Greiter Pegger Kofler Rechtsanwälte

Lundbeck Austria GmbH
17. Oktober 2018, Hohenems

Datenschutz NEU

RA Mag. Melanie Gassler-Tischlinger, LL.M.

1-9827

Geltung

- Geltung der Datenschutzgrundverordnung (DSGVO) seit 25. Mai 2018
  - direkt anwendbar, Harmonisierung in EU
  - Öffnungsklauseln
  - Aufhebung der Richtlinie 95/46/EG
- Ö: Datenschutzgesetz, Datenschutz-Deregulierungs-Gesetz
- Verarbeitung personenbezogener Daten
  - durch Unternehmen im Rahmen einer Niederlassung in der EU
  - durch Unternehmen außerhalb der EU, wenn sich die Verarbeitung auf die EU

Greiter Pegger Kofler Rechtsanwälte

Ziele der DSGVO

- Schutz der
  - Grundrechte und
  - Grundfreiheiten

  natürlicher Personen
  bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 2)

  à geschützt werden Personen, nicht Daten

  à bei Verstößen: empfindliche Geldbußen möglich

Folie 3

Greiter Pegger Kofler Rechtsanwälte

Adressaten der DSGVO

- Wer hat den Datenschutz zu beachten?
  - Der Datenschutz ist mit wenigen Ausnahmen von allen zu beachten, die über die **Zwecke** und **Mittel** der Verarbeitung von personenbezogenen Daten entscheiden
  - Grundsätzlich alle Unternehmen, Vereine und sonstige Organisationen

Folie 4

Greiter Pegger Kofler Rechtsanwälte

Grundbegriffe

- **Personenbezogene Daten** (Art. 4)
  - Alle Informationen über identifizierte oder identifizierbare natürliche Person, zB
    - Name, Adresse, Soz.Vers.-Nr., Email-Adresse, IP-Adresse des Computers einer Person, Fotos/Videos, Gesundheitsdaten, etc.
- **Verarbeitung**
  - jeder manuelle oder automatisierte Vorgang iZm personenbezogenen Daten, zB
    - Erheben, Erfassen, Berichtigen, Speichern, Löschen, Ordnen, Übermitteln, Verbreiten, etc.

Greiter Pegger Kofler Rechtsanwälte

Grundbegriffe

- **Verantwortlicher**
  - Jene natürliche oder juristische Person, die über Mittel und Zweck der Datenverarbeitung entscheidet, zB:
    Ärzte, Krankenhäuser, Apotheken, Therapeuten, Anbieter von Telefonleitungen, Anbieter von Internetleitungen, Post, Rechtsanwälte, Steuerberater, Notare, Behörden, Banken, Sozialversicherungsanstalten

Greiter Pegger Kofler Rechtsanwälte

Grundbegriffe

- **Auftragsverarbeiter**
  - Jede natürliche oder juristische Person, die im Auftrag und über Weisung des Verantwortlichen personenbezogene Daten verarbeitet, zB:
    - IT-Support Unternehmen, die Zugriff auf personenbezogene Daten haben
    - Arztsoftwarehersteller, wenn diese Zugriff auf personenbezogene Daten haben
    - E-Mailprovider
    - Unternehmen, die Direktwerbung anbieten (zB E-Mailversand)
    - Callcenter
    - Unternehmen, das Online Terminvereinbarung durchführt

Grundbegriffe

- **Betroffener**
  - Ein Betroffener ist jene natürliche Person, deren Daten verarbeitet werden (Patienten, Mitarbeiter, Lieferanten etc.)

