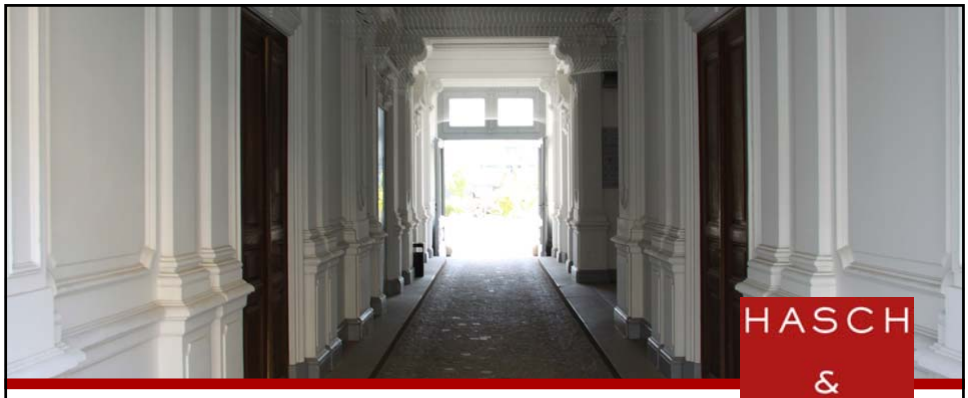


EU-DATENSCHUTZGRUNDVERORDNUNG

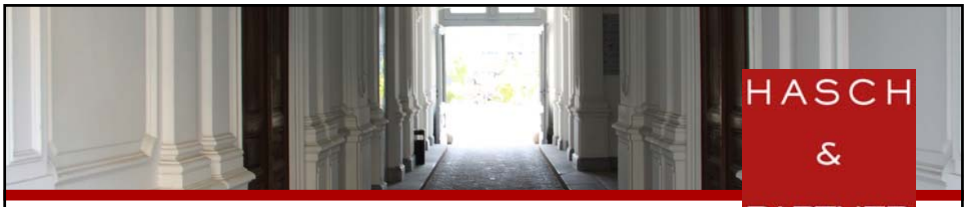
15. Jänner 2018

MAG. FELIX HASCH
RECHTSANWALTSANWÄRTER

BASISUNTERLAGE
(Vortrag ausgewählter Folien)

INHALTSVERZEICHNIS

2



1.

HINTERGRUND DER

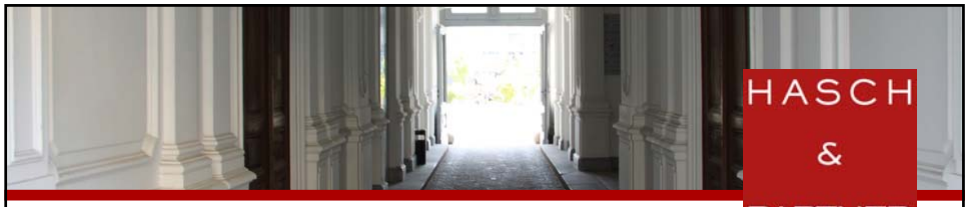
DATENSCHUTZGRUNDVERORDNUNG

HINTERGRUND DER DSGVO

Ziele

- Datenschutz für **natürliche Personen**
- Kontrolle der eigenen Daten
- Transparenz
- Datenspeicherung nur bei Notwendigkeit

2014: Max Schrems / Facebook Ireland Limited



2.

BEGRIFFSBESTIMMUNGEN

BEGRIFFSBESTIMMUNGEN (1)

- personenbezogene Daten (Art 4 Z 1 DSGVO)
  - identifizierte Person (Name, E-Mail Adresse, Geburtsdatum, etc.)
  - identifizierbare Person (Standortdaten, IP Adresse)
  - Personalverrechnung, Lieferanten- und Kundendatei

⇨ Jeder, auch Kleinunternehmer sind erfasst !

