EU-Datenschutz-Grundverordnung

Attersee, 25.04.2018

Dr. Holger Mühlbauer

www.attersee-consulting.com

EU-Datenschutz-Grundverordnung (EU-DSGVO)

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

- wird nach 2jähriger Übergangsfrist am 25.05.2018 wirksam
- gilt als Verordnung unmittelbar in allen EU-Staaten
- wird ggf. ergänzt durch nationale Datenschutzgesetze
- gilt für personenbezogene Datenverarbeitung in Unternehmen und Behörden
- gilt in der EU und auch außerhalb, wenn Daten von EU-Bürgern verarbeitet werden
- enthält Informations-, Dokumentations- und Organisationspflichten
- enthält Betroffenenrechte

Nationale Datenschutzgesetze

- Österreich: Datenschutz-Anpassungsgesetz 2018

- Deutschland: Datenschutz-Anpassungs- und Umsetzungsgesetz 2018

Was droht

- Beschwerden von (vermeintlich) Betroffenen
- Abmahnungen
- Aufsichtsbehörde
- Bußgelder

Informations-, Dokumentations-, Organisationspflichten

- Datenschutzerklärung mit Rechtebelehrung
- Verarbeitungsverzeichnis
- Auftragsverarbeiter-Vereinbarungen
- Information bei Datenschutzvorkommnis: an Betroffenen und an Aufsicht
- ? Datenschutzfolgenabschätzung: bei sensiblen Daten
- ? Datenschutzbeauftragter: bei Behörden, Unternehmen ab 250 MA (in DE ab 9) oder wenn Verarbeitung sensibler personenbezogener Daten; bei Verzicht Gründe dokumentieren
- Schwerwiegende Datenschutzvorkommnisse binnen 72 Stunden an Aufsichtsbehörde melden

Betroffenenrechte

- Information bei Datenerhebung
- Auskunft
- Berichtigung
- Löschung (erweitert: "Vergessenwerden")
- Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch

Auskunftserteilung

Kostenlos, auch mehrfach, innerhalb von 4 Wochen

- Art und Inhalte der Daten, die verarbeitet werden (z.B. "Kundendaten")
- Rechtsgrundlage (z.B. Liefervertrag; steuerrechtliche Vorschriften)
- Verarbeitungszwecke (z.B. Auftragsabwicklung)
- Speicherdauer (= Löschfristen)
- Datenempfänger (wer, wo, wozu: z.B. Unterauftragnehmer, Finanzamt)
- bei Datenübermittlung nach außerhalb der EU: Sicherheitsgarantien
- ob Auftragsverarbeiter (z.B. IT-Dienstleister, Lohnverrechnung, Lieferdienst)
- bei Entscheidungen, die auf automatisierter Verarbeitung beruhen oder Profiling mit rechtlichen Auswirkungen auf die betroffene Person: Angaben zum verwendeten Verfahren und den Auswirkungen
- Hinweis auf Betroffenenrechte
- Hinweis auf Datenschutzaufsichtsbehörde
- Falls gefragt: welche Datensicherheitsmaßnahmen

Pflicht 1: Datenschutzerklärung (auf Webseite)

Gut auffindbar (z.B. neben Impressum), einfache Sprache

Mindestangaben:
- Kontaktdaten des Unternehmens als verantwortliche Stelle
- alle Zwecke, zu denen personenbezogene Daten verarbeitet werden
- Rechtsgrundlagen für die Datenverarbeitung
- Speicherfristen
- Auflistung der Betroffenenrechte gemäß DSGVO
- Kontaktdaten der zuständigen Datenschutzaufsichtsbehörde (für Anfragen und Beschwerden)

