TIME IS RUNNING OUT

Was Sie in den letzten Monaten noch retten können und wie ein Notfallplan zur DSGVO-Compliance aussehen kann

15.2.2018

Nino Tlapak

DORDA

WIR SCHAFFEN KLARHEIT.

Ansprechpartner

Mag Nino Tlapak, LL.M.

- Rechtsanwalt bei DORDA
- Universität Wien, Mag iur 2012
- Universität Wien, Universitätslehrgang Medien- und Informationsrecht, LL.M. (IT-Law) 2013
- Fachliche Schwerpunkte: Datenschutzrecht, IT-Recht, E-Commerce, Outsourcing, Urheber- und Medienrecht
- Autor von Fachpublikationen im Bereich Datenschutz und E-Commerce
- Vortragender für E-Commerce Recht und Social Media bei der Werbe Akademie des WIFI Wien
- Vortragender für Datenschutzrecht beim Master-Lehrgang "Digital Business" an der FH Technikum Wien
- Mitglied der Interessensgemeinschaften "www.it-law.at" und "Privacyofficers.at"

Agenda

I. Status Quo

II. Die 10 wichtigsten To Dos in der Praxis

III. Umsetzung der DSGVO im Unternehmen

IV. Notfallplan bis Mai 2018

I. Status Quo

- DSGVO und DSG Neu ab 25.5.2018 (über Nacht) anwendbar
  - bis dahin Prozesse umstellen, um Compliance sicherzustellen
  - umfangreiche neue Pflichten für Verantwortliche und Auftragsverarbeiter
  - erhöhtes Strafmaß (DSB darf Geldbußen verhängen)
- Umsetzung braucht Zeit und bindet Ressourcen
- einige Punkte weiterhin unklar → Risiko abwägen und Begründung dokumentieren
  - Umfang und Detaillierungsgrad der Dokumentation und der Datenschutz-Folgenabschätzung?
  - bestehende Einwilligungen weiterhin gültig?
  - Einwilligung über AGB weiter möglich?

I. Status Quo

Zeitleiste bis zum Stichtag 25.5.2018

II. Die 10 wichtigsten To Dos in der Praxis

1. Erstellung **Dokumentation** der Verarbeitungsvorgänge
2. Durchführung **Datenschutz-Folgenabschätzungen**
3. Vorbereitung Muster zur **Meldung** etwaiger Verstöße
4. Überarbeitung bestehender Verträge mit **Auftragsverarbeitern**
5. Anpassung **Einwilligungserklärungen**
6. Erfüllung neuer **Informationspflichten** und Sicherstellung **Betroffenenrechte**
7. Bestehende **Sicherheitsmaßnahmen** anpassen
8. Bestellung **Datenschutzbeauftragter**
9. Überarbeitung interner **Policies**
10. Durchführung erforderlicher **Schulungen**

III. Umsetzung der DSGVO im Unternehmen

1. Datenerhebung

- Zusammentragung bestehender Dokumentation (Meldungen, Genehmigungen, Dienstleistungsvereinbarungen, Zustimmungserklärungen, Betriebsvereinbarungen, Datenschutzerklärung, Cookie Policy, AGB etc)
- Erhebung des Ist-Standes

2. Gapanalyse

- Identifizierung erforderlicher Maßnahmen auf Basis der Datenerhebung

3. Umsetzungsmaßnahmen

- Erstellung Verzeichnis von Verarbeitungstätigkeiten
- Erstellung PIA für sensible Verarbeitungen
- Weitere Umsetzungsschritte (soweit möglich parallel)

III. Umsetzung der DSGVO im Unternehmen

- Paradebeispiel: Zuerst umfassende Erhebung und Analyse, dann Umsetzung der erforderlichen Maßnahmen
- ABER: **Allumfassendes Großprojekt** bis Mai 2018 ohne entsprechende Vorarbeit **kaum mehr umsetzbar!**
- Daher **Priorisierung** erforderlich: Schwerpunkte setzen, um kritische Systeme vorzuziehen und Haftungsrisiko zu minimieren

Notfallplan

- ➔ Sensible Verarbeitungen priorisieren!
- ➔ Alle anderen Verarbeitungen: Umsetzungsmaßnahmen priorisieren und richtige Schwerpunkte setzen.