BEGRIFFSBESTIMMUNGEN (2)

- biometrische Daten (Art 4 Z 14 DSGVO)
  - Gesichtsbild
  - Fingerprint
  - Stimmaufzeichnung

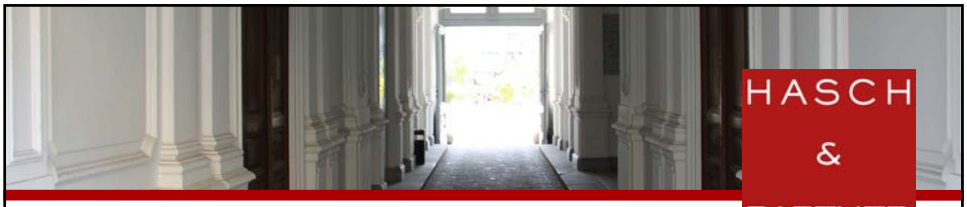
  ⇨ Banken (MiFid II. Richtlinie)

F. HASCH 7

BEGRIFFSBESTIMMUNGEN (3)

- besonders sensible Daten (Art 9 DSGVO)
  - Daten natürlicher Personen über
    - rassische oder ethnische Herkunft
    - politische Meinung
    - Gesundheit
    - Religionsbekenntnis
- Daten über strafrechtliche Verurteilungen oder Straftaten (Art 10 DSGVO)

F. HASCH 8



3.

INKRAFTTRETEN / RECHTSGRUNDLAGEN

F. HASCH 9

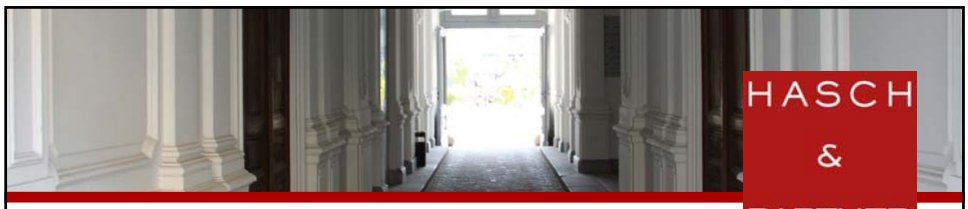
RECHTSGRUNDLAGEN

- bis 25.05.2018 gilt DSG 2000
- ab 25.05.2018 gilt Datenschutz-Anpassungsgesetz (DS-APG 2018)
  - zusätzliche Verwaltungsstrafen bis EUR 50.000,00 für juristische Personen gemäß § 19 DS-APG 2018

Zuständige Behörde: Datenschutzbehörde Wien

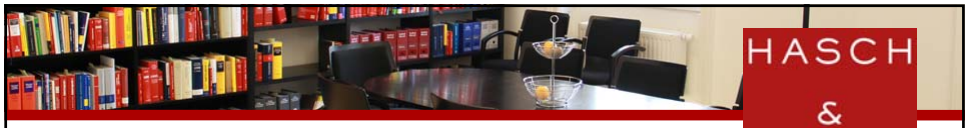
- Unterstützung bei Databreaches (Datenpanne) und Leaks (Datenleck)

F. HASCH 10



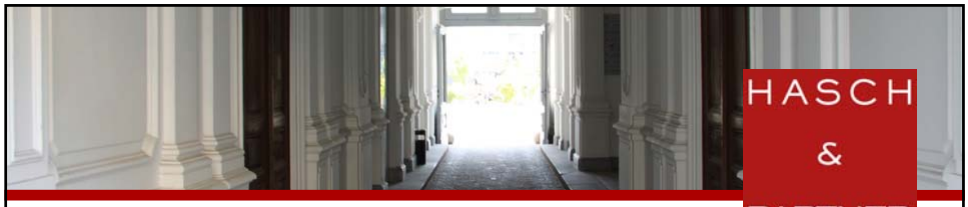
4.

STRAFRAHMEN



STRAFRAHMEN

- bis 25.05.2018 – DSG 2000
  - Strafrahmen je nach Delikt EUR 500,00 bis EUR 25.000,00
- ab 25.05.2018 – DSGVO
  - Verletzung von Pflichten
    - bis zu EUR 10 Mio.
    - oder 2 % des weltweiten Konzernumsatzes
  - Verletzung von Rechten betroffener Personen
    - bis zu EUR 20 Mio.
    - oder bis zu 4 % des weltweiten Konzernumsatzes



5.

