DSGVO – Datenschutzgrundverordnung

Dr. Markus Knasmüller
Leiter SW-Entwicklung

Herausforderungen durch EU-DSGVO

"Registrierkassenpflicht war ein Kinderspiel"

Die Stadt Wien setzt schon um, was auf alle österreichischen Unternehmen in den nächsten Jahren zukommt: Die im Mai 2018 in Kraft tretende Datenschutzgrundverordnung der EU. Ziel ist der verbesserte Schutz der Konsumentinnen und Konsumenten und deren Daten. Für die Wirtschaft bedeutet das aber einen großen bürokratischen Aufwand. Das Internationale Forum für Wirtschaftskommunikation (IFWK) nahm sich dieser neuen Herausforderung für Wirtschaft und Medien an. Im Rahmen einer Podiumsdiskussion, die auf Einladung von HP Österreich stattfand, kam man zum Schluss: Die Einführung der Registrierkassenpflicht war dagegen wie ein Kinderspiel

DATENSCHUTZ-GRUNDVERORDNUNG

81 Prozent sehen keine Chance für eine fristgerechte DSGVO-Einführung

30.05.2017 Von Andreas Th. Fischer (Autor)

Die neue DSGVO enthält fast einhundert Artikel und Vorschriften, die eigentlich bis spätestens zum 25.5.2018 umgesetzt sein müssen. Allein in Deutschland rechnen aber vier von fünf Unternehmen nicht damit, dass sie diesen Termin einhalten können. Die Gründe dafür sind laut einer Studie von Varonis vielfältig.

Webcast mit Live-Chat
am 21. Juni, 14:00 Uhr

47 Prozent der Unternehmen sind blank

05.12.2017 Von Dr. Ronald Wiltscheck (Chefredakteur)

Die Ergebnisse der jüngsten WatchGuard-Umfrage zur Datenschutz-Grundverordnung (DSGVO, engl.: GDPR – General Data Protection Regulation) sind alarmierend.

EU-Datenschutz-Grundverordnung: „Augenzwinkernder" Umgang mit Datenschutz wird zum Auslaufmodell

Teilweise auch wirklich notwendig

GMAIL

Google scannt Mails künftig nicht mehr für Werbung

Künftig will Google auch in der Privatkundenversion von Gmail den Text nicht mehr auf Stichworte für Werbung untersuchen. Stattdessen sollen die gleichen Verfahren wie unter anderem bei der Internetsuche verwendet werden.

Datenschutz

Datenskandal bei der Polizei: Offenbar zehntausende Unschuldige gespeichert

Durch die Recherchen rund um die G20-Presseakkreditierungen

DSGVO: Eckpunkte

- Tritt mit **25.5.2018** in Kraft – egal was passiert
- Ob wir sie wollen oder nicht!
- Trifft jeden!

- In Wahrheit nicht viel Neues, aber es wird ernst
- Strafen bis zu 20 Mio. Euro (bei internationalen Konzernen noch höher – bis zu 4 % des Gesamtumsatzes)

- Wirksam, verhältnismäßig und abschreckend

DSGVO: Personenbezogene Daten

- Personenbezogene Daten: Angaben über natürliche Personen, deren Identität identifiziert oder identifizierbar ist: z. B. auch Adresse, Telefonnummer, Bild auf Foto, IP-Adressen, KFZ-Kennzeichen, …
- Technisches Format: egal, ob Datenfelder in Software, Excel, Word, E-Mail, Videoaufnahme, Foto, ….
- Auch in Freifeldern abgelegte Daten
- Zweckbindung: Daten nur für die festgelegten Zwecke verwenden
- Datenminimierung: nur soviel wie zum Erreichen des Zweckes nötig (etwa Lieblingsfarbe, Hobbies nicht nötig für Erfüllung eines Vertrages)

Unterscheidung Verantwortlicher – Auftragsverarbeiter (Art. 4 DSGVO)

- Verantwortlicher entscheidet alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten
- Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen
- Verarbeitung: jeder Vorgang im Zusammenhang mit persönlichen Daten, wie Erheben, Erfassen, Organisieren, Ordnen, Speichern, Verändern, Auslesen, Abfragen, Verwenden aber auch Löschen
- Unterscheidung ist durchaus wesentlich auf Grund der damit verbundenen Rechte und Pflichten (etwa besteht Auskunftsrecht nur gegenüber Verantwortlichen und nicht Auftragsverarbeiter)

Auftragsverarbeiter (Art. 28) Was ist zu beachten?

