BvD e.V.
DATENSCHUTZ GESTALTEN


# Art. 32 DS-GVO Sicherheit der Verarbeitung - Im Spannungsverhältnis zwischen Pflicht und Zulässigkeit

Referenten: Dr. Jens Eckhardt, Regina Mühlich

Online, 03.11.2021

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

AdOrga Solutions

# Copyright

Diese Seminarunterlage und darin enthaltende Vorlagen und Dokumente sind urheberrechtlich geschütztes Eigentum. Jede Verwertung, auch auszugsweise, außerhalb der engen Grenzen des Urhebergesetzes ist ohne schriftliche Zustimmung der Autorin unzulässig und strafbar.

Dies gilt insbesondere für die Vervielfältigung, Verarbeitung und Verwendung für Vorträge.

Regina Mühlich, Jens Eckhardt
München / Düsseldorf

# Agenda

1 Grundsätze

2 Sicherheit der Verarbeitung

3 Rechtliche Voraussetzungen

4 Praktische Umsetzung

5 Fragen

# 1 Grundsätze

# Grundsätze

## DS-GVO – Verbotsgesetz mit Erlaubnisvorbehalt

Voraussetzung:

Vorhandensein einer ausreichenden und tragfähigen Rechtsgrundlage und
die Gewährleistung der Sicherheit der Datenverarbeitung.

Es gelten:

- Art. 5 DS-GVO Verarbeitungsgrundsätze
- Art. 6 DS-GVO Rechtmäßigkeit der Verarbeitung

anschließend

Datenverarbeitung minimiert (Art. 25 Abs. 2 DS-GVO) und
geeignete Maßnahmen zur Eindämmung des Risikos (Artt. 25 Abs. 1 und 32 Abs. 1 DS-GVO)

**Die Auswahl geeigneter Maßnahmen ist abhängig von den Risiken.**

# Grundsätze

## Artikel 24 DS-GVO

**Art. 24 DS-GVO Verantwortung des für die Verarbeitung Verantwortlichen**

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfang, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten **natürlicher Personen geeignete technische und organisatorische Maßnahmen** um, um sicherzustellen und den **Nachweis dafür erbringen zu können**, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Abs. 1 die **Anwendung geeigneter Datenschutzvorkehrungen** durch den Verantwortlichen umfassen.

**(3) Die Einhaltung […], um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.**

# Grundsätze

## Artikel 32 DS-GVO

- Art. 32 DS-GVO richtet sich sowohl an den Verantwortlichen als auch an Auftragsverarbeiter und beinhaltet die Pflicht, durch geeignete technische und organisatorische Maßnahmen ein **angemessenes Schutzniveau** bzgl. der Verarbeitung zu gewährleisten.
- Dabei werden von Art. 32 Abs. 1 lit. a - d DS-GVO Maßnahmen benannt, die eingeschlossen werden müssen.

- Entsprechend Art. 5 Abs. 2 DS-GVO besteht natürlich eine **allgemeine Nachweisverpflichtung** bzgl. der Einhaltung der Vorgaben des Verantwortlichen.

- Aber Art. 32 Abs. 3 DS-GVO verlangt selbst auch den **Nachweis bzgl. der Einhaltung** bzw. der Erfüllung seiner Vorgaben, und dies gilt sowohl für den Verantwortlichen wie auch – sofern vorhanden – für Auftragsverarbeiter.[1]

[1] Schreibauer M, Spittka J. Art. 32 Rn. 19 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft.

# Grundsätze

## Artikel 32 DS-GVO

**Schutzziele:**

- An erster Stelle steht die Forderung ein **angemessenes Schutzniveau** hinsichtlich des **Risikos** für die Rechte und Freiheiten natürlicher Personen zu gewährleisten.

