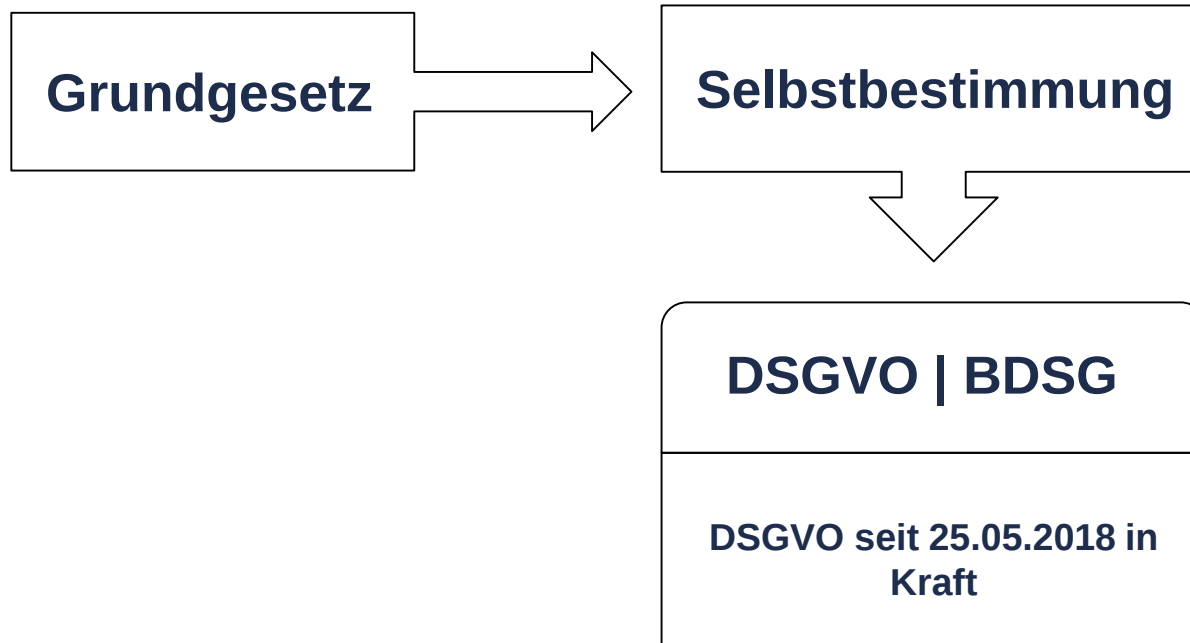


Datenschutz

afm assekuranz-finanz-makler GmbH

Hamburg, den 8. Juni 2018



<https://www.datenschutz-grundverordnung.eu/>

Anwendung DSGVO | BDSG

- nur bei automatisierter Verarbeitung personenbezogener Daten
- Besonderer Schutz:
„Besondere personenbezogene Daten“ (bspw. Gesundheitsdaten, Finanzstatus, ...)
- Regelt Sicherheit beim Umgang mit personenbezogenen Daten

Wesentliche Neuerungen durch die DSGVO

- Erweiterter Geltungsbereich
- Umfassendere Definitionen datenschutzrelevanter Begrifflichkeiten
- Weitreichendere Rechte für die betroffenen Personen
- Erweiterte Haftung für Auftragsverarbeiter
- Verschärfte Sanktionen

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, z.B.

- Name
- Adresse
- Telefonnummer
- Autokennzeichen
- Online Kennungen (wie z.B. die IP-Adresse).

Es ist ausreichend, wenn die Information zu einer Person in irgendeiner Art zugeordnet und somit ein Personenbezug hergestellt werden kann.

Rechtmäßige Verarbeitung personenbezogener Daten

DSGVO folgt dem bisher bekannten Prinzip des sogenannten „Verbotes mit Erlaubnisvorbehalt“ aus dem deutschen Recht. Dies besagt, dass eine Verarbeitung personenbezogener Daten nur dort zulässig ist, wo sie entweder im Wege einer Einwilligung des betroffenen oder eines ausdrücklichen gesetzlichen Erlaubnistatbestandes gestattet ist.

Rechtmäßigkeit nach **Art. 6 Abs. 1 DSGVO** u.a. bei folgenden Voraussetzungen:

- Einwilligung der betroffenen Person
- Die Datenverarbeitung ist zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen notwendig
- Die Datenverarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung nötig
- ...

