

Fachverband Versicherungsmakler

Datenschutzgrundverordnung **DSGVO**

Technische Anforderungen an die Verwaltungsprogramme der Makler

Josef Sylle

Arbeitskreis Technologie des Fachverbandes der Versicherungsmakler

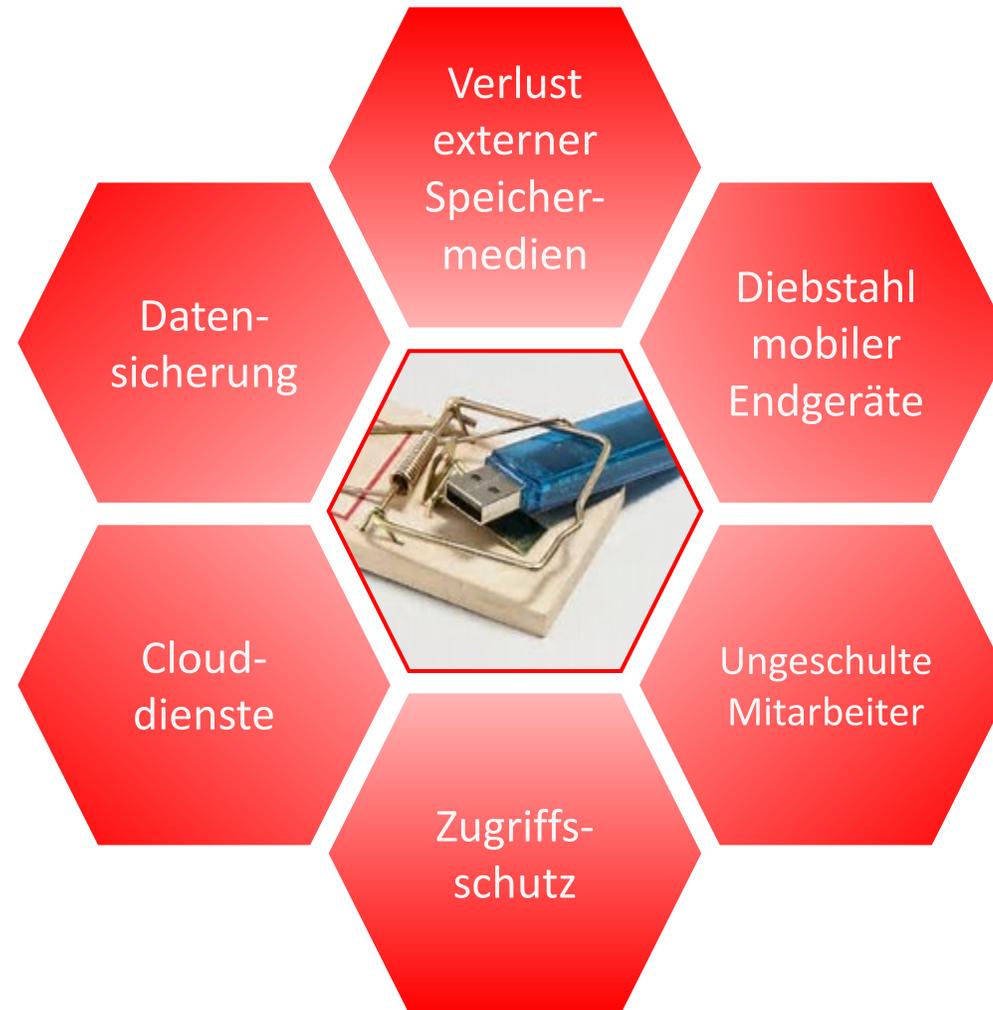
November 2017

Agenda

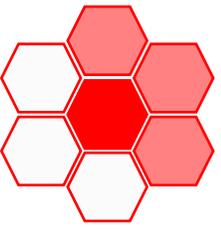
- Anforderungen an den Versicherungsmakler
 - Hardware
 - Mitarbeiter

- Technische Anforderungen an die Verwaltungsprogramme
 - Verzeichnis von Verarbeitungstätigkeiten (Art. 30)
 - Informationspflichten (Art. 13, 14)
 - Recht auf Auskunft (Art. 15)
 - Recht auf Löschung und Einschränkung (Art. 17, 18)
 - Daten-Zugriffsberechtigungen /-einschränkungen
 - Datenübertragbarkeit (Art. 20)
 - Privacy by Design / Default (Art. 25)
 - Dokumentationspflichten (Art. 33)

Datenfallen im Unternehmen



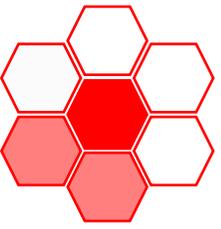
Anforderungen an den Versicherungsmakler (1)



