Datenschutzanforderungen (Privacy by Design / Privacy by Default)

Vertragsleistungen müssen in Übereinstimmung mit den Grundsätzen des Privacy by Design (Datenschutz durch Technik) und des Privacy by Default (datenschutzfreundliche Voreinstellungen) konzipiert, hergestellt und konfiguriert werden. Der Dienstleister stellt sicher und gewährleistetet gegenüber dem Auftraggeber, dass bei Entwicklung, Einsatz, Einbau und/oder Weitervertrieb der Entwicklungen die Datenschutzprinzipien des Art. 5 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) und die Datenschutzvorgaben des Art. 25 DSGVO beachtet werden bzw. beachtet werden können.

Dabei werden bestehende Standards, Methoden und Best Practices gebührend berücksichtigt. Hierzu finden konkretisierend insbesondere die in der Anlage „Controls“ genannten Datenschutzanforderungen Anwendung auf die Entwicklungen. Der Dienstleister dokumentiert die Umsetzung dieser Anforderungen und stellt diese Dokumentation bei Bedarf dem Auftraggeber zum Zwecke des Nachweises zur Verfügung (Rechenschaftspflicht Art. 5 Abs. 2 DSGVO).

Der Dienstleister stellt dem Vertragspartner hinreichende Informationen und ggf. Konfigurationsmöglichkeiten zur Verfügung, damit alle Entwicklungsbeteiligten insoweit ihren jeweiligen Datenschutzverpflichtungen (etwa Rechenschafts-, Lösch- sowie Informationspflichten) gegenüber Geschäftspartnern, Behörden und betroffenen Personen nachkommen und datenschutzrechtliche Ansprüche der betroffenen Personen erfüllen können.

Anlage „Controls“

Bei der Gestaltung der Vertragsleistungen sind nachfolgende Controls zugrunde zu legen. Jedes der Controls muss im Rahmen der Entwicklung projekt- und produktspezifisch weiter verfeinert und hinsichtlich seiner Umsetzung dokumentiert werden. Umsetzungsbeispiele sind im Template zu jedem Control hinzugefügt.

Bitte leiten Sie zu jedem Control entsprechende hardware-, software- und sonstige entwicklungsspezifische Anforderungen ab und beschreiben Sie diese Anforderungen sowie deren Umsetzung.

Darüber hinaus sind den Controls "Prüffragen zu systemischen Grundbedingungen" zugeordnet. Mithilfe dieser ergeben sich Anhaltspunkte, ob die geplante Hardware, Software und sonstigen Entwicklungsergebnisse die technischen Grundvoraussetzungen für die Umsetzung der jeweiligen rechtlichen Anforderungen erfüllt. Mithilfe der Prüffragen zu fachlich-prozessualen Anknüpfungen ergeben sich Anhaltspunkte, ob wesentliche fachliche Anforderungen an die technische Implementierung in Bezug auf den Datenschutz bekannt sind und umgesetzt wurden.

Die "Prüffragen zu systemischen Grundbedingungen" sind nicht Bestandteil der formalen und verbindlichen datenschutzrechtlichen Anforderungen.

Nachfolgende Anforderungen leiten sich aus dem Datenschutzrecht der Europäischen Union - speziell der DSGVO - ab. Bitte beachten Sie, dass je nach Einsatz bzw. Zielmarkt einer Hardware, Software oder sonstiger Entwicklungsergebnisse andere oder zusätzliche Anforderungen gelten können, insbesondere soweit sich diese aus nationalem Recht des betreffenden Landes ergeben.

