Arbeitshilfen zur Auftragsdatenverarbeitung

1 Abgrenzung

Die vorliegenden Excel-Tabellen dienen nur als Beispiel, wie anhand von Checklisten die datenschutzrechtlichen Voraussetzungen für die Vergabe einer Auftragsdatenverarbeitung beim Auftragnehmer geprüft und eine Selbstauskunft bzgl. der Erfüllung der datenschutzrechtlichen Anforderungen beim (potentiellen) Auftragnehmer eingeholt werden kann.

Keine dieser Tabellen kann für die Prüfung in einem vorhandenen Fall 1:1 direkt übernommen werden. Vielmehr bedarf jeder Fall der Prüfung durch einen Datenschutzbeauftragten, welcher die Tabellen entsprechend der jeweils vorhandenen Voraussetzungen anpasst.

2 ADV Selbstauskunft

(Datei: adv_selbstauskunft_fragebogen.alsx)

Diese Excel-Tabelle dient der Einholung einer Selbstauskunft beim Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung. Einzelne Bereiche wurden mittels der „bedingten Formatierung“ bzgl. der Eingabe dahingehend eingeschränkt, dass nur die vorgegebenen Werte zur Eingabe zugelassen sind.

Im Tabellenblatt „Fragenkatalog“ sind Fragen aufgelistet, die im hinsichtlich der Prüfung der Eignung eines (potentiellen) Auftragnehmers im Rahmen einer Auftragsdatenverarbeitung datenschutzrechtlich geprüft werden müssen, ohne dass der Fragenkatalog hierbei einen Anspruch auf Vollständigkeit erhebt. Der Fragenkatalog teilt sich dabei in drei grundlegende Bereiche ein (Abbildung 1):

1) der eigentliche Fragenbereich
2) der vom Auftragnehmer auszufüllende Bereich
3) der vom Auftraggeber auszufüllende Bereich

	Frage		Vom AN auszufüllen		Vom AG auszufüllen	
Kategorie	Kernfrage	Ergänzungsfrage	Ja (x, leeres Feld)	Nein (x, leeres Feld)	Trifft nicht zu (x, leeres Feld)	Gewichtung (Wert zwischen 1 und 10)
	Allgemeines					
Allg.	Wurde beim Auftragnehmer (AN) ein DSB bestellt?					
Allg.	Wurde der AN durch Überprüfung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig					
Allg.	War bei der Auswahlüberprüfung der auftragnehmende Datenschutzbeauftragten ("DSB") aktiv eingebunden?					
Allg.	Gibt es beim AN einen Beauftragten für die IT-/Informationssicherheit?					
Allg.	Existieren beim AN Vertretungsregelungen für die DV-Verantwortlichen?					
Allg.	Ist beim AN eine IT-Revision bzw. interne Revision vorhanden?					

Abbildung 1: Struktureller Aufbau des Fragenkatalogs zur Selbstauskunft des Auftragnehmers

Dabei teilt sich der Fragenbereich in die drei Abschnitte

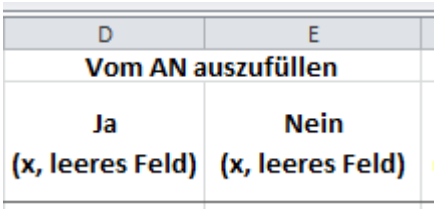
a) Kategorie, zu der die Frage gehört
b) die „Kernfrage“, d.h. die Fragestellung, die geklärt werden muss
c) ggfs. eine Ergänzungsfrage, um die Kernfrage zu präzisieren, zu ergänzen oder spezielle Themen, die zur Kernfrage gehören können, abzufragen

auf. An Kategorien existieren

- Allgemeine Anforderungen (Allg.)
- Dokumentation (Doku.)
- TOMs 1: Zutrittskontrolle (TOMs1)
- TOMs 2: Zugangskontrolle (TOMs2)
- TOMs 3: Zugriffskontrolle (TOMs3)
- TOMs4: Weitergabekontrolle (TOMs4)
- TOMs 5: Eingabekontrolle (TOMs5)
- TOMs 6: Verfügbarkeitskontrolle (TOMs6)
- TOMs 7: Trennungskontrolle (TOMs7)
- TOMs 8: Auftragskontrolle (TOMs8).

2.1 Bereich Auftragnehmer

Der Auftragnehmer trägt lediglich ein „x“ in die zutreffende Spalte ein, d. h., wenn die Frage vom Auftragnehmer bejahend beantwortet wird bei „Ja“, ansonsten bei „Nein“ (siehe Abbildung 2). Wenn weder bei „Ja“ noch bei „Nein“ ein „x“ zu finden ist, wird die Frage als mit „Nein“ beantwortet gewertet, ausgenommen, der Auftraggeber gab in der Spalte „Trifft nicht zu“ an, dass die Frage für die betreffende Auftragsdatenverarbeitung nicht relevant ist.



