Datenschutz-Analyse-Tools

UIMC®

Wie kommen Sie Ihrer Pflicht zur Dienstleisterprüfung effizient nach?

Dienstleister-Auditierungs-Tool

Effizientes Überprüfen beim Auftragnehmer gemäß § 11 BDSG

Nach den Vorgaben des Bundesdatenschutzgesetzes (§ 11 BDSG) sowie weiterer Datenschutzgesetze muss sich der Auftraggeber beim Auftragnehmer vor Beginn der Datenverarbeitung und „sodann regelmäßig" von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen. Dies ist zu dokumentieren.

Probleme

Ein solches „Überzeugen" stellt ein Unternehmen nicht selten vor die Herausforderung, wie dies zu gestalten ist. Zum einen fehlt ein geeigneter Fragenkatalog, nach dem diese Überprüfung vorgenommen werden soll, zum anderen ist eine Papierliste oftmals problematisch in der Durchführung und späteren Auswertung. Darüber hinaus sollte dem Dienstleister auch ein Ergebnisbericht vorgelegt werden und Schwachstellen nicht nur aufgezeigt, sondern auch **Änderungen eingefordert** werden.

Lösungsansatz

Mit Hilfe des UIMC-Dienstleister-Auditierungs-Tools, welches wir technisch auf Basis des bewährten UTAB aufgebaut haben, haben Sie ein umfassendes Tool zur Hand, mit dem Sie sich strukturiert, einfach und effizient von der Einhaltung der geforderten Maßnahmen beim Dienstleister überzeugen können. Ferner werden automatisch Maßnahmen vorgeschlagen, die der Dienstleister in vorgegebener Frist umsetzen sollte. Auch eine kontinuierliche Trendanalyse oder eine **Benchmark**-Funktion im Rahmen der Ausschreibung ist möglich.

Auf der sicheren Seite

Durch das Dienstleister-Auditierungs-Tool sind Sie in die Lage versetzt, den Dienstleister nach den Vorgaben des BDSG zu auditieren. Sei es im Rahmen des **Auswahlverfahrens** (§ 11 Absatz 2 Satz 1 BDSG) oder der (regelmäßigen) **Auditierung** im Sinne des „Sich-Überzeugens" (§ 11 Absatz 2 Satz 4 BDSG)! Mit Hilfe der einfachen Berichterstellung kann auch der **Dokumentationspflicht** nachgekommen werden.

Nutzen für den Dienstleister selbst?

Auch der Dienstleister selbst kann das Tool und die Vorgehensweise für eigene Zwecke nutzen. Sei es, um die eigene Organisation dahingehend zu überprüfen, ob bspw. ausreichende technische und organisatorische Maßnahmen ergriffen wurden (ggf. ist dann auch der Datenschutz-Checkup für Sie interessant) und etwaig erforderliche Gegenmaßnahmen zu ergreifen.

Auch kann er sich auf ein etwaigen Kunden-Audit vorbereiten. Ergänzend kann das Tool dafür genutzt werden, anhand des Berichts bereits proaktiv die Kunden über die Datenschutzmaßnahmen im eigenen Hause zu informieren. Hierbei zeigt sich der etablierte Fragenkatalog des Dienstleister-Auditierungs-Tools als vorteilhaft in der Argumentation gegenüber Kunden.

strukturiert, zielgerichtet, vielseitig

strukturiert

Die Fragen basieren einerseits auf dem zugrunde liegenden Prüfungsgebiet (Gesetze/Normen) und andererseits auf den langjährigen Erfahrungen der UIMC. Ferner sind die Fragen teils so verknüpft, dass irrelevante Themenkomplexe nicht angesteuert werden und somit Zeit gespart wird. Idealerweise sollte die Erhebung unter Beteiligung der relevanten Personengruppen in Form eines Workshops durchgeführt werden. Somit können die Themen an Ort und Stelle diskutiert werden. Das Involvement ist von Anfang an sichergestellt, was sich positiv auf die Akzeptanz des zugrunde liegenden Projekts auswirkt. Der Workshop kann durch einen UIMC-Berater moderiert werden, der mediatorisch in Diskussionen eingreifen und Erfahrungen aus anderen Institutionen einbringen kann.

