Die DSVGO kommt und Jetzt??

TOTZAUER MATTHIAS – IT CONSULTING TOTZAUER

MAIL: M.TOTZAUER@ITCST.DE

PHONE: +491625922574

Wie‘s so aussieht …

25. Mai 2018

~~BDSG~~

DSGVO ✓
EU-Recht

BDSG (neu) ✓
Nationales Recht

Übergangsfrist?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Grundlagen

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Was will die DSGVO?

- Verbraucherschutz
- Europaweite Vereinheitlichung des Datenschutzes
- Anpassung an die Herausforderungen der Digitalisierung
- technikneutrale Ausgestaltung
- Management in die Haftung nehmen
- Wirksame Strafen

- Ziel: Google, Facebook, Amazon & Co.

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Und was heißt das genau?

- **Anpassungsbedarf notwendig!**
- - bis zum Eintritt der DSGVO 25. Mai 2018 umstellen

- Grundsätzlich sind viele Einflüsse des BDSG in der DSGVO eingearbeitet

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Verantwortung!

- **Verantwortlicher**
- Primärverantwortung: Management & Leitung
- Kein Konzernprivileg: Einzelverantwortung natürlicher oder juristischer Person

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Daten mit Personenbezug

- **Neu:**
- „identifizierbar“ anstatt „bestimmbar“
- Berücksichtigung technischer Methoden zur Identifizierbarkeit
- Erweiterung „Besonderer personenbezogener Daten“ um genetische und biometrische Informationen

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Grundsätze der Datenverarbeitung

- **Art. 5 DSGVO Abs. 1**
  - Rechtmäßigkeit, Treu & Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - **Richtigkeit**
  - Speicherbegrenzung
  - Integrität & Vertraulichkeit

- **Abs. 2**
  - **Rechenschatspflicht des Verantwortlichen**

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Rechte der Betroffenen (zwingend)

- Aufklärung (umfassende Informationspflichten) Art. 12ff
- Auskunft (sehr umfassende Auskunftspflicht) Art. 15, **Recht auf Erhalt einer Kopie der Daten**
- Widerspruchsrecht Art. 21
- Berichtigung Art. 16
- Löschung Art. 17, Vergessenwerden Art. 17 Abs. 2
- Einschränkung Art. 18
- **Recht auf Datenübertragbarkeit** Art. 20
- Anrufung Datenschutzbehörde Art. 77
- Recht auf Rechtsbehelf Art. 79
- Schadenersatz Art. 82

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Verbot mit Erlaubnisvorbehalt

- **Verarbeitung nur rechtmäßig, wenn … (Art. 6 1ff)**
  - Vertragsdurchführung „… soweit erforderlich“ (Abs. 1b)
  - Interessenabwägung (Abs. 1f)
    Berechtigte Interessen vs. Schutzwürdigkeit der Person
  - Einwilligungserklärung

- **Noch unklar:**
  - Allgemein verfügbare Daten
  - Postalische Werbung

- **Arbeitsverhältnisse:**
  - Bleiben nationales Recht (beeinflusst von DSGVO)

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Relevante Vorgänge

- **BDSG Bisher**

- Erheben, Verarbeiten (speichern, ändern, übermitteln, sperren, löschen), Nutzen

- **DSGVO Neu:**

- *Verarbeiten*
  Erheben, Erfassen, Organisation, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen, Vernichten

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Schutz der Daten

- **Bisher**
- TOM („8 Gebote“: Zutritt, Zugang, Zugriff, Weitergabe, Eingabe, Auftrag, Verfügbarkeit, Trennung)

- **Neu:**
- Annäherung an Vorgehen der Informationssicherheit ISO 27002 Vertraulichkeit, Integrität, Verfügbarkeit

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Schutz der Daten

- **Umsetzung: Risikobasierter Ansatz**
  - Orientierung am Risiko der Verarbeitung
    => Datenschutzfolgeabschätzung (Branchen / Daten noch nicht klar definiert)
  - Rechenschaftspflicht: Beweislast beim Unternehmen

- **Verstöße**
  - Abstrakt bußgeldbewährt (unabhängig vom Eintritt eines Schadens)
  - Bis zu 10 Mio. € oder 2% weltweiter Jahresumsatz

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Typische Datenschutz-verletzungen

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Bitte unterscheiden …

- Datensicherheit
- Datensicherung
- **Datenschutz**

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Typische Schwachstellen?