- Muss garantieren, dass Verarbeitung im Einklang mit der Verordnung erfolgt
- Dritte werden nicht hinzugezogen, außer bei Verständigung des Verantwortlichen
- Klarer Vertrag mit entsprechenden Bestimmungen muss bestehen
- Nach Abschluss Löschung der Daten, sofern nicht gesetzliche Verpflichtung besteht
- Verarbeitung ausschließlich auf Weisung des Verantwortlichen

Rechtsgrundlage für die Speicherung (Art. 6) als Verantwortlicher

- **Einwilligung** (Art. 6 a)
- **Vertrag** (Art 6 b)
- **Rechtliche Verpflichtung** (Art 6 c)
- Lebenswichtiges Interesse (Art 6 d)
- Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art 6 e)
- **Berechtigtes Interesse** (Art 6 f)

Was ist bei Einwilligung zu beachten

- Kein klares Ungleichgewicht zwischen Betroffenem und dem Verantwortlichen (z. B. Dienstvertrag)
- **Koppelungsverbot**
- Aber zulässig falls Wahl kostenfrei mit Zustimmung, kostenpflichtig ohne Zustimmung, etwa bei APPs
- **Nachweis nötig**
- In Ö ab 14, sonst Erziehungsberechtigter
- **Widerruf so einfach wie Erteilung**

Was ist bei Einwilligung zu beachten

- In Kenntnis der Sachlage und in informierter Weise
  - Auflistung der betreffenden Daten (ErwGr 32)
  - Nennung des Verantwortlichen (ErwGr 42)
  - Beschreibung der Zwecke (ErwGr 42)
  - Auflistung aller Datenempfänger (Art 13 lit e)
  - Hinweis auf jederzeitiges Widerrufsrecht und die Rechtmäßigkeit der Verarbeitung vor Widerruf der Einwilligung (Art 7 Abs 3)
- **Vorausgefülltes Häkchen gilt nicht!!!**

Was ist bei Einwilligung zu beachten

- Einwilligung dokumentieren
- Unterzeichnetes Formular und speichern in Zusammenhang mit Person oder

- Online: Protokollierung: wann zugestimmt
- Beweiswürdigung aber wohl problemlos
- Wenn: Seitengestaltung auch gespeichert

Praxistipp Einwilligung

- Nur einholen wenn wirklich notwendig
- Sonst verschlechtert es eventuell die Situation
  - Bsp: Vertrag: was würde dann passieren, wenn Einwilligung verweigert
  - Bsp: Berechtigtes Interesse: dann wäre ein Speichern absolut nicht mehr möglich, falls Einwilligung nicht erteilt

- Aber natürlich falls erteilt, gibt sie große Rechtssicherheit

Frist für die Speicherung (Art. 5 (1) e)

- Muss immer angeführt sein
- Nichts kann beliebig lange gespeichert werden

- Zweck ist ausschlaggebend
- Hier gibt es aber noch viel Diskussionsbedarf

- Buchhaltung: 7 Jahre
- Lohn: Teilweise Daten 30 Jahre für Zeugnis
- Aus berechtigtem Interesse aber auch länger!
- Kammer für Steuerberater: empfiehlt 30 Jahre

Besondere Kategorien von Daten (Art. 9)

- Rassische oder ethnische Herkunft
- Politische Meinung
- **Religiöse oder weltanschauliche Überzeugung**
- **Gewerkschaftszugehörigkeit**
- Genetische Daten
- **Biometrische Daten**
- **Gesundheitsdaten (Krankenstanddaten, auch SV-Nummer!)**
- Daten zum Sexualleben oder der sexuellen Orientierung

Besondere Kategorien von Daten (Art. 9) Speicherung nur erlaubt wenn:

