Kontrollplan gem. § 22 DA DI

Version	Datum	Bearbeiter/in	Beschreibung/ Änderung	Freigabe durch:
0.1	17.10.2019	Kodde (ITD 7)	Erstentwurf	
0.2	13.12.2019	Grothe (JM)	Formatierung/Überarbeitung	
0.3	01.10.2021	Czaplik (JM)	Überarbeitung	

Dieser Kontrollplan beschreibt,

- welche Tätigkeiten im Rahmen der Dienstanweisung Datenschutz und Informationssicherheit wahrzunehmen sind (Aufgabe),
- wie deren Umsetzung erfolgen kann (Umsetzung),
- welche Stellen für die Erfüllung der Aufgabe zuständig sind (Zuständig für Erfüllung der Aufgabe),
- wie die Kontrolle erfolgen kann (Inhalt der Kontrolle),
- wer in Funktion (Für die Kontrolle zuständiges Dezernat) und in Person (Mitarbeiter/-in) die Kontrollen durchzuführen hat,
- in welchem Vorgang die Kontrolle dokumentiert ist (Vorgang)

Nr.	**Aufgabe**	**Umsetzung**	**Zuständig für Erfüllung d. Aufgabe**	**Inhalt der Kontrolle**	**F. d. Kontrolle zuständiges Dezernat (Mitarbeiter/-in)**	**Vorgang**	**Ergebnis der Prüfung**
1	Bestellung einer/s geeigneten Datenschutzbeauftragten sowie eines Vertreters, § 12 Abs. 1 - 4	Auswahl und Bestellung einer geeigneten, sachkundigen und zuverlässigen Person sowie Gewährleistung einer regelmäßigen Fortbildung		Dokumentation der Auswahlentscheidung, der Bestellung sowie der regelmäßigen Fortbildung			
3	Meldung von Sicherheitsvorfällen an die/den ISB sowie ggf. DSB, § 13 Abs. 2	Festlegung eines Prozesses zur Handhabung von Sicherheitsvorfällen (Erkennen von Vorfällen, Behandlung, Meldung) und Einhaltung des Prozesses		Dokumentation des Prozesses zur Handhabung der Sicherheitsvorfälle sowie Do-			

				kumentation etwaiger Vorfälle und entsprechender Meldungen			
4	Maßnahmen zum Schutz von Räumlichkeiten vor unbefugtem Zutritt, § 14 Abs. 1	Analyse und Festlegung des Schutzbedarfs der jeweiligen Räumlichkeiten		Maßnahmen zum Schutz von Räumlichkeiten vor unbefugtem Zutritt, § 14 Abs. 1			
5	Eingeschränkter Zugang für Externe, § 14 Abs. 2	Überwachung von Externen im Rahmen des Zugangs zu Räumlichkeiten		Eingeschränkter Zugang für Externe, § 14 Abs. 2			
6	Dokumentation und Überwachung der Rechte- und Rollenvergabe, § 15 Abs. 2	Festlegung eines Rechte- und Rollenkonzepts, entsprechende Rechte- und Rollenvergabe sowie Überwachung der Einhaltung		Vorliegen eines Rechte- und Rollenkonzepts sowie Dokumentation der Vergabe			
7	Regelung der Einstellung und des Ausscheidens von Mitarbeiterinnen oder Mitarbeitern, § 16 Abs. 1	Festlegung eines standardisierten Prozesses zur Einstellung und zum Ausscheiden von Mitarbeiterinnen oder Mitarbeitern sowie Dokumentation dessen Einhaltung		Vorliegen eines standardisierten Prozesses sowie Dokumentation der Überwachung			

8	Sensibilisierung der Mitarbeiterinnen und Mitarbeiter, § 16 Abs. 2	Regelmäßige Sensibilisierungsmaßnahmen wie z. B. regelmäßige Bekanntgabe der DADI, Ausgabe von Merkblättern mit Handlungsempfehlungen bei der Ausgabe mobiler Geräte oder anlässlich der Anzeige privater Geräte, Angebot von Vorträgen und Fortbildungen im Bereich des Datenschutzes und der Informationssicherheit		Dokumentation der Durchführung von Sensibilisierungsmaßnahmen			
9	Zurverfügungstellung von für die Diensterfüllung notwendigen IT-Geräten, § 17 Abs. 1	Vorhalten notwendiger Geräte sowie Dokumentation der Aus- und Rückgabe. Regelmäßige stichprobenartige Überprüfung des Vorhandenseins ausgegebener Speichermedien		Dokumentation der Aus- und Rückgabe sowie der stichprobenhaften Überprüfungen			
10	Erwerb und Einsatz validierter IT-Geräte und Zubehör, § 17 Abs. 2	Erwerb und Einsatz validierter IT-Geräte und Zubehör sowie Dokumentation des Erwerbs und Einsatzes der erworbenen Produkte		Dokumentation des Erwerbs und Einsatzes validierter IT-Geräte und Zubehör			

