Zentrales Verfahren: Dokumentationspflichten für die zentrale Stelle und für die beteiligten Stellen

Beschreibung der Verantwortlichkeiten bei der Dokumentation eines zentralen Verfahrens. Wer übernimmt welche Dokumentationsbestandteile?

Kennzeichnung im Dokument:
Z = Zentrale Stelle
B = Beteiligte Stelle

- Grundlage ist die Vorlage (Version 1.3) für eine Verfahrensakte [1]
- Die zentrale Stelle erstellt die Dokumentation mit den Informationen, die unten aufgeführt werden. Die Informationen, die die beteiligten Stellen betreffen, werden „offen gelassen".
- Diese Dokumentation wird den beteiligen Stellen in einer bearbeitbaren Version zur Verfügung gestellt, sodass die beteiligten Stellen die entsprechenden Informationen ergänzen können.
- Die beteiligten Stellen ergänzen die offenen Punkte wie unten beschrieben.

Verfahrensakte 00

Z + B		Beim gesamten Deckblatt übernehmen ***Z und B*** die Dokumentationsbestandteile, die sie selbst betreffen. Insbesondere der Punkt 00-3 (Datenschutzmanagement) müssen von ***Z und B*** ausgefüllt werden.

Verfahrensakte 01

Z	01-1	Beschreibung des Verfahrens, Zweckbestimmung Hier werden die grundsätzlichen Zwecke von KoPers durch die Zentrale Stelle beschrieben. Eine Vorgehensweise kann sein, dass ***Z*** hier alle Module des zentralen Verfahrens aufführt und die tatsächlich verwendeten Module im entsprechenden Vertrag aufgeführt werden.
Z	01-2	Prüfung der Zulässigkeit
Z	01-3	Prüfung der Zulässigkeit nach § 11 Abs. 3 LDSG
Z	01-4	Datenübermittlung
Z	01-5	Auftragsdatenverarbeitung
B	01-6	Maßnahmen zu Auskunftsansprüchen
B	01-7.1	Aufbewahrungszeiten (da die beteiligten Stellen die Verantwortung für die gespeicherten Daten haben)
Z + B	01-7.2	Maßnahmen zur Löschung Die technische Möglichkeit der Löschung wird durch ***Z*** beschrieben. Der tatsächliche Prozess zur Löschung wird durch ***B*** beschrieben.
Z + B	01-7.3	Maßnahmen zur Sperrung Die technische Möglichkeit der Sperrung wird durch ***Z*** beschrieben. Der tatsächliche Prozess der Sperrung wird durch ***B*** beschrieben.

[1] www.datenschutzzentrum.de/dsvo/verfahrensakte

Z + B 01-7.4 Maßnahmen zur Berichtigung
Die technische Möglichkeit der Berichtigung wird durch ***Z*** beschrieben.
Der tatsächliche Prozess zur Berichtigung wird durch ***B*** beschrieben.

Z + B 01-8 Maßnahmen zur Datenvermeidung und Datensparsamkeit
Die Maßnahmen bei den zentralen Bestandteilen werden durch ***Z*** beschrieben.
Die Maßnahmen bei der IT der beteiligten Stelle werden durch ***B*** beschrieben.

Z + B 01-9 Beteiligte Programme (-> siehe 02-1)

Z + B 01-10 IT-Systeme
Die zentrale IT wird durch ***Z*** beschrieben.
Die evtl. IT der beteiligten Stelle wird durch ***B*** beschrieben.

Z 01-11 Netzplan

Z + B 01-12 Verfahrensspezifische Protokollierung
Die technische Möglichkeit wird durch ***Z*** beschrieben.
Der Prozess im Zusammenhang mit der Protokollierung wird durch ***B*** beschrieben.

Verfahrensakte 02

Z + B 02-1 Verwendete Programme

Alle Programme, die durch ***Z*** eingesetzt werden, werden auch durch ***Z*** beschrieben. Setzen beteiligte Stellen noch zusätzliche Programme ein, die im Zusammenhang mit diesem Verfahren verwendet werden, muss ***B*** diese entsprechend ergänzen.

Z + B 02-2 Dokumentation Berechtigungen

Z beschreibt die Berechtigungsvergabe innerhalb der zentralen Stelle, die Prozesse der beteiligten Stelle zur Vergabe von Berechtigungen (Unterpunkte 02-4, 02-5) werden durch ***B*** beschrieben.

Z 02-3 Schritte zur Inbetriebnahme

B 02-4 Berechtigungsvergabe (Benutzer)

B 02-5 Berechtigungsvergabe (Administration)

B 02-4 Revision

Verfahrensakte 03

Z + B 03-1 Test

Die zentralen Komponenten werden durch ***Z*** getestet. Werden die zentralen Komponenten durch einen externen DL betrieben, so werden die zentralen Komponenten durch diesen getestet und der ***Z*** zur Verfügung gestellt

Die eigene IT der beteiligten Stelle und das Vorhandensein der entsprechenden Datenschutzmanagement-Prozesse werden durch ***B*** getestet (siehe Hinweise zu Test und Freigabe weiter unten).