Hieraus abgeleitet resultiert die Forderung, dass

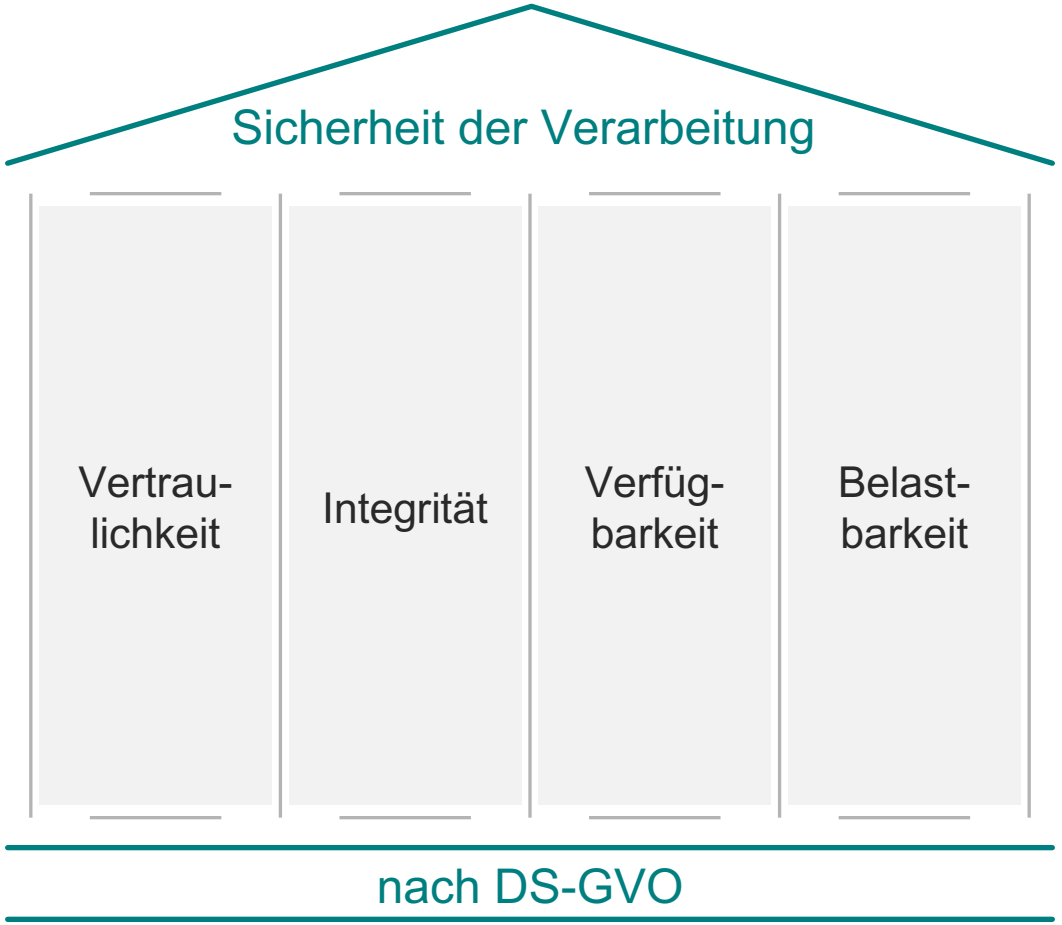
- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und
- Belastbarkeit

für Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten auf Dauer sicherzustellen ist.

# 2 Sicherheit der Verarbeitung

# Wer ist eigentlich TOM …?

## IT-Schutzziele




Quelle: © 2021 Regina Mühlich

# Sicherheit der Verarbeitung

## Privacy by Design and by Default (Art. 25, ErwG 78)

Die DSGVO spricht in Artikel 25 von

“**Datenschutz durch Technikgestaltung**”

und

“**Datenschutz durch datenschutzfreundliche Voreinstellungen**”.

Der Datenschutz durch Technikgestaltung wird in Absatz 1 folgendermaßen definiert:

*“Unter Berücksichtigung […] der unterschiedlichen **Eintrittswahrscheinlichkeit** und Schwere der mit der Verarbeitung verbundenen **Risiken** für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** […], die dafür ausgelegt sind, die Datenschutzgrundsätze […] wirksam umzusetzen […], um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.”*

# 3 Rechtliche Voraussetzungen

# Rechtliche Voraussetzungen

## Rechtsgrundlage der Verarbeitung der Daten

***Ausgangspunkt:***

***Art. 32 DS-GVO ist keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten***

- **Erforderlichkeit einer Rechtsgrundlage?!**
  - Verarbeitung personenbezogener Daten
  - Verbot mit Erlaubnisvorbehalt und Zweckbindung

