Checkliste ADITO CRM-Datenschutz nach EUDSGVO

Datenschutzfunktionen entsprechend Anforderung DS-GVO

Rechtmäßigkeit (DS-GVO Art. 5-11)	
Ist für jede Programmfunktion die Angabe einer gesetzlichen Erlaubnis (z.B. Vertrag, Einwilligung, Unternehmensinteresse) möglich?	☐
Sind Programmfunktionen ohne gesetzliche Erlaubnis per default deaktiviert?	☐
Können einzelne Datensätze und Datenfelder kategorisiert (z.B. Firma, Person, Kunde, Interessent, Mitarbeiter) und mit konkreten Angaben zur Zweckbestimmung (z.B. Vertragsabwicklung, Werbung) versehen werden?	☐
Kann die Wahrnehmung spezieller Betroffenenrechte wie Einwilligung, Widerspruch, Herkunft der Daten, Informationspflicht, Sperrkennzeichen je Datensatz abgespeichert werden?	☐
Datenminimierung (DS-GVO Art. 5, Art. 25, Art 32)	
Werden für jeden Zweck ausschließlich erforderliche Datenfelder verarbeitet?	☐
Werden für jeden Zweck ausschließlich erforderliche Datensätze verarbeitet?	☐
Ist eine Beschränkung der Verarbeitungsschritte zur jeweiligen Zweckerfüllung möglich?	☐
Können Anonymisierungs- und Pseudonymisierungs-Funktionen im Bedarfsfall (z.B. Statistik, Testzwecke) eingesetzt werden?	☐
Kann eine Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten über die Zugriffs-, und Rechteverwaltung erfolgen?	☐
Rechtverwaltung, Sicherheit der Verarbeitung (DS-GVO Art. 25, Art. 32)	
Können Sie Zugriffsrechte pro Benutzer auf Funktions-, Datenfeld oder Datensatzebene vergeben?	☐
Können Sie Lese-, Schreib- und Admin-Rechte getrennt vergeben?	☐
Lassen sich die vergebenen Rechte zu Kontrollzwecken exportieren?	☐
Kann die Vergabe von Passwörtern nur entsprechend Sicherheitsstandard erfolgen?	☐
Werden Zugriffe mit Änderungsfunktion protokolliert und lassen sich zu Kontrollzwecken anzeigen?	☐
Werden Nutzerkonten nach einer bestimmten Anzahl an Fehleingaben gesperrt und die Eingabe von Passwörtern wird verlangsamt?	☐

Betroffenenrechte (DS-GVO Art. 12 - 23)	
Auskunftspflicht: Können gespeicherte Daten zu einer Person vollständig in verständlicher Darstellung ausgedruckt werden?	☐
Können Sie gespeicherte Daten zu einer Person vollständig in maschinenlesbarer Form exportieren?	☐
Sperrpflicht: Lassen sich Datensätze und Datenfelder selektiv sperren, sodass sie nicht mehr verarbeitet werden können?	☐
Löschpflicht: Lassen sich Datensätze und Datenfelder selektiv manuell und durch automatische Regeln vollständig löschen?	☐
Können Informationspflichten bei Datenerhebungen, Datenweitergaben und Werbung bedarfsorientiert integriert werden, z.B. Hinweis Widerspruchsrecht?	☐
Berichtigungspflicht: Können alle gleichartigen Datenfelder einer Person über eine manuelle Selektion berichtigt werden?	☐
Auftragsverarbeitung (DS-GVO Art. 25, Art. 30, Art. 32)	
Verzeichnis Verarbeitungstätigkeiten (Art. 30 DS-GVO)	☐
Werden Unterstützungsfunktionen und Voreinstellungen für eine datenschutzkonforme Verarbeitung zur Verfügung gestellt?	☐
Können diese im Rahmen der Implementierung kundenbezogen festgelegt, konkretisiert und erweitert werden (u.a. Customizing, Anonymisierung, Verschlüsselung)? (Art.25 DSGVO)	☐
Sind die wesentlichen Sicherheitsmaßnahmen der Verarbeitung im Rahmen der Zusammenarbeit und Auftragsabwicklung in den vertraglichen Vereinbarungen u.a. in Form der TOMs festgelegt? (Art. 32 DS-GVO)	☐
Können Sie eine vollständige und verständliche Benutzer-, und Verfahrens-, und Datendokumentation zur Verfügung stellen?	☐
Bei Cloud-Verarbeitung: Ist eine vertragliche Datenschutz-Vereinbarung mit dem Cloudanbieter vorhanden?	☐

Sicherheit der Verarbeitung (DS-GVO Art. 32)	
Entspricht der Entwicklungsprozess den etablierten Standards sicherer Softwareentwicklung und ist qualitätszertifiziert?	☐
Werden ausschließlich Komponenten eingesetzt, wie Codebibliotheken, die dem Stand der Technik entsprechen?	☐
Lässt sich die Software gemäß den Vorgaben der BSI-Grundschutzkataloge konfigurieren?	☐
Bleiben Daten des Kunden entsprechend vertraglicher Vereinbarung ausschließlich auf der IT-Infrastruktur des Kunden?	☐
Bleiben Daten des Clouds-Kunden entsprechend vertraglicher Vereinbarung ausschließlich auf der IT-Infrastruktur des Kunden?	☐
Erfolgen Supportaufträge ausschließlich über ein gesichertes Supporttool (Verfahren) mit Dokumentation des Auftrags (Ticketsystem)?	☐
Verfügbarkeit: Werden Anwendungsfunktionen zur Anfertigung von Sicherheits-kopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß einem getesteten Konzept zur Verfügung gestellt?	☐
Verschlüsselung: Ermöglicht die Software eine gesicherte bzw. verschlüsselte Datenübertragung?	☐
Protokollierung: Erfolgt bei Datenübertragungen, Datenzugriffen und Änderungen eine entsprechende Protokollierung mit Auswertungsmöglichkeit?	☐
Wird die Nutzung von externen Systemschnittstellen mit zusätzlichen Sicherheitsmaßnahmen abgesichert?	☐