SEC4YOU

Advanced IT-Audit Services

Datenschutzgrundverordnung

Interne und externe Dienstleister gemäß Artikel 28

Manfred Scholz / 23.2.2018 V1.01

Rückblick

- WS01 Das Verzeichnis der Verarbeitungstätigkeiten (7.11.2017)
- WS02 Betroffenenrechte (12.12.2017)
- WS03 Technische und organisatorische Maßnahmen gemäß Artikel 32 (18.1.2018)

Teilnehmer erhalten immer die Unterlagen aller Termine!

Nachlese auf https://sec4you.com

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?

Worum geht es beim Datenschutz?

Schutz der Grundrechte und Freiheiten natürlicher Personen

Grundsätze der Datenverarbeitung (Art. 5)

- Rechtmäßigkeit (Rechtsgrundlage)
- Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung (Aufbewahrungsdauer)
- Integrität und Vertraulichkeit

Rechtmäßigkeit der Verarbeitung

Es gilt das Verbot der Verarbeitung personenbezogener Daten
mit **Erlaubnisvorbehalt!**

(Art 6)

Begriffsdefinitionen

Personenbezogene Daten

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

(Art. 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**

(Art. 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.

(Art. 4 Abs. 7)

Begriffsdefinitionen

Der Auftragsverarbeiter

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

(Art. 4 Abs. 8)

Umgang mit Dienstleistern im Auftrag des Verantwortlichen

... arbeitet dieser nur mit Auftragsverarbeitern, **die hinreichend Garantien** dafür bieten,

- **dass geeignete technische und organisatorische Maßnahmen** so durchgeführt werden,
- dass die **Verarbeitung im Einklang mit den Anforderungen** dieser Verordnung erfolgt
- und den **Schutz der Rechte der betroffenen Person gewährleistet**.

(Art 28 Abs. 1)

Wesentliche Anforderung

Rechenschaftspflicht des Verantwortlichen!

(Art. 5 Abs. 2., Art. 24 Abs. 1)

Wesentliche Änderung

Nachweispflicht der Einhaltung und Wirksamkeit der umgesetzten Maßnahmen!

Sicherheit der Verarbeitung (Art. 32 Abs. 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.

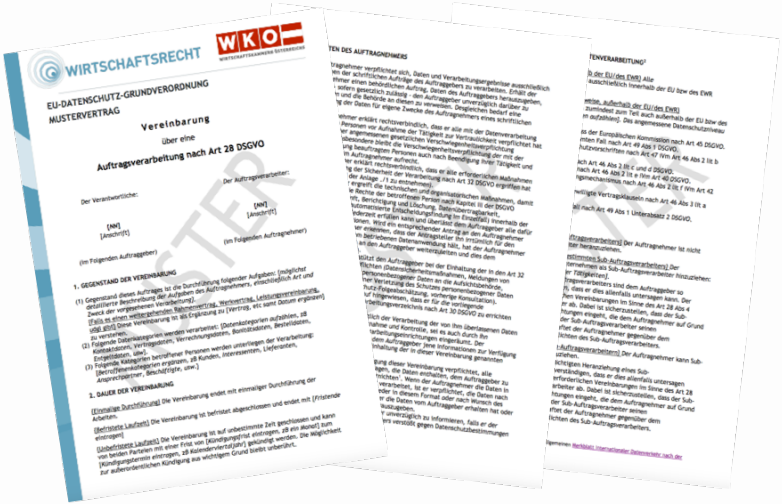
Vertrag zur Auftragsverarbeitung

Die Verarbeitung erfolgt auf der **Grundlage eines Vertrags:**

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- die Art der personenbezogenen Daten
- die Kategorien betroffener Personen und
- die Pflichten und Rechte des Verantwortlichen festgelegt sind.

(Art 28 Abs. 3)

Vertrag zur Auftragsverarbeitung


WIRTSCHAFTSRECHT

EU-DATENSCHUTZ-GRUNDVERORDNUNG
MUSTERVERTRAG

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

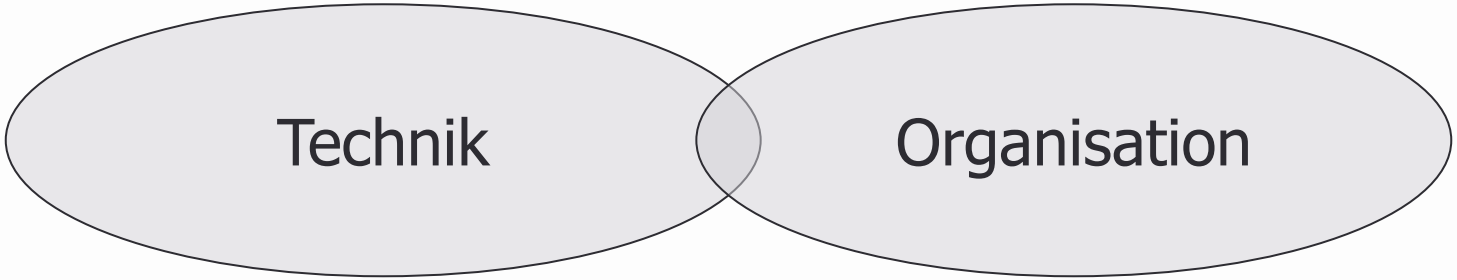
Verarbeitung erfolgt auf **dokumentierte Weisung** des Verantwortlichen

