

# Kundeninformation "DSGVO"

## id newmedia KnowHow - für Sie ...

40 Jahre Erfahrung, 40 Jahre Dienst am Kunden

- ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen
- ganzheitliche, sichere IT-Lösungen für Behörden
- DSGVO / BDSG-neu Umsetzung
- Analyse kritischer IT-Sicherheitsstrukturen
- Digitales Klassenzimmer in Schulen
- Digitales Büro
- Computer Forensik

id newmedia Einsteinstrasse 24 82152 Planegg-Martinsried 0160-48 28 918

id newmedia Büro Germering 089-899 799 39 info@id-newmedia.de www.id-newmedia.de USt.-Id Nr. DE128145303



### Datenschutzgrundverordnung (DSGVO) – Was ist die DSGVO?

Die Datenschutzgrundverordnung der EU (DSGVO) ist eine Reihe von Gesetzen, die seit 25. Mai 2018 anwendbar sind. Sie befassen sich damit, wie Unternehmen die privaten Daten von Einzelpersonen erfassen und handhaben. Die DSGVO ist eine neue Reihe von Gesetzen, die sich auf in der EU ansässige Unternehmen sowie auf in der EU tätige ausländische Unternehmen auswirken. Unternehmen, die die Gesetz Anforderungen der DSGVO nicht seit dem 25. Mai 2018 erfüllen, müssen ggf. mit hohen Strafen rechnen.

Die neue Verordnung soll einen besseren Schutz der Persönlichkeitsrechte des Einzelnen garantieren. Alle Informationen dürfen nur noch mit Zustimmung der betreffenden Person gesammelt werden, wobei diese jederzeit widerrufen werden kann. Artikel 17 der Datenschutz Grundversorgung besagt, dass die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, dem der Verantwortliche unterliegt.



### Warum wurde die DSGVO eingeführt?

Die DSGVO wurde eingeführt, um zu vereinheitlichen, wie Unternehmen, die Online-Dienste anbieten, die Daten eines Besuchers auf ihrer Website oder die Daten ihrer registrierten Nutzer verarbeiten. Die Methoden der Erhebung von personenbezogenen Daten im Internet, und die Gründe dafür haben erheblich verändert. Daraus ergab sich die Notwendigkeit einer aktualisierten Regelung der Datenverarbeitung durch Unternehmen.



## Aufbau der DSGVO

Die DSGVO besteht aus 99 Artikeln in elf Kapiteln:

**Kapitel 1** (Artikel 1 bis 4): Allgemeine Bestimmungen (Gegenstand und Ziele, sachlicher und räumlicher Anwendungsbereich, Begriffsbestimmungen)

**Kapitel 2** (Artikel 5 bis 11): Grundsätze und Rechtmäßigkeit (Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Bedingungen für die Einwilligung, Verarbeitung besonderer Kategorien personenbezogener Daten)

**Kapitel 3** (Artikel 12 bis 23): Rechte der betroffenen Person (Transparenz und Modalitäten, Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten, Berichtigung und Löschung – das „Recht auf Vergessenwerden“ –, Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall einschließlich Profiling)

**Kapitel 4** (Artikel 24 bis 43): Verantwortlicher und Auftragsverarbeiter (Allgemeine Pflichten, Sicherheit personenbezogener Daten, Datenschutz-Folgenabschätzung und vorherige Konsultation, Datenschutzbeauftragter, Verhaltensregeln und Zertifizierung)

**Kapitel 5** (Artikel 44 bis 50): Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

**Kapitel 6** (Artikel 51 bis 59): Unabhängige Aufsichtsbehörden

**Kapitel 7** (Artikel 60 bis 76): Zusammenarbeit und Kohärenz, Europäischer Datenschutzausschuss

**Kapitel 8** (Artikel 77 bis 84): Rechtsbehelfe, Haftung und Sanktionen

**Kapitel 9** (Artikel 85 bis 91): Vorschriften für besondere Verarbeitungssituationen (u. a. Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit, Datenverarbeitung am Arbeitsplatz, Zugang der Öffentlichkeit zu amtlichen Dokumenten, Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken, bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften)

