FORPLANER

ANLAGE ZU DEM SAAS-VERTRAG DER FORPLANER GMBH: VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG ZWISCHEN FORPLANER GMBH, RHEINLANDDAMM 201, 44139 DORTMUND („AUFTRAGNEHMER“) UND DEM KUNDEN („AUFTRAGNEHMER)

STAND: 05/2026

PRÄAMBEL

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Die vorliegende Bedingung konkretisiert als Vereinbarungsbestandteil die zwischen dem Auftragnehmer und Auftraggeber getroffene Vereinbarung.

§ 1 BEGRIFFSBESTIMMUNGEN

1. Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die alleine oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

2. Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

3. Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

4. Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

5. Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

6. Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 ANGABE DER ZUSTÄNDIGEN DATENSCHUTZ-AUFSICHTSBEHÖRDE

1. Die zuständige Aufsichtsbehörde ist die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

2. Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 VERTRAGSGEGENSTAND

1. Der Auftragnehmer erbringt für den Auftraggeber SaaS-Leistungen („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung sowie den Anlagen des Hauptvertrages). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

2. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

3. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

4. Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 WEISUNGSRECHT

1. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragneh-

mer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

2. Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus der Vereinbarung zur Auftragsverarbeitung. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

3. Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

4. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 ART DER VERARBEITETEN DATEN, KREIS DER BETROFFENEN

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf folgende Daten:

a) Lizensierte Nutzer des Programmsystem:
   Art der Daten: Vor- und Nachname, E-Mail-Adresse.
   Kategorie: Normale personenbezogene Daten (Art. 4 Nr. 1 DSGVO). Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO): Nein.

b) Betroffene Personen der vorbereitenden Datensätze (z. B. aus Einwohnermeldedaten oder ähnlichen Quellen):
   Art der Daten: Auswertungsjahr, Alter / Geburtsdatum, Geschlecht, Modellzone / Wohnort, Bewegungsart, Quellort / Zielort, Geburtsdatum / Alter der Mutter; optional: Staatsangehörigkeit, Bereichsart (Sonderadresse). Verarbeitung: Diese Datensätze werden nur vorübergehend zur Vorbereitung des Programmsystems verarbeitet (Anonymisierung / Pseudonymisierung). Anschließend erfolgt eine Übersetzung in Kohortendaten (aggregierte Gruppen). In der Software wird ausschließlich mit anonymisierten Kohortendaten gearbeitet. Kategorie: Während der Vorbereitungsphase: Personenbezogene Daten (teilweise anonymisiert / pseudonymisiert).
   Nach Übersetzung in Kohorten: Anonymisierte Daten kein Personenbezug mehr → DSGVO findet keine Anwendung, Erwägungsgrund 26). Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO): Nein.

§ 6 SCHUTZMASSNAHMEN DES AUFTRAGNEHMERS

1. Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 1** aufgeführten Maßnahmen der

a) Zutrittskontrolle;
b) Zugangskontrolle;
c) Zugriffskontrolle;
d) Weitergabekontrolle;
e) Eingabekontrolle;
f) Auftragskontrolle;
g) Verfügbarkeitskontrolle;
h) Trennungskontrolle.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3. Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS

1. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des

Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren.
Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

2. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.
3. Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.
4. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO liegt.
5. Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.
6. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
7. Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.
8. An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 KONTROLLRECHTE DES AUFTRAGGEBERS

1. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig in angemessenen Abständen von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen, die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.
2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.
3. Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.
4. Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 EINSATZ VON SUBUNTERNEHMERN

1. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt: Forplaner Softwareentwicklungsgesellschaft mbH, Rheinlanddamm 201, 44139 Dortmund (Für die Leistungen: Softwareentwicklung) sowie Schulten Stadt- und Raumentwicklung, Rheinlanddamm 201, 44139 Dortmund (Für die Leistungen: Datenaufbereitung, Ersteinrichtung, Prognoserechnungen und Datenpflege). Für die vorbezeichneten Subunternehmer gilt die Genehmigung des Auftraggebers als erteilt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zum Austausch bestehender Subunternehmer und zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis") befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und der Auftraggeber dem nicht widerspricht, obschon der auf sein Widerspruchsrecht hingewiesen wurde. Für einen begründeten Widerspruch hat der Auftraggeber sachliche Gründe vorzutragen. Liegt ein berechtigter Grund

vor, ist der Auftragnehmer zur sofortigen Beendigung der Vereinbarung berechtigt.

2. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

3. Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 ANFRAGEN UND RECHTE BETROFFENER

1. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

2. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 HAFTUNG

1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

2. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 BEENDIGUNG DES HAUPTVERTRAGS

1. Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger des Auftraggebers zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

2. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

3. Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 SCHLUSSBESTIMMUNGEN

1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB und/ oder Vermieterpfandrecht hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

3. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

4. Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

ANLAGE 1 ZU DER VEREINABRUNG ZUR AUFTRAGSVERARBEITUNG. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN DER FORPLANER GMBH, RHEINLANDDAMM 201, 44139 DORTMUND.

Verantwortlicher: Marc Schulten
Datenschutzbeauftragter: Marc Schulten
Stand: 05/2026

1. KONKRETISIERUNG DER EINZELMAßNAHMEN AM UNTERNEHMENSSITZ

A) MAßNAHMEN ZUR ZUTRITTSKONTROLLE

Anforderung: Es ist zu gewährleisten, dass Bereiche mit Datenverarbeitungssystemen von Unbefugten nicht betreten werden können. **Umsetzung:** Das Betriebsgebäude ist mit einem elektronischem Schließsystem gesichert. Der Zutritt für Besucher ist über die Anmeldung möglich. Der IT-Raum ist über einen elektronischen Zugang gesichert.

B) MAßNAHMEN ZUR ZUGANGSKONTROLLE

Anforderung: Es ist zu gewährleisten, dass Datenverarbeitungssysteme von Unbefugten nicht genutzt werden können. **Umsetzung:** Die Bearbeitung von personenbezogenen Daten erfolgt auf gesicherten Desktoprechnern. Der Zugang zu den Räumen ist über ein elektronisches Schließsystem gesichert. Jeder Einzelplatzrechner ist Passwortgeschützt bzw. über biometrische Sicherungssysteme gesichert. Die Daten werden auf einem NAS mit verschlüsselter Datenablage gesichert. Als DMS kommt Paperoffice zum Einsatz.

C) MAßNAHMEN ZUR ZUGRIFFSKONTROLLE

Anforderung: Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Erfassung, Verarbeitung und Nutzung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. **Umsetzung:** Das Datenverarbeitungssystem verfügt über ein rollenbasiertes Zugriffskonzept (RBAC). Über Paperoffice werden Anmeldung, Anlage, Änderung und Löschung dokumentiert. Zugangsdaten zu geschützten Datenbankbereichen hat nur die Geschäftsführung. Logfiles dokumentieren die Zugriffe auf sensible Daten.

D) MAßNAHMEN ZUR WEITERGABEKONTROLLE

Anforderung: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports nicht unbefugt gelesen, verändert oder gelöscht werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung von personenbezogenen Daten erfolgt bzw. vorgesehen ist. **Umsetzung:** Sensible Daten können über unsere Cloud (Nextcloud) passwortgeschützt ausgetauscht werden. Eine alternative Datenübergabe ist über USB-Stick mit Verschlüsselung und Passwortschutz möglich.

E) MAßNAHMEN ZUR EINGABEKONTROLLE

Anforderung: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht worden sind. **Umsetzung:** Datenzugriffe auf Paperoffice werden über Logfiles dokumentiert. So wird die Nachvollziehbarkeit von Änderungen in Dokumenten und Systemen gesichert.

F) MAßNAHMEN ZUR AUFTRAGSKONTROLLE

Anforderung: Es ist zu gewährleisten, dass die Verarbeitung personenbezogener Daten, nur gemäß Auftrag und nur entsprechend der Absprache mit dem Auftraggeber erfolgt. **Umsetzung:** Personenbezogene Daten des Auftraggebers werden nur nach Absprache mit dem Auftraggeber verarbeitet. Vereinbarungen erfolgen schriftlich (per E-Mail) und sind mit dem Projektleiter oder dem Geschäftsführer abzuschließen. Mit Dienstleistern werden Vereinbarungen gem. Art. 28 DSGVO abgeschlossen. Wichtige Weisungen werden schriftlich dokumentiert.

