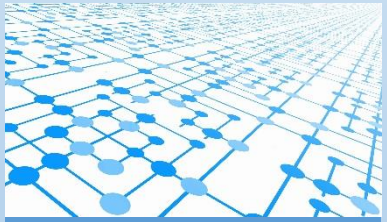
Philipp von Wartburg
CTO / CDO
Geschäftsleiter Technologie & IT
Prokurist

DSGVO – Was Sie als Makler wissen müssen

- **Wie die DGFRP Sie unterstützt**
- **Tipps für die Praxis**
- **Fragen und Antworten**



10.04.2018

Deutsche Gesellschaft für
RuhestandsPlanung
Die Alternative zu Private Banking

Hintergrund

- DSGVO: Datenschutz-Grundverordnung
- BDSG: Bundesdatenschutzgesetz
- LDSG: Landesdatenschutzgesetz
- DSGVO bereits in Kraft getreten, entfaltet am 25.05.2018 ihre Wirkung
- Ziel: EU-einheitliche Regulierung
- Enthält „Öffnungsklauseln“ für nationale Regelungen
- BDSG-Neufassung wird ebenfalls am 25.05.2018 in Kraft treten
- Datenverarbeitungsprozesse und -Dokumente sollten angepasst werden

DSGVO – Was Sie wissen müssen

Die neue DSGVO ist nicht so schlimm, wie man gelegentlich hört oder liest.

Es kommt auf die praktische Umsetzung an („Alltagstaugliche Tiefe“).

Vieles war schon immer so, nur wurde es nicht kontrolliert.

Mehrwert für das eigene Unternehmen schaffen (z.B. Stellvertreter, Notfallpläne, Prozessverbesserung, Vorbeugung, etc.)

Die Aufsichtsbehörde ist kein Gegner!
(Problematisch sind eher die Mitbewerber…)

Der Datenschutz-Beauftragte

- **Datenschutz-Beauftragter**
  Braucht jedes Unternehmen, das entweder besonders schützenswerte/sensible Daten verarbeitet und/oder mehr als 9 Mitarbeiter mit Datenverarbeitungstätigkeit besitzt.
  - Externer Datenschutz-Beauftragter: Macht Sinn, wenn man keinen internen Mitarbeiter ausbilden bzw. beschäftigen möchte.
  - Interner/betrieblicher Datenschutz-Beauftragter: Genießt besonderen Status (Sonder-kündigungsschutz). Darf nicht der IT-Verantwortliche/Geschäftsführer sein (Interessenkonflikt).
  Achtung „besonders sensible Daten“: Gesundheitsdaten? Nur wenn dauerhaft und häufig.

- **Datenschutz-Ansprechpartner**
  Braucht jedes Unternehmen. Kontaktperson für Fragen und Informationen.

Der Datenschutz-Beauftragte ist nur beratend tätig.
Verantwortlich ist immer die Geschäftsleitung!

DSGVO – Was Sie wissen müssen

Der Datenschutz-Beauftragte der DGFRP

Dipl.-Ing. Roland Schad

- IT-Architekt
- DSB mit 23 Jahren Berufserfahrung
- IT-Dienstleister Schwerpunkt IT-Sicherheit
- 11 Jahre DSB für Bundeswehr
- 10 Jahre DSB für FondsKonzept
- ISO 27001 Lead Auditor
- SABSA Security Architecture

Ansprechpartner bei der DGFRP:
Philipp von Wartburg, p.vonwartburg@dgfrp.de

Deutsche Gesellschaft für RuhestandsPlanung
Die Alternative zu Private Banking
Deutsche Gesellschaft für RuhestandsPlanung mbH

BESTELLUNG ZUM DATENSCHUTZBEAUFTRAGTEN

Im Zuge der Umsetzung der DSGVO bestellen wir im gegenseitigen E nvernehmen mit Wirkung zum 1. März 2018

Herrn Roland Schad
Hugo-Weiss-Straße 29
81827 München

zum betrieblichen Datenschutzbeauftragten der

Deutsche Gesellschaft für RuhestandsPlanung mbH

gemäß Art. 37 ff. DSGVO in Verbindung mit §38 BDSG (neu). Wir kommen damit unserer gesetzlichen Verpflichtung nach.

