

# Prüfungen der DSGVO durch Aufsichtsbehörden beginnen



## DSGVO Prüfungsinhalte

# Agenda

**1** Status zu DSGVO Prüfungen der Aufsichtsbehörden

**2** Prüfungsinhalte

**3** Auswirkungen und mögliche Gefahren

**4** Wie CONSUVATION die Prüfungsinhalte gelöst hat

**5** Zusammenfassung

# Status zu DSGVO Prüfungen der Aufsichtsbehörden

- Die Datenschutzbehörden **beginnen Anfang Juli** mit der Prüfung der Umsetzung der DSGVO in Unternehmen
- Die Prüfungen sind als **Querschnittsprüfungen** angelegt. D.h. es werden **verschiedene Branchen und Unternehmen unterschiedlicher Größen** in die Prüfung aufgenommen
- **Erster Schritt** ist ein Anschreiben der Unternehmen und Abfragen des Status mit einem **Fragebogen**
- Dem **folgen** dann **Vor-Ort Termine** der Prüfung
- Die Prüfung umfasst **10 Bereiche** des Datenschutzes
- Aus den **Ergebnissen** kann die Behörde dann **Schwerpunktprüfungen in bestimmten Branchen** ableiten

Damit ist jetzt klar – **es wird Prüfungen geben** und die **beginnen aktuell** durch die Aufsichtsbehörden.

# Agenda

**1** Status zu DSGVO Prüfungen der Aufsichtsbehörden

**2** Prüfungsinhalte


**3** Auswirkungen und mögliche Gefahren

**4** Wie CONSUVATION die Prüfungsinhalte gelöst hat

**5** Zusammenfassung


# Prüfungsfeld I

## Vorbereitung auf die DSGVO

Prüfungsfragen	Umsetzung im Unternehmen?
<p>Wie haben Sie sich als Unternehmen auf die DSGVO vorbereitet?</p> <p>Schildern Sie (kurz) die Vorgehensweise, welche Bereiche involviert waren und welche Maßnahmen initiiert wurden.</p> <p>Sofern noch nicht alle Maßnahmen vollständig umgesetzt wurden, erläutern Sie bitte auch den Umsetzungsstatus.</p>	


# Prüfungsfeld II

## Verzeichnis von Verarbeitungstätigkeiten

Prüfungsfragen	Umsetzung im Unternehmen?
<p>Wie haben Sie sichergestellt, dass alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen wurden?</p> <p>Wie stellen Sie dessen Aktualität sicher?</p> <p>Legen Sie bitte eine Übersicht Ihrer dokumentierten Verfahren sowie ein Beispielfahrer als Muster bei.</p>	


# Prüfungsfeld III

## Zulässigkeit der Verarbeitung

Prüfungsfragen	Umsetzung im Unternehmen?
<p>Wie haben Sie sichergestellt, dass alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen wurden?</p> <p>Wie stellen Sie dessen Aktualität sicher?</p> <p>Legen Sie bitte eine Übersicht Ihrer dokumentierten Verfahren sowie ein Beispielfahrer als Muster bei.</p>	 A 3D white figure in a thinking pose stands next to a large, vibrant red question mark. The figure is positioned to the right of the question mark, with its hand on its chin, suggesting a state of deep thought or uncertainty. The question mark is large and three-dimensional, casting a soft shadow on the ground below it. The background is plain white, making the red question mark and the white figure stand out prominently.

