MaGe Solutions

Die EU-Datenschutz Grundverordnung – ein wichtiger Schritt in die Zukunft

Markus Geiger

26.04.2018

Agenda

- **Kurzvorstellung**
    - **Etwas zur Historie**
        - **Was ist Datenschutz**
            - **Wen geht der Datenschutz was an?**
                - **Wo sind meine Chancen?**
                    - **Die wesentlichen Neuerungen**

- **Wie beginne ich als Unternehmer?**
    - **Der Datenschutzbeauftragte**
        - **Welche Risiken habe ich**

EU-DSGVO – ein wichtiger Schritt in die Zukunft
Kurzvorstellung

- Markus Geiger, 45 Jahre
- Seit 2016 Spezialisierung Datenschutz
- Seit über 10 Jahren Erfahrung im IT Service Management / Automotive (Prozessgestaltung, Betriebssteuerung)
- Seit 2004 selbstständig
- Stationen im Consulting bei T-Systems (div. Standorte), Deutsche Post, AGIS (Allianz), DaimlerChrysler, später Daimler
- Seit 1999 IBM Notes/Domino Spezialist (Admin)
- IT bewandert seit fast 20 Jahren

Etwas zur Historie

Es gibt eine Übergangsfrist…

allerdings endet diese am 25. Mai 2018

„ ... Nach Angaben der Marktforscher von IDC hatten sich **im Sommer 2017 an die 44 Prozent** der deutschen Unternehmen noch nicht oder nur ansatzweise mit der Datenschutz-Grundverordnung auseinandergesetzt ...“

Etwas zur Historie

Woher kommt diese Eile, warum sind alle so hektisch auf einmal?

- „bisher gab es den Datenschutz auch schon“
- Es gab kaum Interesse an den Neuerungen
- Das „Gefühl“ für das Thema war vor 2 Jahren noch nicht präsent
- vielfach keine Vorlagen oder andere Arbeitspapiere, diese wurden erst in den letzten Wochen und Monaten entwickelt (von Verbänden, Behörden und anderen Expertenkreisen)
- Eventuell das Wahrscheinlichste.... Die höheren Bußgelder

Verschiedene Schreibweisen:

- EU-DSGVO, DS-GVO, DSGVO, GDPR (im internationalen Kontext: General Data Protection Regulation)

Was sonst noch interessant ist

- Als EU-Verordnung steht diese über nationalem Recht – ohne erforderliche nationale Ratifizierung
- Bietet jedoch Spielraum, entsprechend wurde das „BDSG-neu“ gefaßt (genauer das DSAnpUG-EU)
- Auch Landesgesetze wurden überarbeitet, leider teils sehr unterschiedlich
- Jegliche spezielle Gesetzestexte überstimmen bei entsprechender Gültigkeit die allgemeineren Rechtsprechungen (TMG/Telemediengesetz, Sozialgesetzbuch, Gesetz gegen unlauteren Wettbewerb, etc.) sofern die Zielrichtung der Verordnung dadurch nicht entschärft wird

Datenschutz ist **nicht** gleichzusetzen mit ***Datensicherheit***,
letztere ist ein Teil des Datenschutzes!

Grundsätzlich gilt...
Es dürfen keine personenbezogenen Daten erhoben werden!

Allerdings definieren die folgenden Grundsätze die Ausnahmen:

Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5 DSGVO und Erwägungsgründe

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (a)
  - *Rechtmäßigkeit* - die Datenverarbeitung muss zulässig sein. Ausgehend vom Verbot mit Erlaubnisvorbehalt muss der Verantwortliche also eine Rechtsgrundlage oder die Erlaubnis für die Verarbeitung haben.

Was ist Datenschutz? II

- *Treu und Glauben* - die betroffene Person darf durch die Verarbeitung nicht überrascht werden. Sie muss diese nach der Lage der Dinge erwarten können und sie darf sie nicht benachteiligen.

- *Transparenz* - wie die Daten in dem Unternehmen verarbeitet werden, darf keine Unklarheiten ergeben, die Dokumentation und Beschreibung der innerbetrieblichen Prozesse muß eindeutig sein. Insbesondere das Verfahrensverzeichnis gibt hierüber Auskunft.

