iproplan®

Datenschutzrichtlinie und

Information für Betroffene gemäß Art. 13 und 14 DSGVO

Stand: 01.07.2023

Änderungsdokumentation

Dokument: Datenschutzrichtlinie

Verfasser: Andrea Schilling, DSB

Version: 2.0

Datum: 01. Juli 2023

Änderungs-nummer	Datum	Seite	Beschreibung / Änderung (neu)
1	15.06.2023	9	Pkt. 8: Umsetzung der DSGVO im Unternehmen: Technisch-organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32 DSGVO

Inhalt

1. Grundlage, Ziel, Verantwortlichkeit

Der Schutz personenbezogener Daten ist iproplan® ein wichtiges Anliegen. Die Verarbeitung der Daten von Mitarbeitern, Bewerbern und Projektbeteiligten erfolgt daher in Übereinstimmung mit den gültigen Rechtsvorschriften der EU-Datenschutz-Grundverordnung (DSGVO). Ziel ist die verantwortungsvolle Gewährleistung der Datensicherheit in allen Geschäftsprozessen.

Verantwortlicher i.S. d. Datenschutzes:

iproplan® Planungsgesellschaft mbH
vertreten durch Geschäftsführer Dipl.-Ing. Jörg Thiele
Bernhardstr. 68, 09126 Chemnitz
info@iproplan.de, Tel. 0371/5265-0

2. Prinzipien für die Verarbeitung personenbezogener Daten

Als personenbezogene Daten im Sinne der Richtlinie gelten alle Informationen, die sich auf eine (identifizierte oder identifizierbare) natürliche Person beziehen, so z. B. Namen, Anschriften, Geburtsdaten, Mailadressen, Telefonnummern, aber auch Kennnummern aller Art (Krankenversicherung, Sozialversicherung, Personalausweis, Matrikelnummer, …), Bankdaten, Angaben über persönliche Merkmale und Hintergründe u.v.m.

Für den Umgang mit diesen Daten gelten die Grundsätze der DSGVO (vgl. insb. Art. 5 Abs. 1 sowie Art. 9):

- Rechtmäßigkeit und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Alle Datenverarbeitungsvorgänge im Unternehmen werden dokumentiert (Verzeichnis der Verarbeitungstätigkeiten, vgl. Art. 30 DSGVO); neue Vorgänge werden einer Risikoprüfung unterzogen (ggf. Datenschutzfolgenabschätzung gem. Art. 35 DSGVO). Bei Verarbeitungstätigkeiten im Auftrag von **iproplan®** werden Verträge zur Auftragsdatenverarbeitung abgeschlossen; alle Auftragnehmer werden hinsichtlich der Einhaltung der Vorgaben zur Datensicherheit überprüft (vgl. Art. 29 DSGVO).

3. Umgang mit Projektbeteiligten-/Kunden-/Interessenten-/Partnerdaten

Personenbezogene Daten von Projektbeteiligten, Kunden, Interessenten und Partnern werden bei iproplan® wie folgt verarbeitet:

Zwecke und Rechtsgrundlagen:
Die Datenverarbeitung im Projektkontext bzw. von Kunden-/Interessenten- und Partnerdaten erfolgt in der Regel
-zur Erfüllung und Abwicklung von Verträgen und vorvertraglichen Maßnahmen,
-zur Erfüllung rechtlicher Verpflichtungen von **iproplan®** oder
-zur Wahrung berechtigter Interessen von **iproplan®**, z.B. zur Bewerbung um Neuaufträge bei Vertragspartnern oder bei Dritten (Referenzen) (vgl. Art 6 Abs. 1 insb. b, c, f DSGVO).
Eine davon abweichende Rechtsgrundlage ist nur gem. DSGVO möglich.

Kategorien personenbezogener Daten, die verarbeitet werden:
Verarbeitet werden Daten von Mitarbeitern des jeweiligen Vertragspartners/Projektbeteiligten, die dieser zur Abwicklung des Vertrages einsetzt, so hauptsächlich Name, Vorname, ggf. akademischer Grad, Berufsbezeichnung, Stellung im Unternehmen, Vertretungsbefugnis, dienstl. Adresse, dienstl. Telefonnummer, dienstl. Mobilfunknummer, dienstl. E-Mail-Adresse.