- **Dateisystem**
  - Ein Dateisystem ist jede strukturierte Datensammlung, die nach bestimmten Kriterien zugänglich ist
  - Unerheblich, ob manuell oder automationsunterstützt
  - Alle Dateiensysteme unterliegen der DSGVO

Grundbegriffe

- **sensible Daten** (Art. 9)
  - Rassische oder ethnische Herkunft
  - politisch, religiöse oder weltanschauliche Überzeugung
  - Gewerkschaftszugehörigkeit
  - Genetische und biometrische Daten zur Identifizierung einer Person
  - Gesundheitsdaten
  - Daten zum Sexualleben oder zur sexuellen Orientierung
- **Daten über Verurteilungen und Straftaten** (Art. 10)

→ Achtung: besondere Regelungen!

Greiter Pegger Kofler Rechtsanwälte

Folie 9

Wann ist Datenverarbeitung erlaubt?

Art. 5: **Grundsätze der Datenverarbeitung**

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz (nachvollziehbar)
- Zweckbindung (wofür? Muss klar sein!)
- Datenminimierung (angemessen)
- Richtigkeit (Aktualität, Löschung)
- Speicherbegrenzung (Dauer)
- Integrität und Vertraulichkeit (TOMs)

„Accountability“ des Verantwortlichen
(Rechenschaftspflicht samt Nachweis)

Greiter Pegger Kofler Rechtsanwälte

Folie 10

Rechtmäßigkeit

- Art. 6: **Rechtmäßigkeit**
  - Vertragserfüllung
  - Erfüllung einer rechtlichen Verpflichtung
  - Schutz lebenswichtiger Interessen
  - Erfüllung einer Aufgabe im öffentl. Interesse
  - Überwiegen berechtigter Interessen
    - zB Direktmarketing; Übermittlung im Konzern
  - Einwilligung des Betroffenen
  - Anmerkung: Besondere Datenkategorien: Art. 9, 10: Verarbeitung nur mit Einwilligung oder aufgrund rechtlicher Verpflichtung möglich

Greiter Pegger Kofler Rechtsanwälte

Sensible Daten – Art 9

- Verarbeitung verboten, außer (bsp.)
  - Einwilligung
  - Arbeits- und sozialrechtliche Bestimmungen
  - Schutz lebenswichtiger Interessen
  - Betroffener hat Daten öffentlich gemacht
  - Geltendmachung von Rechtsansprüchen
  - Gründe des öffentlichen Interesses
  - Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin
  - Schutz vor schwerwiegenden, grenzüberschreitenden Gefahren
  - Archivzwecke, wissenschaftl. oder historische Forschungszwecke oder statistische Zwecke

Greiter Pegger Kofler Rechtsanwälte

§ 51 Ärztegesetz

§ 51 Ärztegesetz:

(1) Der Arzt ist verpflichtet, Aufzeichnungen über jede zur Beratung oder Behandlung übernommene Person, insbesondere über den Zustand der Person bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf sowie über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneispezialitäten und der zur Identifizierung dieser Arzneispezialitäten und der jeweiligen Chargen […] erforderlichen Daten zu führen und hierüber der beratenen oder behandelten oder zu ihrer gesetzlichen Vertretung befugten Person alle Auskünfte zu erteilen. In Fällen eines Verdachts im Sinne des § 54 Abs. 4 sind Aufzeichnungen über die den Verdacht begründenden Wahrnehmungen zu führen. Den […] verständigten Behörden oder öffentlichen Dienststellen ist hierüber Auskunft zu erteilen. Der Arzt ist verpflichtet, dem Patienten Einsicht in die Dokumentation zu gewähren oder gegen Kostenersatz die Herstellung von Abschriften zu ermöglichen.
(2) Ärzte sind zur automationsunterstützten **Ermittlung** und **Verarbeitung personenbezogener Daten** gemäß Abs. 1 sowie zur **Übermittlung** dieser Daten
1. an die Sozialversicherungsträger und Krankenfürsorgeanstalten in dem Umfang, als er für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet, sowie
2.an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, mit Zustimmung des Kranken
berechtigt. Die zur Beratung oder Behandlung übernommene Person hat das Recht auf Einsicht, Richtigstellung unrichtiger und Löschung unzulässigerweise verarbeiteter Daten.