- *Erwägungsgrund 39: Grundsätze … Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Erforderlichkeit, Sicherheit*

Was ist Datenschutz? III

- Zweckbindung (b)
  - Der Willkürlichkeit wird Einhalt geboten. Die Verarbeitung der Daten muß nach einem klaren und präzise formulierten Zweck definiert sein, ein „man könnte es mal brauchen“ darf es nicht geben

- *Erwägungsgrund 47: Überwiegend berechtigte Interessen* - hier interessanter Passus: „… zum Zwecke der Direktwerbung kann als eine einen berechtigten Interesse dienende Verarbeitung betrachtet werden.“
- *Erwägungsgrund 50: Weiterverarbeitung*

Was ist Datenschutz? IV

- Datensparsamkeit / Datenvermeidung (c)
  - Nur *so viel Daten wie nötig* erheben. Wozu benötigen Sie die Religionszugehörigkeit als Maschinenbauer für den Newsletter-Versand? Weniger ist mehr!
  - Auch das *Löschen* von personenbezogenen Daten sollte klar sein. Werden die Daten nicht mehr benötigt und ist man nicht gesetzlich verpflichtet die Daten aufzuheben, dann sollten sie auch gelöscht werden.

- Richtigkeit (d)
  - *Sachlich richtig* und auf dem neuesten Stand
  - Sofern im Hinblick auf die Verarbeitung die Daten unrichtig sind, müssen diese unverzüglich berichtigt oder gelöscht werden.

- Speicherbegrenzung (e)
  - Speicherung in einer *Form der max. erforderlichen* Identifizierbarkeit
  - Längere Speicherung [..als notwendig..] nur für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke, oder für statistische Zwecke … .

Was ist Datenschutz? V

- Integrität und Vertraulichkeit (f)
  - Die personenbezogenen Daten müssen *angemessen* durch technische und organisatorische Maßnahmen geschützt werden, einschließlich Schutz vor unbefugter oder unrechtmässiger Verarbeitung und vor unbeabsichtigten Verlust, Zerstörung oder ebensolcher Schädigung

- Rechenschaftspflicht (Art. 5, Abs. 2, DSGVO)
  - „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muß dessen Einhaltung nachweisen können“

Was ist Datenschutz? VI

- **Und noch ein paar Formulierungen, …**

- Verbot mit Erlaubnisvorbehalt / Einwilligung (*Erwägungsgrund 43*)
  - Das bedeutet, dass dies nur dann zulässig ist, wenn eine Einwilligung oder mindestens eine andere den Vorschriften entsprechende Ausnahme vorliegt.

- **Besonders geschützte Daten** - Als sensibel – mit entsprechender Beachtung auch bei der Aufsichtsbehörde – und mit erhöhter Sorgfalt anzuwenden gelten Angaben über

  - die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
  - Und natürlich: Kinder (bis 16 Jahre) *(s. aktueller Pressebericht, WhatsApp dürfe nicht weiter von jüngeren Personen genutzt werden, eine Altersbestätigung wird in der app angefordert)*

Wen geht der Datenschutz was an?

Die DSGVO gilt für **alle Unternehmen** !!!

die personenbezogene Daten von in der EU aufhältigen Personen verarbeiten

Was sind personenbezogene Daten?

- allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Adresse, E-Mail, Tel#...)
- Kennnummern (Sozialversicherungsnummer, Steuer identifikationsnummer, KV-Nr,, Personalausweisnr, Matrikelnummer usf.)
- Bankdaten (Kontonr, Kreditinformationen, usf.)
- Online-Daten (IP-Adresse, Standortdaten usf.)
- physische Merkmale (Geschlecht, Haut-, Haar-, Augen-farbe, Statur, Kleidergröße usf.)
- Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten usf.)
- Kundendaten (Bestellungen, Adressdaten, Kontodaten usf.)
- Werturteile (Schul- und Arbeitszeugnisse usf.)
- u. v. m.

EU-DSGVO – ein wichtiger Schritt in die Zukunft
Wo sind meine Chancen? I

- Sie haben ein **Unternehmens-Image** zu verlieren
- Sie benötigen den **Schutz Ihrer Unternehmens-Werte**
- Das gewonnene **Kundenvertrauen** muß erhalten bleiben

- Der Bedarf nach Sicherheit wächst – und die **Bereitschaft**, etwas dafür zu tun
- Die aktuellsten Gefahren der IT:
  - Trojaner und Würmer
  - Spam und Phishing
  - Botnetze, Denial-of-Service-Attacken

  bisher zumeist „ganz weit weg“ können sehr schnell **Ihre** Realität werden, somit auch die **Ihrer Kunden, Geschäftspartner, Mitarbeiter**

- Der Bedarf nach **Standardisierung** bei Sicherheit wächst
- Noch (!) gibt es keinen festen Standard im Rahmen einer z.B. ISO-Zertifizierung (ist allerdings in der Entstehung)

EU-DSGVO – ein wichtiger Schritt in die Zukunft

Wo sind meine Chancen? II

- Mit dem prophylaktischen Schutz durch ein durchdachtes Datenschutz- und Datensicherheitssystem übernehmen Sie die Verantwortung und die Kontrolle