Ihre Aufgabe als Datenschutzbeauftragter ist es, durch Beratung und Schulungen auf die Einhaltung der Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes und anderer Rechtsvorschriften über den Datenschutz hinzuwirken. Im Einzelnen ergibt sich die Aufgabe des betrieblichen Datenschutzbeauftragten aus Artikel 39 DSGVO. Sie sind bei der Erfüllung Ihrer Aufgabe von allen Mita beitern und Mitarbeiterinnen zu unterstützen.

Alle Mitarbeiter und Mitarbeiterinnen können sich in Angelegenheiten des Datenschutzes an Sie wenden.

Sie sind auf dem Gebiete des Datenschutzes weisungsfrei und der Geschäftsleitung direkt unterstellt. Zuständig ist Herr Philipp von Wartburg.

Altötting, 2018 — München, 2018

Philipp von Wartburg — Roland Schad

DIE ALTERNATIVE ZU PRIVATE BANKING
Geschäftsführer Peter Härtling · Amtsgericht Traunstein · HRB 8039 · Gerichtsstand Altötting
VR-Bank Altötting · BLZ 710 610 09 · BIC GENODEF1AOE · KONTO 655 309 · IBAN DE03 7106 1009 0000 6553 09
Gläubiger-ID DE51 ZZZ0 0000 7459 51 · USt-ID DE155068659 · Steuer-Nr. 141/132/70005

Art. 5 DSGVO – Grundsätze für die Verarbeitung (1)

Personenbezogene Daten müssen…

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“)
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)

Art. 5 DSGVO – Grundsätze für die Verarbeitung (2)

- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“)
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Grundprinzipien des Datenschutzes

1. **Rechtmäßigkeit** – Sie dürfen Daten nur entsprechend dem Gesetz verarbeiten, was an sich selbstverständlich ist.
2. **Transparenz** – Die Verarbeitung personenbezogener Daten muss für Betroffene nachvollziehbar sein, was zum Beispiel eine verständliche und vollständige Datenschutzerklärung erfordert. Die Informationspflichten wurden mit Art. 13 und 14 DSGVO erhöht und erfordern beispielsweise einen Hinweis auf die Rechtsgrundlage der Verarbeitung.
3. **Verbot mit Erlaubnisvorbehalt** – Das bedeutet, dass jede Verarbeitung personenbezogener Daten verboten ist, außer wenn sie per Gesetz erlaubt wurde.
4. **Zweckbindung** – Das Gebot der Zweckbindung soll sicherstellen, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben worden sind. Das heißt man muss sich bereits zu Beginn von Verarbeitungsprozessen Gedanken machen, wofür die Daten benötigt werden und dies dokumentieren. Eine nachträgliche Zweckänderung ist nur zulässig, wenn sie „mit dem ursprünglichen Zweck vereinbar ist“.
5. **Datenminimierung** – Unternehmen müssen die Verarbeitung von personenbezogenen Daten auf das dem Verarbeitungszweck notwendige Maß beschränken. Eine „Datenerhebung auf Vorrat“ ist verboten.
6. **Integrität und Vertraulichkeit** – Daten müssen durch technische und organisatorische Maßnahmen vor unbefugter Verarbeitung, Zerstörung, Veränderung oder Verlust geschützt werden.

DSGVO – Was Sie wissen müssen

Welche Fragen sollte ich mir als Unternehmer stellen?

