

Prüfbericht

Personio – Produkt und Organisation

11.05.2018

Seite 1

Zusammenfassung

Die Prüfung der Software sowie des Unternehmens in Bezug auf die Verarbeitung von personenbezogenen Daten im Auftrag ergibt, dass die Personio GmbH die datenschutzrechtlichen Anforderungen der EU Datenschutz-Grundverordnung (DS-GVO) erfüllt. Das Datenschutzmanagement der Personio GmbH ist im Vergleich mit anderen Unternehmen mit vergleichbarer Größe und Alter bereits sehr ausgereift und wird derzeit weiter strukturiert und ausgebaut, um ein Datenschutz- und Informationssicherheitsmanagementsystem mit samt einem kontinuierlichen Verbesserungsprozess aufzubauen.

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

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

Dabei hat der Kunde die Rechtmäßigkeit der Datenverarbeitung selbst sicherzustellen und kann den Umfang der Verarbeitung entsprechend über die Software selbst steuern. Zudem hat der Kunde die Möglichkeit, den Zugang anhand eines granularen Berechtigungskonzepts selbst zu steuern. Entsprechende Voreinstellungen sowie zusätzliche technische und organisatorische Maßnahmen stellen dabei sicher, dass Unbefugte keinen Zugriff auf die Software erhalten.

Zudem hat Personio ein umfangreiches Datenschutz- und IT-Sicherheitskonzept aufgestellt und daraus entsprechende technische und or-

Bitkom Servicegesellschaft mbH

Tobias Göldner
Leiter Bitkom Consult
Datenschutzbeauftragter
T +49 30 27576-280

t.goeldner@
bitkom-service.de

Albrechtstraße 10
10117 Berlin

Geschäftsführung
Anja Olsok

organisatorische Maßnahmen abgeleitet, welchen den Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO genügen. Zudem sind entsprechende Prozesse implementiert, 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 sicherstellen.

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 wird somit festgestellt, dass die Software in ihrer Konzeption und Umsetzung den Anforderungen an Entwicklung und Betrieb von Software im Sinne der EU DS-GVO grundsätzlich erfüllt. Selbiges gilt für die Organisation und das Datenschutzmanagement in Bezug auf die Auftragsverarbeitung für die Kunden von Personio.



Tobias Göldner
Leiter Bitkom Consult
Datenschutzbeauftragter