- **„Flankierende“ Regelungen, insbesondere:**
  - Grundsätze des Art. 5 DS-GVO (v.a. Datenminimierung und Speicherbegrenzung)
  - Betroffenenrechte, insbesondere proaktive Unterrichtung nach Artt. 12, 13, 14 DS-GVO
  - Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)
  - Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)

# Rechtliche Voraussetzungen

## Rechtsgrundlage der Verarbeitung der Daten

***Schlagwort: „Der Zweck“ bestimmt die Rechtsgrundlage!***

- **Verarbeitung zur Erreichung der „Sicherheit der Verarbeitung“**
  - Primärzweck oder Sekundärzweck („zweckändernde Weiterverarbeitung“, Art. 6 Abs. 4 DS-GVO)
  - Abgrenzung?!
- **Abgrenzung zum Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) und TKG**

- **Rechtsgrundlage zur Umsetzung des Art. 32 DS-GVO**
  - Art. 6 Abs. 1 Satz 1 lit. c DS-GVO (Erfüllung einer gesetzlichen Pflicht)
  - Art. 6 Abs. 1 Satz 1 lit. a DS-GVO (Einwilligung) (ggf. plus Art. 9 DS-GVO)
  - Art. 6 Abs. 1 Satz 1 lit. b DS-GVO (Vertragserfüllung) (ggf. plus Art. 9 DS-GVO)
  - Sonderfall: § 26 Abs. 2 Satz 1 BDSG (Sperrwirkung gegenüber Art. 6 Abs. 1 Satz 1 lit. f DS-GVO?)
  - Art. 6 Abs. 1 Satz 1 lit. f, Abs. 4 DS-GVO (Interessenabwägung)

# Rechtliche Rahmenbedingungen

## Das Spannungsverhältnis

***Schlagwort: Der Zweck heiligt nicht die Mittel!***

- **Im Ergebnis: keine Zulässigkeit ohne Verhältnismäßigkeitsprüfung bzw. Interessenabwägung**

Ausgangspunkt: Berechtigtes Interesse (Art. 32 DS-GVO, ErwGr. 47, 49 DS-GVO) als Ziel

➔ Geeignet des Mittels zur Zielerreichung

➔ Mildestes Mittel zur Zielerreichung

➔ Angemessenheit des Mittels zur Zielerreichung (Verhältnismäßigkeit i.e.S.)

**Contra:**
- Art der Daten
- Quantität der Daten
- Art der Verarbeitung
- Missbrauchsrisiko
- Missbrauchsanfälligkeit
- Unzureichende Sicherheit der Verarbeitung
- …

**Pro:**
- Transparenz gegenüber den betr. Personen
- (objektive) Erwartungshaltung der betroffenen Personen
- Pseudonymität
- Datenminimierung, Speicherbegrenzung, …
- Sicherheit der Verarbeitung
- …

# Rechtliche Konsequenzen

***Schlagwort: Kein „Im Zweifel für die Sicherheit der Verarbeitung“?***

- **Unzureichende Sicherheit der Verarbeitung nach Art. 32 DS-GVO**
  - **Auf den ersten Blick**
    - Geldbuße nach Art. 84 Abs. 4 DS-GVO („kleines Bußgeld“)
    - Bei weitere Voraussetzungen: Melde-/Benachrichtigungspflicht nach Artt. 33, 34 DS-GVO
  - **Auf den zweiten Blick**
    - Art. 82 DS-GVO der betroffenen Personen
    - § 823 BGB und Vertrag der geschädigten Personen
    - Unzulässigkeit der Verarbeitung
    - Behördliche Maßnahmen, insbesondere Untersagung
  - **Auf den dritten Blick:**
    - auch bei Verstößen gegen „flankierende Regelungen“