- Papierentsorgung & Abfalleimer
- USB-Sticks, Speicherkarten & Datenträger
- Mobile Endgeräte
- Kommunikation & eMail
- Datensicherung & Datensicherheit
- Rechtesystem

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Fehler

- Zugang zu Betriebsräumen
- Aussagen am Telefon
- Offener Umgang mit vertraulichen Unterlagen
- Datenschutz nur im Büro (vs. Reise, HomeOffice, …)
- Schwache Passwörter & Weitergabe
- Schlecht gewartete Hard- und Software

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Angriffszenarien

- Intern (Social Hacking, Datenklau, ... > 90% aller Fälle!)
- Trojaner, Phishing, Viren, Erpressung
- Zero-Day-Exploits
- Automatisierte Angriffe / Hardware-Fehler
- Reputation
- Distributed Denial of Service (DDoS)

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Wie gehe ich nun korrekt mit meinen Daten um?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Regelkonforme Datenverarbeitung

- Gibt es ein Gesetz?
- Habe ich eine Einwilligung (zweckgebunden!)?
- Wer erhält sonst Zugriff auf meine Daten:
  gibt es eine Auftragsdatenverarbeitung?

- Zu beachten:
- Ist die Einwilligung DSGVO-konform?
- Kenne ich die Löschfristen?
- Ist das Verfahren dokumentiert?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Einwilligungserklärung (nach DSGVO)

- Eindeutig bestätigende Handlung (ErwäGr Art. 32)
- Nachweisbarkeitspflicht (Art. 7 Abs. 1)
- Transparenzpflicht / Informiertheit (Art. 7 Abs. 2)
- Hervorhebungsgebot
- Rechtmäßigkeitspflicht
- Treu & Glauben
- Jederzeit widerrufbar (Art. 7 Abs. 3)
- Freiwilligkeit (ErwäGr Art. 42)
- Sonderregelung für Einwilligung von Kindern (Art. 8)

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Auftragsdatenverarbeitung (ADV)

- Übertragung von kompletten Funktionen (weisungsgebunden!)
- Keine Minderung des Datenschutzniveaus
- **Keine zusätzliche Rechtsgrundlage** (da keine „Übermittlung“)
- Verantwortung hat Auftraggeber
- aber: **Gesamtschuldnerschaft** mit Auftragnehmer! (Soweit nicht voller Entlastungsbeweis)

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Drittlandtransfer

- Zweistufige Prüfung
  Rechtsgrundlage?
  Angemessenes Datenschutzniveau
- Bisher anerkannt durch EU:
  Andorra, Argentinien, Faröer Inseln, Guernsey, Isreal, Isle of Man, Kanada, Neuseeland, Schweiz, Uruguay
- Sonst:
  Akzeptanz der EU-Standardvertragsklauseln
  Verbindliche Unternehmensrichtlinien
  Privacy Shield?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Datenschutzbeauftragter

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Brauche ich einen Datenschutzbeauftragten?

- Automatisierte Verarbeitung personenbezogener Daten
- Mehr als 9 Personen (auch Azubi, Teilzeit, ...)
- Mehr als 20 Personen
- Bei Verarbeitung besonderer personenbezogener Daten
- Bei Verfahren, die einer besonderen Risikofolgeabschätzung bedürfen

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Datenschutzbeauftragter

- Europaweite Pflicht zur Bestellung eines DSBA
  Wettbewerbsvorteil in D, da keine wesentlichen Änderungen
- Stärkere Betonung der Beratungsfunktion, klare Abgrenzung zu den Verantwortlichen
- Voraussetzung DSBA
  berufliche und fachliche Qualifikation Art. 37 Abs. 5
  kein Interessenskonflikt