- Der Grad wie der Schutz der Daten – nicht nur der personenbezogenen oder personenbeziehbaren – in einem Unternehmen angesehen und gelebt wird, wird unumstößlich einen höheren Stellenwert erhalten
- Dadurch können Sie auch gesichert im Markt auftreten und im Wettbewerb punkten

- **Ihre Orientierung zur sicheren Zukunft ist der erste Schritt zu mehr Sicherheit**

EU-DSGVO – ein wichtiger Schritt in die Zukunft

Die wesentlichen Neuerungen I

- Harmonisierung des Datenschutzniveaus (einheitliches Datenschutzrecht f. privaten und öffl. Bereich)

- Informierte eindeutige Einwilligung (Betroffener ist informiert und aufgefordert diese unmissverständlich abzugeben)
- Verbotsgesetz mit Erlaubnisvorbehalt (analog zum heutigen BDSG)
- Recht auf Vergessenwerden (Löschung auf Wunsch des Betroffenen (vgl. Google-Urteil 2014)

- Europaweite Pflicht zur Bestellung eines Datenschutzbeauftragten (für DE zusätzlich im DSAnpUG-EU („BDSG-neu“)

- Deutliche Anhebung der Bußgelder bei Verstoß (Details weiter unten)

EU-DSGVO – ein wichtiger Schritt in die Zukunft

Die wesentlichen Neuerungen II

- Besseres Verständnis für „personenbezogene Daten“ (Erweiterung um genetisch u. biometrisch; direkt u. indirekt bestimmbar)

- Für Software-Entwickler wichtig genauso wie bei Software-Anschaffungen: Privacy by Design & Privacy by Default

- Datenschutz-Folgenabschätzung:
  Mit dem Inkrafttreten der DSGVO wird die sogenannte Datenschutz-Folgeabschätzung (DSFA) eingeführt, welche die bisher bekannte Vorabkontrolle ablöst. Ziel ist es, die Risiken und die möglichen Folgen für die persönlichen Rechte der Betroffenen zu bewerten zur Ableitung weiterer Maßnahmen

EU-DSGVO – ein wichtiger Schritt in die Zukunft

Die wesentlichen Neuerungen III

- Der One-Stop-Shop-Mechanismus - *Das bedeutet, dass für Unternehmen, die Niederlassungen in mehreren Ländern haben, künftig nur die Aufsichtsbehörde an ihrem Hauptsitz zuständig sein wird.*

- Die Anwendbarkeit europäischen Datenschutzrechts auf außereuropäische Internetdienstleister (Facebook, Google ....)

EU-DSGVO – ein wichtiger Schritt in die Zukunft

Wie beginne ich als Unternehmer? I

1. Beginn mit der Bestandsaufnahme, wo & welche Daten überhaupt erfaßt werden ➔ GAP-Analyse

2. Umfangreiche Informationspflichten sind einzuhalten (Zweck, Dauer, Rechte) ➔ Update der Homepage

3. Verfahrensverzeichnis erstellen bzw. (wenn schon vorhanden) aktualisieren (neue Bezeichnung: Verarbeitungsverzeichnis). Mit mehr Transparenz soll der rechtmäßige Umgang mit deren Daten nachweisbar sein

Wie beginne ich als Unternehmer? II

4. Prüfung ob die Erfassung und Verwendung der Daten durch eine Rechtsgrundlage gerechtfertig ist (z.B. Vertrag, Einwilligung, berechtigtes Interesse) Dokumentationspflichten z.B. über rechtmäßige Verarbeitung personenbezogener Daten, Einwilligungen, Abwägung ob ein hohes Risiko für personenbezogene Daten besteht

5. Aufbau einer IT-Sicherheit (angepasst an die Größe des Unternehmens)

6. Risikobewertung der verarbeiteten Daten und der TOM‘s (Angemessene technisch-organisatorische Maßnahmen sind zum Schutz zu gewährleisten, regelmäßige Überprüfungen sind dafür einzuplanen)

7. Prozesserstellung – zügige Reaktion zur Meldung Datenschutzverstoß an die Aufsicht und an die Betroffenen. Datenpannen (Verlust, Beschädigung) sind binnen 72 Stunden der Aufsichtsbehörde zu melden

Wie beginne ich als Unternehmer? III

8. Anpassung bzw. Abschlüsse von Verträgen mit Auftragsverarbeitern

9. Thema Informationspflicht - Betroffene haben Recht auf Auskunft, Berichtigung, Löschung und Übertragbarkeit Ihrer Daten:
    8. Wie kann ein Betroffener Kontakt aufnehmen
    9. wie erfolgt das Vorgehen bei eingehender Nachfrage
    10. wer ist zuständig
    11. wo sind die personenbezogenen Daten gespeichert

10. Mitarbeiter-Schulung – Sensibilisierung für das Thema, Erstellung einer Unternehmensrichtlinie

11. Verpflichtung auf das Datengeheimnis - Alle Personen (nicht nur interne Mitarbeiter), die mit personenbezogenen Daten arbeiten, sind auf das Datengeheimnis zu verpflichten. Sie dürfen ihnen bekannte Daten nur für den vorgesehenen Zweck verwenden.

