungsfristen



Home > Themen > Wirtschaftsrecht und Gewerberecht > Datenschutz
> EU-Datenschutz-Grundverordnung (DSGVO): Speicher- und
Aufbewahrungsfristen

EU-Datenschutz-Grundverordnung (DSGVO): Speicher- und Aufbewahrungsfristen

Auswahl einiger wichtiger bundesgesetzlicher
(Aufbewahrungs-)Fristen

Stand: 26.09.2017

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html>

Recht auf Einschränkung der Verarbeitung

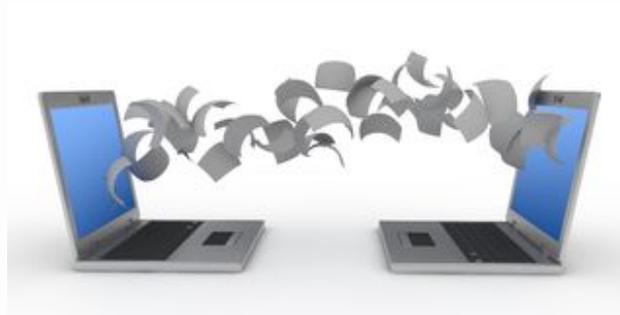
- Richtigkeit der Daten wird bestritten
- Verarbeitung ist unrechtmäßig
- Wegfall des Zwecks, aber zur Durchsetzung von Rechtsansprüchen Betroffener

Informationspflicht bei Löschung oder Einschränkung

Der Verantwortliche muss alle anderen Verantwortlichen informieren, denen er diese Daten offengelegt hat, dass eine Löschung oder eine Einschränkung der Verarbeitung beantragt wurde.

(Art. 19)

Recht auf Datenübertragbarkeit



Eine betroffene Person hat das Recht **jene Daten, welche sie dem Verarbeiter zur Verfügung gestellt hat**, in maschinenlesbarer Form **zu erhalten** und einem anderen Verantwortlichen zu übermitteln, oder zu erwirken, dass diese **direkt an einen anderen Verantwortliche übermittelt** werden.

Recht auf Widerspruch

Die betroffene Person kann jederzeit der Verarbeitung, die auf Art 6 lit e (Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) oder lit. f (**Wahrung berechtigter Interessen des Verantwortlichen**) widersprechen, außer die Interessen des Verantwortlichen überwiegen (→ Nachweispflicht).

Gegen Direktwerbung kann ohne Abwägung der Interessen widersprochen werden.

Recht auf Widerspruch bei automatisierten Entscheidungen

Die betroffene Person hat das Recht, nicht einer **ausschließlich** auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Ausnahmen:

- a) Erfüllung eines Vertrages
- b) Rechtsvorschriften
- c) Vorliegen einer Einwilligung

Seminartipp



Datenschutzgrundverordnung (DSGVO) (CPE 7)

Kurstermin	CPE	Veranstaltungsort	
22.01.2018	7	Akademie Interne Revision GmbH Anfahrt	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Seminarthema:

Nach vielen Jahren intensiver Verhandlungen haben sich die Mitgliedsstaaten der EU auf eine Reform des Datenschutzes in Europa geeinigt. Die DSGVO ist am 24.05.2016 in Kraft getreten und ist ab 25.05.2018 anzuwenden. In Fachkreisen wird diese Verordnung als Meilenstein für einen einheitlichen Standard für die Verarbeitung personenbezogener Daten in Europa gefeiert. Aufgrund der zahlreichen Öffnungsklauseln, die nationale Anpassungen ermöglichen, erntete diese aber auch starke Kritik. Letztendlich bleibt abzuwarten welchen Handlungsspielraum der Europäische Gerichtshof den Mitgliedsstaaten tatsächlich gewährt, oder ob der Grundgedanke der Öffnungsklauseln "Präzisierung" sehr eng ausgelegt wird.

<http://www.internerevision.at/seminare/it-revision/seminar/datenschutzgrundverordnung-dsgvo-210/>

Vorankündigung

DSGVO Workshop „Was & Wie“
Technische & organisatorische Maßnahmen gemäß Artikel 32
18. Jänner 2018
Star Inn Hotel Wien Schönbrunn, Linke Wienzeile 224, 1150 Wien

Finale



Manfred.Scholz@sec4you.com
<https://sec4you.com>
XING, LinkedIn
Tel.: +43 1 2531 797-10