Informationen zur Verarbeitung personenbezogener Daten gem. Art. 13 DSGVO im NOVIPLAN-Mitarbeiterportal und in der NOVIPLAN-App

1. Allgemeines

Die INTENSIO Software und Consulting GmbH bietet mit dem Mitarbeiterportal NOVIPLAN [e.portal] und der dazu passenden App NOVIPLAN [e.motion] eine komfortable Lösung, um sowohl sämtliche Dokumente der HR-Abrechnung als auch beliebige Mitarbeiterinformationen vollautomatisch und mit höchsten technischen Sicherheitsstandards digital zur Verfügung zu stellen.

2. Verantwortliche für die Datenbereitstellung und -verarbeitung

Verantwortlich für die Bereitstellung des Portals ist die

INTENSIO Software und Consulting GmbH
Ohiostraße 13
76149 Karlsruhe

Für die Verarbeitung der personenbezogenen Daten im Portal ist der jeweilige Arbeitgeber verantwortlich. Dies beinhaltet auch die Rechte der Betroffenen in Abschnitt 7.

3. Zweck der Datenverarbeitung und Maßnahmen zum Datenschutz

(1) Zweck der Datenverarbeitung ist die Bereitstellung von Lohn- und Gehaltsabrechnungen, Lohnsteuerbescheinigungen, SV-Meldebescheinigungen sowie u. U. Zeitnachweisen, Mitarbeiterinformationen oder weiteren Dokumentarten an die aus diesen Dokumenten hervorgehenden Empfänger in elektronischer Form. Es werden nur die für diese Dokumente vorgeschriebenen und relevanten personenbezogenen Daten verarbeitet.

(2) Weiterhin werden zum Zwecke der Anmeldung im Mitarbeiterportal bzw. in der App die folgenden, durch die jeweiligen Benutzer (Mitarbeiter) mitgeteilten Daten verarbeitet:

- Benutzername,
- Daten zur Authentifizierung,
- Daten zur Erfüllung des jeweiligen Dienstes.

(3) Angaben zur technischen Datenverarbeitung durch die Website:

- Eingehende Requests werden vom Webserver nicht protokolliert.
- Die Website verwendet aber Cookies. Bei Cookies handelt es sich um Textdateien, die im Internetbrowser bzw. vom Internetbrowser auf dem Computersystem des Benutzers gespeichert werden. Sie dienen insbesondere der Gewährleistung der Systemsicherheit. In Cookies werden der Benutzername, die Sitzungs-ID sowie einige wenige Benutzereinstellungen wie z. B. die zulässigen Authentifizierungsmodi verschlüsselt gespeichert.

- Darüber hinaus verwendet die Website die Browser-Sprache sowie die Version des Browsers und die Betriebssysteminformation.
- Bei der Benutzung der Funktionalität „Diesem Gerät vertrauen“ wird in der Datenbank gespeichert, wann die Zwei-Faktor-Authentifizierung zuletzt von einem bestimmten Browser durchgeführt wurde. Dabei wird nicht die IP-Adresse, sondern eine beim ersten Aufruf der Website generierte Device-ID, die in einem Cookie gespeichert wird, verwendet.
- Die Verarbeitung dieser Daten erfolgt zum Zweck des Verbindungsaufbaus (Ermöglichen der Nutzung der Website und App), der Systemsicherheit und der technischen Administration. Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen.

(4) Um sicherzustellen, dass nur Zugriffsberechtigte Einsicht in das Portal nehmen können, erfolgt das Login mit Benutzername und Passwort. Als zusätzliche Sicherheitsmaßnahme kann eine Zwei-Faktor-Authentifizierung eingerichtet werden. Ein automatischer Logoff aus dem Portal erfolgt nach einer vom Arbeitgeber festgelegten Zeit, in der Regel nach 15 Minuten. Hierdurch wird verhindert, dass Dritte bei Vergessen des manuellen Logouts ungehindert Zugriff auf die im Portal stehenden personenbezogenen Daten erhalten können.

(5) Vorgesetzte haben keinen Zugriff auf die Dokumente im Portal und kennen auch nicht die Zugangsdaten der Mitarbeiter.