Kategorien von Empfängern der personenbezogenen Daten:
- eigene Mitarbeiter von iproplan®, die zur Abwicklung von Verträgen/Projekten eingesetzt werden
- ggf. Mitarbeiter von Nachunternehmern oder anderen Projektbeteiligten, mit denen iproplan® zur Abwicklung von Verträgen/Projekten in Kontakt steht
- ggf. Mitarbeiter potenzieller Auftraggeber, bei denen sich iproplan® um Neuaufträge bewirbt
- ggf. Mitarbeiter von Aufsichtsbehörden und Wirtschaftsprüfern, mit denen iproplan® zur Erfüllung seiner gesetzlichen Verpflichtungen in Kontakt steht
- ggf. Mitarbeiter von Berufshaftpflichtversicherungen, Rechtsanwaltskanzleien, Gerichten, mit denen iproplan® zur Durchsetzung seiner Interessen in Kontakt steht

Quelle der personenbezogenen Daten:
Die Daten stammen i.d.R. aus der Kommunikation mit dem Vertragspartner selbst, d.h. sind vom Vertragspartner selbst zur Verfügung gestellte Daten. Darüber hinaus werden ggf. öffentlich zugängliche Informationen aus dem Internetauftritt des jeweiligen Partners genutzt.

Automatisierte Entscheidungsfindung/Profiling:
findet nicht statt

Datenübermittlung in Drittland:

findet i.d.R. nicht statt; falls zur Projektabwicklung erforderlich, wird der Betroffene informiert

Dauer der Datenspeicherung:

Die personenbezogenen Daten werden, jeweils bezogen auf Vertragsverhältnisse, gespeichert bis zum Eintritt der Verjährung von Mängelansprüchen des Auftraggebers von **iproplan®** gegen **iproplan®**, mindestens jedoch 10 Jahre zum Jahresende, in dem **iproplan®** die Schlussrechnung an seinen Auftraggeber gestellt hat.

Eine über diesen Zeitraum hinausgehende Speicherung oder Verarbeitung von Projektbeteiligten-/Kunden-/Partnerdaten, die zur Durchsetzung, Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, bleibt unbenommen.

4. Umgang mit Bewerberdaten

Personenbezogene Daten von Bewerbern werden bei **iproplan®** wie folgt verarbeitet:

Zwecke und Rechtsgrundlagen:
Die Erhebung und Verarbeitung personenbezogener Bewerberdaten erfolgt ausschließlich zweckgebunden für die Besetzung von Stellen innerhalb des Unternehmens, d.h. zur Anbahnung von Arbeitsverhältnissen (i.d.R. Art. 6 Abs. 1 b).
Eine davon abweichende Rechtsgrundlage ist nur gem. DSGVO möglich.

Kategorien personenbezogener Daten, die verarbeitet werden:
Im Zuge der Bewerbung werden von uns die folgenden Daten verarbeitet und in unserem internen Bewerbermanagementsystem gespeichert: Name, Vorname; Adresse; Telefonnummer; E-Mail-Adresse; eingesandte Bewerbungsunterlagen (Bewerbungsschreiben, Lebenslauf, Zeugnisse, Zertifikate etc.).

Kategorien von Empfängern der personenbezogenen Daten:
Die Daten werden grundsätzlich nur an die für das konkrete Bewerbungsverfahren zuständigen innerbetrieblichen Stellen und Fachabteilungen des Unternehmens weitergeleitet.

Quelle der personenbezogenen Daten:
Der Bewerber stellt seine Daten selbst zur Verfügung.

Automatisierte Entscheidungsfindung/Profiling:
findet nicht statt

Datenübermittlung in Drittland:
findet nicht statt

Dauer der Datenspeicherung:
Die Löschung von Bewerberdaten erfolgt spätestens 6 Monate nach Abschluss des Bewerbungsverfahrens. Dies gilt nicht, sofern gesetzliche Bestimmungen einer Löschung entgegenstehen, die weitere Speicherung zum Zwecke der Beweisführung erforderlich ist oder der Bewerber einer längeren Speicherung ausdrücklich (schriftlich oder elektronisch) zugestimmt hat.

5. Umgang mit Mitarbeiterdaten

Der Umgang mit personenbezogenen Daten von Mitarbeitern ist in **Anlage 4 der iproplan®-Betriebsvereinbarung** detailliert geregelt. Das Unternehmen stellt sicher, dass alle Mitarbeiter diese Information erhalten.

6. Betroffenenrechte

Der Betroffene hat ein Recht auf Auskunft über die von ihm verarbeiteten personenbezogenen Daten, ebenso wie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten (vgl. Art. 15, 16, 17, 18, 20 DSGVO).

Ferner steht dem Betroffenen ein Beschwerderecht bei der Aufsichtsbehörde zu (Sächsischer Datenschutzbeauftragter, Devientstr. 1, 01067 Dresden, saechsdsb@slt.sachsen.de, Tel. +49(351)4935401).