D	E
Vom AN auszufüllen	
Ja (x, leeres Feld)	Nein (x, leeres Feld)

Abbildung 2: Vom Auftragnehmer auszufüllender Bereich

Es wurden statt einer „Ja/Nein“-Antwort zwei Spalten gewählt, sodass der Datenschutzbeauftragte des Auftraggebers bei Nicht-Ausfüllung seitens des Auftragnehmers hier rückfragen kann. Ggfs. kann der Auftragnehmer auch das Tabellenblatt „Begründung“ nutzen, um dem Auftragnehmer hier Erläuterungen zu seiner Auswahl zukommen zu lassen.

2.2 Bereich Auftraggeber

Der Auftraggeber legt zu jeder Frage fest, ob die Frage für die zu vergebende Auftragsdatenverarbeitung zutrifft oder die Beantwortung der Frage vom Aufragnehmer ignoriert werden kann (Spalte „Trifft nicht zu“, siehe Abbildung 3). Dieses Feld ist sinnvollerweise auszufüllen, bevor die Excel-Tabelle zum Auftragnehmer geschickt wird.

F	G
Vom AG auszufüllen	
Trifft nicht zu (x, leeres Feld)	Gewichtung (Wert zwischen 1 und 10)

Abbildung 3: Vom Auftragnehmer auszufüllender Bereich des Fragebogens

Weiterhin kann der Auftraggeber eine Gewichtung der Frage vornehmen. Standardmäßig werden alle Kernfragen einer Kategorie gleich berücksichtigt, der Standardwert ist „1“. Misst der Auftraggeber bzgl. der Auftragsdatenverarbeitung einer oder mehreren Fragen in der betreffenden Kategorie eine besondere Bedeutung zu, kann er der jeweiligen Frage für die Auswertung ein größeres Gewicht zuweisen, wobei 10 der Maximalwert ist. Ob der Auftraggeber die Gewichtung vor der Zusendung der Tabelle zum Auftragnehmer oder nach Rückerhalt durch den Auftragnehmer ausfüllt, kann nicht empfohlen werden; beides bietet Vor- und Nachteile: Einerseits kann der Auftragnehmer Fragen, die für den Auftraggeber besonders wichtig sind, mehr Aufmerksamkeit schenken, andererseits fallen evtl. die Antworten bei Kenntnis einer Gewichtung anders aus. Daher kann hier nur im Einzelfall das Vorgehen festgelegt werden.

Im Tabellenblatt „Begründung“ findet der Auftraggeber die Möglichkeit, festzuhalten

- warum eine Frage für den jeweiligen Auftrag datenschutzrechtlich nicht relevant ist, er also „Trifft nicht zu“ markierte
- die eine Relevanz einer Frage, die vom Auftragnehmer mit „Nein“ beantwortet wurde, hinsichtlich der Auftragsvergabe zu beleuchten.

Dieses Tabellenblatt soll eine Hilfe darstellen, wenn im Rahmen einer Prüfung durch die Aufsichtsbehörde erklärt werden muss, warum trotz einzelner datenschutzrechtlicher „Schwachstellen“ beim Auftragnehmer dieser trotzdem den Auftrag bekommen hat. Ebenso soll es dem Datenschutzbeauftragten eine Hilfestellung geben, wenn zwischen verschiedenen potentiellen Auftragnehmern ausgewählt werden muss und der Datenschutzbeauftragte gegenüber der Geschäftsleitung eine Empfehlung aussprechen soll.

2.3 Auswertung

Im Tabellenblatt „Auswertung“ werden die Antworten auf die Fragen zusammengefasst dargestellt, einmal in Form einer Tabelle, einmal in Form einer grafischen Darstellung (siehe Abbildung 4).

A	B	C	D
Bereich	Punkte	Mögliche Punkte	Bewertung (0= schlecht, 100 gut)
Allgemeine Anforderungen	55	129	42,22%
Dokumentation	37	339	10,87%
TOMs 1: Zutrittskontrolle	20	136	14,38%
TOMs 2: Zugangskontrolle	-29	177	-16,32%
TOMs 3: Zugriffskontrolle	5	236	1,96%
TOMs4: Weitergabekontrolle	7	154	4,58%
TOMs 5: Eingabekontrolle	4	96	4,17%
TOMs 6: Verfügbarkeitskontrolle	-89	373	-23,94%
TOMs 7: Trennungskontrolle	24	144	16,67%
TOMs 8: Auftragskontrolle	147	239	61,29%