WESENTLICHE NEUERUNGEN IM ÜBERBLICK

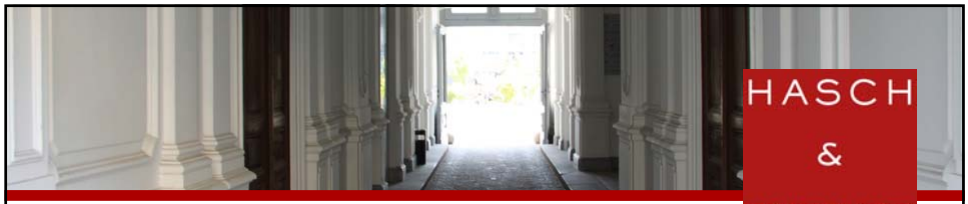
WESENTLICHE NEUERUNGEN (1)

- Meldung von Databreaches innerhalb von 72 Stunden (Art 33 DSGVO)
- zwingende Bestellung eines Datenschutzbeauftragten (Art 37 DSGVO)
- Datensicherheitsbestimmungen (Art 32 DSGVO) (privacy by design, privacy by default)
- Datenschutzfolgenabschätzung (Art 35 DSGVO)

WESENTLICHE NEUERUNGEN (2)

- Entfall der DVR Meldung
- Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGVO)
- Informationspflichten (Art 13, 14 DSGVO)
- Betroffenenrechte (Art 16 – 22 DSGVO)

F. HASCH 15



6.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

F. HASCH 16

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN (1)

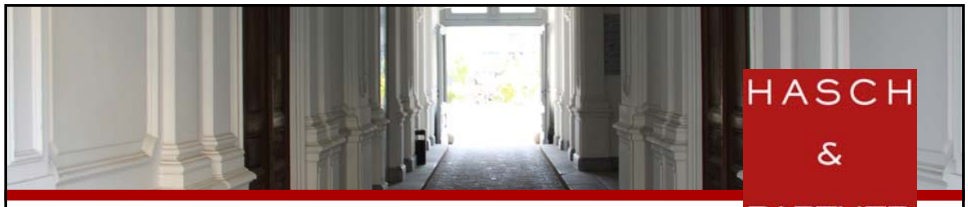
- bis 25.05.2018 wie bisher Meldung an Datenschutzbehörde im Zuge der DVR-Meldung
- ab 25.05.2018 Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGVO)

F. HASCH 17

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN (2)

- Jeder Verarbeiter hat selbstständig ein Verzeichnis der Verarbeitungstätigkeiten zu führen (§ 49 Abs 1 DS-APG 2018)
- Verarbeiter ist dafür beweispflichtig (Art 30 Abs 4 DSGVO)

F. HASCH 18



7.

INFORMATIONSPFLICHT DES VERARBEITERS

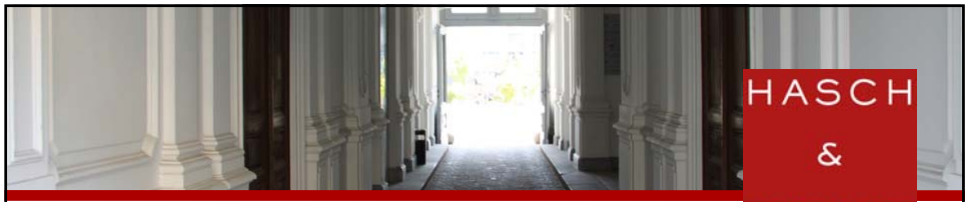
INFORMATIONSPFLICHT (ART 13 DSGVO) (1)

- Informationen müssen dem Betroffenen unverzüglich, auf Antrag innerhalb eines Monats, zur Verfügung gestellt werden (Art 15 Abs 3 DSGVO)

Strafrahmen: bis EUR 10 Mio. oder 2 % des Konzernumsatzes

INFORMATIONSPFLICHT (ART 13 DSGVO) (2)

- Kontaktdaten des Datenschutzbeauftragten
- Zweck der Datenverarbeitung
- Rechtsgrundlage
- Empfänger der Daten
- Speicherdauer
- gegebenenfalls die Absicht die Daten in ein Drittland zu exportieren
- umfassende Rechtsbelehrung



8.