Einwilligung

- **Bestimmtheit** (Art. 7)
  - Separation von Sachverhalten
- **Freiwilligkeit**
  - Koppelungsverbot, Widerrufsrecht
- **Informiertheit**
  - Zweck / Umfang
  - Verantwortlicher
  - Widerruf
- **Unmissverständlichkeit**
  - Klare, einfache Sprache
  - Leicht zugängliche Form
- Beweislast bei Verantwortlichem
- Kinder (Art. 8)
  - Erziehungsberechtigter, Prüfung

Einwilligung

- **E-Mails mit vertraulichen Informationen (Gesundheitsdaten und Befunde):**
  - An Patient:
    - Unverschlüsselte E-Mails nur mit Einwilligung
      Verschlüsselte E-Mails ohne Einwilligung möglich
  - An andere medizinische Einrichtungen:
    - Nur mit Zustimmung des Patienten (§ 51 Abs 2 Z 2 Ärztegesetz)
  - Empfehlung:
    - Vorgefertigte **Einwilligungserklärung** von Patienten unterfertigen lassen und in Patientenakte ablegen
    - Mündliche Einwilligungserklärung in Patientenakte **dokumentieren**

Greiter Pegger Kofler Rechtsanwälte

Folie 15

Tipps & Informationen

- Daher: mit Einwilligungen arbeiten!
- Besondere Vorsicht bei der Weiterleitung von Daten!
- Datenschutz auch im Gerichtsprozess beachten!
  - Schwärzen von Patientennamen
  - Antrag auf Ausschluss der Öffentlichkeit
- Forschungsorganisationsgesetz: Registerforschung und Verwendung von *Big Data* in der Forschung ab 2019: Zugriff auf ELGA (anonymisiert)

Greiter Pegger Kofler Rechtsanwälte

Folie 16

Rechte der Betroffenen

- **Informationsrechte**
- **Auskunftsrechte**
- **Berichtigungsrecht**
- **Recht auf Löschung** (Recht auf „Vergessenwerden“)
- **Datenportabilität**

Greiter Pegger Kofler Rechtsanwälte

Informationen

- Proaktiv bei Datenerhebung (Art. 13, 14)
  - Wer ist der Verantwortliche?
  - Gibt es einen Datenschutzbeauftragten?
  - Zweck u. Rechtsgrundlage der Erhebung, Änderung
  - Überwiegende berechtigte Interessen
  - Empfänger von Daten
  - Übermittlung in Drittland
  - Speicherdauer
  - Rechtsbelehrung
    - Auskunft, Löschung, Berichtigung, Widerspruch, Beschwerderecht (kostenlos!)
  - Bei automatisierter Entscheidungsfindung
    - Programmlogik
  - Quelle, Datenkategorien

Greiter Pegger Kofler Rechtsanwälte

Auftragsverarbeiter

- Art. 28: Schriftlicher Vertrag über:
  - Pflichten des Auftragsverarbeiters
  - Dauer und Gegenstand der Verarbeitung
  - Art und Zweck der Verarbeitung
  - Art der Daten und Kategorien der Betroffenen
- Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen
- Rechte der Betroffenen sind zu wahren
- Standardvertragsklauseln der Kommission
  - Standardvertragsklauseln der EU Kommission, die angemessene Garantien bei Übermittlung von Daten von der EU in Drittländer gewährleisten

Sicherheit

- Datenverarbeitung muss DSGVO entsprechen (Art. 24, 25, 32)
- TOMs zur Sicherstellung der
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Belastbarkeit der Systeme / Dienste
- Maßnahmen
  - Risikoanalysen
  - Evaluierungen
  - Anonymisierung, Pseudonymisierung
  - Privacy by Design / by Default
  - Backup-Systeme (Wiederherstellbarkeit)
  - Verhaltensregeln, Zertifizierung

