UIMCert® GmbH

**Unternehmens- und Informations-Management Certification**

Ob ISO 27001 oder Auftragsverarbeitung:

# Lieferantenbewertung / Dienstleister-Audit

Sobald sensible Daten durch einen Dienstleister verarbeitet werden (bzw. ein Zugriff hierauf nicht auszuschließen ist), muss sich der Auftraggeber von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen. Ein solches „Überzeugen“ stellt viele Unternehmen nicht selten vor eine Herausforderung. Zum einen fehlt ein geeigneter Fragenkatalog, nach dem diese Überprüfung vorgenommen werden soll, zum anderen fehlt oft eine **effiziente Methodik**, z. T. auch die Fachkompetenz und sehr oft **ausreichend Zeit**, um ein solches Audit vorzubereiten, durchzuführen und die Ergebnisse auszuwerten.

## *Wie kann die UIMCert hierbei unterstützen?*

Neben der fachlichen Kompetenz in diversen Datenschutzgesetzen und der **Erfahrung** aus der Durchführung vieler Auditierungen, kann die UIMCert als Außenstehender oftmals **schneller und routinierter** prüfen.

Hierbei kann die UIMCert sowohl **Fach- als auch Methodenkompetenz** vorweisen und bedient sich im Rahmen der Ordnungsmäßigkeitsprüfung sowohl in der Erhebungs- als auch der Phase der Dokumentation eines Tools zur **Effizienz- und Effektivitätssteigerung**. Basierend auf dem UIMC-Tool zur Auswertung und Berichterstellung (kurz: UTAB), umfasst es Fragen zur Organisation und zu den Sicherheitsmaßnahmen des Dienstleisters.

„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.**“

**[Artikel 28 Absatz 1 DSGVO: Auftragsverarbeiter]**

Die UIMCert erstellt sowohl einen Status-Quo-/**Schwachstellen-Bericht** als auch einen **Maßnahmenkatalog** mit Vorgaben an den Dienstleister zur Verbesserung. Eine **quantitative Darstellung bzw. Auswertung** bietet zudem die Möglichkeit für den Auftraggeber, eine Tendenzbetrachtung (hat sich der Auftragnehmer verbessert?) oder ein Benchmarking im Rahmen der Auswahl des Dienstleisters vorzunehmen.

### *Vorteile und Nutzen einer UIMCert-Unterstützung:*

**Kostenreduktion** durch Koordinierung (gemeinsame Prüfung)

Sicherstellung von Datenschutz/ **Compliance** beim Outsourcing

Zugriff auf hohe **Fach- und Methodenkompetenz** in Datenschutz und Auditierung

Höherer Stellenwert durch **unabhängige** Prüfung

Nutzung eines etablierten Tools zur Effektivitäts- und **Effizienzsteigerung**

**Qualitätsverbesserung** in Dienstleister-Prozessen

## *Warum sollten Sie uns beauftragen?*

Die UIMCert kann eine solche Auditierung wesentlich **effektiver** und **routinierter** durchführen. Sie hat hierbei beim Auftragnehmer auch oftmals eine erhöhte „Autorität“ als der Auftraggeber selbst. Dies verbessert die **Akzeptanz** der Befragung und Ergebnisse; auch beim Dienstleister selbst.

Gerne kann die UIMCert eine solche Audtierung auch **koordinieren**, indem weitere Kunden des Dienstleisters angesprochen und von einer gemeinsamen Auditierung überzeugt werden; der Dienstleister hat „nur“ ein Audit zu „ertragen“ und die verschiedenen Auftraggeber können die Aufwände aufteilen, so dass erhebliche **Kosteneinsparungen** möglich sind.

Weitere Informationen finden Sie unter **www.UIMCert.de/Lieferantenbewertung**

UIMCert GmbH
Otto-Hausmann-Ring 113
42115 Wuppertal
Tel: (0202) 9467 726-300
Fax: (0202) 9467 726-9300
E-Mail: certification@uimcert.de
Internet: www.UIMCert.de

Klimaneutral Druckprodukt

UIMCert GmbH + Otto-Hausmann-Ring 113 + 42115 Wuppertal + Tel: (0202) 9467 726-300 + Fax: (0202) 9467 726-9300 + Mail: certification@uimcert.de + Internet: www.UIMCert.de

UIMCert GmbH + Otto-Hausmann-Ring 113 + 42115 Wuppertal + Tel: (0202) 9467 726-300 + Fax: (0202) 9467 726-9300 + Mail: certification@uimcert.de + Internet: www.UIMCert.de

UIMCert® GmbH

**Unternehmens- und Informations-Management Certification**

## *Eine Dienstleister-Auditierung durch die UIMCert ist...*

### *strukturierter*

Durch die Nutzung eines etablierten Tools ist die Auditierung stark vorstrukturiert. Die Befragung wird durch einen UIMCert-Auditor durchgeführt; auch die anschließende Begehung wird durch den erfahrenen Prüfer durchgeführt, so dass an der richtigen Stelle nachgefragt oder tiefer geprüft werden kann.

### *effizienter*

Die Routine und die Tool-Unterstützung steigern die Effizienz aller Phasen: Erhebung, Auswertung und Maßnahmenplanung. So wird ein Bericht mit farblich hervorgehobenen Erkenntnissen erstellt, so dass ein schneller Überblick ermöglicht wird. Ebenfalls werden Maßnahmenempfehlungen ausgesprochen und priorisiert, die der Dienstleister entsprechend umsetzen sollte.