BETROFFENENRECHTE

BETROFFENENRECHTE

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Datenübertragbarkeit (Art 20 DSGVO)
- Recht auf Widerspruch gegen die Datenverarbeitung (Art 21 DSGVO)
- automatisierte Entscheidungen (Art 22 DSGVO)

F. HASCH 23

RECHT AUF AUSKUNFT (ART 15 DSGVO) (1)

- Recht auf Kopie der verarbeiteten Daten (Spiegelakt)
- Auskunftsrecht 1 x pro Jahr gratis, öfter kostenpflichtig
- sofern elektronisch Antrag gestellt wird, ist Auskunft auch elektronisch zugänglich zu machen (Art 15 Abs 3 DSGVO)

F. HASCH 24

RECHT AUF AUSKUNFT (ART 15 DSGVO) (1)

- Verarbeiter muss Auskunft geben über:
  - dass Daten der betroffenen Person verarbeitet wurden
  - Verarbeitungszweck
  - Kategorien von Empfängern
  - Speicherdauer
  - Informationen über die automatisierte Entscheidungsfindung (Parametergewichtung)

RECHT AUF BERICHTIGUNG (ART 16 DSGVO)

- Pflicht zur regelmäßigen Aktualisierung, Richtigstellung und Ergänzung von personenbezogenen Daten,
- auf Antrag der betroffenen Person muss richtig gestellt, sowie ergänzt werden.

RECHT AUF LÖSCHUNG (ART 17 DSGVO)

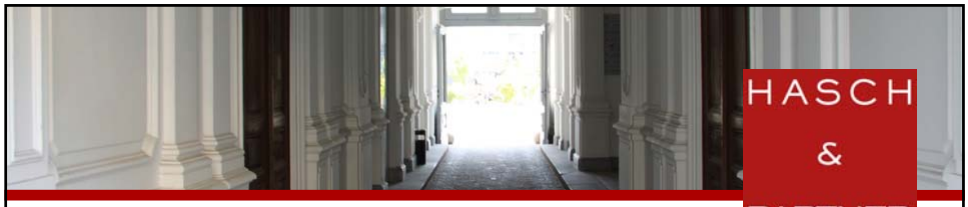
- Daten müssen gelöscht werden, wenn
  - Notwendigkeit der Verarbeitung weggefallen ist
  - Einwilligung widerrufen wird
  - bei unrechtmäßiger Verarbeitung
  - Sonderfall: Einwilligung von Minderjährigen
- Verständigung aller Empfänger des Datensatzes
- umfassende Löschung! (Backup, Server)
- systematische Löschintervalle installieren

F. HASCH 27

RECHT AUF DATENÜBERTRAG-BARKEIT (ART 20 DSGVO)

- soll Wechsel zwischen Dienstleistern erleichtern
- Pflicht zur Übertragung der Kundendaten
  - an die jeweilig betroffene Person zur selbständigen Übermittlung an den neuen Verantwortlichen (Art 20 Abs 1 DSGVO)
  - an einen von der betroffenen Person angegebenen Verantwortlichen (Art 20 Abs 2 DSGVO)

F. HASCH 28

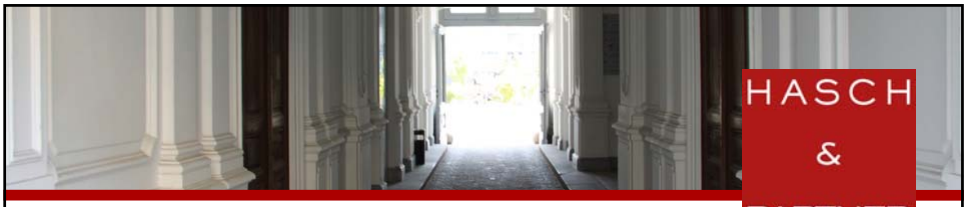


9.

MELDUNG BEI DATABREACH

MELDUNG BEI DATABREACH (ART 33 DSGVO)

- Pflicht zur Vorbereitung auf Databreach (Checkliste und technische Voraussetzungen)
- Information der betroffenen Personen
- Meldung an die Datenschutzbehörde innerhalb von 72 Stunden
- Strafrahmen: bis EUR 10 Mio. oder 2 % des Konzernumsatzes



10.