Sicherheit

- Kriterien für Technische und organisatorische Maßnahmen (TOMs)
  - Stand der Technik,
  - Art, Umfang, Umstände und Zweck der Datenverarbeitung
  - Eintrittswahrscheinlichkeit,
  - Implementierungskosten
  - Schwere des Risikos für die Rechte und Freiheiten Betroffener
- **Angemessenes Sicherheitsniveau** ist sicher zu stellen

Greiter Pegger Kofler Rechtsanwälte

Verarbeitungsverzeichnis

- Verzeichnis aller Verarbeitungstätigkeiten (Art. 30)
  - Ersetzt die bisherige Meldung an das Datenverarbeitungsregister
  - Enthält alle Datenverarbeitungen im Unternehmen und beschreibt TOMs
  - Bei ≥ 250 Mitarbeitern: immer
  - Bei < 250 Mitarbeiter, wenn
    - Risiko für Rechte und Freiheiten Betroffener oder
    - Verarbeitung nicht nur gelegentlich erfolgt, oder
    - Verarbeitung besonderer Datenkategorien (Art. 9, 10)
  - Betrifft Verantwortliche und Auftragsverarbeiter

Greiter Pegger Kofler Rechtsanwälte

Verarbeitungsverzeichnis

Inhalt:

- Daten des Verantwortlichen / Auftragsverarbeiters
- Zweck der Verarbeitung
- Beschreibung der Datenkategorien
- Beschreibung der Betroffenenkategorien
- Empfängerkategorien
- Übermittlung in Drittländer
- Fristen für die Löschung
- Beschreibung der TOMs

Privacy Impact Assessment

Datenschutz-Folgenabschätzung (Art. 35)

- bei hohem Risiko für die Rechte und Freiheiten natürlicher Personen
- Das ist immer vorhanden zB bei
  - Systematischer umfangreicher Bearbeitungen **besonderer Datenkategorien** (Art. 9, 10)
  - Systematischer Überwachung öffentlicher Bereiche
  - Profiling
- Keine PIA – „white list“: Patienten-/Klienten-/Kunden-verwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheken
- Black list – für Arztpraxen verpflichtend? Noch nicht geklärt

Meldepflichten

- **Meldung an Aufsichtsbehörde** von risikobehafteten Verletzungen des Schutzes personenbezogener Daten (Art. 33)
- Unverzüglich, binnen 72 Stunden
  - Kontaktdaten des Datenschutzbeauftragten
  - Beschreibung der Verletzung
  - Anzahl und Kategorie der betroffenen Personen
  - Betroffene Datenkategorien
  - wahrscheinliche Folgen
  - Abhilfemaßnahmen
- Vollständige Dokumentation aller Fakten und Abhilfemaßnahmen

Benachrichtigung

- Benachrichtigung Betroffener bei hohem Risiko für deren Rechte und Freiheiten (Art. 34)
- Unverzüglich
- Inhalt der Benachrichtigung
  - Kontaktdaten des Datenschutzbeauftragten
  - wahrscheinliche Folgen
  - Abhilfemaßnahmen
- Bei unverhältnismäßig hohem Aufwand **à** öffentliche Bekanntmachung

Datenschutzbeauftragter

- Zwingend für
  - Öffentliche Stellen
  - Kerntätigkeit erfordert regelmäßige und systematische Überwachung Betroffener
  - Kerntätigkeit erfordert umfangreiche Verarbeitung besonderer Kategorien von Daten (Art. 9, 10)
- Weisungsfrei, Budgethoheit
- Keine Abberufung oder Benachteiligung wegen Erfüllung seiner Aufgaben
- Berichtet höchster Managementebene
- Ein einzelner Arzt sowie Ordinations- und Apparategemeinschaften benötigt keinen Datenschutz-beauftragten; unklar, ab welcher Praxisgröße einer benötigt wird (Ärztekammer empfiehlt ab 10 Mitarbeiter)