Z + B 03-2 Freigabe

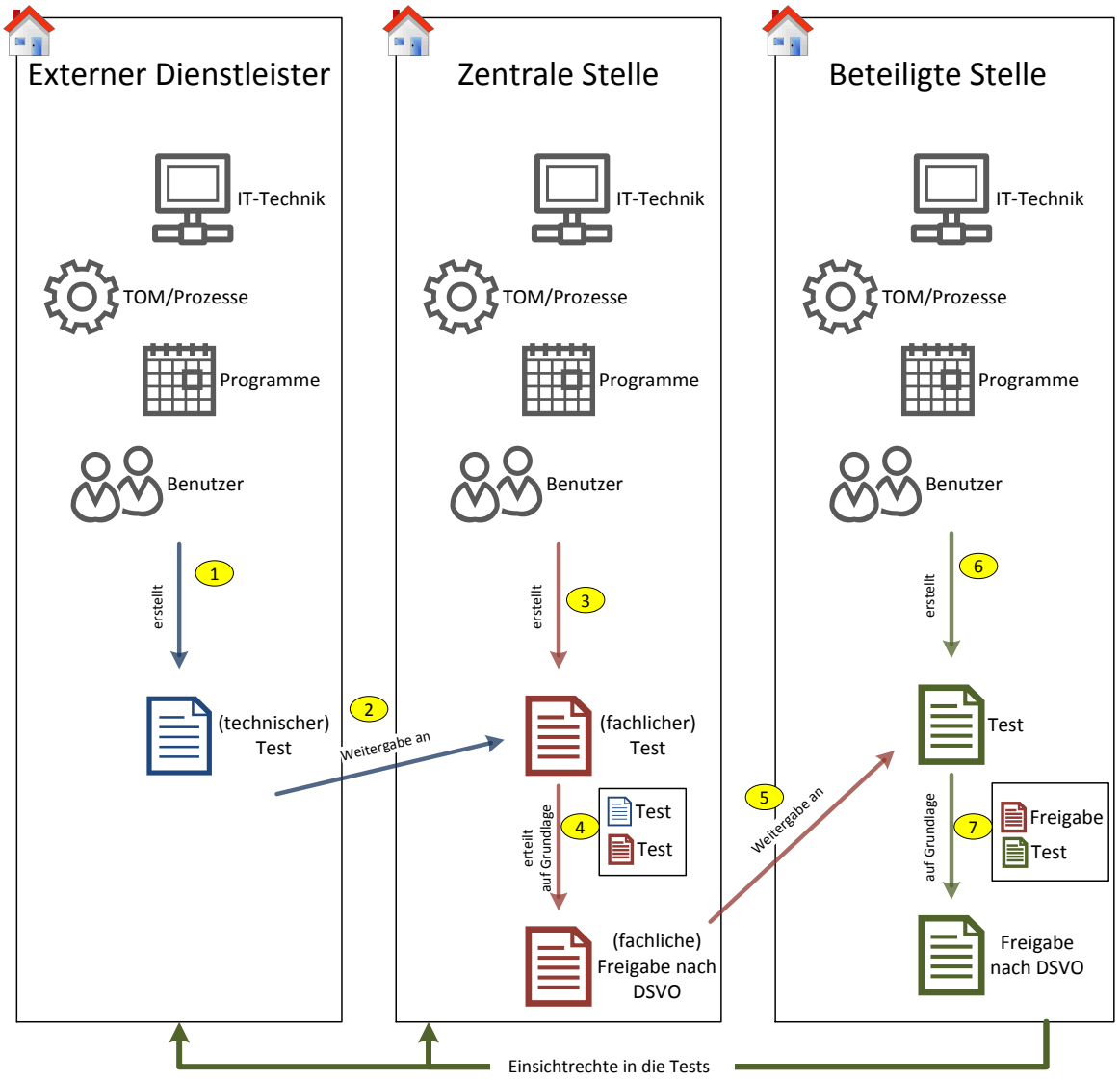
Die technische Freigabe des Verfahrens erfolgt durch ***Z***. Sie dient den beteiligten Stellen als Grundlage zur Freigabe in ihrem eigenen Verantwortungsbereich. ***B*** gibt als Daten verarbeitende Stelle das Verfahren in Verbindung mit der technischen Freigabe von ***Z*** und dem eigenen Test nach 03-1 das Verfahren als „oberste Instanz“ frei (siehe Hinweise zu Test und Freigabe weiter unten).

Verfahrensakte 04

Z	Beschreibung der Auftragsdatenverarbeitung

Hinweise zu Test und Freigabe

Beschreibung des Test- und Freigabeverfahren bei Verfahren mit einer zentralen Stelle (gestaffeltes Test- und Freigabeverfahren).