Wir empfehlen, Anfragen und Beschwerden immer zunächst an unseren betrieblichen Datenschutzbeauftragten zu richten (Kontaktdaten Abschnitt 7).

7. Der Datenschutzbeauftragte

Das Unternehmen bestellt nach Maßgabe der DSGVO einen betrieblichen Datenschutzbeauftragten (DSB).
Schwerpunktmäßig überwacht dieser die Einhaltung der datenschutzrechtlichen Vorschriften sowie den datenschutzkonformen Umgang mit personenbezogenen Daten im Unternehmen gem. Art 39 DSGVO.

Der betriebliche Datenschutzbeauftragte ist darüber hinaus Ansprechpartner für betroffene Personen und Mitarbeiter zu allen Vorgängen im Zusammenhang mit der Verarbeitung ihrer Daten und der Wahrnehmung ihrer Rechte.

Kontaktdaten DSB:

iproplan® Planungsgesellschaft mbH
Betrieblicher Datenschutzbeauftragter
Bernhardstr. 68
09126 Chemnitz
Tel.: 0371/5265-0; E-Mail: dsb@iproplan.de

8. Umsetzung der DSGVO im Unternehmen: Technisch-organisatorische Maßnahmen für die Gewährleistung der Sicherheit der Verarbeitung (gem. Art. 32 DSGVO)

Das Unternehmen stellt den notwendigen organisatorischen, technischen und personellen Rahmen, um die ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes gem. DSGVO zu gewährleisten.

I Vertraulichkeit

Zugangskontrolle

- Manuelles Schließsystem mit Sicherheitsschlössern
- Zentrale Schlüsselregelung: Schlüsselausgabe und Personenkontrolle am Empfang
- Chipkarten-/Transponder-Schließsystem in ausgewählten Bereichen
- Protokollierung der Besucher/Besucherbuch
- sorgfältige Auswahl von Service- und Sicherheitspersonal (z.B. Reinigung)
- Systemauthentifikation mit Benutzername/Passwort
- Einsatz von Virtual Private Network-Technologie (VPN)
- Einsatz von Anti-Viren-Software → zentral gesteuerte Anti-Virus-Software auf den Workstations und Servern mit EDR und NGAV / Zentrale Prüfung aller E-Mails mit Microsoft Defender für Office 365
- Einsatz einer Software-Firewall auf den Workstations und Servern
- Einsatz einer Hardware-Firewall → zentraler Firewall Cluster mit Network Protection, Web Protection, Webserver Protection
- Verpflichtung von Mitarbeitern, Praktikanten, Freelancern auf das Datengeheimnis mündlich oder via Online-Schulung (Proliance)
- besondere Verschlussmaßnahmen bei sensiblen personenbezogenen Daten, z. B. Personal

Datenträgerkontrolle

- Verschlüsselung von mobilen Datenträgern (z.B. USB-Stick, Smartphone, Tablett, Externe Festplatte, Laptop)

→Laptops, mobil genutzte Rechner (Bitlocker)

- Einsatz von zentraler Smartphone-Administrations-Software (z .B. zum externen Löschen von Daten) → MDM
- Schreib-/Leseschutz → besonders geschützte Laufwerke sind nur zugänglich für zentral ausgewählte Nutzer: Archivlaufwerk (nur Leserechte), Personallaufwerk, Abrechnung/Buchhaltung, Marketing/Ausschreibungen mit Firmeninformationen und Mitarbeiterlebensläufen

Speicherkontrolle

- Erstellung eines Berechtigungskonzepts →Zugriffsregelung in IT je nach Mitarbeiterkategorie
- anlassbezogene Löschung von nicht mehr benötigten Daten

- feste Richtlinien für die Dateiorganisation via Arbeitsanweisung im Qualitätsmanagementhandbuch (QMH)
- revisionssichere E-Mail-Archivierung
- keine Installationen ohne Admin-Rechte möglich
- datenschutzfreundliche Voreinstellungen in Systemen und Programmen

Benutzerkontrolle

- Benutzerprofile lt. Tätigkeitsgruppe zur Verteilung von Software, zur Festlegung von Zugriffsrechten
- Erstellung eines Berechtigungskonzepts → zentrale Zugriffsregelung in IT nach Mitarbeiterkategorie
- differenzierte Zugriffsregelung (need-to-know-Prinzip) → s. zentrale Zugriffsregelung
- Netzwerkzugangskontrolle Network Access Control (NAC) vor Implementierung