1. **„Bin ich von der DSGVO betroffen?“**
   Ja. Betroffen sind alle Unternehmen, die personenbezogene Daten verarbeiten, auch wenn sie außerhalb der EU sitzen und Daten von EU-Bürgern verarbeiten.
2. **„Darf ich die Daten verarbeiten?“**
   Eine Datenverarbeitung muss rechtmäßig sein. Legitimer Zweck definieren. Abfrage des Geburtsdatums für Newsletter-Versand z.B. nicht erlaubt. Kopplungsverbot.
3. **„Sind die Daten sicher und geschützt?“**
   Zugriffsschutz und Verschlüsselung notwendig.
   Notebook-Festplatte muss verschlüsselt sein.
4. **„Sind die Verarbeitungsprozesse bekannt und klar?“**
   Transparenz wird erfordert. Verarbeitungstätigkeiten müssen in einem Verzeichnis dokumentiert werden.
5. **„Was sind personenbezogene Daten?“**
   Alle Informationen zu einer identifizierten oder identifizierbaren natürlichen Person.

Welche Änderungen kommen auf uns zu?

- E-Mail wird auch in unserer Branche nicht sterben!
  - Allgemeine Nachrichten und Informationen
  - Verschlüsselte Mitteilungen
- E-Mail-Signatur erweitern:
  Datenschutz-Ansprechpartner und Datenschutzbeauftragter
- Lokale wird durch zentrale Datenhaltung abgelöst.
- Alle Maßnahmen sollten dokumentiert werden.
- Datenschutzerklärungen anpassen: Ansprechpartner, Kontaktdaten, Rechtsgrundlagen, etc.
- „Recht auf vergessen werden“ umsetzen.
- Bestehende Datenverarbeitungserklärungen bleiben gültig.

Welche Lösungen bietet die DGFRP? (1)

- Die DGFRP ist Full Service Provider
- Alle DGFRP-Systeme sind sicher und verschlüsselt
  egal ob Quixx, Extranet, FINALIFE, etc.
  Nicht-konforme Systeme werden mittelfristig Außerbetrieb gesetzt
  ⇨ mFiN muss lokal verschlüsselt werden
- Nachrichten-/Dokumentaustausch mit Bezug auf Kundendaten:
  - DGFRP Extranet ⇨ vorgangsbezogener Chat
  - Quixx Ticketsystem ⇨ Kommunikation DGFRP und Makler
  - Quixx Ticketsystem ⇨ auch für Kommunikation mit Kunde
  - FINALIFE ⇨ sicherer Dokument-Austausch

Welche Lösungen bietet die DGFRP? (2)

- Quixx wird in Bezug auf Datenschutz-Einhaltung zertifiziert
- Unterstützung durch DGFRP-Ansprechpartner (Philipp von Wartburg)
- Webinare und Schulungen
- Abklärungen zum Thema Datenschutz mit externen Stellen
- Unterlagen, Dokumente und Vorlagen für Makler
  Wir stellen Ihnen DSGVO-konforme Vorlagen zur Verfügung:
  ⇨ Muster Verzeichnis der Verarbeitungstätigkeiten
  ⇨ Einwilligung zur Datenverarbeitung (≠ Datenschutzerklärung)
  ⇨ viele weitere Muster

Fragen und Antworten (1)

Wann liegt eine Auftragsverarbeitung vor? (alter Begriff: Auftragsdatenverarbeitung)
Bei einer Auftragsverarbeitung verarbeitet ein Dienstleister (Auftragsverarbeiter bzw. Auftragnehmer) personenbezogene Daten weisungsabhängig im Auftrag der verantwortlichen Stelle (Verantwortlicher/Auftraggeber). Typische Fälle einer Auftragsverarbeitung sind externe Lohn- oder Gehaltsabrechnung, Datenträgerentsorgung, Versand eines Newsletters durch eine Agentur oder Nutzung von Cloud-Diensten.
Weisungsabhängig: Wird sozusagen zur internen Abteilung.

Wann brauche ich eine Einwilligung?
Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn die betroffene Person vorher schriftlich ihre Einwilligung erteilt hat. Ansonsten muss eine gesetzliche Grundlage greifen (Art. 6 Abs. 1 DSGVO).