# Rechtliche Konsequenzen

***Schlagwort: Kein „Im Zweifel für die Sicherheit der Verarbeitung“?***

- **„Überschießende“ Maßnahmen der Sicherheit der Verarbeitung nach Art. 32 DS-GVO**
  - **Auf den ersten Blick**
    - Geldbuße nach Art. 84 Abs. 4 DS-GVO („kleines Bußgeld“)
    - Bei weitere Voraussetzungen: Melde-/Benachrichtigungspflicht nach Artt. 33, 34 DS-GVO
  - **Auf den zweiten Blick**
    - Art. 82 DS-GVO der betroffenen Personen
    - § 823 BGB und Vertrag der geschädigten Personen
    - Unzulässigkeit der Verarbeitung
    - Behördliche Maßnahmen, insbesondere Untersagung

# 4 Praktische Umsetzung

# Praktische Umsetzung

## § 64 BDSG öffentliche Stellen – ein kleiner Tipp aus der Praxis

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

Bildschirmfo

Quelle: https://www.gesetze-im-internet.de/bdsg_2018/__64.html

# Praktische Umsetzung

## Organisation

Mögliche Verfahren:

- Umsetzung des Need-To-Know-Prinzips
- Umsetzung des Minimal-Ansatzes (einschl. Härtung)
- Umsetzung von Logging-, Monitoring-, Reporting- und Response-Management-Systemen
- Umsetzung von Malware-Schutz
- Einsatz von sicheren Backup-Systemen zur Sicherung vor Verlust von Daten
- Mehrfache Auslegung der Systeme zur Umsetzung von Hochverfügbarkeit, etc.
- …
- …

Sinnvoll und „angebracht“ – Art. 32 DS-GVO

# Praktische Umsetzung

## Accountability

### Dokumentation

**Checkliste Zugangskontrolle**

*(es sind Maßnahmen zu treffen die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden k…*

**Technische und organisatorische Maßnahmen:**

- ☐ Server sind gegen unbefugten Zugang geschützt
  - ☐ Bootschutz ☐ Schnittstellenabsicherung ☐ Keine Laufwerke (CD, DVD, USB) …anden
  - ☐ Firewall(s) ☐ Anti-Viren-Software ☐ VPN-Technologie
- ☐ Endgeräte sind gegen unbefugten Zugang geschützt
  - ☐ Bootschutz ☐ Schnittstellenabsicherung ☐ Keine Laufwerke (C… …D, USB) vorhanden
  - ☐ Firewall(s) ☐ Anti-Viren-Software ☐ VPN-Technologie
  - ☐ zentralisierte Mobilgeräteverwaltung mittels Software
- ☐ Per Richtlinie ist verboten, auf Endgeräte / Server eigene b… …geprüfte Dateien aufzuspielen
  - ☐ Laptops eingeschlossen oder mit Kensington-Sch… …esichert ☐ PC-Gehäuse verschlossen
  - ☐ Nutzung und Aufbewahrung mobiler Endger… …urch Richtlinie geregelt
- ☐ Zugangskontrolle mittels Berechtigungen
  - ☐ Benutzer + Passwort ☐ Benutzer + …ware-Authentifikation ☐ Benutzer + Biometrie
- ☐ Zugangsberechtigungen werden indivi… …nach Erfordernis eingerichtet
- ☐ Endgeräte werden mittels Softwar… …egelung (Bildschirmschoner) geschützt
  - Softwareverriegelung wird … …s ☐ Passwort ☐ Biometrie ☐ sonstiges _____ aufgehoben
- ☐ Softwareverriegelung scha… …ch nach _____ Minuten automatisch ein
- ☐ Passwortregelungen f… …ere Passwörter werden maschinell erzwungen
- ☐ Eine Passwortrich… …gibt Auskunft über sichere Passwortmerkmale
- ☐ Datenträger … …bile Datenträger ☐ Smartphones sind verschlüsselt

☐ sonsti… _____

☐ …nstiges: _____

# Praktische Umsetzung

## Accountability

**Art. 24 DS-GVO Verantwortung des für die Verarbeitung Verantwortlichen**

(1) […] S. 2: Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) […] die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung […], um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

**Außerdem - Art. 28 DS-GVO**

*Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die **hinreichend Garantien** dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung **im Einklang mit den Anforderungen** dieser Verordnung erfolgt und den **Schutz der Rechte** der betroffenen Person gewährleistet.*