ERNENNUNG EINES

DATENSCHUTZBEAUFTRAGTEN

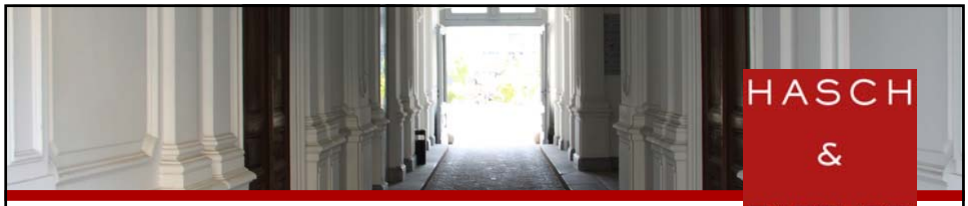
DATENSCHUTZBEAUFTRAGTER (ART 37, 38, 39 DSGVO) (1)

- ist zwingend zu ernennen
  - bei hoheitlicher Verwaltung
  - bei Videoüberwachung im Unternehmen
  - bei Daten im Zusammenhang mit Strafverfolgung (Art 10 DSGVO)
  - bei besonders sensiblen Daten (Art 9 DSGVO)
    - wie Gesundheitsdaten, biometrische Daten, etc.

DATENSCHUTZBEAUFTRAGTER (ART 37, 38, 39 DSGVO) (2)

- sollte unbedingt schriftlich ernannt werden
- fachkundige Person (Art 37 Abs 5 DSGVO)
  - technisches Fachwissen
  - Datenschutzpraxis
- Veröffentlichung und Mitteilung der Kontaktdaten (Art 37 Abs 7 DSGVO)

F. HASCH 33



11.

DATENSCHUTZFOLGENABSCHÄTZUNG

F. HASCH 34

DATENSCHUTZFOLGEN-ABSCHÄTZUNG (ART 35 DSGVO) (1)

- zwingend, wenn Verarbeitung ein erhöhtes Risiko für die Daten darstellt
- Positivliste der Aufsichtsbehörde (Art 35 Abs 4 DSGVO)
  - Datenschutzbehörde **muss** Liste von Verarbeitungsvorgängen veröffentlichen, die Folgenabschätzung notwendig machen
- Ausnahmen (ErwGr 91)
  - Patientendaten des Hausarztes
  - Mandantendaten des **einzelnen** StB, RA, UB

F. HASCH 35

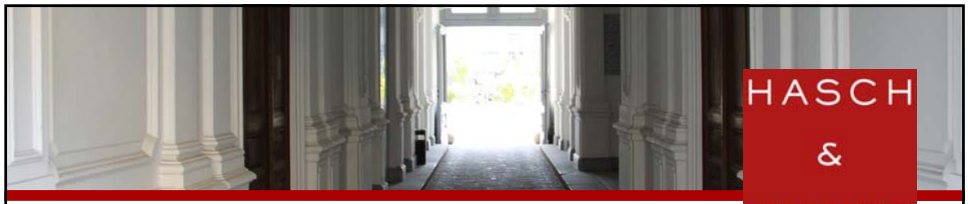
DATENSCHUTZFOLGEN-ABSCHÄTZUNG (ART 35 DSGVO) (2)

- Negativliste der Aufsichtsbehörde (Art 35 Abs 5 DSGVO)
  - Datenschutzbehörde **kann** Liste von Verarbeitungsvorgängen veröffentlichen, die **keine** Folgenabschätzung notwendig machen
- Folgenabschätzung auch für Auftraggeber und Nachunternehmer

F. HASCH 36

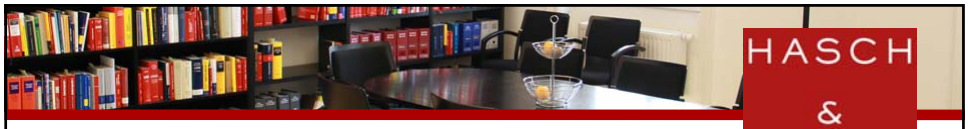
DATENSCHUTZFOLGEN-ABSCHÄTZUNG (ART 35 DSGVO) (2)

- Mindestinhalt
  - Beschreibung der Verarbeitungsvorgänge
  - Zweck der Verarbeitung
  - berechtigtes Interesse an der Speicherung
  - Risikobewertung
  - Abhilfemaßnahmen
    - Sicherheitsvorkehrungen
    - Verfahren bei Missbrauch



12.