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html

Mindestinhalte des Vertrages

Verpflichtung des Personals zur Vertraulichkeit

Mindestinhalte des Vertrages



Gewährleistung **technischer und organisatorischer** Sicherheitsmaßnahmen (Art. 32)

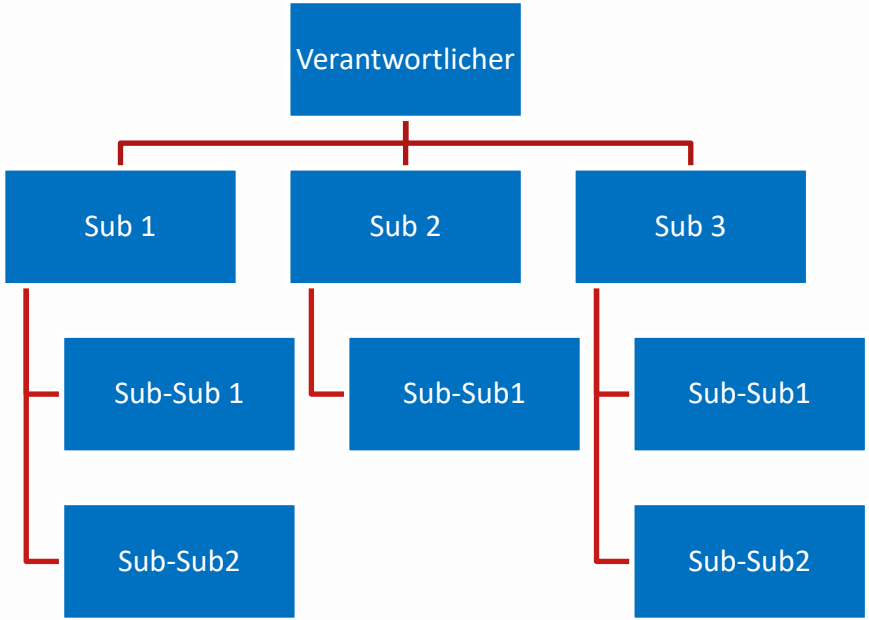
Subauftragnehmer

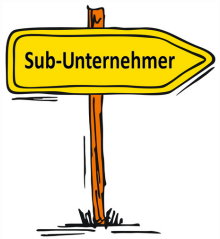
Der Auftragsverarbeiter:

- nimmt **keinen weiteren Auftragsverarbeiter ohne** vorherige gesonderte oder allgemeine **schriftliche Genehmigung des Verantwortlichen** in Anspruch.
- Im Fall einer **allgemeinen schriftlichen Genehmigung** informiert der Auftragsverarbeiter den Verantwortlichen immer über **jede beabsichtigte Änderung** in Bezug auf die **Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter**,
- wodurch der Verantwortliche die **Möglichkeit** erhält, gegen derartige Änderungen **Einspruch** zu erheben.

(Art 28 Abs. 2)

Subauftragnehmer





Mindestinhalte des Vertrages

Verpflichtung der Auftragsverarbeiters zur **Rückgabe oder Löschung** von Daten nach Beendigung der Leistung

Mindestinhalte des Vertrages

Recht zur Überprüfung (Audit-Recht inkl. Mitwirkungspflicht) → Informationspflicht

Mindestinhalte des Vertrages

Unterstützung bei der Umsetzung der Rechte der Betroffenen

Mindestinhalte des Vertrages

Unterstützungspflicht im Hinblick auf Art. 32 – 36

(TOM‘s, Datenschutzverletzungen, DSFA, Konsultation der Behörde)

Auswahl des Dienstleisters

Der Verantwortliche arbeitet nur mit Auftragsverarbeitern,
die **hinreichend Garantien** bieten !!!

Verhaltensregeln als geeignete Garantien

Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern

- die **Ausarbeitung von Verhaltensregeln**, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und
- der **besonderen Bedürfnisse von Kleinstunternehmen** sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.

Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, **können Verhaltensregeln ausarbeiten** …

Art. 40 (1,2)

Zertifizierungen als geeignete Garantien

Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern

- die Einführung von **datenschutzspezifischen Zertifizierungsverfahren**
- sowie von **Datenschutzsiegeln und -prüfzeichen**, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.
- Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

Art. 42 (1)

Zertifizierung

Information Security Management Systeme (ISMS)

European Privacy Seal

https://www.european-privacy-seal.eu

Seminartipp

Security Awareness - die menschliche Firewall (CPE 7)

Kurstermin	CPE	Veranstaltungsort
19.04.2018	7	Akademie Interne Revision GmbH | Anfahrt

Seminarthema

In diesem Seminar werden die notwendigen Elemente erfolgreicher Security Awareness Kampagnen vermittelt. Ausgehend von psychologischen Aspekten und den typischen Herausforderungen werden die erfolgreichen Maßnahmen zur Sensibilisierung, zur Schulung und zum regelmäßigen Training behandelt. Im Rahmen einer Live-Demo wird gezeigt wie die Planung eines Socials Engineering Angriffs durchgeführt wird und welche Werkzeuge typischerweise hierzu angewendet werden (Pishing Emails, USB-Sticks, etc.)

http://www.internerevision.at/seminare/spezialseminare/seminar/security-awareness-die-menschliche-firewall-185/

Vorankündigung

DSGVO Workshop „Was & Wie“

Risikoanalyse als Vorstufe zur Datenschutz-Folgenabschätzung

21. März 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