Zugriffskontrolle

- Verwaltung der Rechte durch Systemadministrator
- Nur Einsatz der notwendigen Anzahl an Administratoren
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ordnungsgemäße Vernichtung von Datenträgern über zertifizierte Entsorger
- sichere Aufbewahrung von Datenträgern →Aufbewahrung von Datensicherung zusätzlich an sicherem, externem Ort
- Protokollierung der Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern
- Einsatz von Dienstleistern zur Entsorgung (nach Möglichkeit mit Zertifikat)
- verschließbare Aktenschränke
- Festlegung von Aufbewahrungsfristen für gespeicherte Daten unter Angabe von Mindestaufbewahrungszeiträumen lt. Empfehlung der Ingenieurkammer Sachsen; betriebsinterne Regelung lt. Betriebsvereinbarung (Anlage 4) für Mitarbeiter- und Bewerberdaten
- differenzierte Archivbestände →Ordnungssystem / verschlüsselte Inventarliste

II Integrität

Übertragungskontrolle

- Einrichtung von Standleitungen bzw. VPN-Tunneln
- Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen von Informationen im DATEV
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen → Empfängerkontrolle: Postausgangsbuch, E-Mail-Archivierung

Eingabekontrolle

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Einsatz einer E-Mail-Signatur zur Identifikation des Signaturerstellers

Transportkontrolle

- sichere Transportbehälter/-verpackungen
- Anforderungen von Quittungen
- Verschlüsselung von mobilen Datenträgern
- Versand von E-Mail-Anhängen passwortgeschützt oder via verschlüsseltem Archiv bei sensiblen Daten (Teaming Box)
- sicheres Internetprotokoll - Hypertext Transfer Protocol Secure (https)

III Verfügbarkeit und Belastbarkeit

Wiederherstellbarkeit

- regelmäßige Testung der Datenwiederherstellbarkeit
- Backup- & Recoverykonzept vorhanden
- Protokollierung und Auswertung von Störungsvorfällen →Monitoring der IT-Infrastruktur
- Einsatz von zentralem Netzwerk

Zuverlässigkeit

- Anzeige von Fehler- und Störmeldungen in den IT-Systemen →Monitoring der IT-Infrastruktur
- externe und interne technische Sicherheitsanalysen (IT-Systeme, Infrastruktur oder Anwendungen) → vierteljährliche Überprüfung des Microsoft Tenants, zyklische Prüfung der Hybrid - AD
- Einsatz von Intrusion-Detection-Systemen (Angriffserkennung) → Firewall / Antivirus-Programm
- Test- und Freigabeverfahren z. B. bei Einführung neuer Soft- oder Hardware
- Penetrationstests (vertiefte Feststellung von Angriffen in die Infrastruktur) vor Implementierung
- Auswertung von Aufzeichnungen und Protokolle der Detektionsmaßnahmen
- Sensibilisierungen der Mitarbeiter zum Datenschutz und/oder -sicherheit

Datenintegrität

- Erstellung eines Sicherheitskonzepts vor Implementierung

Auftragskontrolle

- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten
- schriftliche Datenschutzweisungen Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag)
- Möglichkeit der Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

Verfügbarkeitskontrolle

- Sicherstellung unterbrechungsfreier Stromversorgung
- Geräte zur Überwachung der Temperatur in den Serverräumen
- Serverräumen mit Klimaanlage / Abluftanlage
- Schutzsteckdosenleisten in den Serverräumen

- Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in Serverräumen
- Serverräume oberhalb der Wassergrenze im Falle eines Hochwassers
- Aufbewahrung von Datensicherung an einem sicheren, externen Ort

Trennbarkeit

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- zentrale Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem
- Erstellung eines Berechtigungskonzepts → s. zentrale Regelung der Zugriffsberechtigungen

IV Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Software-Lösung für Datenschutz-Management im Einsatz (Proliance)
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz verfügbar für alle Mitarbeiter (vgl. Betriebsvereinbarung, Intranet)
- Regelmäßige technische Überprüfung der IT-Sicherheit im Unternehmen durch IT-Abteilung (Tests, Stichproben)
- Interner DSB mit regelmäßigen Schulungsintervallen
- Mitarbeiterschulungen und Sensibilisierung im Onboarding-Prozess
- Bei Bedarf: Datenschutz-Folgenabschätzungen, Risikoanalysen, Auftragsverarbeitungsverträge
- Implementierung des Datenschutzes in bestehendes Qualitätsmanagement und kontinuierliche Fortschreibung der Prozesse

Alle Datenschutz-Prozesse sowie technisch-organisatorischen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben in allen Bereichen sind Bestandteil interner und externer Audits im Rahmen des **iproplan®** Qualitätsmanagements und werden kontinuierlich dokumentiert, überprüft und angepasst.