- Ansonsten weitgehend in Übereinstimmung mit BDSG

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Ohne Datenschutzbeauftragter

- Ordnungswidrigkeit bis 50.000 €
- Meldepflicht bei Aufsichtsbehörde für alle Verfahren der automatisierten Datenverarbeitung personenbezogener Daten
- Haftungsgefahr Management
  Persönliche Haftung wg. Verstoß Sorgfaltspflicht (HGB)
  Ordnungswidrigkeit (OWiG §130 bis zu 1 Mio. €)
- Ansonsten:
  Abmahnungen
  Auskunfts-/Schadenersatzansprüche
  Reputations-/Kundenverlust

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Konsequenz Datenschutzverstöße

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

… und wenn‘s ganz schlimm kommt

- **Art. 83 DSGVO: Ahndungspflicht!**
  10 Mio. € oder 2% weltweiter Jahresumsatz
  - Bestimmung bei Einwilligung von Kindern missachtet
  - Einsatz datenschutzunfreundlicher Technologie
  - Hinderung des DSBA bei Ausführung seiner Tätigkeit

- 20 Mio. € oder 4% weltweiter Jahresumsatz
  - Datenschutz-/Rechenschaftsgrundsätze verletzt
  - Datenverarbeitung ohne Rechtsgrundlage
  - Missachtung Voraussetzungen für Einwilligung
  - Missachtung Betroffenerechte

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

IHRE - Pflichten

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Pflichten des Managements nach DSGVO

- Datenschutzleitlinien erstellen
- Datenschutz-Management-System installieren
- Technische und organisatorische Maßnahmen ergreifen
- Privacy-by-design, Privacy-by-default
- Zusammenarbeit mit Aufsichtsbehörden
- Meldeverfahren installieren
- Mitarbeiter schulen
- Regelmäßige Bewertung und Überprüfung der Maßnahmen
- Dokumentation

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Und jetzt . .. .??

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Handlungsempfehlungen!

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Wo stehe ich denn momenetan?

Ist-Stand kennen!

- Datenschutzanalyse
- Datenschutzkette prüfen: wo sind und wer arbeitet mit meinen Daten?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Wo sind und wohin fließen meine Daten?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Wohin will ich mit meinem Unternehmen?

- Datenschutzniveau definieren: was will ich umsetzen? Wieviel benötige ich / will ich mir leisten? Welches Risiko bin ich bereit einzugehen? Betriebswirtschaftliche Betrachtung?
- Soll-Konzept erarbeiten
- Bedarf Datenschutzbeauftragter feststellen

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Was sollte ich unbedingt tun?

Dokumente prüfen!

- **Außenwirkung!**
- Impressum
- Datenschutzhinweise
- Verträge mit personenbezogenen Daten & Datenschutzerklärungen
- ADV
- Mitarbeiterverträge
- Datenschutzordner

