

Jede(r) Mitarbeiter/in der UMGIS Informatik GmbH hat zumindest gelegentlich mit personenbezogenen Daten zu tun. Es ist daher notwendig, sich mit den wichtigsten Bestimmungen des Bundesdatenschutzgesetzes (BDSG) vertraut zu machen.

Im Folgenden werden die wichtigsten Abschnitte des BDSG dargestellt, die bei der täglichen Arbeit von Bedeutung sein können.

I. Grundbegriffe

Grundlage für den Datenschutz ist das Bundesdatenschutzgesetz (BDSG) vom 23.05.2001. Es ersetzt das bisherige „Bundesdatenschutzgesetz vom 20.12.1990“.

Zweck des Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Personenbezogene Daten (§3 BDSG) sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener):

Automatisierte Verarbeitung ist die **Erhebung, Verarbeitung oder Nutzung** personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht-automatisierte Datei ist jede nicht-automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

Das BDSG unterscheidet im Einzelnen

Erheben:	Beschaffen von Daten über den Betroffenen,
Verarbeiten:	das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten Im Einzelnen ist dies, ungeachtet der dabei angewendeten Verfahren:
1. Speichern:	das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern:	das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln:	das Bekannt geben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass a) die Daten an den Dritten weitergegeben werden oder b) der Dritte zur Einsicht oder zum Abruf bereitgehaltener Daten einsieht oder abrufen
4. Sperren:	das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
Löschen:	das Unkenntlichmachen gespeicherter personenbezogener Daten.
Nutzen:	jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Anonymisieren:	das Verändern personenbezogener Daten derart, dass Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
Pseudonymisieren:	ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.
Verantwortliche Stelle:	jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
Empfänger:	jede Person oder Stelle, die Daten erhält
Dritter:	ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte ist nicht der Betroffene!

II. Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (§4).

Eine Auflistung für zulässige Datenverarbeitung in so genannten nicht öffentlichen Stellen erfolgt im BDSG § 28: Die wichtigsten Zulässigkeitsvoraussetzungen sind:

- Im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses (Beispiel: Firma speichert die Daten des Mieters)
- Wenn es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass dadurch das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung Nutzung überwiegt (Kundendatenspeicherung)
- Wenn die Daten aus allgemein zugänglichen Quellen zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Diese Daten müssen „nach Treu und Glauben und auf rechtmäßige Art erhoben werden“.

Weitere „Spezialregelungen“ für zulässige Erhebung, Verarbeitung und Nutzung siehe BDSG §§ 28 – 31.

III. Schutzmaßnahmen für personenbezogene Daten

Wer im Rahmen der Zulässigkeitsvoraussetzungen Daten verarbeitet, ist verpflichtet, die vom Gesetz geforderten Schutzmaßnahmen zu beachten!

Den mit der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (DATENGEHEIMNIS). Diese Personen müssen bei der Aufnahme ihrer Tätigkeiten auf das Datengeheimnis verpflichtet werden. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort!

Hierzu dient das Formblatt „Verpflichtung auf das Datengeheimnis“.

Alle Stellen, die personenbezogene Daten verarbeiten, müssen – im angemessenen Verhältnis zu dem angestrebten Schutzzweck- die technischen und organisatorischen Maßnahmen treffen, die notwendig sind, um die Ausführung der im BDSG genannten Anforderungen zu gewährleisten. (§ 9 und Anlage zum § 9).

Dies muss von allen Verantwortlichen beachtet werden, da im Falle eines durch unzulässige oder unrichtige automatisierte Datenverarbeitung entstehenden Schaden der Betroffenen berechtigt ist, Schadenersatz zu fordern. Geeignet sind allgemein alle Schutzmaßnahmen, die den Missbrauch von personenbezogenen Daten verhindern; dies beginnt bei der Beschränkung des Kreises der Zugriffsberechtigten bis zum Gebrauch von Pass- und Kennwörtern am PC. Manuelle Dateien sowie Datenträger müssen in verschließbaren Schränken/Schreibtischen so gesichert sein, dass sie von Unbefugten nicht eingesehen oder benutzt werden können.

Der Gesetzgeber hat für die Verstöße gegen die Bestimmung des Datenschutzes in Bußgeldvorschriften (§ 43) und Strafvorschriften (§44) Geldbußen bis zu 250.000,00 € und Freiheitsstrafen bis 2 Jahren angedroht.

IV. Betrieblicher Datenschutz und Datensicherheit

Der Beauftragte für Datenschutz hat nach § 4g BDSG die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen und hierzu umfassende Überwachungsaufgaben; er arbeitet eng mit dem Beschäftigten für Datensicherheit zusammen; über Vorhaben der automatisierten Datenverarbeitung personenbezogener Daten ist er deshalb rechtzeitig zu unterrichten. („**BRINGSCHULD**“ der Verantwortlichen!)

Für weitere Detailinformationen wenden Sie sich bitte an den betrieblichen Datenschutzbeauftragten.

Darmstadt, den 01.06.2016

Martin Wacker
Geschäftsführung

Kennzeichnung Mitarbeiter

Datum

Unterschrift

W:\Mitarbeiter_Dokumente_Anweisungen\Betriebsanweisung_Datenschutz.docx