# Prüfungsfeld IV


## Betroffenenrechte

Prüfungsfragen	Umsetzung im Unternehmen?
<p>Wie stellen Sie die Einhaltung der Betroffenenrechte (auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit) sicher?</p> <p>Skizzieren Sie Ihre diesbezüglichen Prozesse und gehen Sie insbesondere detailliert darauf ein, wie Sie Ihren Informationspflichten nachkommen.</p> <p>Vorhandene Musterinformationen fügen Sie bitte bei.</p>	




# Prüfungsfeld V

## Technischer Datenschutz

Prüfungsfragen	Umsetzung im Unternehmen?
<p>a. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen bzw. die Ihrer Dienstleister ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten?</p> <p>b. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen an den jeweiligen Stand der Technik angepasst werden?</p> <p>c. Wie stellen Sie sicher, dass Sie für die von Ihnen aktuell oder zukünftig eingesetzten IT-Anwendungen ein dokumentiertes datenschutzkonformes Rollen- und Berechtigungskonzept haben?</p> <p>d. Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Privacy by Design und by Default)?</p>	


# Prüfungsfeld VI

## Datenschutz-Folgeabschätzung

Prüfungsfragen	Umsetzung im Unternehmen?
<p>a. Wie stellen Sie sicher, dass Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen erkannt und für diese eine Datenschutz-Folgenabschätzung durchgeführt wird?</p> <p>b. Haben Sie in Ihrem Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen identifiziert? Welche?</p> <p>Fügen Sie bitte die jeweilige Dokumentation zur Datenschutz-Folgenabschätzung bei.</p>	


# Prüfungsfeld VII

## Auftragsdatenverarbeitung

Prüfungsfragen	Umsetzung im Unternehmen?
<p>Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern an die neuen Regelungen der DS-GVO angepasst?</p> <p>Sofern Sie Musterverträge verwenden, fügen Sie diese bitte bei, darüber hinaus fügen Sie bitte einen aktuellen Beispielvertrag mit einem Ihrer Auftragsverarbeiter bei.</p>	


# Prüfungsfeld IX

## Meldepflichten

Prüfungsfragen	Umsetzung im Unternehmen?
<p>Wie stellen Sie sicher, dass Ihr Unternehmen Datenschutzverstöße fristgemäß an die Aufsichtsbehörde meldet?</p> <p>Skizzieren Sie Ihre diesbezüglichen Prozesse.</p>	

# Prüfungsfeld X

## Dokumentation

Prüfungsfragen	Umsetzung im Unternehmen?
<p>Wie können Sie die Einhaltung aller vorstehend in Ziff. 2 – 9 genannten Pflichten nachweisen?</p>	

Quelle: Die Prüfungsfragen sind einer aktuellen Prüfung von einer Datenschutz-Aufsichtsbehörde entnommen.

# Agenda

**1** Status zu DSGVO Prüfungen der Aufsichtsbehörden

**2** Prüfungsinhalte

**3** Auswirkungen und mögliche Gefahren

**4** Wie CONSUVATION die Prüfungsinhalte gelöst hat

**5** Zusammenfassung

# Auswirkungen und Gefahren

- Die **Aufsichtsbehörden beginnen mit den Prüfungen** zur Umsetzung der DSGVO in Unternehmen
- Zielsetzung ist den **Status der Umsetzung** seit der zweijährigen Umsetzungsphase zu bewerten
- **Entdecken sie im Rahmen der Prüfung Verstöße** gegen den Datenschutz, werden sie Verfahren eröffnen und **Bußgelder aussprechen**
- In diesem Zusammenhang ist es auch wichtig zu wissen, das **nachfolgende Prüfungen** auch den Zeitraum **rückwirkend prüfen können**
- Damit ist klar, dass **die „Warten-wir-mal-ab“ Vorgehensweise** für den Verantwortlichen (Unternehmen) als auch die Geschäftsführung ein **hohes Risiko** bergen kann
- Der Prüfungsinhalt spricht **viele Elemente** des Datenschutzsystems an. In der Literatur wird diese Datenschutzsystem bereits als **Datenschutz Managementsystem** bezeichnet. Denn es verlangt nach DS-Prozesse, DS-Richtlinien, DS-Dokumentationen usw. die heute alle Bestandteile eines Managementsystem darstellen
- Außerdem sieht Art. 43 der DSGVO bereits eine Zertifizierung in der Zukunft vor