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

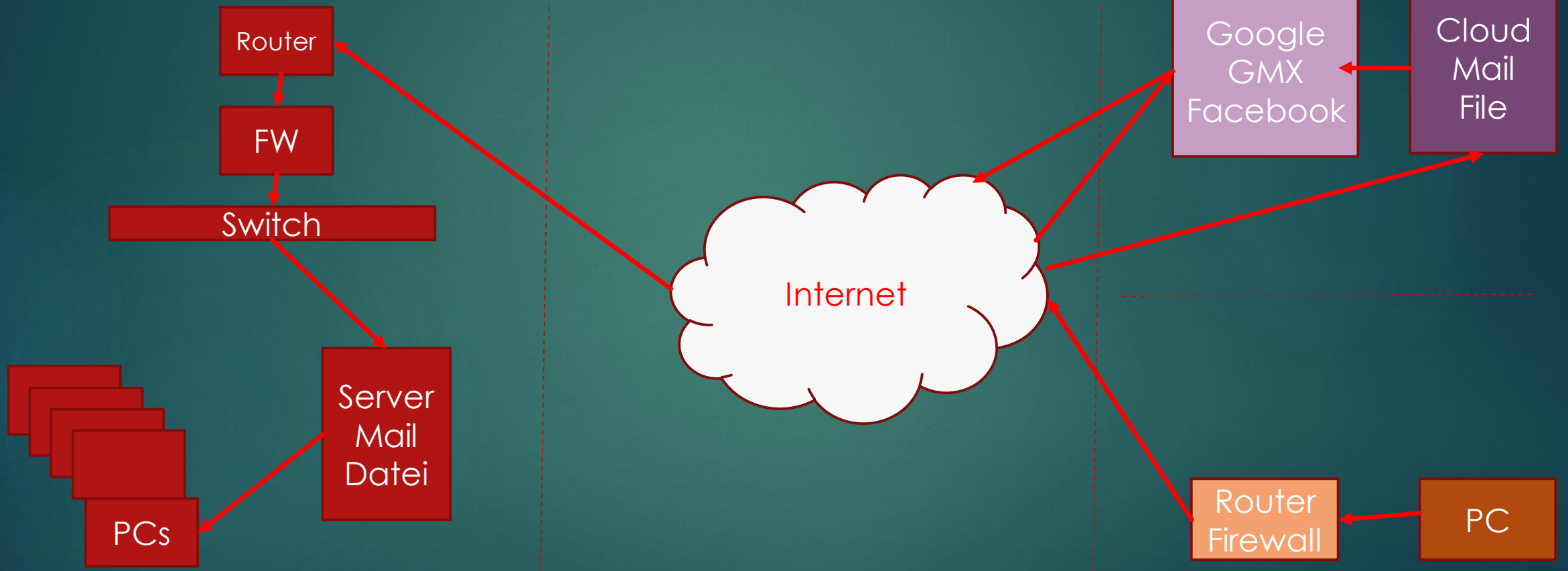
Was sollte ich unbedingt tun?

Technik prüfen!

- IT, EDV
- Externe Zugänge, VPN, Verschlüsselungen
- CRM, Dokumentenmanagement, Buchhaltung, HR
- Kommunikation: Telefon, eMail, Messenger
- Büro- und Ablauforganisation
- Papier: Druck & Entsorgung
- …

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Technik



Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Was muss ich tun?

- Handlungsanweisungen & Notfallpläne erstellen
- Organisation anpassen
- Mitarbeiter schulen

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Was muss ich dann noch tun

- Dokumentations- und Meldeverfahren installieren
- Entscheidungen dokumentieren
- Verfahren kontrollieren und justieren

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Und wenn nicht?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Eigentlich ist mir die DSGVO ziemlich egal …

Konsequenzen

- Verpflichtung der Produktgeber auf DSGVO
- Nachfrage der Kunden nach Datenschutz
- Imageschaden & Reputationsverlust
- Anhaltslose Prüfungen durch LDA
- Anonyme Anzeigen von Mitbewerbern
- Bestandswertverringerung
- Zunehmendes juristisches Risiko
- Strafbewehrte Verstöße nach DSGVO

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

OK, ist mir aber alles zu viel Aufwand und alles zu teuer …

Risikomanagement

- Betriebswirtschaftlichen Nutzen erkennen
- Große Risiken vermeiden
- Kleine Risiken akzeptieren

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Alles nur Admin Zeug‘s?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Chancen: es ist nicht alles schlecht …

Aufwand

DSGVO: Umsetzung

Risikomanagement

Anwälte fragen

Techniker fragen

Mitarbeiter schulen

Und sonst?

Nutzen

Arbeitsabläufe optimieren

Schlüsselprozesse kennen

Sicherheit gewinnen

IT optimieren

Qualifikation

Wettbewerbsvorteil

Bestandswert

Kundenzufriedenheit

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574

Sind Sie Fit für die DSGVO?

Totzauer Matthias – IT Consulting Totzauer
MAIL: m.totzauer@itcst.de
Phone: +491625922574