Datenschutzbeauftragter

- Aufgaben des DSB
  - Unterrichtung und Beratung der Geschäftsleitung
  - Überwachung der Einhaltung der DSGVO und nationaler Datenschutzgesetze
  - Überwachung der Einhaltung der Datenschutz-Strategie
  - Sensibilisierung und Schulung der Mitarbeiter
  - Überwachung / Durchführung des PIA
  - Zusammenarbeit mit und Anlaufstelle für die Aufsichtsbehörde

Übermittlung in Drittländer

- Angemessenheitsbeschluss der Kommission (Art. 44 ff)
  - zB CH, CAN, NZ, ARG
- Ansonsten geeignete Garantien
  - Durchsetzbare internationale Vereinbarungen
  - Genehmigte interne Datenschutzvorschriften
  - Genehmigte Standardschutzklauseln
  - Genehmigte Verhaltensregeln oder Zertifizierungen
- Ansonsten Verarbeitung nur möglich
  - Informierte Einwilligung
  - Vertragserfüllung
  - Lebenswichtige Interessen

Dokumentation / Nachweise

- Beispiele für Dokumentationspflicht
  - Weisung an Auftragsverarbeiter
  - Verarbeitungsverzeichnis
  - Verletzungen Datenschutz
  - Drittlandübermittlung (Garantien)
- Beispiele für Nachweispflicht
  - Einhaltung der Verarbeitungsgrundsätze (Art. 5)
  - Nachweis der Einwilligung (Art. 7, 8)
  - Nachweis zwingender Gründe bei einem Widerspruch (Art. 21)
  - Nachweis der rechtmäßigen Verarbeitung (Art. 28)

Geldbußen – Art. 83 ff

- Bis EUR 10 Mio. oder 2 % des weltweiten Konzernumsatzes (jeweils der höhere Betrag)
  - Art. 8 (Kinder)
  - Art. 25 bis 39 (Sicherheit, TOMs)
  - u.a.
- Bis EUR 20 Mio. oder 4 % des weltweiten Konzernumsatzes (jeweils der höhere Betrag)
  - Art. 5, 6, 7 und 9 (Grundsätze),
  - Art. 12 – 22 (Betroffenenrechte),
  - Art. 44 – 49 (Drittlandübermittlung),
  - u.a.

Schadenersatz / Haftung

- Haftung für materiellen und immateriellen Schaden (Art. 82)
- Solidarhaftung
  - Verantwortlicher haftet zusammen mit Auftragsverarbeiter
- Auch Auftragsverarbeiter können haften
- Gemeinsame Verantwortliche, zB Facebook und Betreiber einer Facebook-Fanpage haften zusammen

Aufsichtsbehörden

Mindestens eine Aufsichtsbehörde pro EU-Mitgliedstaat

- unabhängig, ausreichende Ressourcen
- Sicherstellung Einhaltung DSGVO
- Umfangreiche Befugnisse (Art. 58)
  - Auskunftsverlangen
  - Untersuchungen
  - Zugang zu Geschäftsräumen und EDV
  - Anordnung von Abhilfemaßnahmen
  - Verhängung von Geldbußen
- „One-Stop-Shop“ - Grenzüberschreitung
  - federführende Aufsichtsbehörde
  - Kohärenzverfahren
- Überprüfung durch Gerichte

Österr. DatenschutzG

- Restriktiver Gebrauch der Öffnungsklauseln
- Regelungen zu Bildaufnahmen
- Verbandsverantwortung
- Black & White Lists (PIA)
- Beschwerden an DSB / BVwG
- Verwaltungsübertretungen
  - Außerhalb des Art. 83 DSGVO
  - Strafen bis EUR 50.000,-, zB bei Verweigerung der Einschau
- „Bloße Verwarnungen“ – Datenschutz-DeregulierungsG

Erste Erfahrungen seit 25. Mai

- 810 Beschwerden, davon 530 Inland und 280 grenzüberschreitend
- 265 Data Breach Notifications
- 66 amtswegige Prüfverfahren
- 116 Verwaltungsstrafverfahren (davon 79 übernommen von Bezirksverwaltungsbehörden)
- 2 Geldbußen in Höhe von EUR 300,- und EUR 4.800,- (letztere ohne vorherige Verwarnung!)