- **Einwilligung** (Art 9 (2) a)
- **Arbeitsrecht, Kollektivvertrag, Betriebsvereinbarung** (Art 9 (2) b)
- Lebenswichtiges Interesse (Art 9 (2) c)
- Geeignete Garantie und nur für Mitglieder (Art 9 (2) d)
- **Selbst öffentlich gemacht** (Art 9 (2) e)
- **Rechtsansprüche** (Art 9 (2) f)
- Erhebliches öffentliches Interesse (Art 9 (2) g)
- **Gesundheitsvorsorge oder Arbeitsmedizin** (Art 9 (2) h)
- Öffentliches Interesse im Bereich der öffentlichen Gesundheit (Art 9 (2) i)
- Archivzwecke im öffentlichen Interesse (Art 9 (2) j)

Transparenz (Art. 12 ff)

- Transparenz wird groß geschrieben
- **Betroffener muss informiert werden, dass Daten über ihn gespeichert werden**
- **Ebenso hat betroffene Person Rechte**

- **Frist** zur Erfüllung der Rechte ist immer unverzüglich, spätestens **innerhalb eines Monats**
- Bei komplexen Anliegen kann Frist um zwei Monate erstreckt werden
- **Möglichkeit der Beschwerde an die DSB**

Wen treffen diese Rechte?

- Recht auf Information, Auskunft, Löschung, etc. treffen den Verantwortlichen, nicht den Auftragsverarbeiter.
- Gegebenenfalls an den Auftraggeber verweisen, bzw. das Begehren weiterleiten (nicht verpflichtend)
- Unterstützungspflicht ist vorhanden

Informationspflicht (Art. 13)

- Zum Zeitpunkt der Erhebung nötig:
  - Verantwortlicher (+ ev. Datenschutzbeauftragter)
  - Zweck, Rechtsgrundlage
  - Gegebenenfalls Empfänger der Daten
  - Dauer der Speicherung
  - Information über Rechte
  - Besteht Verpflichtung zur Bereitstellung
  - Etwaige negative Folgen falls nicht bereitgestellt
  - Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
  - https://dsgvo-informationsverpflichtungen.wkoratgeber.at/

Informationspflicht (Art. 14)

- Wenn nicht direkt erhoben:
  - Im Prinzip wie bei Art. 13
  - Zusätzlich
    - Datenkategorien
    - Art der Quelle
  - Nicht: Verpflichtung, negative Folgen, …
- Innerhalb angemessener Frist (max. 1 Monat)
- Spätestens bei erster Mitteilung bzw.
- Bei erster Offenlegung für anderen Empfänger
- Ausreichend: auf leicht auffindbare Weise zugänglich gemacht.

Informationspflicht (Art. 14)

Nicht nötig wenn:

- betroffene Person bereits über Information verfügt
- Erlangung durch Rechtsvorschriften ausdrücklich geregelt ist
- personenbezogene Daten dem Berufsgeheimnis unterliegen und vertraulich behandelt werden müssen
- Erteilung der Information erweist sich als unmöglich oder erfordert unverhältnismäßigen Aufwand

Recht auf Auskunft (Art. 15)

- Betroffene Person kann vom Verantwortlichen Bestätigung verlangen, ob über sie personenbezogene Daten verarbeitet werden
- Bestimmte Informationen müssen dann angegeben werden
- Sofern nicht Rechte anderer Personen verletzt werden
- Und das kostenfrei (zumindest die erste Auskunft/Kopie)
- KSV hat bspw. bereits jetzt jährlich 140.000 Ansuchen

Recht auf Auskunft (Art. 15) Informationen

- Verarbeitungszwecke
- Kategorien der betroffenen Daten
- Eventuelle Empfänger
- Speicherdauer
- Hinweis auf Recht auf Berichtigung oder Löschung, sowie Einschränkung und Widerspruchrecht
- Hinweis auf Beschwerderecht an die Datenschutzbehörde
- Information über die Herkunft der Daten
- Bestehen einer automatisierten Entscheidungsfindung
- **Vollständige Kopie der Daten** (z. B. Ausdruck)

Recht auf Auskunft (Art. 15)
Anmerkungen

- Nicht vom Auftragsverarbeiter!
- Identität muss überprüft werden
- Bei umfangreichen Daten darf verlangt werden, dass die Person präzisiert worauf sich ihr Auskunftsersuchen bezieht
- Unverzüglich, jedenfalls aber innerhalb einer Frist von einem Monat (kann um weitere zwei Monate erstreckt werden)
- Vorzugsweise elektronisch
- Recht auf Berichtigung (Art. 16)