Fragen und Antworten (2)

Wann erfolgt eine Datenverarbeitung?
Jeder Vorgang, bei dem Daten betroffen sind, stellt eine Datenverarbeitung dar. Also das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Verwenden und Übermitteln.

Wann muss ich die Daten löschen?
Wenn das Vertragsverhältnis beendet ist, so kann der Kunde verlangen, dass seine Daten gelöscht werden. Wenn die Daten noch, z.B. aufgrund von Dokumentationsgründen benötigt werden, so müssen die Daten zumindest gesperrt werden.
Hinweis: Löschung aus Archiv bzw. Backup nicht notwendig

Merke: Wenn etwas passiert, muss eine Meldung innert 72 Stunden erfolgen.

Das sollte ich als Makler tun (1)

- Alle Daten sichern und schützen.
- Datenschutz betrifft Hardware und Software, i.d.R. auch Papier.
- Alte IT-Systeme und Gewohnheiten überprüfen.
- Word-Dokument mit allen Maßnahmen und Aktivitäten laufend nachführen.
- Verzeichnis der Verarbeitungstätigkeiten erstellen (WICHTIG).
- Liste und Beschreibung der verwendeten IT-Systeme erstellen.
- Datenverarbeitungs-Einwilligung mit Kunden aktualisieren bzw. erstellen (WICHTIG) (!).
- Datenschutzerklärung aktualisieren bzw. erstellen.
- Datenschutzkonzept erstellen (WICHTIG).

Das sollte ich als Makler tun (2)

- Webseite aktualisieren
- Klar planen, kommunizieren und dokumentieren.
- Mitarbeiter informieren und schulen.
- Mitarbeiter-Verträge kontrollieren.
- Betroffenenrechte wahren ⇨ *siehe nächste Folie*
- Alternative Kanäle anbieten, damit keine Verletzung entsteht.
- Löschfristen einhalten ⇨ *siehe Datenschutz-Einwilligung*

Info: Betroffenenrechte

1. Transparenz / Auskunftsrecht
2. Berichtigung und Vervollständigung der gespeicherten Daten
3. Löschung der gespeicherten Daten
4. Recht auf Einschränkung der Verarbeitung
5. Recht auf Datenübertragbarkeit
6. Beschwerderecht

Können/sollten auf der Einwilligung zur Datenverarbeitung aufgeführt sein.

Info: Betroffenenrechte

Zum Schluss möchten wir Sie noch über Ihre Rechte informieren:

- Ihre Einwilligung ist FREIWILLIG.
- Sie können eine erteilte Einwilligung jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft WIDERRUFEN. Wenn Ihre Einwilligung Voraussetzung für die Erfüllung Ihres Auftrages ist, kann der Widerruf Einschränkungen der Leistungen bis hin zur Beendigung Ihres Auftrages an uns zur Folge haben.
- Sie haben das Recht AUSKUNFT über Ihre Daten zu erhalten und können die EINSCHRÄNKUNG der Nutzung (z.B. keine Informationen über Finanzprodukte mehr zu erhalten) sowie KORREKTUR Ihrer Daten verlangen
- Sie können die LÖSCHUNG Ihrer Daten fordern. Im Fall der Löschung möchten wir Sie darüber informieren, dass aufgrund gesetzlicher Vorgaben Ihre Daten noch eine Weile gespeichert bleiben Die gesetzlichen Aufbewahrungsfristen betragen bis zu 10 Jahre Verjährungsfristen bis zu 30 Jahren. Beratungsnachweise speichern wir, solange hieraus Ansprüche geltend gemacht werden können.
- Sie haben das Recht auf BESCHWERDE bei einer Aufsichtsbehörde, wenn Sie den Eindruck haben, dass Ihre Daten rechtswidrig verarbeitet werden.