(Stand 24.09.2018)

Umsetzung

- Vorbereitung
  - Projektmanagement
    - Wer ist für Herstellung der DSGVO-Konformität zuständig? Achtung: diese Person ist formell nicht der Datenschutzbeauftragte!
  - Beiziehung externer Experten?
    - Insbesondere in komplexeren Fällen
  - Bereitstellung der benötigten Ressourcen
  - To-do-Liste
    - Zeitplan: wer macht was und bis wann?

Umsetzung

- Erhebung IST-Zustand (I)
  - Erhebung der Verarbeitungen

    Was wird ermittelt und erhoben, zB Lohnverrechnung, Meldung an Soz.Vers., Direktwerbung an Kunden, etc.
    - Befragung Mitarbeiter
    - Prüfung der registr. Datenanwendungen lt DVR
    - Durchsicht der Standardanwendungen
    - Durchsicht von Verträgen mit Geschäftspartnern, Kunden und Mitarbeitern
    - Prüfung Website (Kontaktformular, Newsletter, etc).
    - Bildaufzeichnungen/Videoüberwachung

Umsetzung

- Erhebung IST-Zustand (II)
  - Auflistung Datenkategorien
    - Vorname, Name, Alter, Geschlecht, Adresse, Soz.Vers.-Nr., etc.
  - Erhebung der Zwecke der Verarbeitungen, zB
    - Personalverwaltung, Geschäftsabwicklung mit Kunden und Lieferanten, etc.
  - Bestimmung der jeweiligen Rechtsgrundlagen
    - Für jede Datenverarbeitung: Rechtfertigungsgrund
  - Werden sensible Daten (zB Gesundheitsdaten, biometrische Daten etc) verarbeitet?

Umsetzung

- Erhebung IST-Zustand (III)
  - Profiling
    - automatisierte Datenverarbeitung zur Erstellung eines Profils über persönl. Aspekte eines Betroffenen, zB wirtschaftliche Lage, Gesundheit, Vorlieben uä.
  - Übermittlung von Daten an Dritte und Auftragsverarbeiter
    - welche Rechtsgrundlage?
    - gibt es Auftragsverarbeitervertrag?
    - Verpflichtung der Mitarbeiter, Daten nur auf Anordnung zu übermitteln und Datengeheimnis einzuhalten, etc.
  - Zusammenfassung IST-Zustand
    - Welche Erhebungsschritte wurden getätigt?
    - Welche Ergebnisse brachten die Erhebungen?

Umsetzung

- Erforderliche Maßnahmen (I)
  - Verarbeitungsverzeichnis
  - Techn. und organisat. Sicherheitsmaßnahmen (TOMs)
    - Stand der Technik
    - IT-Betreuer
    - Interne Datenschutzrichtlinie für Mitarbeiter: Umgang mit personenbezogenen Daten (zB „Clean Desk Policy“).
    - Regelmäßige Schulung von Mitarbeitern

Umsetzung

- Erforderliche Maßnahmen (II)
  - Herstellung von Transparenz
    - Informationspflichten nach Art. 13 und 14 DSGVO = Umstände, über die Betroffene bei der Datenerhebung informiert werden müssen
    - Datenschutzerklärung auf Website, Informationen auf Anmeldeformularen, Information der Mitarbeiter über die Verarbeitung ihrer Daten (zB im Arbeitsvertrag) uä.