11	Schutz mobiler IT-Geräte, § 17 Abs. 3	Erwerb und Ausgabe hardwareverschlüsselter USB-Sticks; Installation geeigneter Verschlüsselungssoftware auf mobilen IT-Geräten		Dokumentation des Erwerbs und der Ausgabe hardwareverschlüsselter USB-Sticks sowie der Installation geeigneter Verschlüsselungssoftware			
12	Information des/der ISB und DSB bei Verlust von Speichermedien und IT-Geräten, §§ 6 Abs. 3, 13 Abs. 1, 2	Festlegung eines Prozesses zur Handhabung des Verlusts von IT-Geräten (Festlegung und Bekanntgabe eines Meldewegs innerhalb der Behörde) und Einhaltung des Prozesses		Dokumentation des Prozesses und der im Prüfzeitraum gemeldeten Vorfälle			
13	Rechtzeitige, § 17 Abs. 5, und sichere, § 17 Abs. 6 und 7, Löschung von Daten	Festlegung eines Löschkonzepts und Einhaltung dessen		Dokumentation des Konzepts und dessen Durchführung			
14	Sichere Aufbewahrung von zur Archivierung verwendeten Speichermedien mit sensiblen Infor-	Verschlüsselung der Daten oder Aufbewahrung in Tresoren, eindeutige Kennzeichnung der verwendeten Speichermedien sowie Erfassung		Stichprobenartige Überprüfung der Aufbewahrung der Speichermedien und deren			

	mationen oder personenbezogenen Daten, § 17 Abs. 7	in einem Verzeichnis; sichere Verwahrung der Passwörter		Kennzeichnung; stichprobenartige Kontrolle des Verzeichnisses			
15	Hinterlegung von Kennwörtern, § 17 Abs. 8	Sichere Hinterlegung von Kennwörtern, soweit es für die technische Systembetreuung erforderlich ist, sowie Kennwortschutz; Dokumentation der Hinterlegung, des Austauschs und jeden Zugriffs		Stichprobenartige Überprüfung der Hinterlegung und des Schutzes; Dokumentation der Hinterlegung, des Austauschs und jeden Zugriffs			
16	Erwerb und Einsatz validierter Softwareprodukte, § 18 Abs. 1, 2	Erwerb und Einsatz validierter Softwareprodukte sowie Erfassung der eingesetzten Software in einem entsprechenden Verzeichnis		Stichprobenartige Prüfung des Verzeichnisses			
17	Datensicherung, § 19	Erstellung und Einhaltung eines Datensicherungskonzepts, soweit die Sicherung des Datenbestands nicht zentralisiert erfolgt Falls kein Datensicherungskonzept erstellt wird, ist der		Vorliegen eines Datensicherungskonzepts Dokumentation der Datensicherungen			

		Datenbestand mindestens einmal wöchentlich vollständig zu sichern; außerdem ist eine tägliche Sicherung der Änderungen des Datenbestandes erforderlich Fertigung von Aufzeichnungen über die Sicherungen					
18	Überwachung von Wartung und Reparatur, § 20 Abs. 1 und 2	Sicherstellung der Überwachung von Wartung bzw. Pflege durch justizfremdes Personal sowie Dokumentation der Genehmigung dessen Einsatzes		Dokumentation der Genehmigung			
19	Reparatur außerhalb des Dienstgebäudes, § 20 Abs. 3	Vollständige Sicherung der auf dem betreffenden IT-Gerät gespeicherten vertraulichen Informationen und personenbezogenen oder sensiblen Daten sowie anschließende revisionssichere Löschung (oder ggf. Ausbau des Datenträgers)		Dokumentation der Sicherung und Löschung oder des Ausbaus			

20	Notfallhandbuch, § 21	Erstellung und regelmäßige Aktualisierung des Notfall-handbuchs sowie dessen Be-kanntgabe an alle Beteiligten entsprechend ihrer dienstli-chen Betroffenheit zur Kennt-nis zu geben Vorhalten des Notfallhand-buchs sowohl elektronisch als auch schriftlich		Vorliegen eines aktuellen Notfall-handbuchs sowie Dokumentation der Bekanntgabe			