Nr.	Control	Beschreibung	Prüffragen zu systemischen Grundbedingungen [nicht formaler und verbindlicher Bestandteil der rechtlichen Anforderungen]	Prüffragen zu fachlich-prozessualen Anknüpfungen
1	**Datenminimierung**	Daten dürfen nur in dem Umfang verarbeitet werden der für den jeweiligen Zweck der Verarbeitung angemessen und erheblich ist. Die Datenverarbeitung muss auf das für den Zweck notwendige Maß beschränkt sein	Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, Daten zu löschen (Daten sind nach Löschung dauerhaft und unwiederbringlich vollständig aus der Hardware, Software oder dem sonstigen Entwicklungsergebnis zu entfernen, zu überschreiben, sicher und abschließend zu anonymisieren)? Kann die Hardware, Software oder das sonstige Entwicklungsergebnis Daten sperren (Zugriffsmöglichkeiten einschränken und Weiterverarbeitung ausschließen)?	Liegen für die auf der Hardware, Software oder dem sonstigen Entwicklungsergebnis betriebenen Verarbeitungstätigkeiten fachliche Löschkonzepte gem. Prozess Löschkonzept vor? Wurden diese zu einem Löschkonzept konsolidiert? Wurde ein technisches Löschkonzept abgeleitet und dieses umgesetzt?
2	**Transparenz**	Daten müssen in einer für die betroffene Person	Bei Hardware, Software oder sonstigen	Liegen die zur Implementierung ggf.

		nachvollziehbaren Weise verarbeitet werden. Informationen und Mitteilungen über die Verarbeitung müssen für den Betroffenen leicht zugänglich und verständlich sein.	Entwicklungsergebnissen mit Userinterface für Betroffene: Bietet die Hardware, Software oder das sonstige Entwicklungsergebnis die Möglichkeit, Hinweistexte / Icons zum Datenschutz an leicht zugänglicher Stelle (z.B. maximal über 2 Klicks) anzuzeigen und zu managen?	erforderlichen Datenschutzhinweise und weiteren Datenschutzinformationen nach fachlichen Vorgaben gem. Prozess Datenschutzhinweise vor? Wurden diese Anforderungen für die Hardware, Software oder das sonstige Entwicklungsergebnis konsolidiert? Wurden fachliche Umsetzungsanforderungen abgeleitet und wurden diese implementiert?
3	**Integrität und Vertraulichkeit**	Daten dürfen nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Dazu gehört der Schutz vor unrechtmäßiger oder unbefugter Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.	Wurde für die Hardware, Software oder das sonstige Entwicklungsergebnis die Umsetzung erforderlicher IT-Sicherheitsanforderungen nachweisbar bestätigt?	Wurden die für die vorliegende Hardware, Software oder das sonstige Entwicklungsergebnis erforderlichen IT-Sicherheitsprozesse durchgeführt? Liegt insbesondere ein freigegebenes Sicherheitskonzept vor?

4	**Zweckbindung**	Die Zwecke, zu denen die Datenverarbeitung erfolgt, müssen eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der Daten bereits feststehen.	Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, Berechtigungen und Schnittstellen individuell zu steuern und jederzeit einzuschränken? Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage Mandaten physisch oder zumindest logisch voneinander zu trennen (Mandatentrennung)?	Liegen für die, auf der Hardware, Software oder dem sonstigen Entwicklungsergebnis betriebenen Verarbeitungstätigkeiten fachliche Berechtigungskonzepte vor? Wurden diese zu einem Berechtigungskonzept konsolidiert? Wurde ein technisches Löschkonzept abgeleitet und dieses umgesetzt?
5	**Datenrichtigkeit**	Die verarbeiteten Daten müssen sachlich richtig und aktuell sein. Unrichtige Daten sind unverzüglich zu löschen oder zu berichtigen.	Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, dass die Datenfelder mit personenbezogenen Daten geändert werden (z.B. Datenfelder überschreiben)? Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, Daten zu löschen (Daten sind nach Löschung dauerhaft und unwiederbringlich vollständig aus der Hardware, Software oder dem sonstigen	

			Entwicklungsergebnis zu entfernen, zu überschreiben, sicher und abschließend zu anonymisieren)? Kann die Hardware, Software oder das sonstige Entwicklungsergebnis Daten sperren (Zugriffsmöglichkeiten einschränken und Weiterverarbeitung ausschließen)?	
6	**Speicherbegrenzung**	Daten müssen in einer Form gespeichert werden, die eine Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist.	Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, Daten zu löschen (Daten sind nach Löschung dauerhaft und unwiederbringlich vollständig aus Hardware, Software oder sonstigen Entwicklungsergebnissen zu entfernen, zu überschreiben, sicher und abschließend zu anonymisieren, so dass auch durch Verknüpfung mit weiteren Daten, kein Rückschluss auf eine natürliche Person möglich ist)? Kann die Hardware, Software oder das sonstige Entwicklungsergebnis Daten sperren (Zugriffsmöglichkeiten einschränken und	Liegen für die auf der Hardware, Software oder dem sonstigen Entwicklungsergebnis betriebenen Verarbeitungstätigkeiten fachliche Sperr-, Pseudonymisierungs- und Anonymisierungsanforderungen* vor? Wurden diese zu entwicklungsspezifischen Anforderungen konsolidiert?* Wurden technischen Sperr-, Pseudonymisierungs- und Anonymisierungsanforderungen abgeleitet und umgesetzt? *