- Verlust / Diebstahl mobiler Endgeräte und externer Speichermedien
 - Problembewusstsein bei den Mitarbeitern schaffen
 - Mitarbeiter schulen
 - Gezielter Einsatz, Verwaltung, Dokumentation und Verschlüsselung mobiler Endgeräte / externer Speichermedien
 - Benutzung außerhalb der Firmen-Infrastruktur (öffentl. WLAN, GMX-Accounts, etc.) - auf verschlüsselte Verbindungen achten

- Ungeschulte Mitarbeiter/innen
 - Mitarbeiter-Schulungen: verantwortungsvoller Umgang mit Daten
 - Verpflichtungserklärung zur Einhaltung des Datenschutzes
 - Verfahren bei personellen Änderungen
 - PC-Benutzungsregelungen bzw. –einschränkungen
 - Regelung bei Einsatz von Fremdpersonal

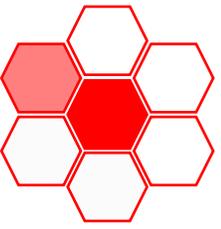
Anforderungen an den Versicherungsmakler (2)



- Zugriffsschutz
 - Anlage verschiedener Benutzer
 - Regelung zur Auswahl von Passwörtern
 - Zugriffsberechtigungen
 - Sichere Ablage von Zugangsdaten
 - IT-Dokumentation (Verträge mit IT-Dienstleister, Einsatz von Clouddiensten, Datenspeicherung/Server innerhalb der EU?)

- Clouddienste
 - Daten verschlüsselt speichern
 - Virenschutz
 - Geräte / Wechselmedien vor unberechtigtem Zugriff schützen (Verschlüsselung)
 - Sind EDV-Systeme und Geräte „up-to-date“ – Aktualisierungszeitpunkte für Updates, Sicherheitstools, ServicePack dokumentieren und festlegen

Anforderungen an den Versicherungsmakler (3)



- Datensicherung
 - IT-Sicherheitsstrategien und –richtlinien für Administratoren und Benutzer
 - Firewalls, Sicherheit von Web-Browsern sicherstellen
 - Erstellung eines Datensicherungskonzepts
 - Regelung für Backup-Datenträger – manipulationssicher, unzugänglich für Unbefugte, belastbar
 - Lokalisierbarkeit von gespeicherten Kundendaten – wo und mit welcher Redundanz werden personenbezogene Daten abgelegt (gilt auch für Backups und archivierte Dateien)
 - Physischer Schutz von IT-Systemen
 - Zutrittskontrollen (Wer hat Zutritt zum Gebäude / zum Server? Physische Zutrittskontrollen?)
 - Zugangsbeschränkungen festlegen
 - Infrastruktur (Klimaanlage, Notstromversorgung,...)

Technische Anforderungen an die Verwaltungsprogramme betreffend DSGVO

Verzeichnis von
Verarbeitungstätigkeiten
(Art. 30)

Informationspflichten
(Art. 13, 14)

Recht auf Auskunft
(Art. 15)

Recht auf
Löschung/Einschränkung
(Art. 17, 18)

Daten-
Zugriffsberechtigungen

Datenübertragbarkeit
(Art. 20)

Privacy by
Design / Default
(Art. 25)

Dokumentationspflicht
(Art. 33)

Verzeichnis von Verarbeitungstätigkeiten (Art. 30)

- **Verarbeitungszweck** unter Angabe der Rechtsgrundlage
- **Verarbeitungsart** – zB Kunden- u. Vertragsverwaltung, Schadenbearbeitung, Marketing,...
- Betroffene **Personengruppen** – zB Kunden/VN, versicherte Personen, VUs, Interessenten,...
- **Datenkategorien** – zB Name, Adresse, Geburtsdatum, Bankdaten, Polizzennummern,...
- **Empfängerkategorien** – zB VUs, Kreditunternehmen, externe Dienstleister
- Vorgesehene **Löschfrist** für die verschiedenen Datenkategorien

- **Anforderungen**
 - Möglichkeit die Datenherkunft im System anzugeben (stammen die Daten vom Betroffenen selbst oder von einer dritten Person)
 - automatische Erstellung eines Verzeichnisses in verarbeitbarer Form (zB Excel)

