Prüfbericht

Personio – Produkt und Organisation

12.05.2022

Zusammenfassung

Die Prüfung des Unternehmens sowie der Software in Bezug auf die Verarbeitung von personenbezogenen Daten im Auftrag ergibt, dass die Personio GmbH datenschutzrechtlich gut aufgestellt ist und dass im Laufe des Jahres 2020 zahlreiche datenschutzrechtliche Prozesse bezüglich der Anforderungen der EU Datenschutz-Grundverordnung (DS-GVO) weiterentwickelt und optimiert worden sind. Das Datenschutzmanagementsystem der Personio GmbH ist bereits gut aufgesetzt und wird fortlaufend weiter strukturiert, ausgebaut und kontinuierlich optimiert. Die Personio GmbH hat sich zum Ziel gesetzt, das bereits bestehende Prinzip der fortlaufenden und anlasslosen datenschutzrechtlichen Überprüfung weiter auszubauen, um den Datenschutz in der Unternehmensentwicklung auch weiterhin stets mitzudenken. Aus diesem Grunde wurden 2020 mehrere interne Kontrollmechanismen eingeführt und es wurden regelmäßig anlasslose Security Days durchgeführt.

Das Produkt berücksichtigt die Anforderungen nach Privacy by Design und Privacy by Default nach Artikel 25 DS-GVO. Der Kunde, als verantwortliche Stelle, kann dabei zusätzliche Maßnahmen treffen und ist für die Umsetzung der entsprechenden Einstellungen innerhalb der Software selbst verantwortlich.

Weiterhin werden die Grundsätze der Verarbeitung von personenbezogenen Daten, insbesondere Transparenz, Treu und Glauben, Zweckbindung und Datenminimierung beachtet. Es werden grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet.

Der Kunde hat als Verantwortlicher, die Rechtmäßigkeit der Datenverarbeitung selbst sicherzustellen und kann den Umfang der Verarbeitung demgemäß über die Software selbst steuern. Zudem hat der Kunde die Möglichkeit, den Zugang

Bitkom Servicegesellschaft mbH

Ali Tschakari
Leiter Bitkom Consult
T +49 30 27576-280

a.tschakari@
bitkom-service.de

Albrechtstraße 10
10117 Berlin

Geschäftsführung
Anja Olsok

anhand eines granularen Berechtigungskonzepts selbst zu steuern. Adäquate datenschutzrechtliche Voreinstellungen sowie zusätzliche technische und organisatorische Maßnahmen stellen dabei sicher, dass Unbefugte keinen Zugriff auf die Software erhalten.

Des Weiteren hat die Personio GmbH ein Datenschutz- und IT-Sicherheitskonzept aufgestellt und weiterentwickelt und daraus technische und organisatorische Maßnahmen abgeleitet, welche den Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO genügen. Zudem sind bereits in der Vergangenheit entsprechende Prozesse implementiert worden, um die kontinuierliche Verbesserung der Prozesse und Prüfung und Weiterentwicklung dieser Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sicherzustellen.

Zudem ist in Vorbereitung einer zukünftigen ISO 27001-Zertifizierung für 2023 eine GAP-Analyse durchgeführt worden, bei der ebenfalls die gegenwärtigen internen Prozesse untersucht wurden. Die GAP-Analyse wurde durch externe Dienstleister durchgeführt, um eine unabhängige und objektive Kontrolle zu gewährleisten.

Die hieraus gewonnenen Erkenntnisse werden ausschließlich intern verwendet und bilden in diesem Zusammenhang einen integralen Bestandteil des Ausbaus des internen Informationsmanagementsystems.

Personio hat zudem sowohl innerhalb der Software als auch prozessual sichergestellt, dass der Kunde bei der Wahrung der Betroffenenrechte ausreichend unterstützt wird. Beispielhaft zu nennen sind hierzu insbesondere die Möglichkeiten der Datenlöschung, Sperrung, Auskunft und Berichtigung durch Self-Service sowie die Datenportabilität von Daten und Dokumenten der digitalen Personalakte.

Zusammenfassend kann festgehalten werden, dass die Software in ihrer Konzeption und Umsetzung die datenschutzrechtlichen Anforderungen an Entwicklung und Betrieb von Software erfüllt. Selbiges gilt für die Organisation und das Datenschutzmanagement in Bezug auf die Auftragsverarbeitung für die Kunden der Personio GmbH.

Zudem hat die Personio GmbH durch die Neuschaffung der Stelle eines Datenschutzkoordinators einen weiteren Schritt in Richtung Optimierung und Vereinheitlichung des internen Datenschutzmanagements getan.