Praxishinweis I

- Akquise Firmenkunden und Empfehlungsnahme aus unsere Sicht unverändert
- übergeordnetes Interesse überwiegt (mutmaßliche Einwilligung)

Praxishinweis II

- Bestandskunden haben i.d.R. bereits einen Maklerauftrag unterschrieben oder es liegt ein Auftragsverhältnis vor
- Einwilligung empfohlen im Rahmen der Service-Checks

Grundsätze bei der Umsetzung der DSGVO

- **Rechtmäßigkeit** - Verarbeitung nach Treu und Glauben
- **Zweckbindung** - Datenerhebung für festgelegte, eindeutige und legitime Zwecke
- **Datenminimierung** - dem Zweck angemessene und für die Zwecke der Verarbeitung notwendige Maß beschränkte Datenerhebung
- **Richtigkeit** - Daten sollen sachlich richtig und auf dem neuesten Stand sein
- **Speicherbegrenzung** - die Identifizierung der betroffenen Personen soll nur so lange möglich sein, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- **Integrität und Vertraulichkeit** - Gewährleistung einer angemessenen Sicherheit der personenbezogenen Daten, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Rechte der betroffenen Person nach Art. 12-23 DSGVO

- Einsicht
- Änderung
- Löschung („Recht auf Vergessenwerden“)
Ausnahmen nach Art. 17 Ziffer 3 DSGVO u.a. soweit die Verarbeitung erforderlich ist:
 - zur Erfüllung einer rechtlichen Verpflichtung
 - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Sperrung
- Übertragung

Allgemeine Pflichten

		afm Holding	Büro vor Ort
Bestellung eines Datenschutzbeauftragten (intern oder Dienstleister)	i. d. R. ab 10 Personen die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind - generell sofern die Kerntätigkeit in der Verarbeitung besonders schützenswerter personenbezogener Daten nach Art. 9 DSGVO besteht (z.B. Gesundheitsdaten)	☒	
Führen des Verzeichnisses über Verarbeitungstätigkeiten (früher „Verfahrensverzeichnis“)	- Bildet den Datenfluss im Unternehmen ab - Geht allgemein um Daten: von Kunden bis Mitarbeiter; von der Erhebung über Speicherung bis zur Löschung	☐	☐
Quercheck Technisch Organisatorische Maßnahmen (TOMs);	Die einzelnen Verfahren werden noch mal mit einem „Sicherheitslevel“ versehen (Login, Schlüssel, Anonymisierung der Daten...)	☐	☐
Datenschutzrichtlinie	Das interne Datenschutzkonzept ergänzt um Verhaltensregeln, Passwordkonvention und Social Media Guideline	☒	
Datenschutzerklärung	Wird z.B. auf der Webseite veröffentlicht – hier werden u.a. diverse Tools dargestellt, die auf der Seite genutzt werden	☒	
Verträge und Dokumente	- Verträge zur Auftragsverarbeitung (z.B. Vergleichsprogramme, Dropbox) - Verschwiegenheitserklärungen (z.B. Hausmeister, Putzfirmen)	☐	☐
Schulungen	Regelmäßige Schulung der Mitarbeiter	☐	☐



Typische Schwachstellen

- Papierentsorgung & Abfalleimer
- USB-Sticks und -Ladefunktion, Speicherkarten & Datenträger
- Mobile Endgeräte
- Kommunikation & eMail
- Datensicherung & Datensicherheit

Typische Schwachstellen

- Social Hacking
- Trojaner, Phishing, Viren, Erpressung
- Automatisierte Angriffe
- Datendiebstahl
- Reputation & DDoS

Typische Fehler

- Zugang zu Betriebsräumen
- Aussagen am Telefon
- Offener Umgang mit vertraulichen Unterlagen
- Datenschutz nur im Büro (vs. Reise, HomeOffice, ...)
- Schwache Passwörter & Weitergabe

Technische Schutzmaßnahmen nach DSGVO

geeignete technische und organisatorische Maßnahmen (TOM) sowie interne Strategien und Maßnahmen, die

- a) den Grundsatz des Datenschutzes durch Technik (privacy by design) entsprechen und
- b) datenschutzfreundliche Voreinstellungen (privacy by default) sicherstellen

Maßnahmen können sein:

- Minimierung der Verarbeitung personenbezogener Daten
- Pseudonymisierung personenbezogener Daten
- Überwachung der Datenverarbeitung
- Verbesserung der Sicherheitsfunktionen

Meldung Datenschutzverletzung

Meldung innerhalb von 72 Stunden ab Kenntnis des Verstoßes an die zuständige Aufsichtsbehörde

- Beschreibung des Vorfalls
- Kontaktdaten der verantwortlichen Stelle
- Wahrscheinliche Folgen des Vorfalls
- Informationen über die ergriffenen Maßnahmen

Unverzügliche Benachrichtigung des Betroffenen

Neue Unterlagen

- Verträge und Einwilligungen IWM | BeraterPortal
- afm Datenschutzrichtlinie BeraterPortal
- afm Verhaltensregeln BeraterPortal
- afm Social Media Guideline BeraterPortal
- FAQs und Präsentation BeraterPortal
- Notfallpläne BeraterPortal
- Weitere Unterlagen und Mustervorlagen folgen....