# Praktische Umsetzung

## Nachweisdokumentation

| | |
|---|---|
| • Logische Mandantentrennung | |
| • Festlegung von Datenbankrechten | entsprechende Anmeldevorgänge, gesonderte Benutzer Log-in<br>siehe Rollen- und Berechtigungskonzepte |
| • Mehrstufiges Berechtigungskonzept für einzelne Nutzer hinsichtlich Eingabe, Änderung und Löschung von Daten in der Benutzeroberfläche | siehe Rollen- und Berechtigungskonzepte |

**2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

**2.1 Weitergabekontrolle**

Wir haben Maßnahmen umgesetzt und implementiert, die eine Weitergabe personenbezogener Daten kontrollieren.

Dies sind folgende Maßnahmen:

| Maßnahmen | Nachweis |
|---|---|
| • Weboberflächen verwenden Verschlüsselung nach Stand der Technik | siehe https-Zertifikat |
| • Sämtliche Mitarbeiter sind auf die Vertraulichkeit und Verschwiegenheit verpflichtet | siehe Vertraulichkeit- und Verschwiegenheitserklärung (Personalakte) |
| • Sämtliche Mitarbeiter sind auf § 88 TKG verpflichtet | siehe Verpflichtungserklärung Fernmeldegeheimnis (Personalakte) |
| • Fristen und Vorgänge zum Löschen von personenbezogenen Daten entsprechen den gesetzlichen Vorgaben und sind vertraglich geregelt | siehe Kunden- und Dienstleister-AVs<br>siehe Lösch- und Aufbewahrungskonzept |

**2.2 Eingabekontrolle**

Wir haben Maßnahmen umgesetzt und implementiert, die die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege gewährleisten.

Dies sind folgende Maßnahmen:

| Maßnahmen | Nachweis |
|---|---|
| • Alle Dateneingaben und -änderungen im ASMC werden protokolliert | siehe Log-in Protokoll ASMC |
| • Organisatorisch können alle Eingaben, Änderungen und Löschvorgänge in einer Übersicht nachvollzogen werden (individuelle Benutzernamen oder automatischen Verarbeitungen vermerkt) | siehe Rollen- und Berechtigungskonzept |
| • Zugriffe erfolgen nutzerspezifisch mit individuellen und passwortgeschützten Nutzerzugängen | siehe Rollen- und Berechtigungskonzept |
| • Protokollierung von Supporttickets | siehe JIRA-System |
| • Versionierung von Quellcodes | |
| • Doppelte Sichtprüfung mit Freiagbe "Code Reviews / Pull Requests" von Quelltextänderungen | siehe Bitbucket |

**3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

Wir haben Maßnahmen umgesetzt und implementiert, die die Verfügbarkeit und Belastbarkeit von personenbezogenen Daten gewährleisten.

Quelle: © 2021 Regina Mühlich

# Praktische Umsetzung

## Dokumentenlenkung

AdOrga Solutions

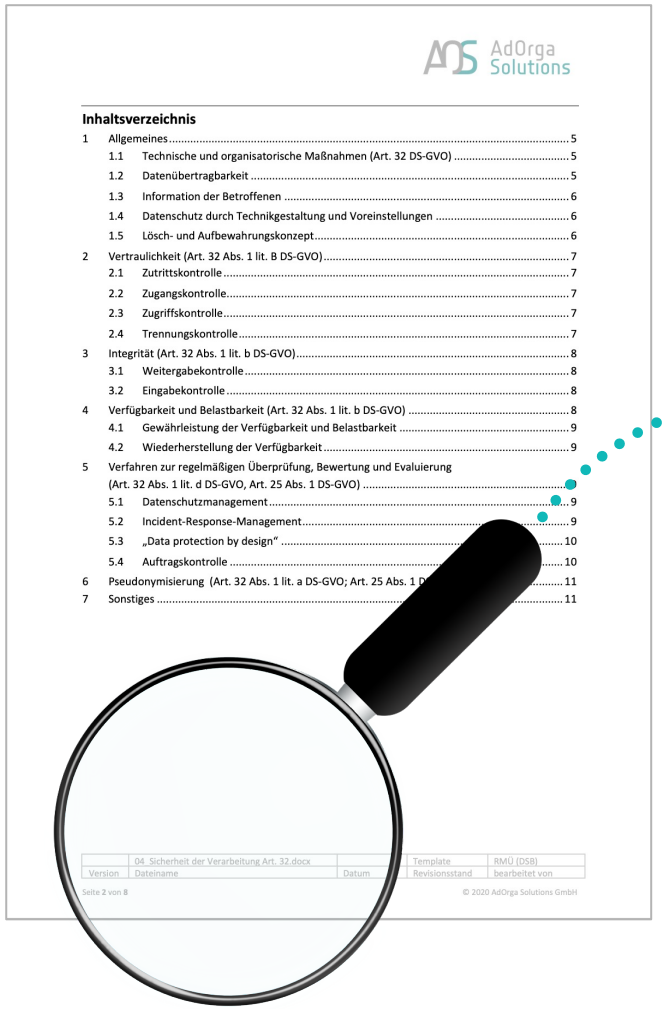
**Sicherheit der Verarbeitung**
**Art. 32 DS-GVO**

