Checkliste: Feststellung des Handlungsbedarfs bei der Umsetzung von DSGVO, KDG und EKD-DSG 2018

	Umgesetzt?	
	Ja	Nein
Informationssicherheitsmanagement-System		
Ein Konzept zur Informations- bzw. IT-Sicherheit gemäß Art. 32 DSGVO / § 26 KDG / § 27 EKD-DSG 2018 existiert.		
Ein Konzept zur Überwachung der Wirksamkeit sämtlicher Maßnahmen der Informationssicherheit existiert.		
Die Prozesse zur Aktualisierung des Konzepts zur Informationssicherheit und der Wirksamkeitsprüfungen sind dokumentiert und wirksam.		
Die Prüfergebnisse der Wirksamkeitsprüfungen sind vollständig dokumentiert.		
Ein Prozess zur Dokumentation aller Sicherheitsvorfälle gemäß Art. 33, 34 DSGVO / §§ 32, 34 KDG / §§ 32, 33 EKD-DSG 2018 ist vorhanden und wirksam.		
Ein Prozess zur Meldung von Sicherheitsvorfällen an die Datenschutzaufsichtsbehörde gemäß Art. 33 DSGVO / § 32 KDG / § 32 EKD-DSG 2018 ist dokumentiert und wirksam.		
Ein Prozess zur Meldung von Sicherheitsvorfällen an die betroffenen Personen gemäß Art. 34 DSGVO / § 33 KDG / § 32 EKD-DSG 2018 ist dokumentiert und wirksam.		
Ein Prozess zur Prüfung von Hardware, Software sowie Services auf Konformität mit der DSGVO / KDG / EKD-DSG 2018 beim Einkauf ist dokumentiert und wirksam.		
Datenschutzmanagementsystem		
Es ist festgelegt und dokumentiert, welche Positionen im Unternehmen für die Überprüfung der Befolgung der Datenschutzvorschriften in jeder Abteilung verantwortlich sind.		
Es ist festgelegt und dokumentiert, für welche Aktivitäten eine datenschutzrechtliche Prüfung erforderlich ist.		
Es ist festgelegt und dokumentiert, für welche Beauftragungen von externen Unternehmen / Dritten eine datenschutzrechtliche Prüfung zu erfolgen hat.		
Ein Datenschutzbeauftragter ist – sofern durch DSGVO / BDSG 2018 / KDG / EKD-DSG 2018 vorgeschrieben – bestellt und verfügt über die notwendige Fachkunde. Er ist frei von Interessenkonflikten.		
Der bestellte Datenschutzbeauftragte ist der Aufsichtsbehörde gemeldet und seine Kontaktdaten sind veröffentlicht worden.		
Ein Prozess zur Bearbeitung von Anfragen betroffener Personen hinsichtlich Auskunft, Berichtigung, Sperrung, Löschung, Datenmitnahme sowie Widerspruch ist dokumentiert und wirksam. Der Prozess erfüllt die Vorgaben von DSGVO/ KDG / EKD-DSG 2018.		
Ein Konzept zur Löschung von nicht mehr benötigten gespeicherten Daten ist vorhanden und wird umgesetzt.		
Für jeden Dienstleister (Auftragsdatenverarbeiter)		
Alle alten und neuen Verträge zur Auftragsdatenverarbeitung erfüllen die Vorgaben von Art. 28 DSGVO / § 29 KDG / § 30 EKD-DSG.		
Es liegen ausreichende Garantien nach Art. 28 DSGVO / § 29 KDG / § 30 EKD-DSG 2018 für jeden Auftragsdatenverarbeiter vor.		
Für jede Betriebsvereinbarung		
Alle geltenden Betriebsvereinbarungen sind konform mit DSGVO / BDSG 2018 / KDG / EKD-DSG 2018.		

	Umgesetzt?	
	Ja	Nein
Für jede Software und jeden Prozess		
Für jede Programmfunktion und jeden Prozessschritt liegt eine gesetzliche Erlaubnis vor und dies ist dokumentiert.		
In allen Programmen und Prozessen werden ausschließlich für den jeweiligen Zweck erforderliche Datenfelder und Datensätze verarbeitet. Die Erforderlichkeit ist dokumentiert.		
Alle vergebenen Zugriffsrechte sind für die Tätigkeit der Nutzer erforderlich. Die Erforderlichkeit ist dokumentiert.		
Ein Prozess zur Beantragung oder Gewährung von Zugriffsrechten ist dokumentiert und wirksam.		
Ein Prozess zur regelmäßigen Prüfung der Notwendigkeit von vergebenen Zugriffsrechten ist dokumentiert und wirksam.		
Die Ergebnisse der Notwendigkeitsprüfung werden vollständig dokumentiert.		
Prüfungsmechanismen zur Erkennung unberechtigter Zugriffe sind dokumentiert und wirksam.		
In allen Softwareprogrammen (auch von Fremdherstellern) werden ausschließlich Komponenten (z. B. Codebibliotheken) eingesetzt, die nachgewiesenermaßen dem Stand der Technik entsprechen.		
Alle Softwareprogramme und IT-Geräte sind – sofern einschlägig – gemäß den Vorgaben der BSI-Grundschutz-Kataloge oder vergleichbarer Normen konfiguriert.		
Aus allen Softwareprogrammen können die gespeicherten Daten zu einer Person vollständig und in verständlicher Darstellung ausgedruckt werden.		
Aus allen Softwareprogrammen können die gespeicherten Daten zu einer Person vollständig in maschinenlesbarer Form exportiert werden.		
In allen Softwareprogrammen lassen sich Datensätze und Datenfelder einzeln sperren, so dass sie nicht mehr verarbeitet werden können.		
In allen Softwareprogrammen lassen sich Datensätze und Datenfelder sowohl manuell als auch durch automatische Regeln löschen.		
Ein Prozess zur fristgerechten Information des Betroffenen bei der direkten oder indirekten Datenerhebung entsprechend Art. 12 – 14 DSGVO / §§ 14 – 16 KDG / §§ 16 – 18 EKD-DSG 2018 ist dokumentiert und wirksam.		
Für jedes Datenfeld ist als Speicherfrist definiert, wann der letzte Zweck entfallen und eine eventuell bestehende gesetzliche Aufbewahrungsfrist abgelaufen ist.		
In allen Softwareprogrammen, abgelegten Dateien und E-Mails werden personenbezogene Daten unmittelbar nach Ablauf der Speicherfrist gelöscht.		
Nachweisfähigkeit		
Die Tätigkeiten mit Bezug zu personenbezogenen Daten sind festgelegt und dokumentiert. Dazu zählen Prozessbeschreibungen, Richtlinien und Arbeitsanweisungen.		
Ein Prozess zur Aktualisierung der Tätigkeitsfestlegungen ist dokumentiert und wirksam.		
Ein Dokumentationssystem ist etabliert, das erlaubt, die Einhaltung aller Vorschriften von DSGVO / KDG / EKD-DSG 2018 jederzeit nachweisen zu können.		
Alle Zwecke, für die personenbezogene Daten im Unternehmen verarbeitet werden (inkl. Ad-hoc-Auswertungen mit Excel), sind dokumentiert.		
Alle Datenfelder für personenbezogene Daten im Unternehmen sind dokumentiert.		
Alle von einer Datenverarbeitung betroffenen Personengruppen sind dokumentiert.		