Zur Ausübung Ihrer Rechte bitten wir Sie uns per Email an oder per Post über Ihren Wunsch zu kontaktieren.

Verzeichnis der Verarbeitungstätigkeiten

Verarbeitungstätigkeiten

Name: Max Mustermann

Nr.	Tätigkeit	Daten	Datenherkunft	Personengruppen	IT-System	Std./Tag
Muster	Versicherungsantrag erfassen	Personendaten Adressdaten Kontaktdaten Geburtsdatum Bankverbindungsdaten Legitimationsdaten Vertragsdaten	Antragsformular	Kunde Makler	mDB Quixx	3,00
Muster	Seminarteilnehmer verwalten	Personendaten Adressdaten Kontaktdaten Seminardaten	Teilnehmeranmeldung zu Seminar	Makler	Extranet Quixx	1,00
1						
2						
3						

Tipps und Tricks

- Ich möchte Daten erhalten…
  …somit benötige ich eine Einwilligung des Betroffenen („Klare Sprache“)
  …und muss möglichst eine Widerrufmöglichkeit anbieten
- Ich bekomme Daten vom Betroffenen…
  …somit kann ich davon ausgehen, dass er einverstanden ist
- Ich bekomme Daten von einem Dritten…
  …somit muss ich abklären, ob ich die Daten verarbeiten darf

„Visitenkarte an Messestand erhalten…“

Interessante Links und Quellen

- DSGVO Gesetzestext: https://dsgvo-gesetz.de/
- BDSG Gesetzestext: https://dsgvo-gesetz.de/bdsg-neu/
- Was ist Datenverarbeitung: https://www.datenschutzzentrum.de/artikel/1091-Was-versteht-man-unter-Datenverarbeitung.html
- Technischer DSGVO-Ratgeber von t3n:
  DSGVO: Diese Änderungen kommen auf dein Online-Business zu (Teil 1)
  DSGVO: Welche Daten du nutzen darfst – und welche nicht (Teil 2)
  DSGVO: So holst du Einwilligungen richtig ein (Teil 3)
  DSGVO: In 4 Schritten zum Verzeichnis der Verarbeitungstätigkeiten (Teil 4)
  DSGVO: So gibst du Daten rechtssicher an Dritte weiter (Teil 5)
- Verschlüsselung: https://www.psw-group.de/blog/die-dsgvo-und-verschluesselung/4844
- Verschlüsselung: https://www.datenschutz-praxis.de/fachartikel/dsgvo-verschluesselung-ist-trumpf/
- Verschlüsselung: https://www.security-insider.de/e-mail-verschluesselung-gehoert-zur-dsgvo-a-671565/
- Datenlöschung vs. Aufbewahrungspflicht:
  http://www.procontra-online.de/artikel/date/2017/09/anspruch-auf-datenloeschung-vs-aufbewahrungspflicht/
- Praxishilfen: https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- Aufsichtsbehörden: https://www.was-ist-datenschutz.de/fuer-betroffene/aufsichtsbehoerden-datenschutz-in-deutschland.html
- Kurzpapiere und weitere Dokumente: https://www.lda.bayern.de/de/datenschutz_eu.html
- Datenlöschkonzept: https://www.activemind.de/magazin/datenschutz-loeschkonzept/
- Datenschutzerklärung-Generator für Webseiten: https://www.activemind.de/datenschutz/datenschutzhinweis-generator/
- Verschiedene Dokumente: https://www.activemind.de/datenschutz/dokumente/

Mehr Informationen zu DSGVO, IDD und MiFID II

>> 17.04.2018 - Bayreuth

>> 18.04.2018 - Stuttgart

>> 19.04.2018 - Altötting

>> 24.04.2018 - Köln

>> 25.04.2018 - Walsrode

>> 26.04.2018 - Berlin

Top-Themen mit Top-Referenten mit aktuellen Highlights!

Anmeldung wie gewohnt über den Seminarkalender
oder Mail an seminare@dgfrp.de.