IV. Notfallplan bis Mai 2018

Phase I: Projektstart

1. Bestimmung der **Projektverantwortlichen**
   - zB geleitet von IT, Recht oder Compliance Abteilung
   - Ansprechpartner in allen Abteilungen sinnvoll
2. Prüfung, ob **Datenschutzbeauftragter** erforderlich
   - falls ja, gleich mit einbeziehen
   - Datenschutzbeauftragten bis 25.5.2018 an Datenschutzbehörde melden!
3. Benötigte **externe Unterstützung** (insb IT und Recht) sichern
4. **Budget** definieren
5. **Timeline** festlegen (klare Deadline für priorisierte Bereiche: 25.5.2018; Rest realistisch asap)

IV. Notfallplan bis Mai 2018

Phase II: Identifikation sensibler Verarbeitungen

- Verarbeitung mit **voraussichtlich hohem Risiko** für die Betroffenen?
  - Bewertung auf Basis automatisierter Entscheidungen (Profiling)
  - umfangreiche Verarbeitung strafrechtlicher Daten
  - systematische Überwachung
- Verarbeitung **sensibler** (besonderer Kategorien personenbezogener) Daten?
- Verarbeitung in einem geschäftskritischen Bereich (businessrelevante Anwendung)?

IV. Notfallplan bis Mai 2018

Phase III: Umsetzung bei sensiblen Verarbeitungen

1. **Erhebung und Analyse** der Verarbeitungstätigkeiten
   - Welche Daten werden zu welchem Zweck verarbeitet?
   - Rechtsgrundlage?
   - Verhältnismäßigkeit/Datensparsamkeit?
2. Prüfung der erforderlichen **Umsetzungsmaßnahmen**
   - Etwaige Einwilligungserklärung?
   - Zusätzliche Sicherheitsmaßnahmen?
   - Datenschutz-Folgenabschätzung?
3. **Umsetzung** diverser Maßnahmen jedenfalls noch bis Mai 2018

IV. Notfallplan bis Mai 2018

Phase IV: Umsetzung bei anderen Verarbeitungen

1. Überarbeitung bestehender **Einwilligungserklärungen**
   - Text der Erklärung gegebenenfalls präzisieren (Rechtsprechung streng!)
   - Keine zukünftige Einholung innerhalb von AGB
   - Getrennte Checkbox für jede Verarbeitungstätigkeit
   - Eventuell Anpassung bestehender **Marketingabläufe**
     - Newsletter nur mit vorheriger Einwilligung versenden
     - Kein Cold Calling
2. Abschluss DSGVO-konformer **Auftragsverarbeiter-vereinbarungen**
   - Bestehende Muster anpassen
   - Abschluss mit neuen und als auch mit bestehenden Dienstleistern!