Der Datenschutzbeauftragte I

- Ab wann ist er verpflichtend? Ab 10 Mitarbeiter, die ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt sind (Behörden, öffentliche Stellen ohne Einschränkung immer)

- Seine Aufgaben:

  - Begleitung der Unternehmen (der Geschäftsleitung berichtend)
    - Der DSB **berät**, **entwickelt** zu betrieblichen Regelungen zum Datenschutz
      die Leitung setzt diese in Kraft (Art. 24 mit ErwGr74 DSGVO, Art 5 DSGVO)

    - Der DSB überprüft die Umsetzung und Einhaltung der Vorgaben und informiert die Leitung über Abweichungen

Der Datenschutzbeauftragte II

- Er ist **unabhängig** und **weisungsfrei** (Art. 38 Abs. 3 mit ErwGr 97 DSGVO)

- Wann intern / extern?
  Diese Frage ist sehr individuell zu beantworten, tendentiell empfiehlt sich ein externes Engagement je „kleiner“ das Unternehmen ist.

- Datenschutzmanagementsystem – es stellt sicher daß Geschäftsprozesse, Systeme und Strukturen einer Organisation inkl. interner und externer Schnittstellen regelmäßig überpüft und – falls erforderlich – angepaßt werden

Welche Risiken habe ich? I

- Wesentlich höhere Bußgelder drohen als bisher – einhergehend mit möglichen Schadenersatzforderungen und einem potentiellen Imageverlust

- **Bei Verstoß hierzu / bis zu 10 Mio Bußgeld bzw. 2% des weltweiten Jahresumsatzes**

- Führen eines Verfahrensverzeichnisses
- Bedingungen für die Einwilligung von Kunden
- Vorgaben Datensparsamkeit (privacy by design / by default)
- Regelungen Auftragsdatenverarbeitung
- Zusammenarbeit mit den Aufsichtsbehörden
- Sicherheit der Datenverarbeitung (ehemals "TOM")
- Meldepflichten ("data breach notification")

Welche Risiken habe ich? II

- Wesentlich höhere Bußgelder drohen als bisher – einhergehend mit möglichen Schadenersatzforderungen und einem potentiellen Imageverlust

- **Bei Verstoß hierzu / bis zu 20 Mio Bußgeld bzw. 4% des weltweiten Jahresumsatzes**

- Grundlegende Prinzipien des Datenschutzes
- Fehlende Zulässigkeit bei der Datenverarbeitung
- Verletzung der Betroffenenrechte
- Vorgaben zum Datentransfer außerhalb der EU
- Missachtung von Vorgaben der Aufsichtsbehörden

Kontakt

Ich empfehle….

- Nehmen Sie die Chance wahr,
- nehmen Sie das Thema ernst,
- Machen Sie aus dem MUSS ein IST,
- Ihre unternehmerische Zukunft dankt es Ihnen

Viel Erfolg bei der Umsetzung IHRES Datenschutzes!

Wir hoffen, der Vortrag konnte Sie ermutigen, das Thema anzugehen,

vielen Dank für Ihre Aufmerksamkeit!

Sie haben noch Fragen oder denken über eine Unterstützung nach,

Meine Kontaktdaten....

Backup

Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
   - Zutrittskontrolle
   - Zugangskontrolle
   - Zugriffskontrolle
   - Trennungskontrolle

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
   - Weitergabekontrolle
   - Eingabekontrolle/Verarbeitungskontrolle
   - Dokumentationskontrolle
   - Auftragskontrolle
   - Verfügbarkeitskontrolle

3. Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)

- geregelt für:
  - 6 Jahre Geschäftsbriefe
  - 10 Jahre steuerrelevante Unterlagen
  - 6 Monate Bewerbungsunterlagen

- Alle anderen Daten und Dokumente mit personenbezogenen Daten müssen gelöscht beziehungsweise vernichtet werden, **wenn sie nicht mehr benötigt werden** (Datensätze löschen, Datenträger zerstören, Papierunterlagen mit personenbezogenen Daten schreddern).