Kennzeichnung im Dokument:

DL = Externer Dienstleister
Z = Zentrale Stelle
B = Beteiligte Stelle

DL/Z Für den Fall, dass ein externer Dienstleister eingesetzt wird, ansonsten übernimmt diese Aufgabe die Zentrale Stelle:

Der ***DL*** bzw. die ***Z*** erstellt einen technischen Test (1) und (2). Mit diesem Test muss nachvollziehbar sein, dass die Anforderungen an die Datensicherheit und den Datenschutz innerhalb des Rechenzentrums des ***DL*** oder im Netzwerk der ***Z*** gewährleistet werden.
Inhaltliche Beispiele (nur zur Verdeutlichung der inhaltlichen Gestaltung an einen Test ohne den Anspruch auf Vollständigkeit) :

- Nachweis eines störungsfreien Betriebs der am Verfahren beteiligten IT-Komponenten und Softwareprodukte.
- Nachweis einer störungsfreien Integration der am Verfahren beteiligten IT-Komponenten in den Netzwerkbetrieb.
- Nachweis einer schadsoftwarefreien IT-Umgebung.
- Nachweis der Implementierung von technischen und organisatorischen Maßnahmen beim IT-Betrieb beim ***DL*** oder der ***Z***, z. B. Maßnahmen für Zugangs- und Zugriffssicherheit (auf Ebene von Betriebssystemen und Netzwerkkomponenten)
- usw.

Z Auf Grundlage des technischen Tests erstellt die ***Z*** einen Test (3) nach DSVO (in der Abbildung oben als fachlichen Test bezeichnet), der nachweist, dass die Anforderungen an die DSVO und die getroffenen TOM (technischen und organisatorischen Maßnahmen) innerhalb der ***Z*** und innerhalb des zentralen Verfahren, einschließlich aller Datenschutzmanagementprozesse, eingehalten werden.
Inhaltliche Beispiele (nur zur Verdeutlichung der inhaltlichen Gestaltung an einen Test ohne den Anspruch auf Vollständigkeit):

- Nachweis der Implementierung von technischen und organisatorischen Maßnahmen beim Betrieb des Verfahrens, z. B. Maßnahmen für Zugangs- und Zugriffssicherheit (innerhalb des Zuständigkeitsbetriebs der ***Z***).
- Nachweis der Implementierung von technischen und organisatorischen Maßnahmen in Bezug auf die Transparenz und der Revisionsfähigkeit (Protokolle, Kontrollen) innerhalb des Zuständigkeitsbetriebs der ***Z***.
- Nachweis der fachlichen Richtigkeit der verarbeiteten Daten.
- Nachweis der Implementierung von Datenschutzmanagementmaßnahmen zur Wahrung der Betroffenenrechte (Information, Berichtigung, Löschung, Sperrung) innerhalb des Zuständigkeitsbereichs der ***Z*** .
- usw.

Auf Grundlage des technischen Tests und des fachlichen Tests gibt die ***Z*** das zentrale Verfahren frei (4).

Ist vertraglich festgehalten, dass die ***Z*** das Verfahren für die ***B*** testet und freigibt (nach DSVO), dann entfällt für die ***B*** der nächste Schritt.

B Auf Basis (5) des fachlichen Tests und der Freigabe der ***Z*** erstellt die ***B*** einen (ergänzenden) Test nach DSVO (6), der nachweist, dass die Anforderungen an die DSVO und die getroffenen TOM innerhalb der eigenen Daten verarbeitenden Stelle (IT-Technik, Programme, Prozesse, Benutzer) eingehalten werden.

Inhaltliche Beispiele (nur zur Verdeutlichung der inhaltlichen Gestaltung an einen Test ohne den Anspruch auf Vollständigkeit):

- Nachweis der Implementierung von technischen und organisatorischen Maßnahmen beim Betrieb des Verfahrens, z. B. Maßnahmen für Zugangs- und Zugriffssicherheit (innerhalb des Zuständigkeitsbetriebs der ***B***).
- Nachweis der Implementierung von technischen und organisatorischen Maßnahmen in Bezug auf die Transparenz und der Revisionsfähigkeit (Protokolle, Kontrollen) innerhalb des Zuständigkeitsbetriebs der ***B***.
- Nachweis der Implementierung von Datenschutzmanagementmaßnahmen zur Wahrung der Betroffenenrechte (Information, Berichtigung, Löschung, Sperrung) innerhalb des Zuständigkeitsbereichs der ***B*** .
- usw.

Auf Grundlage dieses Tests gibt die ***B*** das Verfahren für die eigene Organisation frei (7)(Freigabe nach DSVO).

Ist vertraglich festgehalten, dass die ***Z*** das Verfahren für die ***B*** testet und freigibt (nach DSVO), dann entfällt für die ***B*** dieser Schritt.