**CONSUVATION** hat bereits ein Datenschutz Managementsystem – dieses baut auf bereits bestehenden Normen zum Datenschutz auf und stellt somit eine Investitionssicherung für die Zukunft dar

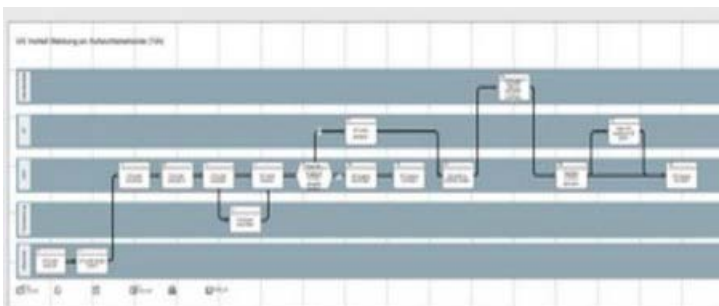
# Agenda

- 1 Status zu DSGVO Prüfungen der Aufsichtsbehörden
- 2 Prüfungsinhalte
- 3 Auswirkungen und mögliche Gefahren
- 4 Wie CONSUVATION die Prüfungsinhalte gelöst hat
- 5 Zusammenfassung

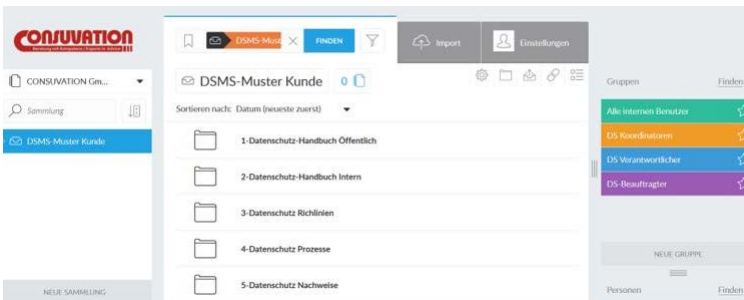


# Wie **CONSVATION** die Prüfungsinhalte gelöst hat

DS-Prozessmodell



DS-Portal



**CONSVATION** hat ein **Datenschutz Managementsystem (DSMS)** entwickelt. Das besteht aus einem DS-Prozessmodell. In diesem werden

- Die Rollen und Verantwortlichkeiten
- Datenschutzprozesse und Verfahren
- Richtlinien, Prozessbeschreibungen, Formulare abgebildet.

Das **DSMS** beinhaltet auch ein DS-Portal, indem für den Datenschutzbeauftragten, die notwendigen Regelwerke und Nachweisdokumente zur Rechenschaftspflicht abgelegt werden können.

Dies kann der Mandant auch nutzen.

# Agenda

**1** Status zu DSGVO Prüfungen der Aufsichtsbehörden

**2** Prüfungsinhalte

**3** Auswirkungen und mögliche Gefahren

**4** Wie CONSUVATION die Prüfungsinhalte gelöst hat

**5** Zusammenfassung

# Zusammenfassung

- **Die Aufsichtsbehörden werden** im nächsten Monat **mit den DSGVO Prüfungen beginnen**
- **Inhalt soll** unter anderem auch sein, wie Unternehmen die **zweijährige Übergangsfrist genutzt** haben
- Prüfungsinhalt werden **10 Prüfungsbereiche** sein
- Die **Behörden weisen darauf hin**, dass es natürlich zu **entsprechenden Verfahren kommt**, wenn sie **während der Prüfung Verstöße gegen die DSGVO feststellen**
- Aus den Ergebnissen dieser ersten Prüfungen sollen **Schwerpunktprüfungen für bestimmte Branchen sich anschließen**

Nach der ersten Prüfung durch das Bayerische Landesamt für Datenschutzaufsicht zum Status der Projektumsetzung **folgen jetzt die angekündigten Prüfungen zur Umsetzung der DSGVO – ggf. auch mit entsprechenden Bußgeld Verfahren**