			Weiterverarbeitung ausschließen)? Kann die Hardware, Software oder das sonstige Entwicklungsergebnis Daten pseudonymisieren (Entfernung des Namens und Ersetzen durch ein Pseudonym)?	(*fachliche Anforderung und technische Umsetzung erfolgen z.B. im Rahmen des Löschkonzepts s. hierzu. Prozess Löschkonzept)
7	**Rechtmäßigkeit**	Personenbezogene Daten dürfen nur verarbeitet werden, sofern hierfür eine Rechtsgrundlage besteht.	Nur bei Hardware, Software oder sonstigen Entwicklungsergebnissen mit Userinterface für Betroffene: Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, Einwilligungserklärungen anzuzeigen und zu managen (z.B. one-klick, per e-mail)? • falls ja: ist per Default eine Einwilligung NICHT gesetzt? • falls ja: ist der Widerruf so einfach wie die Einwilligung (z.B. one-klick, per Email)?	Liegen für die auf der Hardware, Software oder dem sonstigen Entwicklungsergebnis betriebenen Verarbeitungstätigkeiten Anforderungen an die technische Umsetzung von Einwilligungs- und Widerrufsmechanismen vor? Wurden diese zu entwicklungsspezifischen Anforderungen konsolidiert? Wurden technische Umsetzungsanforderungen abgeleitet und implementiert? Liegen die zur Implementierung ggf. erforderlichen Einwilligungserklärungen und weiteren

				Datenschutzinformationen nach fachlichen Vorgaben gem. Prozess Datenschutzhinweise vor und wurden diese implementiert?
8	**Betroffenenrechte**	Es muss gewährleistet sein, dass Betroffene hinsichtlich ihrer Daten folgende Rechte geltend machen können: Auskunft/ Kopie Berichtigung Löschung Einschränkung der Verarbeitung Datenübertragung Widerspruch	Kann die Hardware, Software oder das sonstige Entwicklungsergebnis alle Datenfelder in ein gängiges Datenformat exportieren z.B. Excel, csv, xml, pdf? Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, dass die Datenfelder mit personenbezogenen Daten geändert werden (z.B. Datenfelder überschreiben)? Ist die Hardware, Software oder das sonstige Entwicklungsergebnis in der Lage, Daten zu löschen (Daten sind nach Löschung dauerhaft und unwiederbringlich vollständig aus Hardware, Software oder sonstigen Entwicklungsergebnissen zu entfernen, zu überschreiben, sicher und abschließend zu anonymisieren, so dass	Liegen für die auf der Hardware, Software oder dem sonstigen Entwicklungsergebnis betriebenen Verarbeitungstätigkeiten fachliche Betroffenenrechtekonzepte gem. Prozess Betroffenenrechtekonzept vor? Wurden diese zu entwicklungsspezifischen Betroffenenrechtekonzepte konsolidiert? Wurden technische Betroffenenrechtekonzepte abgeleitet und umgesetzt?

			auch durch Verknüpfung mit weiteren Daten kein Rückschluss auf eine natürliche Person möglich ist)? Kann die Hardware, Software oder das sonstige Entwicklungsergebnis Daten sperren (Zugriffsmöglichkeiten einschränken und Weiterverarbeitung ausschließen)? Kann die Hardware, Software oder das sonstige Entwicklungsergebnis Daten pseudonymisieren (Entfernung des Namens und Ersetzen durch ein Pseudonym)?	
9	**Treu und Glauben**	Die Verarbeitung personenbezogener Daten darf nicht unter Ausnutzung eines ungleichen Kräfteverhältnisses zwischen verantwortlicher Stelle und Betroffenem oder unter unbilliger Einwirkung auf den Betroffenen erfolgen und hat sich am Maßstab der Billigkeit und Loyalität zu orientieren.		