PROBLEMFELDER IN DER PRAXIS



PROBLEMFELDER IN DER PRAXIS (1)

- Datenübermittlung an Drittländer
  - Safe Harbour Entscheidung 2015
  - seit 2016 EU-US Privacy Shield
  - Pflicht zur Wahrung eines angemessen Schutzniveaus
    - Prüfung ob Datenflüsse außerhalb der EU
    - wenn ja ⇨ Zustimmungserklärung einholen

F. HASCH 39

PROBLEMFELDER IN DER PRAXIS (2)

- Zustimmungserklärung einholen
  - in AGBs nicht ausreichend, da Zustimmungsakt erforderlich
  - Nachweispflicht des Verarbeiters (Art 7 Abs 1 DSGVO)
  - vorangekreuzte Häkchen ungültig (ErwGr 32) (Double-Opt-In (=Einwilligung und Dokumentation))

F. HASCH 40

PROBLEMFELDER IN DER PRAXIS (3)

- Koppelungsverbot (Art 7 Abs 4 DSGVO)
  - Dienstleistung darf nicht an Einwilligung zur Verarbeitung von persönlichen Daten gekoppelt werden, die für die Leistungserbringung nicht unbedingt notwendig sind !
  - pauschale Kontaktformulare sind daher künftig unzulässig !

F. HASCH 41

PROBLEMFELDER IN DER PRAXIS (4)

- Visitenkarten auf Messen
  - bestenfalls Zeit und Ort notieren (VerarbeitungsVz)
  - Im Zuge der erstmaligen Korrespondenz sollte Informationsbelehrung gemäß Art 13 DSGVO übermittelt werden

F. HASCH 42

PROBLEMFELDER IN DER PRAXIS (5)

- Visitenkarte bei Anbahnung eines Geschäfts
  - Keine Informationsbelehrung notwendig
  - Öffnungsklausel gemäß Art 6 Abs 1 lit b DSGVO
    - Notwendigkeit der Verarbeitung für die vertragliche Leistungserbringung
    - Notwendigkeit zur Erbringung vorvertraglicher Leistungen

F. HASCH 43

PROBLEMFELDER IN DER PRAXIS (6)

- Bewerbungsunterlagen
  - ohne Zustimmungserklärung des Bewerbers: Bewerbungsunterlagen dürfen nur 6 Monate aufbewahrt werden (Art 17 Abs 1 lit a DSGVO)
  - mit Zustimmungserklärung des Bewerbers: Zustimmung kann jederzeit nach Ablauf von 6 Monaten widerrufen werden (Art 17 Abs 1 lit b DSGVO)
  - Auch Papierakten sind erfasst ! (§ 2 Abs 1 DS-APG 2018)

F. HASCH 44

PROBLEMFELDER IN DER PRAXIS (7)

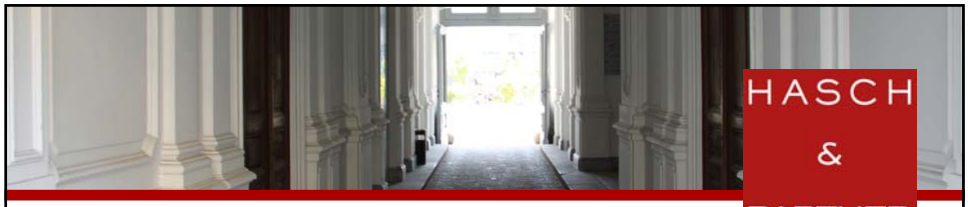
- Newsletter
  - kann "berechtigtes Interesse" des Unternehmers darstellen iSd Art 6 Abs1 lit f DSGVO
  - Direktmarketing (EG. 47 Satz 7)
  - § 7 Abs 3 UWG gilt gemäß Art 95 DSGVO als "besondere Bestimmung" der E-Privacy-Richtlinie (Art 13 2002/58/EG) fort !