## Geschäftsfelder

### CONSUATION GmbH

#### CONSUATION-UB

Betw. Unternehmensberatung

- BASEL III / Rating
- Unternehmensführung/ -planung (Businessplan ..)
- Finanzprozesse (SOX etc.)
- Innovationsmanagement
- Risikomanagement, -analysen u.a. nach ISO31000 & ONR49000
- Notfallmanagement nach ISO22301
- Controlling
- Kostenoptimierung
- Projektmanagement (PMI, CMMi, Spice ISO 15504)
- Business Process Management
- Prozessmodellierung und -optimierungen

#### CONSUATION-ISM

Integrierte Managementsysteme

- Qualitätsmanagement (ISO9000, TS16949, VDA, Six Sigma, CMMI)
- Umweltmanagement
- Arbeitssicherheit
- Projektmanagement
- IT-Qualitätsmanagement (CMM, Spice, BS15000 ..)

#### CONSUATION-DS/DSI

Datenschutz/-sicherheit u. Audit

- Aufbau Datenschutz (BDSG)
- Externer Datenschutz-beauftragter
- Datenschutz-Audits
- Risikoanalysen
- Aufbau von Informationssicherheitsmanagement-Systemen (ISMS) u.a.
- Vorbereitung zur Zertifizierung nach ISO27000/GSH & TISAX
- IT-Audits und IT-Government (COBIT, Sarbanes Oxley Act, IDW Prüfungsstandards) SAS-70 / neu: ISAE 3402 und SSAE

#### CONSUATION-IT

EDV Beratung u. Umsetzung

- IT-Managementberatung (Strategie, IT-Prozess-Optimierung, ITIL, BS15000, ISO20000, eTom, Prince, IBM FW, CMMi, ISO15504, Spice, V-Modell, PMI, Vertragsoptimierung, IT-Controlling, IT Value Management, IT Projekt-Management PMI, GMP)
- Anwendungsentwicklung (alte Technologien/neue Technologien, SAP)
- Systemmanagement

#### CONSUATION-Akademie

Training und Ausbildung

- Ausbildungen im Bereich:
  - BWL
  - Risikomanagement
  - Business Continuity Mgmt.
  - Informationstechnologie
  - Software:
    - MS Produkte
    - ViFlow
  - Qualitätsmanagement
  - Datenschutz
  - COBIT
  - ITIL (ISO 20000)
  - Security (ISO27001/GSH)
- Anerkanntes Partnerinstitut des Österreichischen Normungsinstitut für die Ausbildung zum „ON Risk Manager“ und „ISO27001 Auditor“

Wir führen keine Beratungsleistungen durch, die irgend welchen Berufsständen wie Rechtsanwälte, Steuerberater, Wirtschaftsprüfer oder ähnlichen vorbehalten sind.

Wir sind Beratende Betriebswirte und Ingenieure - ICG Controller (Prof. Dr. Horvarth) - Softwarearchitekten und -entwickler - Auditoren für ISO 9001 - Auditoren ISO 14001 - Auditoren für ISO27001 - Auditoren SCC/OHSAS 18001 - Risikomanager/-auditoren ISO31000/ONR49000 - Business Continuity Manager/Auditoren ISO 22301 - Assessoren für ISO 15504 (Spice) - Berater für CMMi - Business Auditoren (Riskmanagement etc.) - SOX Auditoren - CISA (Certified System Information Auditor) - CISM (Certified Information Security Manager) - CGEIT (Certified in Governance of Enterprise IT - CRISC (Certified in Risk and Information System Control) - Privatdozenten und Fachautoren - Schlichter der DRGI e.V. und Freie Gutachter und Sachverständige

Vielen Dank

**CONSUVATION GmbH**

Ziegelstr. 20

71063 Sindelfingen

[www.consuvation.com](http://www.consuvation.com)

[contact@consuvation.com](mailto:contact@consuvation.com)

Telefon +49 (0) 7031/4181-860

Telefax +49 (0) 7031/4181-861