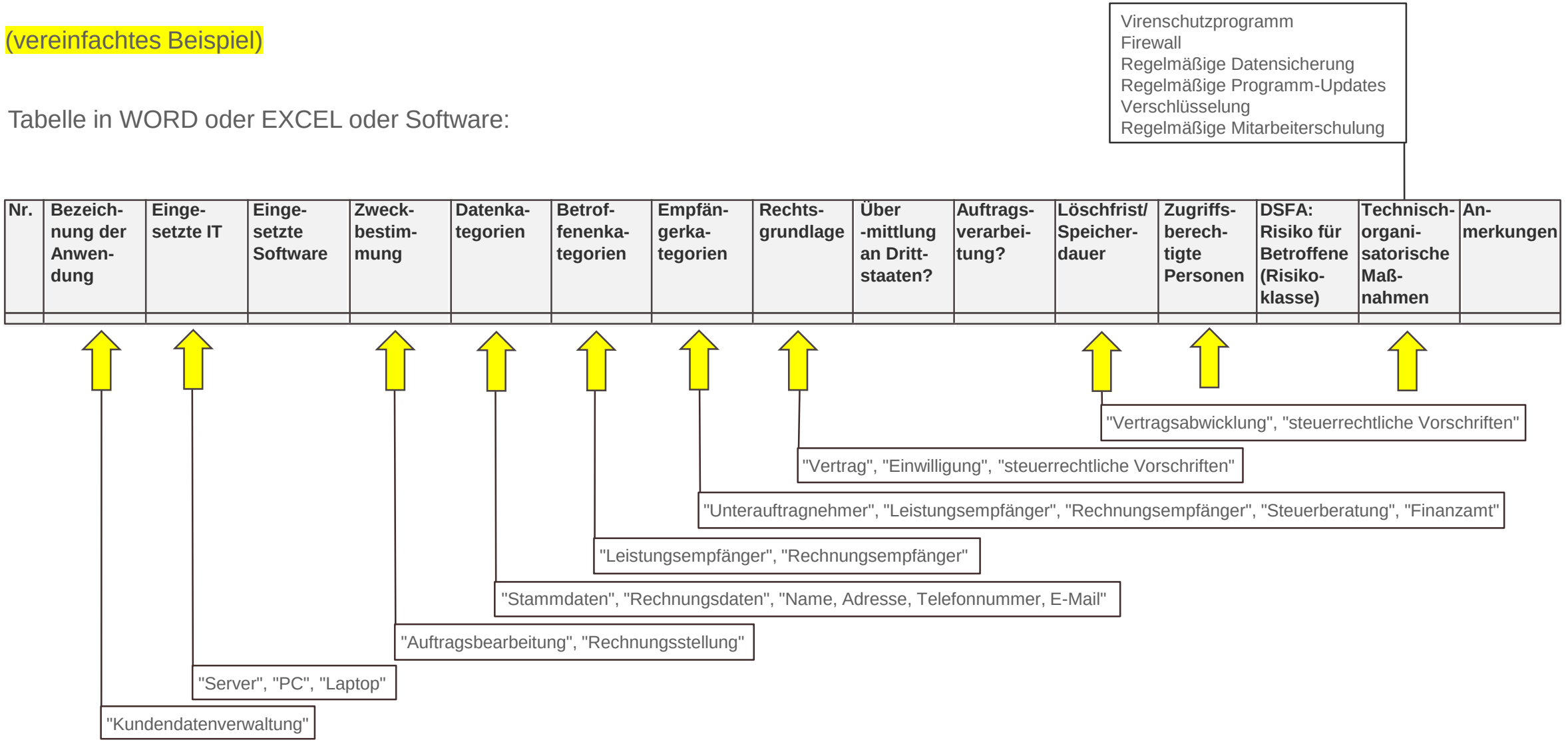
Einzelfallbezogene Informationspflichten je nach tatsächlichen Gegebenheiten:
- Kontaktdaten des Datenschutzbeauftragten, sofern einer bestellt ist
- berechtigte Interessen, die mit der Datenverarbeitung verfolgt werden
- Empfänger (Dritte), an die erhobene Daten übermittelt werden
- Absicht, die Daten ins Nicht-EU-Ausland zu übertragen und der diesbzügliche Rechtsrahmen
- ggf. Verpflichtung zur Bereitstellung der Daten seitens des Betroffenen und Folgen der Nichtbereitstellung
- Einsatz von automatisierten Entscheidungsfindungen, wenn praktiziert
- Einsatz von Tools zur Webseitennutzungsanalyse und deren Funktionsweise bzw. Art der Datenerhebung und -verarbeitung
- Einsatz von Cookies und deren Art, Umfang und Zweck
- Social-Media-Applikationen und deren Art und Zweck, sowie die sich aus der Nutzung für den Betroffenen ergebenden technisch-rechtlichen Implikationen, z.B. Datenübermittlung an den Social Media Provider
- Auftragsdatenverarbeitung

Hinweis: Diese Angaben sind nicht abschließend. Es gibt keine für alle Konstellationen einheitlich gültige oder anwendbare Datenschutzerklärung, sondern diese muss auf die tatsächlichen Verhältnisse angepasst sein. Die Erklärung muss in verständlicher Sprache, d.h. nicht in juristischem oder IT-Kauderwelsch verfasst sein und sollte eine sinnvolle Länge nicht überschreiten. Sofern auf längere Erläuterungen nicht verzichtet werden kann, bietet sich eine Kurzversion mit "anklickbaren" Textfenstern für nähere Ausführungen an.

