Sparkassenverband
Baden-Württemberg

Prüfungsstelle

Rolf Bose
Tel. 0711 127-77812
Rolf.Bose@sv-bw.de

28. August 2025/Bo

Erklärung zur Umsetzung des § 25 DSGVO in den Anwendungen „KPP-Prüfungstool“ und „KPP-Auswahltool“ zur Weitergabe an anfragende Sparkassen

Mit diesem Dokument geben wir Ihnen unsere Einschätzung zu Artikel 25 DSGVO. Damit wollen wir Ihnen als verantwortliche Stelle eine Hilfestellung geben, die erforderlichen Maßnahmen zu definieren und umzusetzen:

Die DSGVO insgesamt schützt lediglich die Verarbeitung von Daten natürlicher Personen. Dies ist bei KPP bei einer Teilmenge der Fall. Artikel 25 beschäftigt sich mit der Frage, ob eine Anwendung die Einhaltung der Rechte, die der Betroffene insbesondere aus Kapitel 3 der DSGVO (Artikel 12-23) im Rahmen einer rechtmäßigen Datenverarbeitung hat, durch den ordnungsgemäßen Einsatz der Anwendung sicherstellt. Dazu geben wir die folgenden Hinweise.
Da KPP lediglich eine Auswahl von Daten aus OSP beinhaltet, sind diese Pflichten primär in OSP zu erfüllen. Auch in OSP gilt, dass „Verantwortlicher“ im Sinne der DSGVO die Sparkasse ist. KPP verwaltet diese Daten für einen begrenzten Zeitraum im Rahmen der **rechtmäßigen** Verarbeitung. Die Frage wäre also, ob KPP über ein eigenes, zur Sicherstellung der DSGVO vom Hersteller entwickeltes, technisches System verfügen muss, um den Anforderungen aus Art. 25 DSGVO zu genügen. Ein solches System würde beispielsweise die Speicherdauer maschinell festlegen. Eine solche Anforderung lässt sich nach unserer Einschätzung aus Artikel 25 DSGVO nicht ableiten.

Begründung: Gem. Art. 25 DSGVO sind Maßnahmen abhängig von der „Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“. Es handelt sich nicht um eine verändernde Verarbeitung (Art). Es liegt eine eingeschränkte Datenmenge vor, die lediglich teilweise unter die DSGVO fällt (Umfang). Wir haben eine begrenzte Personengruppe, die eine, auch zeitlich eng eingegrenzte, zweckbestimmte Verarbeitung vornehmen darf (Umstände und Zweckbestimmung). Daher ist die „Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“ lediglich marginal. Anders ausgedrückt, die Wahrscheinlichkeit, dass sich aus dem sachgemäßen Einsatz von KPP ein Datenschutzvorfall für die Sparkasse ergibt, tendiert gegen Null. Art. 25 DSGVO verlangt unter Berücksichtigung dieser Punkte vom „Verantwortliche(n) sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen“. Die Verantwortliche ist die Sparkasse. Der Zeitpunkt der „Festlegung der Mittel“ ist die Entscheidung zur

Nutzung von KPP bis zur Implementierung der Anwendung. Der Zeitpunkt der eigentlichen Verarbeitung ist der konkrete Einsatz in der Sparkasse. Im Rahmen des Programmeinsatzes bestimmt die Sparkasse z. B. Zugriffsberechtigungen sowie Speicherort und -dauer der Daten. Der konkrete Einsatz wird durch technische (z. B. Zugriffsrechte) und organisatorische (z. B. Speicherdauer) Maßnahmen geregelt. Derartige, von der Sparkasse definierte Maßnahmen sind zur Erfüllung von Art. 25 DSGVO ausreichend, wenn sie angemessen ausgestaltet sind. Es steht der Sparkasse frei sich gem. Art. 25 DSGVO Ziffer 3 zertifizieren zu lassen. Wir halten das in Anbetracht der Bedeutung und des Risikos der Anwendung nicht für erforderlich.

Gez.: Susanne Pejak Rolf Bose