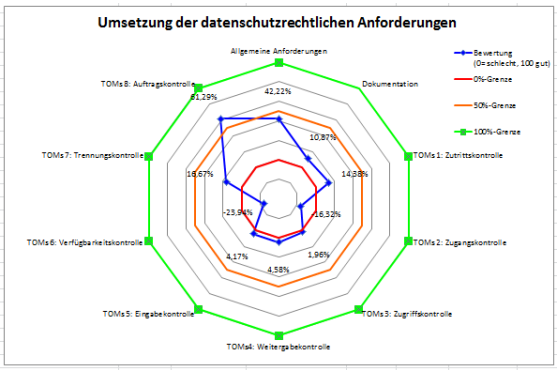


Abbildung 4: Zusammengefasste Darstellung der Antworten auf den Fragebogen zur Selbstauskunft

Fragen, die mit „Nein“ beantwortet werden, bekommen einen negativen Punktwert, sodass bei einzelnen Abschnitten vom Auftragnehmer auch ein negativer Punktwert erreicht werden kann.

3 Datenschutzrechtliche Prüfung der Vertragsvergabe

(Datei: adv_pruefung.alsx)

Diese Excel-Tabelle dient der Prüfung der Vergabe einer Auftragsdatenverarbeitung beim Auftraggeber. Einzelne Bereiche wurden ebenfalls mittels der „bedingten Formatierung“ bzgl. der Eingabe dahingehend eingeschränkt, dass nur die vorgegebenen Werte zur Eingabe zugelassen sind.

Im Tabellenblatt „Fragenkatalog“ sind Fragen aufgelistet, die im hinsichtlich der datenschutzrechtlichen Prüfung einer Auftragsvergabe geprüft werden müssen, ohne dass der Fragenkatalog hierbei einen Anspruch auf Vollständigkeit erhebt. Der Fragenkatalog teilt sich dabei in zwei grundlegende Bereiche ein (Abbildung 5):

1) der eigentliche Fragenbereich
2) der vom Datenschutzbeauftragten auszufüllende Bereich.

A	B	C	D	E	F
	Frage		Vom DSB auszufüllen		
Kategorie	Kernfrage	Ergänzungsfrage	Trifft nicht zu (x, leeres Feld)	Ja/Nein	Gewichtung (Wert zwischen 1 und 10)
Vertragsgestaltung					
Vertrag	Ist der Vertragsgegenstand genau bezeichnet?				
Vertrag	Ist die Dauer des Auftrags geregelt?				
Vertrag	Sind die Pflichten, die über das Vertragsende hinausreichen, beschrieben? (Z.B. Schweigepflicht, Wahrung des Datengeheimnisses)				
Vertrag	Sind Umfang, Art und Zweck der Datenverarbeitung benannt?				
Vertrag	Ist die Art und Weise der erlaubten Verarbeitung vertraglich geregelt?				
Vertrag	Ist beim AN Telearbeit bzw.die Datenverarbeitung in Privatwohnungen erlaubt?				
Vertrag	Ist vertragtlich geregelt, dass die Beschäftgten des AN entsprechend BDSG bzw. den entsprechenden landesrechtlichen/kirchlichen Bestimmungen auf das Datengeheimnis zu verpflichten sind.				
Vertrag	Ist der Kreis der Betroffenen im Vertrag bezeichnet?				
Vertrag	Ist der Einsatzort genau bezeichnet?				

Abbildung 5: Struktureller Aufbau des Fragenkatalogs zur Prüfung einer Vergabe hinsichtlich einer Auftragsdatenverarbeitung

Der Fragenbereich ist analog zur Tabelle hinsichtlich der Selbstauskunft aufgebaut, an Kategorien existieren

- Vertragsgestaltung (Vertrag)
- Organisation (Org.).

Ebenso wie bei der Selbstauskunft kann der Datenschutzbeauftragte auch hier wieder angeben, dass eine Frage bzgl. der betrachteten Auftragsdatenverarbeitung nicht relevant ist (Spalte „Trifft nicht zu“), desgleichen kann er wieder eine Gewichtung vornehmen, um Fragen innerhalb einer Kategorie in der Auswertung stärker berücksichtigt zu sehen. Mittels „Ja“ bzw. “Nein“ gibt der Datenschutzbeauftragte an, wie die Frage aus seiner Sicht zu beantworten ist.

Im Tabellenblatt „Begründung“ ist analog zur Tabelle bzgl. der Selbstauskunft wieder die Möglichkeit gegeben, zu jeder Frage einen Kommentar hinzuzufügen.

4 Abkürzungen

AG	Auftraggeber
AN	Auftragnehmer
DSV	Datenschutzbeauftragter
TOM	Technisch-organisatorische Maßnahmen