Kategorien der betroffenen Personen- gruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Lfd. Nr.	Datenkategorien	Besondere Daten- kategorien iSd Art 9 DSGVO ¹⁰ , strafrechtlich relevant iSd Art 10 DSGVO ¹¹	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)
1	1	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	X	X	X	X	X	X	X	X	X	X
	2	Anschrift	Nein	X	X	X	X	X	X	X	X	X	X
	3	Kontaktdaten (Tel., Mail,Fax)	Nein	X	X	X	X	X	X	X	X	X	X
	4	Firmenbuchdaten	Nein	X	X	X	X	X	X	X	X	X	X
	5	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		X		X						
	6	Bankverbindungen	Nein	X	X	X	X	X	X	X	X	X	
	7	Kreditkartennummern und - unternehmen	Nein	X	X	X	X						
	8	UID-Nummer	Nein	X	X	X	X	X	X	X	X	X	
	9	Namen der Kontaktpersonen	Nein	X	X	X	X	X	X	X	X	X	X
	10	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.)	Nein	X	X	X	X	X	X	X	X	X	X

Informationspflichten (Art. 13, 14)

- Zum Zeitpunkt der Datenerhebung
- In präziser, transparenter, verständlicher, schriftlicher und leicht zugänglicher Form
- Informationsblatt mit
 - Name und Kontaktdaten des Versicherungsmaklers
 - Verarbeitungszweck und Rechtsgrundlage der Verarbeitung
 - Empfänger der Daten – zB VUs, Banken, externe Dienstleister,...
 - Dauer der Datenspeicherung
 - etc.
- Anforderungen
 - Implementierung des Informationsblattes
 - Erstellung des Informationsblattes aus dem System (Angabe der Datenkategorie insbesondere dann, wenn die Daten von Dritten stammen)
 - Bei Neuanlage von Kundendaten: Hinweis auf Vorlage des Informationsblattes

Recht auf Auskunft (Art. 15)

- Angabe der Datenkategorien und die konkret verarbeiteten Daten
- Kopie aller verarbeiteter Daten (zB E-Mails, Briefe, Auszüge aus Datenbanken,...)
- Angabe der Verarbeitungszwecke (zB Beratung/Vermittlung von Versicherungsverträgen, Schadenberatung, Prämieninkasso,...)
- Angabe der Empfängerkategorien
- Rechtsgrundlage der Verarbeitung
- Speicherfrist für die Daten
- Angabe zur Datenherkunft

- Anforderungen
 - Automatische Erstellung einer „Datenverarbeitungsaufstellung“ mit den oben angeführten Punkten
 - Erstellung eines zB PDF-Dokuments mit allen im System abgelegten Daten (inkl. Korrespondenz)

Recht auf Löschung und Einschränkung (Art. 17, 18)

■ Anforderungen

- Löschung der Daten aus dem System
- Automatische Archivierung der Daten, wenn Löschung nicht möglich ist (Haftungsthematik, Aufbewahrungs- und Dokumentationspflichten)
- (Weiter-)Verarbeitung der Daten muss unzulässig sein
- Automatische Weiterleitung in ein Back-Up-System
- Verschlüsselung der Daten
- Automatische Erstellung einer E-Mail an sämtliche Datenempfänger mit der Information über die Löschung, Einschränkung oder Berichtigung (Art. 16)

Daten-Zugriffsberechtigungen / -einschränkungen

- Anforderungen
 - Je Datenkategorie festlegen, wer welche Zugriffsberechtigungen erhält
 - Unsensible Daten (zB allgemeine Kundendaten, wie Name, Adresse, Status,...) für alle Nutzer lesbar (evtl. auch änderbar)
 - Sensible Daten (zB spezifische Kundendaten, wie Vertrags- u. Schadendaten, ...) nur für den Kundenbetreuer les- und änderbar
 - Kundenbetreuer kann Zugriffsberechtigungen (zB Lesefreigabe) für andere Nutzer festlegen
 - Bei Ausscheiden des Kundenbetreuers:
 - automatische Ausgabe einer „Kundenbestandsliste“, um einen neuen Betreuer zu hinterlegen
 - Subsidiär vergebene Nutzer-Zugriffsberechtigungen auf „Standard“ zurücksetzen

Weitere Anforderungen gem. DSGVO

- Datenübertragbarkeit (Art. 20) – nicht zwingend, nur wenn technisch machbar
 - Automatische Auflistung aller gespeicherten Daten der betroffenen Person in strukturierter und lesbarer Form
 - Bei Verwendung derselben Software-Systeme oder Online-Portale Übertragbarkeit der Daten „per Mausklick“
- Privacy by Design / Default (Art. 25)
 - Datenminimierung bei der Verarbeitung personenbezogener Daten sicherstellen, ohne dabei die Funktionalität des Systems zu beeinträchtigen (Privacy Enhancing Technologies)
 - Daten-Pseudonymisierung und Verschlüsselung ermöglichen (siehe auch Art. 32)
- Dokumentationspflicht (Art. 33)
 - Änderung von Daten und Zugriffe im System dokumentieren und nachverfolgbar machen

Vielen Dank

für Ihre Aufmerksamkeit!

Josef Sylle

Arbeitskreis Technologie des Fachverbandes der Versicherungsmakler