Verantwortlicher: [Firmenname]
[Straße]
[PLZ, Ort]

Stand: TT.MM.JJJJ
Version: 1.0

| | 04_Sicherheit der Verarbeitung Art. 32.docx | | Template | RMÜ (DSB) |
|---|---|---|---|---|
| Version | Dateiname | Datum | Revisionsstand | bearbeitet von |

Seite 1 von 8 © 2020 AdOrga Solutions GmbH




| | 04_Sicherheit der Verarbeitung Art. 32.docx | | Template | RMÜ (DSB) |
|---|---|---|---|---|
| Version | Dateiname | Datum | Revisionsstand | bearbeitet von |

Seite 2 von 8 © 2020 AdOrga Solutions GmbH

Quelle: © 2021 Regina Mühlich

# Praktische Umsetzung

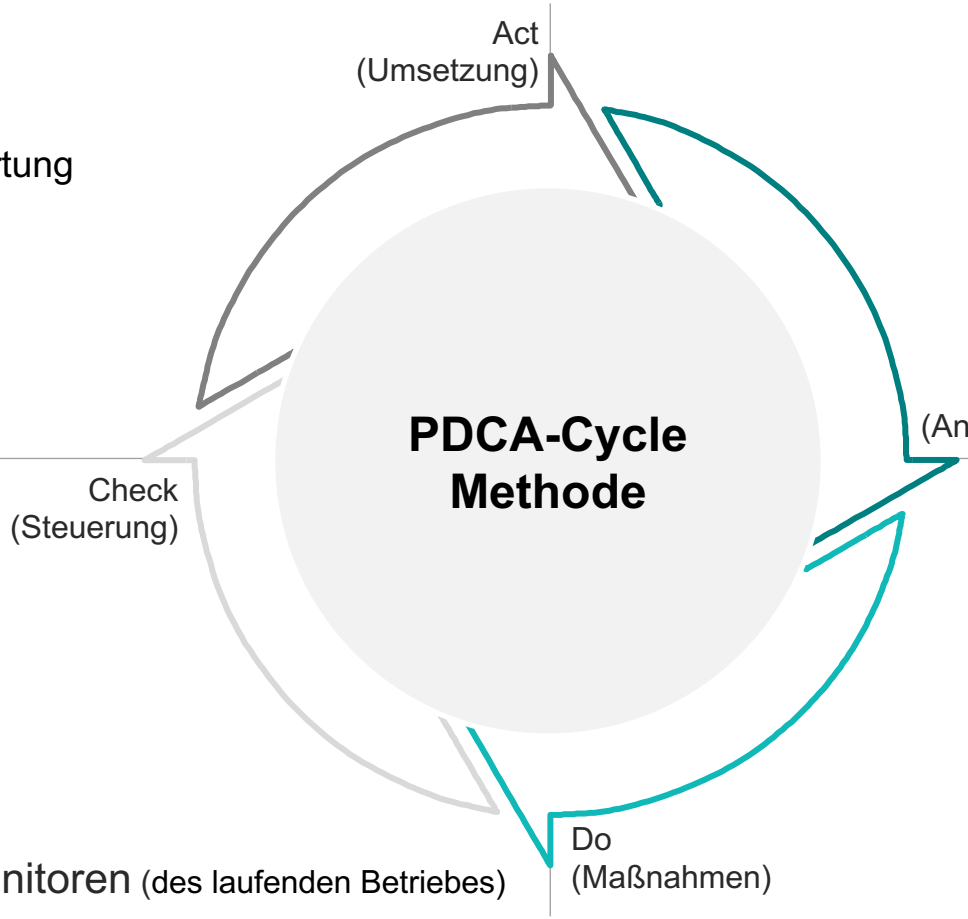
## plan-do-check-act

**A**ct (Verbessern)

Übernahme von Managementverantwortung

Umsetzung von Maßnahmen

Kommunikation




**P**lan – Planen, Ist, (DSFA)

Überprüfung der Ist-Situation

Problemerkennung, Risk Management

Sensitivitäts-, Schwellenwertanalyse

Handlungsempfehlung

Abweichungsanalysen

Controlling, Reporting, Dokumentation

Audits, Soll-/Ist-Analyse

Coaching

**C**heck, Kontrollieren, Prüfen, Monitoren (des laufenden Betriebes)

Sicherheit der Verarbeitung (TOM)

inkl. der Herstellung der Prüfbarkeit (Accountability)

**D**o – Implementieren

Quelle: © 2021 Regina Mühlich

AdOrga Solutions | DERRA, MEYER & PARTNER Rechtsanwälte PartGmbB

# Praktische Umsetzung

## Fazit

Verantwortlichkeit von Organisationen:

- Präventionsmaßnahmen
- Transparente Unternehmensorganisation
- „saubere“ Prozesse
- Schulungen und Mitarbeitersensibilisierung
- „umfassende“ Dokumentationen
- „gute“ Rechenschaftspflicht

# 5 Fragen

# Link-Tipps

Bundesverband IT-Sicherheit e. V. “Handreichung zum Stand der Technik“
https://media-exp1.licdn.com/dms/document/C511FAQH2Qy5CKFo3wQ/feedshare-document-pdf-analyzed/0?e=1582556400&v=beta&t=oPsovAf93b3kEY_LGRNERGxRjg8tYxEMuuZ5A3j0VOo