zielgerichtet

Das UTAB löst den „Spagat“ zwischen vorstrukturierten Fragen und individueller Anpassbarkeit; aber auch Hilfefunktionen sind integriert, die die Erhebung und Auswertung vereinfachen. Auch die Erstellung des Ergebnisberichts wird durch das Tool effektiv unterstützt. Ein Bericht mit farblich hervorgehobenen Erkenntnissen wird computergestützt erstellt, so dass ein schneller Überblick ermöglicht wird. Die neue Management-Summary-Funktion erleichtert zudem die Aufbereitung für die Entscheidungsebene.

vielseitig

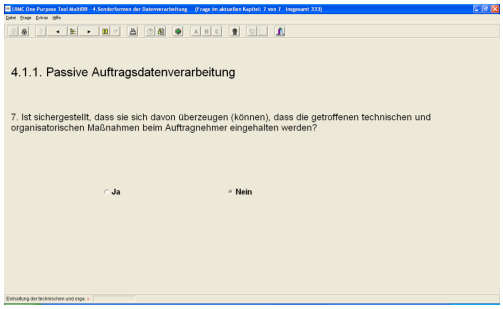
Quasi auf Knopfdruck werden die Berichte als qualitative Erkenntnisse und die quantitativen Ergebnisse dem Auswertenden zur weiteren Bearbeitung zur Verfügung gestellt. Die Exportmöglichkeiten in Tabellenform erlauben eine aggregierte Darstellung der Befragungsergebnisse. Durch die quantitative Komponente wird der Vergleich von durchgeführten Analysen im Sinne eines Benchmarkings „kinderleicht“.

Vorteile des Dienstleister-Auditierungs-Tools

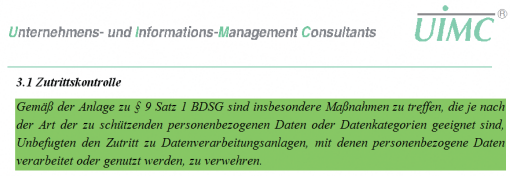
- umfassender, bewährter Fragenkatalog
- automatisierte Erstellung von Ergebnisbericht und Maßnahmenkatalog
- Management-Summary-Funktion
- Quantitative Auswertung

Ihr Nutzen

- strukturierte Vorgehensweise
- effiziente Durchführung und Auswertung



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


Unternehmens- und Informations-Management Consultants UIMC

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.

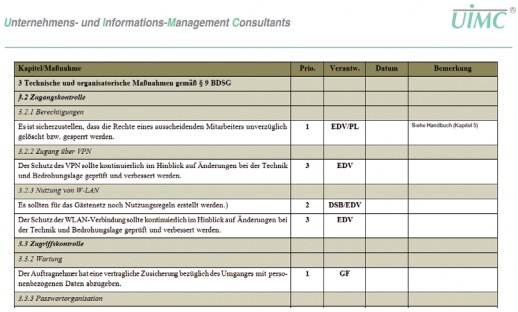
3.1.1 Allgemeines

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.


Unternehmens- und Informations-Management Consultants UIMC

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 kontinuierlich 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 kontinuierlich im Hinblick auf Änderungen bei der Technik und Bedrohungslage geprüft und verbessert werden.	3	EDV		
3.3 Zugriffskontrolle				
3.3.2 Wartung				
Der Auftragnehmer hat eine vertragliche Zusicherung bezüglich des Umganges mit personenbezogenen Daten abzugeben.	1	GF		
3.3.3 Passwortorganisation				

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

Kontaktdaten

UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119, 42115 Wuppertal
consultants@uimc.de, Tel: 0202 / 265 74 - 0

Mehr Informationen unter
Audit.UIMC.de