Recht auf Datenübertragung (Art. 20)

- Die einem Verantwortlichen überlassenen Daten müssen auf Antrag bereitgestellt werden
- Nur diese, keine abgeleiteten Daten
- In einem strukturierten, gängigen und maschinenlesbaren Format

- Betrifft nur die Daten die wissentlich und willentlich an den Verantwortlichen übermittelt wurden
- Nur bei Einwilligung oder Vertrag, nicht etwa bei gesetzlicher Verpflichtung oder berechtigtem Interesse
- Grundsätzlicher Gedanke: Wechsel eines Systems
- Beispiel: Facebook

Recht auf Löschung (Art. 17)

- Daten unverzüglich löschen auf Aufforderung
- Falls für Zweck nicht mehr nötig
- Einwilligung wird widerrufen
- Widerspruch wird eingelegt und es liegen keine vorrangig berechtigten Gründe vor
- Unrechtmäßige Verarbeitung liegt vor

- Auch Auftragsverarbeiter und Empfänger von Daten müssen informiert werden

Recht auf Löschung (Art. 17)
Beispiele

- Informationszusendungen – Zustimmung widerrufen
- Bewerbung zurückgezogen
- Buchhaltungsunterlagen (abhängig vom Alter!)
- Berechtigtes Interesse des Verantwortlichen wird nicht anerkannt (etwa will keine Werbung)
- Ehemalige/r Mitarbeiter/in und Verzicht auf Dienstzeugnis
- …

Recht auf Löschung (Art. 17)
Wie tief muss das gehen?

- Vollständig!
- Es reicht nicht, z.B. nur den Mitarbeiterstammsatz zu anonymisieren
- Auch Bewegungsdaten gehören entsprechend gelöscht bzw. wirklich anonymisiert
- Ebenso Protokolle
- Es darf keine Identifizierung mehr möglich sein, auch nicht indirekt über einen Termin, Auftrag, etc.
- Software gefragt: selbst kaum möglich
- Mit Herstellern sprechen!

Recht auf Löschung (Art. 17)
Was ist mit Sicherungen

- Grundsätzlich sind auch diese zu löschen
- Eigentlich logisch, aber dennoch starker Kritikpunkt, da de facto unmöglich
- Etwa WORM-Platten

- DSG § 4: Falls nicht unmittelbar möglich, bis zu diesem Zeitpunkt einzuschränken

Recht auf Löschung (Art. 17) Einwände zur Löschung

- Recht auf freie Meinungsäußerung und Information
- **Erfüllung einer rechtlichen Verpflichtung**
- Gründe des öffentlichen Interesses im Bereich der öffentlichen Sicherheit
- Für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke
- **Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen**

Verzeichnis der Verarbeitungstätigkeiten (Art 30) Führen

- Pflicht jedenfalls ab 250 Mitarbeiter/innen für alle Verarbeitungstätigkeiten, sonst nur wenn Verarbeitung nicht gelegentlich oder besondere Datenkategorien beinhaltet (oder ein Risiko für die Rechte und Freiheiten der betroffenen Person birgt)
- Aber auch dann für Personalverwaltung (sensible Daten!) oder Buchhaltung
- Ersetzt DVR-Register

- Ausgangspunkt für alles
- Nur so ist Recht auf Auskunft möglich
- Nur so kann man planen

Verzeichnis der Verarbeitungstätigkeiten (Art 30) Inhalt

- Name und Kontaktdaten des Verantwortlichen
- Verarbeitungszweck
- Datenarten
- Kategorien betroffener Personen
- Datenübermittlungsempfänger
- Datenübermittlung in Drittstaaten
- Soweit möglich die geplante Speicherdauer von Daten
- Datensicherheitsmaßnahmen

Verzeichnis der Verarbeitungstätigkeiten (Art 30)

- Nicht nur Sache der IT
- Alle Abteilungen, Teams miteinbeziehen

- Access-Datenbanken
- Excel-Listen

- Etwa auch Exporte von CRM-Daten (BI-Auswertungen)
- Excel-Liste mit Lohn-Erhöhungen, Prämien
- …