ULD - Das Standard-Datenschutzmodell
https://www.baden-wuerttemberg.datenschutz.de/datenschutzthemen

VdS – Richtlinien zur Umsetzung der DSGVO
https://shop.vds.de/de/download/ccb240fd9da9da2ab92f63c27c36cc2c

BSI Datenschutz
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html

BSI – IT Grundschutzkompendium 2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6

# Ihre Referenten

AdOrga Solutions

## Regina Mühlich

rm@adorgasolutions.de

DERRA, MEYER & PARTNER Rechtsanwälte PartGmbB

## Dr. Jens Eckhardt

eckhardt@derra-de.de

Regina Mühlich, Geschäftsführerin der Managementberatung AdOrga Solutions GmbH, ist Expertin für Datenschutz, Sachverständige für EDV und Datenschutz (TÜV) sowie Datenschutz-Auditorin (TÜV, DEKRA), Qualitätsmanagementbeauftragte (DQS, DEKRA) und zert. Compliance Officer. Als Compliance Officer und DSB berät und unterstützt sie nationale und internationale Unternehmen aus unterschiedlichsten Branchen. Im Datenschutz ist sie seit über 23 Jahren tätig und ist Mitglied des Vorstandes des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Dr. Jens Eckhardt ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Datenschutz-Auditor (TÜV) und Compliance Officer (TÜV). Seit 2001 ist er in den Bereichen Datenschutz, Marketing, Informationstechnologie und Telekommunikation sowohl strategisch beratend als auch gerichtlich bundesweit tätig. Außerdem ist er Dozent zum Datenschutzrecht an der Ulmer Akademie für Datenschutz und IT-Sicherheit (udis) gGmbH sowie Mitglied des Vorstandes des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.

# FORTBILDUNGSTERMINE DES BVD

## Praxisnahe Wissensvermittlung

Weitere Informationen: https://www.bvdnet.de/termine/