IV. Notfallplan bis Mai 2018

Phase IV: Umsetzung bei anderen Verarbeitungen

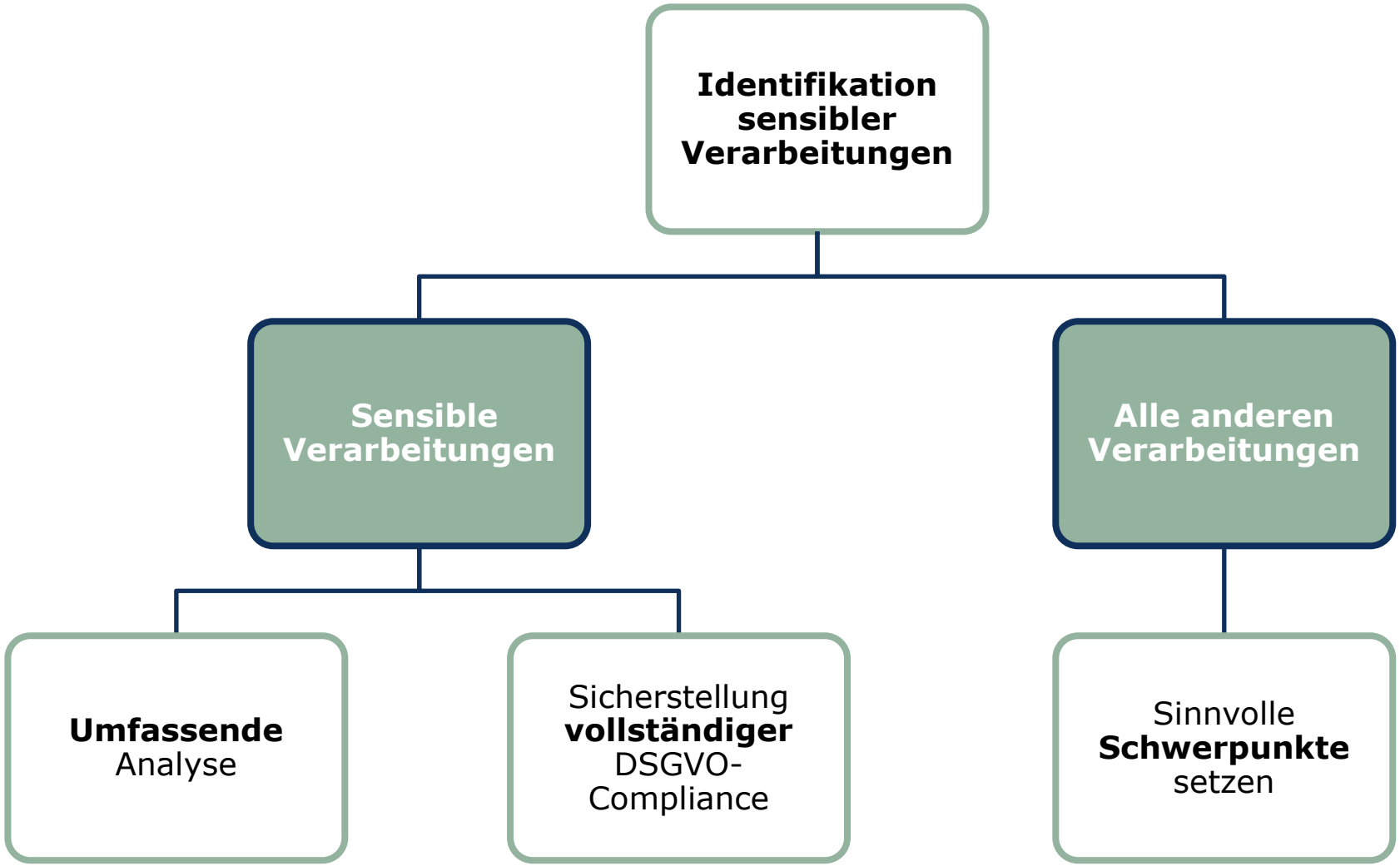
3. Implementierung der **Informationspflichten**
   - Anpassung bestehender Privacy Policies, Cookie Policies, Datenschutzerklärungen und Betriebsvereinbarungen
   - Gleichzeitig: Prüfung und gegebenenfalls Anpassung Cookie-Einwilligung (sicherste Lösung: Banner auf der Startseite)
4. Sicherstellung **Betroffenenrechte**
   - Verantwortlichkeit definieren
   - Prozess aufsetzen, damit insb Recht auf Auskunft und Recht auf Löschung fristgerecht gewahrt werden können
5. Daten**sicherheitsmaßnahmen** setzen
   - Privacy by design/by default
   - Eventuell mit externem IT Berater
6. Für den Ernstfall: **Meldung** an Datenschutzbehörde vorbereiten

IV. Notfallplan bis Mai 2018

Phase IV: Umsetzung bei anderen Verarbeitungen

7. Erstellung **Verzeichnis der Verarbeitungstätigkeiten**
   - Auf Basis bestehender DVR-Meldungen
   - Ergänzen um umfassende Ist-Stand-Analyse
8. Gegebenenfalls **Datenschutz-Folgenabschätzung**
9. Überarbeitung **interner Policies**
   - IT Policy
   - Mitarbeiter Datenschutz Policy
   - Betriebsvereinbarung
10. Mitarbeiter**schulung**

IV. Notfallplan bis Mai 2018



IV. Notfallplan bis Mai 2018

Fazit

- Vollständige Datenerhebung praktisch kaum realisierbar!
- Notfallplan reduziert Haftungsrisiko faktisch
  - in der Praxis kommt Priorisierung daher große Bedeutung zu
  - für den konkreten Einzelfall zu optminieren
- WICHTIG: Auch nach Mai 2018 laufend Compliance sicherstellen
  - Nachziehen offener Punkte
  - Dokumentation aktualisieren
  - PIA anpassen
  - Datensicherheitsmaßnahmen am Stand der Technik
  - tourliche Prüfung und Anpassung an Letztstand der Rechtsprechung

Kontakt

Dr Axel Anderl, LLM
T: +43 1 533 47 95 – 23
E: axel.anderl@dorda.at

MMag Dr Felix Hörlsberger
T: +43 1 533 47 95 – 17
E: felix.hoerlsberger@dorda.at

Mag Nino Tlapak, LLM
T: +43 1 533 47 95 – 23
E: nino.tlapak@dorda.at

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien

International Law Office - Information Technology Award for Austria 2014, 2015, 2016, 2017 & 2018
International Law Office - E-Commerce Award for Austria 2012 & 2013
JUVE - Austrian Law Firm of the Year 2017