Empfänger der Daten
Beispiele

- Banken
- Rechtsvertreter im Geschäftsfall
- Wirtschaftstreuhänder
- Gerichte im Anlassfall
- Verwaltungsbehörden im Anlassfall
- Fremdfinanzierer (z. B. Leasing)
- Mitwirkende Vertrags- und Geschäftspartner
- Versicherungen im Anlassfall
- Provider (IT-Dienstleister)

Datenpanne (Data Breach, Art. 33, 34)

- Verletzung des Schutzes personenbezogener Daten
- **Meldung binnen 72 Stunden an die Datenschutzbehörde**
- Außer Verletzung des Schutzes führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen
- Bei voraussichtlich hohem Risiko auch Benachrichtigung an die betroffenen Personen
- Dies kann gegebenenfalls auch von Aufsichtsbehörde verlangt werden (falls Ansichten über die Höhe des Risikos auseinandergehen)

Datenpanne: Beispiele

- Hackerangriff Kreditkartendaten werden „abgesaugt“ (z. B. US-Baumarktkette Home Depot 2014, 56 Millionen Kreditkartendaten)
- Ebay Inc 2014, 145 Millionen Datensätze mit E-Mail, Usernamen und Passwort (!!!)
- Seitensprungportal Aslheymadison.com, 32 Millionen Userdaten mit Name, Adresse, Telefonnummer (darunter 32 Mail-Adressen mit gv.at)

- Lohndaten werden exportiert und irrtümlich auf ungeschütztem Verzeichnis im Intranet veröffentlicht
- Mail geht Cc statt Bcc an Teilnehmerliste
- Unverschlüsselter Laptop (auch Handy) liegen gelassen

Datenpanne: Meldung (Art. 33 Abs. 3-5)

- Muster: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.pdf

WIRTSCHAFTSRECHT

WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO):

Data Breach Notification[1]

(Art 33 EU-Datenschutzgrund-Verordnung (DSGVO)) -
Meldung an die Aufsichtsbehörde:
Österreichische Datenschutzbehörde,
Hohenstaufengasse 3, 1010 Wien
E-Mail: dsb@dsb.gv.at

1. Name und Kontaktdaten des Verantwortlichen[2]:

a. Name und Anschrift:

b. E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):

Speicherung in Drittländern (Art. 44 ff) bzw. auch nur Übermittelung

- Grundlage Angemessenheitsbeschluss: Schweiz, Israel, Kanada, Neuseeland, Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Jersey, Uruguay und
- USA: Privacy Shield !? (Max Schrems)
- Großbritannien: wird DSGVO trotz Brexit umsetzen

- Vorliegen geeigneter Garantien
  - Genehmigte verbindliche interne Datenschutzvorschriften
  - Standarddatenschutzklauseln werden befolgt (von Behörde herausgegeben)
  - Genehmigte Verhaltensregeln
  - Genehmigte individuelle Vertragsklauseln

Speicherung in Drittländern (Art. 44 ff) bzw. auch nur Übermittelung

- **Ausdrückliche Einwilligung**
- **Erforderlich für die Erfüllung eines Vertrages**
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Lebenswichtiger Interessen
- Wichtige Gründe des öffentlichen Interesses

- Todo:
  - Datenflüsse in Ihrem Unternehmen untersuchen
  - Gibt es etwas im EU-Ausland (Konzernmutter, -Tochter, Dienstleister, …)

Datenschutz durch Technik (Art 25 Abs 1)

- Privacy by Design
- Sowohl bei Festlegung der Mittel
- als auch bei der Verarbeitung selbst, müssen
- technische und organisatorische Maßnahmen getroffen werden,
- um die Datenschutzprinzipien (Art 5 DSGVO, z. B. die Datenminimierungspflicht) effektiv zu implementieren,
- um die Anforderungen der DSGVO zu erfüllen.

Maßnahmen müssen dem Stand der Technik entsprechen und wirtschaftlich vertretbar sein und im Verhältnis zu Art, Zweck, Umfang und Kontext der Verarbeitung und den Risiken für die Privatsphäre der Betroffenen stehen.

