Wie muss ich mit meinen Daten umgehen?

Datenschutz in der Praxis für EPU und KMU

Vorstellung

- Christoph Pozdena
- Staatlich zertifizierter Datenschutzbeauftragter
- Beratung und Umsetzung der EU-DSGVO für EPU und KMU

Wie aus Tinte und Papier Daten werden und warum wir das Internet neu betrachten sollten…

Verstöße und Strafen

- Verstöße gegen die Grundsätze:
- Geldbußen bis zu EUR 20 Millionen oder 4% des Umsatzes
- Verstöße gegen geringere Auflagen:
- Bis zu EUR 10 Millionen oder 2% des Umsatzes

Was ist die EU-DSGVO?
Betrifft mich die EU-DSGVO?

- Sachlicher Anwendungsbereich
  - Ganz oder teilweise automatisierte Verarbeitung
- Räumlicher Anwendungsbereich
  - Ort der Datenerhebung

Beispiel

- Maria Musterberaterin
- EPU
- Legt Protokolle von Beratungen handschriftlich als Kartei in einem Ordner ab
- Verwaltet Termine und Kundendaten in einer online CRM Lösung

Was sind überhaupt personenbezogene Daten?

- Informationen einer identifizierten oder identifizierbaren natürlichen Person
  - Name
  - SV-Nummer
  - Adresse
  - Geburtsdatum

Sensible Daten

- Rassische und ethische Herkunft
- Politische Meinungen
- Gewerkschaftszugehörigkeit
- Religiöse oder weltanschauliche Überzeugungen
- Genetische und biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Beispiel Fr. Musterberaterin

- Schreibt bei Sitzungen mit Klienten mit:
  - Essenszeiten und Häufigkeit
  - Kranken- und Operationsgeschichte
  - Macht ein Foto des Gesichts des Kunden

Einwilligungserklärung

- Rechtsgrundlage prüfen
- Formen: Schriftlich, elektronisch, mündlich
- Bestehende Einwilligungserklärungen prüfen
  - Achtung: KEIN stillschweigendes Einverständnis
- Verarbeitung von sensiblen Daten – Immer strenge Auflagen

Schriftliche Einwilligung gemäß Datenschutz (Muster!)

Die im Vertrag angegebenen personenbezogenen Daten, im Detail Name, Anschrift, Telefonnummer sowie Bankdaten, die allein zum Zwecke der Durchführung des entstehenden Vertragsverhältnisses notwendig und erforderlich sind, werden auf Grundlage gesetzlicher Berechtigungen erhoben.

Für jede darüber hinausgehende Nutzung der personenbezogenen Daten und die Erhebung zusätzlicher Informationen bedarf es regelmäßig der Einwilligung des Betroffenen. Eine solche Einwilligung können Sie im Folgenden Abschnitt freiwillig erteilen.

<u>Einwilligung in die Datennutzung zu weiteren Zwecken</u>

Sind Sie mit den folgenden Nutzungszwecken einverstanden, kreuzen Sie diese bitte entsprechend an. Wollen Sie keine Einwilligung erteilen, lassen Sie die Felder bitte frei.

☐ Ich willige ein, dass mir (Vertragspartner) postalisch Informationen und Angebote zu weiteren Produkten zum Zwecke der Werbung übersendet.

☐ Ich willige ein, dass mir (Vertragspartner) per E-Mail/Telefon/Fax/SMS Informationen und Angebote zu weiteren Produkten zum Zwecke der Werbung übersendet.

[Ort, Datum] [Unterschrift des Betroffenen]

Beispiel

- Fr. Musterberaterin hatte bisher eine Einverständniserklärung für Speicherung und Verarbeitung personenbezogener Daten
- Rechtsgrundlage für Datenverarbeitung prüfen
- Einwilligungserklärung für sensible Daten einholen

Verantwortlicher und Auftragsverarbeiter

- „Auftraggeber“ nach DSG 2000
  - Entscheidet über Verarbeitung von personenbezogener Daten
- „Dienstleister“ nach DSG 2000
  - Auftragsverarbeiter – Verarbeitet Daten für einen Verantwortlichen

Beispiel

- Fr. Musterberaterin
- Verantwortliche
- Cloudanbieter eines CRM Tools
- Auftragsverarbeiter

Pflichten des Verantwortlichen

- Datensicherheitsmaßnahmen
- Datenschutztechniken
- Datenschutzfreundliche Voreinstellungen
- Verzeichnis aller Datenverarbeitungstätigkeiten
- "data breach" Notification

Datensicherheit

- Backup
- Wiederherstellbarkeit und Verfügbarkeit
- Zugang- und Zutrittskontrolle

Beispiel

- Fr. Musterberaterin sichert elektronischen Kundendaten und E-Mails ab sofort jeden Abend auf einer externen Festplatte
- Diese an einem anderen, sicheren Ort versperren
- Sicheres Passwort für geschäftskritische Anwendungen

Datenschutz

- Pseudonymisierung, Anonymisierung
- Verschlüsselung
- TOM‘s - Technische und Organisatorische Maßnahmen

Beispiel

- Passwortschutz für alle elektronischen Geräte
- Sensible Daten anderer Kunden nicht zu externen Terminen mitnehmen
- Kundennummer statt Klarnamen in Dokumentationen verwenden

Datenschutzfreundliche Voreinstellungen

- „Privacy by Design“
- „Privacy by Default“

Beispiel

- Auf seiner Webseite müssen Kunden explizit die Newsletter-Checkbox anhaken
- Nach dem Eintragen zum Newsletter muss dieser bestätigt werden – Opt-In

Name *

First

Last

E-mail *

Comment or Message *

Stay Connected

Join My Newsletter

Submit

KURIER.at Horoskop

Bitte bestätigen Sie Ihre Anmeldung zum täglichen KURIER.at-Horoskop-Newsletter.