Pflicht 2: Verarbeitungsverzeichnis (vorzuzeigen bei Kontrolle)

(vereinfachtes Beispiel)

Tabelle in WORD oder EXCEL oder Software:



Pflicht 3: Technisch-organisatorische Maßnahmen (intern)

- Datenhaltung (Sicherung)
- Kommunikation (Verschlüsselung?)
- Management (Verantwortlichkeiten)
- Zutrittskontrolle (wer kommt hinein)
- Zugangskontrolle (wer nutzt)
- Zugriffskontrolle (wer greift auf was zu)
- Weitergabekontrolle (an wen)
- Eingabekontrolle (durch wen)
- Auftragskontrolle (Datenlauf)
- Verfügbarkeitskontrolle (physischer Schutz)
- ggf. getrennte Verarbeitung (Zweckbestimmung)

- Webseitenzertifikat!
- E-Mail- und Datenträgerverschlüsselung
- Mitarbeiterschulung!

Besonderheit 1: Auftragsverarbeitung?

- externer IT-Dienstleister?
- externer Server, Cloud?
- externe Lohnverrechnung?
- ...

➡ Vertrag mit Datenschutzbestimmungen!

Besonderheit 2: Datenübermittlung in Drittländer?

- "Geeignete Garantien“
- "EU-Standardvertrag"
- "Privacy Shield" (USA)
- "Corporate Binding Rules"

Besonderheit 3: Newsletter

Mit Einwilligung oder bei berechtigtem Interesse

Bei bestehender Geschäftsbeziehung

Altkunden: Bisheriger Versand kann fortgesetzt werden, wenn im Rahmen der Zweckbestimmung der bisherigen Geschäftsbeziehung, und nicht widersprochen wurde, nachträgliche Einwilligungseinholung ist gleichwohl empfehlenswert (wenn praktikabel)

Neukunden ab 25.05.2018: Mit Einwilligung
- mit doppelter Bestätigung ("Double opt-in"), um sicherzugehen
- Einwilligung darf nicht versteckt, voraktiviert oder an eine Leistungserbringung gekoppelt sein

Newsletter-Versendung muss regelmäßig erfolgen, andernfalls "erlischt" die Einwilligung (mindestens ein- bis zweimal jährlich)
Empfänger muss jederzeit abwählen können

Bei keiner bestehenden Geschäftsbeziehung

Sofern keine ausdrückliche Einwilligung vorliegt, Betrachtung analog zu Direktmarketing, d.h. Interessenabwägung zwischen berechtigtem Interesse des Versenders und des Betroffenen

- Nachweis der vorgenommenen Interessenabwägung
- Vorsicht: Datenschutzrechtliche und wettbewerbsrechtliche Grauzone!

"ECG-Liste" beachten (https://www.rtr.at/de/tk/TKKS_ECGListe)

Technische Maßgaben

Newsletterfunktionalität auf Webseite (Eintragungsmöglichkeit)
- mit doppelter Bestätigung ("Double opt-in")
- Einwilligung darf nicht versteckt, voraktiviert oder an eine Leistungserbringung gekoppelt sein
- empfehlenswert: Protokollierung des Zeitpunktes

Bei Versand über Dienstleister, z.B. Web-Applikationen
- wenn Dienstleister in der EU ansässig, dann = Auftragsverarbeitung i.S.d. DSGVO
- wenn nicht in der EU ansässig, dann "EU-Standardvertrag" notwendig
- wenn z.B. in den USA ansässig, dann "Privacy Shield"-Anwendung

- Abbestellmöglichkeit (Mailkontakt, Link)
- Tracking des Leseverhaltens (z.B. Tracking Pixel, die beim Öffnen nachgeladen werden) nur mit vorheriger Einwilligung
- Problem: bei einigen Newsletter-Programme muss Tracking vom Versender deaktiviert werden, manche Programme ermöglichen keine Deaktivierung
- Newsletter-Funktionalität muss mit Sicherheitszertifikat gesichert sein

1. Postkarte an Bestandskunden

Sehr geehrte secuview Abonnentin,
sehr geehrter secuview Abonnent,

zweimal im Jahr senden wir Ihnen kostenfrei unsere Kundenzeitschrift **secuview** zu, die Ihnen Neuigkeiten, Trends und Hintergrundinformationen aus der Welt der Cybersicherheit für Behörden und Unternehmen bietet.

Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung (EU-DSGVO) in Kraft. Diese Veränderung macht es notwendig, dass Sie secuview erneut abonnieren und dabei die neue Datenschutzerklärung akzeptieren. **Ohne diese Bestätigung können wir Ihnen das Magazin ab sofort leider nicht mehr zustellen.**

Die gute Nachricht: Die Neuanmeldung dauert **nur ca. eine Minute.** Rufen Sie einfach die folgende Webseite auf, geben Sie die erforderlichen Daten ein und erhalten Sie secuview weiterhin wie gewohnt und kostenfrei:

www.secunet.com/secuview

Vielen Dank!

Beste Grüße und bis zur nächsten Ausgabe!