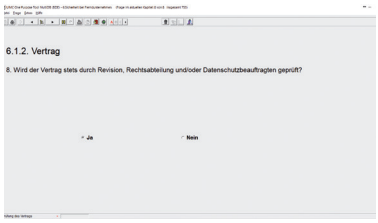
### *nützlicher*

Die Exportmöglichkeiten in Tabellenform erlauben eine aggregierte Darstellung der Befragungsergebnisse. Durch die quantitative Komponente wird der Vergleich von durchgeführten Audits im Sinne eines Benchmarkings und einer Trendbewertung „kinderleicht“. Doch auch die neue Management-Summary-Funktion erleichtert die Aufbereitung für die Entscheidungsebene.

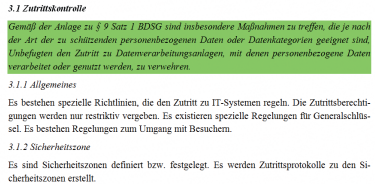
### *kostengünstiger*

Nicht nur durch die geringere Einarbeitungszeit durch ein hohes Maß der Routine, sondern auch durch die Koordinierung mit weiteren Auftraggebern beim zu prüfenden Dienstleister, können Aufwände von mehreren „Schultern getragen“ werden und somit Kosten gespart werden. Durch das Angebot an den Dienstleister hinsichtlich einer Siegelung/Zertifizierung können weitere Kosten verteilt werden.

**Funktionen des Dienstleister-Auditierungs-Tools zur Effizienzsteigerung:**




Gemeinsam mit dem Dienstleister kann ein Fragenkatalog bearbeitet werden. Hierin sind schwerpunktmäßig, wenn auch nicht ausschließlich, Anforderungen der technischen und organisatorischen Maßnahmen enthalten.



*3.1 Zutrittskontrolle*

*Gemäß der Anlage zu § 9 Satz 1 BDSG sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*

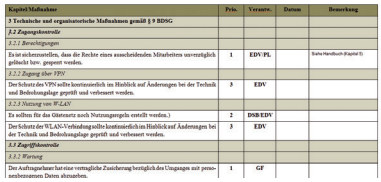
*3.1.1 Allgemeines*

Es bestehen spezielle Richtlinien, die den Zutritt zu IT-Systemen regeln. Die Zutrittsberechtigungen werden nur restriktiv vergeben. Es existieren spezielle Regelungen für Generalschlüssel. Es bestehen Regelungen zum Umgang mit Besuchern.

*3.1.2 Sicherheitszone*

Es sind Sicherheitszonen definiert bzw. festgelegt. Es werden Zutrittsprotokolle zu den Sicherheitszonen erstellt.

Im Ergebnisbericht werden jene Prüfungsfelder, bei denen eine Abweichung festgestellt wurde, farblich kenntlich gemacht.



| Kapitel/Maßnahme | Prio. | Verantw. | Datum | Bemerkung |
|---|---|---|---|---|
| **3 Technische und organisatorische Maßnahmen gemäß § 9 BDSG** | | | | |
| ***3.2 Zugangskontrolle*** | | | | |
| *3.2.1 Berechtigungen* | | | | |
| Es ist sicherzustellen, dass die Rechte eines ausscheidenden Mitarbeiters unverzüglich gelöscht bzw. gesperrt werden. | 1 | EDV/PL | | Siehe Handbuch (Kapitel 5) |
| *3.2.2 Zugang über VPN* | | | | |
| Der Schutz des VPN sollte konzeptionell im Hinblick auf Änderungen bei der Technik und Bedrohungslage geprüft und verbessert werden. | 3 | EDV | | |
| *3.2.3 Nutzung von W-LAN* | | | | |
| Es sollten für das Gästenetz noch Nutzungsregeln erstellt werden.) | 2 | DSB/EDV | | |
| Der Schutz der WLAN-Verbindung sollte konzeptionell im Hinblick auf Änderungen bei der Technik und Bedrohungslage geprüft und verbessert werden. | 3 | EDV | | |
| ***3.3 Zugriffskontrolle*** | | | | |
| *3.3.1 Wartung* | | | | |
| Der Auftragnehmer hat eine vertragliche Zusicherung bezüglich des Umgangs mit personenbezogenen Daten abzugeben. | 1 | GF | | |

Der Maßnahmenkatalog zeigt wiederum jene Aktivitäten auf, die umgesetzt werden sollten. Diese Ausführungen können Teil der SLA mit dem Dienstleister werden.

## Mehrwert für Dienstleister!?

Wenn Sie selbst Dienstleister sind, können Sie mit Hilfe des UIMCert-Gütesiegels einen hohen Qualitätsstandard proaktiv gegenüber (potentiellen) Kunden dokumentieren.

Dies ist nicht nur eine vertrauensbildende Maßnahme, sondern kann auch Kunden-Audits ersetzen oder zumindest reduzieren.

Dies ist auch in Verbindung mit der Dienstleister-Auditierung möglich.

## *Leistungsüberblick*

- » **Kontaktierung des Dienstleisters** und Vorbereitung/Organisation
- » **Koordinierung** des Audits mit anderen Auftraggebern des Dienstleisters (Kostenverteilung)
- » **Durchführung eines Dienstleister-Audits** auf Basis der DSGVO, ISO 27001 (und/oder entsprechende Norm im Kirchen-, Landes- oder Sozialrecht)
- » sofern erforderlich/sinnvoll: **Begehung** der Räumlichkeiten
- » **Auswertung des Audits:** Erstellung eines Schwachstellenberichts und eines Maßnahmenkatalogs
- » im Rahmen einer Ausschreibung: **Benchmarking** zwischen verschiedenen Dienstleistern
- » bei Wiederholungsaudits: Erstellung eines **Trendanalyse**

***Bei Interesse oder weiteren Fragen, zögern Sie nicht und sprechen uns an!***
***Tel.: 0202-9467 726-300 E-Mail: certification@uimcert.de***