**Kapitel 10** (Artikel 92 bis 93): Delegierte Rechtsakte und Durchführungsrechtsakte

**Kapitel 11** (Artikel 94 bis 99): Schlußbestimmungen (u. a. Aufhebung der Richtlinie 95/46/EG und Inkrafttreten der DSGVO)

## Was bedeutet das für mein (kleines) Unternehmen ?

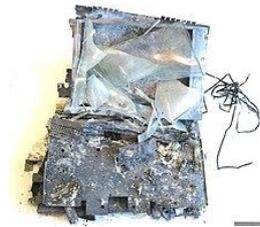
Die Definition des Begriffs der „personenbezogenen Daten“ umfaßt nunmehr nicht nur die Merkmale, die eine Person *direkt* identifizieren (z.B. Name und Anschrift), sondern auch die Angaben, die sie *mittelbar identifizierbar* machen, wie z.B.



- IP-Adressen(email-Korrespondenz, Internet),
- Cookies (Internet-Shops, Besuch der Firmen-Webseite),
- RFID-Tags (Ware, Ausweise, Schließanlagen, etc.),
- Standortdaten (Mobiltelefon-Daten, Fuhrparküberwachung, Türspione, etc.).



## Was muß ich als (kleines) Unternehmen tun ?



### Technische Sicherheitsmaßnahmen einrichten !

Die zu implementierenden technischen und organisatorischen Sicherheitsmaßnahmen sollen sich an den Schutzziele der Vertraulichkeit, der Integrität und Authentizität der personenbezogenen Daten orientieren.



### Organisatorische Sicherheitsmaßnahmen einrichten !

Unternehmen (und Behörden) müssen eine Sicherheitspolitik etablieren und nachweisen, die auf der Grundlage einer Risikoanalyse die unter anderem die nachfolgend genannten Punkte umfaßt :

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten ;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit und den Zugang zu Daten im Falle eines physischen oder technischen Zwischenfalls rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.



Im Ergebnis sind Unternehmen und Behörden damit verpflichtet, ein Informationssicherheit - Managementsystem und ein Risikomanagement zu etablieren, um den Anforderungen der DSGVO zu genügen :

→ **KRITIS**

Diese Verpflichtung trifft nicht nur Unternehmen und Behörden, die ihre eigenen Daten verarbeiten, sondern ausdrücklich auch diejenigen, die die Daten im Auftrag anderer verarbeiten.

**Was ist also zu tun ?**



### **Datenschutzrechtliche Freigabe**

= Aufgabe des verarbeitenden Geschäftsbereiches & Datenschutzbeauftragte/r

1. Bezeichnung des Verfahrens;
2. Zweck & Rechtsgrundlage der Erhebung-Verarbeitung-Nutzung;
3. Art der gespeicherten Daten;
4. Kreis der Betroffenen;
5. Art der regelmäßig zu übermittelnden Daten und der Empfänger;
6. Regelfristen für die Löschung bzw. Prüfung der Löschung;
7. verarbeitungs- und nutzungsberechtigte Personengruppen;
8. im Fall des Art. 6 Abs. 1 bis 3 die Auftragnehmer;
9. Empfänger vorgesehener Datenübermittlungen in Drittländer.