Ihre secuview Redaktion

secunet

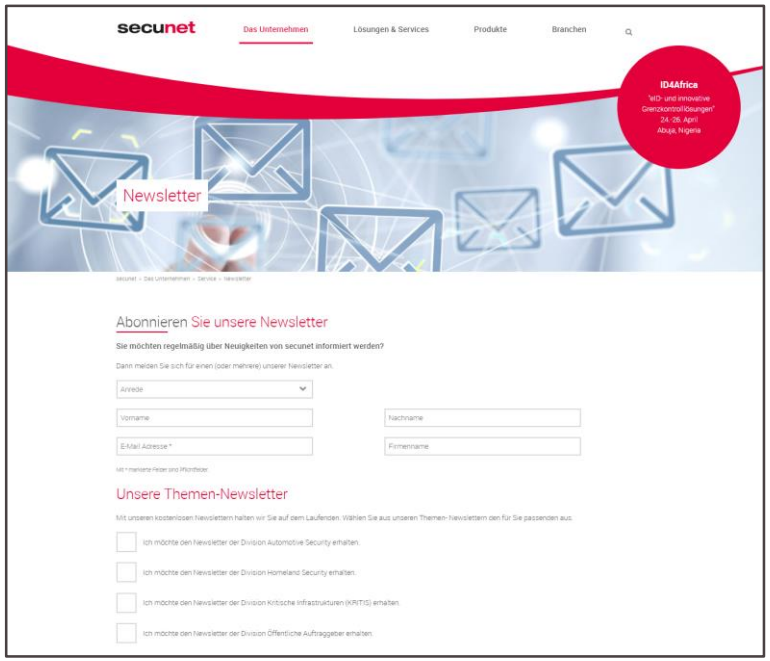
secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Kontakt: Marc Pedack
Telefon: +49 201 5454-3831

POSTEINGANG 23. APR. 2018 TeleTrusT Bundesverband IT-Sicherheit e.V.

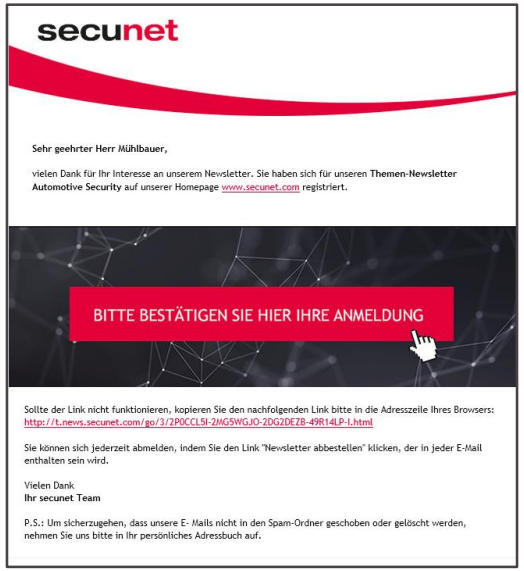
Deutsche Post DIALOGPOST

TeleTrusT
Bundesverband
Herrn Dr. Holger Mühlbauer
Chausseestraße 17
10115 Berlin

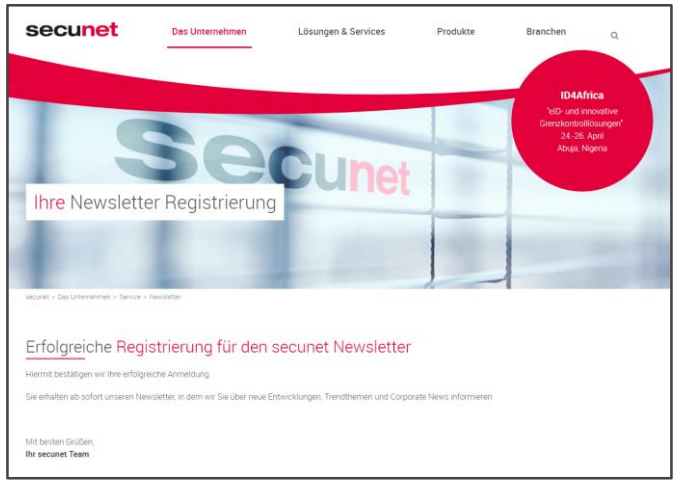
2. Webseite mit Neueintragung



3. Mail mit Bestätigungs-Link ("Double opt-in")



4. Bestätigungsmail



Vorsicht

- "DSGVO-Zertifizierung"
- Abonnement für "DSGVO-Software"
- teure Berater

Sehr gut: WKO

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html

EU-Datenschutz-Grundverordnung

Danke, viel Spaß und viel Glück.

Dr. Holger Mühlbauer
@ttersee consulting
Zell/Mitterweg 8
4865 Nussdorf a. A.
holger.muehlbauer@attersee-consulting.com