Datenschutz durch Technik (Art 25 Abs 1) Typische Beispiele

- keine Abfrage der SV-Nummer bei Bewerbung
- Kreditkartendaten verschlüsselt speichern
- Passwörter verschlüsselt speichern
- Exportmöglichkeiten reduzieren bzw. verhindern
- entsprechende Berechtigungskonzepte
- https statt http
- automatisches Session-Timeout erzwingen
- Gesichter aus Bildern ausschneiden
- Aktuelle Patches/Updates einspielen
- Virenscanner

Datenschutzbeauftragter Notwendigkeit (Art. 37)

- Behörde oder öffentliche Stelle (z. B. Gebietskörperschaften)
- Kerntätigkeit macht eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich
- Kerntätigkeit liegt in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder Daten über strafrechtliche Verurteilungen
- Schriftlich dokumentieren warum nicht!
- Dennoch Vorteil bei Strafverfahren
- International könnte es strenger sein! (D)

Datenschutzbeauftragter Aufgaben (Art. 39)

- Beratung des Verantwortlichen bzw. Auftraggebers
- Schulung der Beschäftigten
- Überwachung der Einhaltung der Vorschriften
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für Fragen

- Keine „Strafabwälzung“
- Bei schuldhafter Pflichtverletzung aber zivilrechtlich Haftung möglich

Datenschutzbeauftragter Stellung (Art. 38)

- Frühzeitig einbinden
- Erforderliche Ressourcen müssen ihm zur Verfügung gestellt werden
- Weisungsfrei bei Erfüllung seiner Aufgaben
- Weitreichender Kündigungsschutz
- Bericht direkt an Geschäftsführung
- Betroffene Personen können ihn direkt kontaktieren
- An Wahrung der Geheimhaltung und Vertraulichkeit gebunden
- Kann weitere Aufgaben haben, sofern kein Interessenskonflikt

Was darf Datenschutzbehörde? (Art. 58) Untersuchungsbefugnisse (DSG § 22)

- Kündigen sich an
- Einsicht in alle Unterlagen
- Räume betreten, Anlagen in Betrieb setzen, Sicherungen erstellen
- Unter möglichster Schonung des Verantwortlichen
- Verschwiegenheitspflicht, ausschließlich zur Kontrolle datenschutzrechtlicher Vorschriften
- ABER: Anzeigepflicht falls strafbare Handlung mit mehr als 5 Jahren Freiheitsstrafe
- Daneben: Abhilfebefugnisse (verbindliche Anordnungen)
- Beratungs- und Genehmigungsbefugnisse

Wann ermittelt Datenschutzbehörde?

- Grundsätzlich immer möglich
- Allerdings sicher zu wenig Personal
- Beschwerde (da müssen sie!!)

- Schwerpunktverfahren (z. B. Kreditinstitute, Personenversicherer)

To-do-Liste

- Unterstützung notwendig, Verantwortlichen festlegen
- Welche Daten verarbeiten Sie?
- Verzeichnis der Verarbeitungstätigkeiten
  - Welche Anwendungen
  - Welche Zwecke
  - Rechtsgrundlagen
  - Sensible Daten?
  - Werden Kinder angesprochen?
  - Liegt Profiling vor?
- Wird mit Auftragsverarbeitern zusammengearbeitet (Muster: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html)
- Informationspflicht erfüllen
- Durchgehen Verträge, AGBs, Webseiten

To-do-Liste

- Entscheidung Datenschutzbeauftragter dokumentieren
- Unabhängig ob ja oder nein: Verantwortlichen bestimmen
- Datenverkehr mit EU-Ausland?
- Umsetzung angemessener Sicherheitsmaßnahmen
- Verbesserung der Datenschutzfreundlichkeit
- Verschwiegenheitserklärung
- Dokumentation von Mitarbeiterschulungen
- Protokollierungen beachten, Exportmöglichkeiten
- Rechte der Betroffenen: Vorbereitungen treffen

- JETZT ANFANGEN! OHNEHIN SCHON SEHR SPÄT
- Laufend darauf sehen!

To-do Verschwiegenheitserklärung

- Sollte jede/r Mitarbeiter/in unterschreiben
- Siehe DSG (2018) § 6 bzw. Art. 29 DSGVO
- Mitarbeiter/innen sind zu verpflichten

- Einfachste Form: einfach eine Kopie des § 6 DSG (in der Fassung von 2018) unterschreiben lassen