### **Sicherheit der Verarbeitung**

= Aufgabe der Geschäftsleitung & Datenschutzbeauftragte/r

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

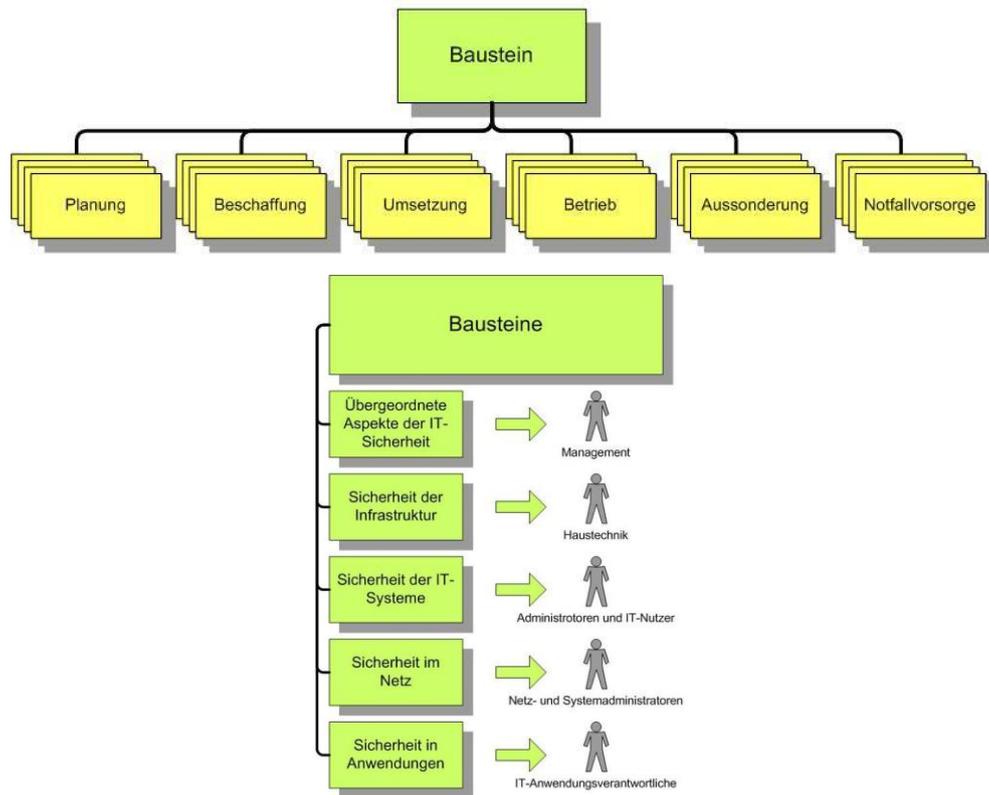
treffen der **Verantwortliche** und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung wie folgt verbunden sind :

- Vernichtung, Verlust oder Veränderung;
- unbeabsichtigte
- oder unrechtmäßige
- oder unbefugte Offenlegung bzw. unbefugter Zugang zu



personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden (z. B. Kundenkartei, -datenbank, Debitoren-/Kreditorendaten).

Alles verwendete Bildmaterial : licensed by Vital Imagery Ltd. / id-newmedia / BSI



**id-newmedia unterstützt Sie wie folgt :**

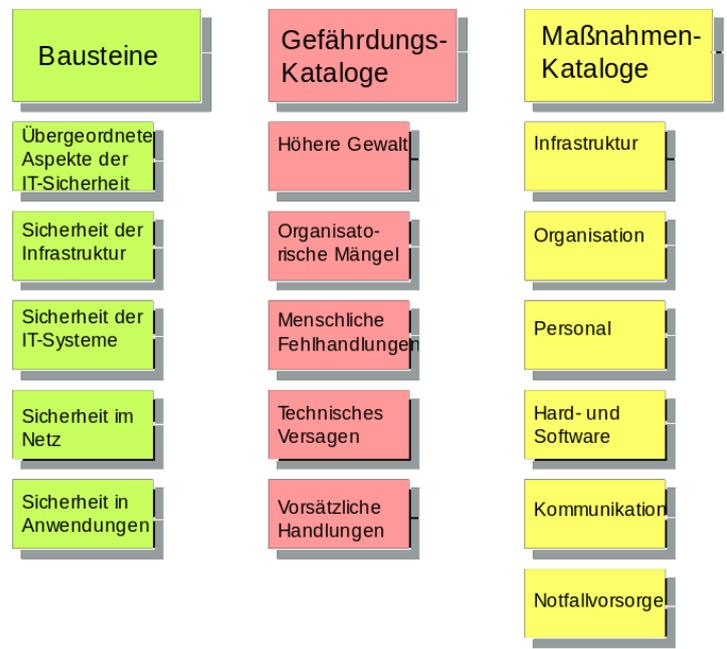


Diagramme :BSI / id-newmedia