Bitte klicken Sie hier, um die Anmeldung zu bestätigen

Falls Sie diese E-Mail versehentlich erhalten haben, löschen Sie sie einfach. Sie erhalten den Newsletter nur, wenn Sie auf den Bestätigungslink klicken.

Für Fragen zu diesem Newsletter wenden Sie sich bitte an:
technik@kurier.at

Verzeichnis von Verarbeitungstätigkeiten

- Ablöse des Datenverarbeitungsregister (DVR)
- Kontaktdaten des Verantwortlichen, etwaigen Datenschutzbeauftragten
- Zwecke der Datenverarbeitung

Grundsätze der Verarbeitung

- Transparenz
- Zweckbindung
- Datenminimierung
- Speicherbegrenzung - Löschfristen

Meldung von Datenschutzverletzungen „data breach“

- Binnen 72 Stunden Meldung an Aufsichtsbehörde
- Benachrichtigung der betroffenen Personen
- Öffentliche Bekanntmachung bei großem Umfang

Risikoanalyse

- Welche Daten verarbeite ich?
- Welche Anwendungen verwende ich?
- An wen gebe ich die mir anvertrauten Daten weiter?

Betroffenenrechte

- Auskunftsrecht
- Recht auf Löschung
- Recht auf Datenübertragbarkeit
- Informationspflicht
  - Bei Erhebung von personenbezogenen Daten der betroffenen Person

Wann brauche ich einen Datenschutzbeauftragten?

- Wenn Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht

Wann brauche ich einen Datenschutzbeauftragten?

- Wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung sensibler Daten besteht.
- Haftung: Liegt immer bei der Geschäftsführung

- Welche personenbezogene Daten werden verarbeitet?
- Was sind die Zwecke meiner Datenverarbeitungen?
- Was ist die Rechtsgrundlage der Datenverarbeitung?
- Welche sensiblen Daten werden verarbeitet?
- Werden Auftragsverarbeiter herangezogen?
- Wie werden die Informationspflichten (nach der DSGVO) erfüllt?
- Wie werden die Betroffenenrechte (nach der DSGVO) erfüllt?
- Welche Datensicherheitsmaßnahmen sind vorhanden?
- Wie ist privacy by design/privacy by default implementiert?
- Besteht für meine Datenverarbeitungen Dokumentationspflicht?
- Welche Vorkehrungen gegen Datenschutzverletzungen existieren schon in meinem Unternehmen?
- Brauche ich einen Datenschutzbeauftragten?

Die 10 wichtigsten Schritte

- **Feststellung des Ist-Zustandes**
  Erheben Sie in Ihrem Betrieb welche Daten wie verarbeitet und wo und wie lange diese gespeichert bzw. aufbewahrt werden. Weiters erheben Sie an wen diese aufgrund welcher Rechtsgrundlage weitergegeben werden.
- **Bestellung eines Datenschutzbeauftragten oder verantwortliche Person für Datenschutzfragen**
- **Erstellung einer Dokumentation der Verarbeitungsvorgänge**
  Erarbeiten Sie Verfahrensverzeichnisse, gegebenenfalls unter zu Hilfenahme von Mustern.
- **Durchführung einer Datenschutz-Folgenabschätzungen**
  Prüfen Sie, ob ein Sie verpflichtend eine Datenschutz-Folgeabschätzung durchführen müssen bzw. wenn dies nicht der Falls ist, entscheiden Sie ob es dennoch machen möchte.
- **Meldung etwaiger Verstöße**
  Erstellen Sie oder besorgen Sie sich ein Muster für die Meldung von Datenschutzverletzungen.

- **Verträge mit Auftragsverarbeitern**
  Überarbeiten Sie bestehende Verträge mit Auftragsverarbeitern und evaluieren Sie, ob etwaige Neuabschlüsse sinnvoll sind.
- **Prüfung und Anpassung der bisher verwendeten Formulare**
  Evaluieren Sie die bislang verwendeten Formulare (z.B. Aufklärungs- und Einwilligungsbögen sowie Zustimmungserklärungen in AGB und auf Ihren Webseiten)
- **Informationspflichten und Betroffenenrechte**
  Überprüfen Sie, ob Sie die vorgesehen Informationspflichten erfüllen und stellen sich sicher, dass Sie die Betroffenenrechte wahren.
- **Sicherheitsmaßnahmen**
  Überprüfen und passen Sie bestehende Sicherheitsmaßnahmen an. Überlegen Sie sich ein Kontrollsystem.
- **Mitarbeiterschulungen**
  Führen Sie Mitarbeiterschulung durch und schließen Sie eine schriftliche Vereinbarung mit den Mitarbeitern ab.

Weiterführende Literatur

- http://www.wko.at/Datenschutz
- https://dsgvo.wkoratgeber.at/

Haftungsausschluss

Ich mache darauf aufmerksam, dass dieser Vortrag sowie die vorliegenden Folien lediglich einem unverbindlichen Informationszweck dienen und keine Rechtsberatung im eigentlichen Sinne darstellen.

Der Inhalt dieses Angebots kann und soll eine individuelle und verbindliche Rechtsberatung, die auf Ihre spezifische Situation eingeht, nicht ersetzen. Insofern verstehen sich alle angebotenen Informationen ohne Gewähr auf Richtigkeit und Vollständigkeit.

Bildquellen: Künstler: bokehlicia; http://bokehlicia.deviantart.com

Vielen Dank für Ihre Aufmerksamkeit!

Christoph Pozdena || 0699 1718 8861

datenschutz@ubertas.at || www.ubertas.at