F. HASCH 45

PROBLEMFELDER IN DER PRAXIS (8)

- Ergebnis:
  - Newsletter Werbung bei bestehenden Kundenverhältnissen zulässig (§ 7 Abs 3 Z 2 UWG)
  - auch bei Neuabonnenten zulässig, sofern diese ihre Adresse selbst bekannt gegeben haben und ausreichend über Widerrufsmöglichkeiten belehrt worden sind (§ 7 Abs 3 Z 1 UWG)

F. HASCH 46



13.

HANDLUNGSEMPFEHLUNGEN

DATENSCHUTZMANAGEMENT

HANDLUNGSEMPFEHLUNGEN FÜR DIE PRAXIS (1)

- Vorbereitung auf Informationspflichten und Betroffenenrechte
- Informationsformular gemäß Art 13 DSGVO
- Notfallkontakt für IT (Cybersecurity)
- Checkliste für einen Databreach erstellen
- Muster für Databreach Meldung an die Datenschutzbehörde (72-Stunden-Frist)

HANDLUNGSEMPFEHLUNGEN FÜR DIE PRAXIS (2)

- Liste der im Unternehmen verwendeten Software anlegen
- Prüfung ob die Softwareanbieter die Voraussetzungen der DSGVO erfüllen
- Liste der externen Auftragsverarbeiter anlegen
- Vertragliche Verpflichtung der Auftragsverarbeiter zur Gewährleistung der Bestimmungen der DSGVO und des DS-APG 2018

HANDLUNGSEMPFEHLUNGEN FÜR DIE PRAXIS (3)

- Regelmäßige Wartung von Firewalls, Folgenab-schätzungen und des Verarbeitungsverzeichnisses
- Verschlüsselung von USB Sticks
- Nutzung von privatem E-Mail Account oder Smartphone für Firmenagenden untersagen, da diese oftmals nicht ausreichenden Datenschutz bieten
- Möglichkeit von Verschlüsselung sensibler E-Mail Korrespondenz und Personaldaten

HANDLUNGSEMPFEHLUNGEN FÜR DIE PRAXIS (5)

- Erstellung von Verarbeitungsverzeichnis, Folgenabschätzung, sowie Benennung eines Datenschutzbeauftragten und Veröffentlichung seiner Kontaktdaten auf der Homepage

F. HASCH 51

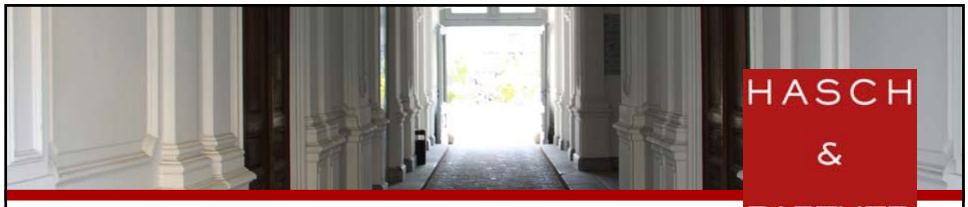
WEITERFÜHRENDE LINKS

Ausführliche Präsentation DSGVO
www.hasch.eu/news/archive

Datenschutzbehörde Wien
https://www.dsb.gv.at

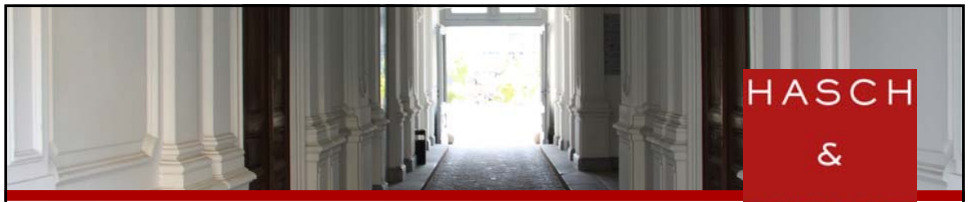
Österreichisches Informationssicherheitshandbuch
https://www.sicherheitshandbuch.gv.at

F. HASCH 52



DANKE FÜR IHRE

AUFMERKSAMKEIT



LINZ:
Landstraße 47, 4020 Linz
Tel: 0732 / 77 66 44-0
f.hasch@hasch.eu

WIEN:
Zelinkagasse 10, 1010 Wien
Tel: 01 / 532 12 70-0
f.hasch@hasch.eu

www.hasch.eu