Umsetzung

- Erforderliche Maßnahmen (III)
  - Wahrnehmung der Betroffenenrechte
    - Konzept, wie Betroffenenrechte (zB Auskunftsverlangen) wahrgenommen werden
    - Festlegung der intern zuständigen Person
    - Festlegung des Verhaltens bei der Geltendmachung von Betroffenenrechten (Auskunft, Widerspruch, Löschung etc.)
    - Festlegung der zu ergreifenden Maßnahmen (Checkliste)
    - Vorkehrungen, dass jedem Betroffenen kurzfristig Auskunft gegeben werden kann, was Unternehmen mit seinen Daten macht

Umsetzung

- Erforderliche Maßnahmen (IV)
  - Data Breach Notification
    - Klare Regelung, was passiert, wenn etwas passiert (zB Hackerangriff, Verlust eines unverschlüsselten Notebooks mit Daten)
    - Verhalten bei einer Verletzung
    - Festlegung der intern zuständigen Person
    - Festlegung der zu ergreifenden Maßnahmen (Checkliste)
    - Benachrichtigung der Geschäftsleitung, des Datenschutzbeauftragten, der Datenschutzbehörde und des Betroffenen

Greiter Pegger Kofler Rechtsanwälte

Umsetzung

- Erforderliche Maßnahmen (V)
  - Schriftliche Verpflichtung der Mitarbeiter zur Wahrung des Datengeheimnisses
  - Vertragsprüfungen
    - Prüfung aller Verträge, AGBs, Datenschutz-erklärungen, Einwilligungen, etc.
  - Datenschutz-Folgenabschätzung
    - Wenn voraussichtlich hohes Risiko für die Rechte und Freiheiten nat. Personen besteht
  - Löschkonzept
    - Personenbezogene Daten dürfen nur so lange verarbeitet werden dürfen, bis der Zweck der Verarbeitung entfällt

Greiter Pegger Kofler Rechtsanwälte

Umsetzung

- Erforderliche Maßnahmen (VI)
  - Social Media
  - Dokumentation
    - umfassende Dokumentationspflichten
    - Nachweis der Einhaltung gegenüber Datenschutzbehörde
    - Unterlage (auch digital möglich) erstellen, anhand derer zu sämtlichen Aspekten des Datenschutzrechtes jederzeit Auskunft gegeben werden kann

Greiter Pegger Kofler Rechtsanwälte

Checkliste (I)

- Verantwortlichen / Team für Datenschutz bestimmen
- Erhebung des Ist-Zustandes
- Verarbeitungsverzeichnis
- Angemessenes Datenschutzniveau (TOMs)
  - Technische Maßnahmen: IT-Betreuer einschalten
    - Stand der Technik
    - Virenschutz
    - Firewall
    - Aktuelle Software
    - Zugriffsberechtigungen, etc.

Greiter Pegger Kofler Rechtsanwälte

Checkliste (II)

  - Organisatorische Maßnahmen
    - Mitarbeiterschulungen,
    - interne Datenschutzrichtlinie,
    - Zugangsbeschränkungen,
    - Clean Desk Policy, etc.
- Transparenz
  - Datenschutzerklärung für die Website
  - Information an Mitarbeiter
  - Sonstige Bereitstellung von Informationen
- Einwilligungen
  - Prüfung, ob Einwilligungen benötigt werden, bereits vorhanden sind, exakt formuliert sind

Checkliste (III)

- Auftragsverarbeiterverträge
- Drittlandübermittlungen
  - Prüfung der Zulässigkeit
- Datenschutzfolgenabschätzung?
- Verpflichtungserklärung für Mitarbeiter zur Wahrung des Datengeheimnisses
- Löschkonzept
- Konzept zur Wahrnehmung von Betroffenenrechten
- Konzept über Vorgehensweise bei Verletzungen
- Hinreichende Dokumentation

Wir danken für Ihre Aufmerksamkeit !

Greiter Pegger Kofler & Partner · Maria-Theresien-Straße 24 · AT 6020 Innsbruck · Austria
Tel +43 (0) 512 - 57 18 11 · Fax +43 (0) 512 - 58 49 25 · www.greiter.lawfirm.at · office@lawfirm.at

Greiter
Pegger
Kofler
Rechtsanwälte

Folie 49