4. App-Berechtigungen und Push-Nachrichten

(1) Durch die NOVIPLAN-App werden bestimmte Berechtigungen und Zugriffe auf das Smartphone des Benutzers angefordert. Diese dienen ausschließlich der Funktionsfähigkeit der App.

(2) Push-Benachrichtigungen sind Meldungen, die auf dem Gerätedisplay der Benutzer angezeigt werden, ohne dafür die NOVIPLAN-App zu öffnen. Möchten Benutzer Push-Benachrichtigungen erhalten, müssen sie das erlauben. Sie werden bei der Installation (Android) oder beim ersten Verwenden (iOS) der NOVIPLAN-App danach gefragt. Sämtliche Benachrichtigungen oder Zugriffsmöglichkeiten können im Einstellungsmenü nachträglich an- oder ausgeschaltet werden. INTENSIO verwendet für die Push-Benachrichtigungen die Dienste Firebase Cloud Messaging der Firma Google (Android) und Apple Push Notifications (iOS). Dabei generieren Firebase und Apple einen berechneten Schlüssel, der sich aus der Kennung der App und ihrer Geräte-Kennung zusammensetzt. Dieser Schlüssel wird auf der NOVIPLAN Push-Plattform mit den vom Benutzer gewählten Einstellungen hinterlegt, um eine gerätegenaue Zustellung der Push-Nachrichten entsprechend der Push-Konfiguration in der App zu gewährleisten. Die Firebase- bzw. Apple-Server können keinerlei Rückschlüsse auf die Anfragen von Nutzenden ziehen oder sonstige Daten ermitteln, die mit einer Person im Zusammenhang stehen. Firebase bzw. Apple dienen ausschließlich als Übermittler.

(3) Rechtsgrundlage für die Datenverarbeitung im Zusammenhang mit Push-Benachrichtigungen ist die Einwilligung der Benutzer gem. Art. 6 (1) lit. a DSGVO. Benutzer können die Push-Nachrichtenfunktion jederzeit deaktivieren, indem sie in den Einstellungen ihres Smartphones die NOVIPLAN-App auswählen und dort die Benachrichtigungsfunktion wunschgemäß konfigurieren.

5. Rechtsgrundlage der Verarbeitung

Die Datenverarbeitung erfolgt im Einklang mit den Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG). Die Rechtsgrundlage der Verarbeitung stellen die Erfüllung vertraglicher Pflichten (Art. 6 (1) lit. b DSGVO) und das berechtigte Interesse (Art. 6 (1) lit. f DSGVO) dar.

6. Empfänger der Daten

(1) Die Daten werden durch die Personalabteilung des Arbeitgebers und der jeweils für den Verarbeitungszweck zuständigen Abteilung verarbeitet. Die Bereitstellung der Plattform erfolgt dabei über die INTENSIO Software und Consulting GmbH, mit welcher ein Vertrag zur Auftragsverarbeitung geschlossen wurde.

(2) Die Datenverarbeitung erfolgt ausschließlich innerhalb der Bundesrepublik Deutschland. Eine Datenübermittlung in ein Land außerhalb der Europäischen Union / des Europäischen Wirtschaftsraums (sog. Drittland) findet nicht statt.

7. Speicherdauer

(1) Die Daten werden nur so lange gespeichert, wie dies zur Erfüllung des angegebenen Zwecks notwendig ist. Weiterhin bestehen ggf. gesetzliche Aufbewahrungspflichten, bis zu deren Ablauf Daten aufbewahrt werden müssen.

(2) Ausgeschiedene Mitarbeiter haben die Möglichkeit, nach ihrem Ausscheiden eine Zeit lang auf die im Portal bereitgestellten Daten zuzugreifen. Diese sog. Karenzzeit ist vom Arbeitgeber individuell festlegbar. Nach Ablauf der Karenzzeit wird der Zugriff auf das Portal deaktiviert.

8. Rechte der Betroffenen

Betroffene haben das Recht auf Auskunft (Art. 15 DSGVO) über ihre gespeicherten personenbezogenen Daten sowie auf Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) oder Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie das Recht, der Verarbeitung zu widersprechen (Art. 21 DSGVO), das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) und auf Beschwerde (Art. 77 DSGVO). Ansprechpartner für die Ausübung dieser Rechte ist der jeweilige Arbeitgeber.