G) MAßNAHMEN ZUR VERFÜGBARKEITSKONTROLLE

Anforderung: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. **Umsetzung:** Für das NAS erfolgt eine tägliche Sicherung. Alle Datenverarbeitungssysteme sind über USV-Anlage abgesichert. Das Gebäude und alle Räume sind nach aktuellen Vorgaben mit Feuerlöscher und Brandmelder ausgestattet. Sämtliche DV-Systeme verfügen über eine aktuelle Antivirensoftware und eine Netzwerk-Firewall bzw. eine Personal Firewall auf Endgeräten. Für alle DV-Systeme erfolgen regelmäßige Updates von Betriebssystemen und Anwendungen.

H) MAßNAHMEN ZUR ZWECKBESTIMMUNG / GETRENNTEN VERARBEITUNG

Anforderung: Es ist zu gewähr-leisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. **Umsetzung:** Sämtliche Dateizugriffe in Paperoffice werden protokolliert. Das Löschen der Versionshistorie kann nur durch den Administrator / Geschäftsführer erfolgen. Es besteht ein differenziertes Rechtekonzept, das auf der Unternehmensstruktur basiert (Unternehmensleitung / Administration, Projektleitung, wiss. Mitarbeiter, studentische Hilfskräfte). Die Projektleitung hat Zugriff auf sämtliche Projektdaten (außer verschlüsselte Dateien). Wissenschaftliche Mitarbeiter haben Zugriff auf den Arbeitsbereich (exkl. Projektmanagement + verschlüsselte Dateien). Studentische Hilfskräfte haben eingeschränkte Rechte (teilw. nur lesend).

Alle Mitarbeiter sind in das Rechtesystem eingeführt und haben mit dem Arbeitsvertrag eine Verpflichtungserklärung auf Vertraulichkeit, Verschwiegenheit und die Einhaltung des Datenschutzes gemäß EU DSGVO unterschrieben. Der Zugriff auf verschlüsselte Daten ist eingeschränkt und nur dem eingewiesenen Mitarbeiter möglich.

2 INFORMATIONEN ZUM BEAUFTRAGTEN RECHENZENTRUM

Die ForplanerTools werden in der jeweils aktuellen Version als cloudbasierte Anwendung bereitgestellt. Hierzu gehören die Bereitstellung der nötigen Rechenkapazitäten, Speichermedien und die erforderliche Infrastruktur an einem zertifizierten Rechenzentrumsstandort. Unser Rechenzentrum: netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe. Zertifizierung: ISO 9001, ISO 14001, ISO 27001, ISO 27701 (Dokumentation unter: https://www.netcup.com/de/ueber-netcup/zertifizierungen).

A) DATENSCHUTZ UND ZUGRIFFSSICHERHEIT

Vertragsverhältnis und Datenverarbeitung: Der Betrieb erfolgt auf virtuellen Servern in Deutschland, basierend auf einem Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO. Eine Datenübermittlung an Dritte oder in Drittländer erfolgt nicht. Verarbeitete personenbezogene Daten: Vor- und Nachname, E-Mail-Adresse, Nutzername (optional), Rolleninformationen, IP-Adresse, Nutzungsverhalten. Zugriff auf personenbezogene Daten erfolgt ausschließlich im Kontext der Authentifizierung, Rechtevergabe oder Systemkommunikation. Alle Verarbeitungsvorgänge sind gemäß Datenschutzprinzipien nachvollziehbar dokumentiert. **Verarbeitungszwecke und Maßnahmen:** Authentifizierung: Nutzung von personenbezogenen Daten zur Anmeldung und Rechtevergabe innerhalb der Software. Zugriffsprotokollierung: Speicherung von IP-Adresse, Browseragent, Fingerprint zur Angriffserkennung. Löschung nach max. 6 Monaten, Verlängerung nur bei Sicherheitsvorfall. Archivierung: Anonymisierung personenbezogener Daten bei Archivierung oder Löschung. Löschung: Vollständige Löschung oder Anonymisierung von Accounts gemäß gesetzlicher Fristen.

B) TECHNISCHE SCHUTZMAßNAHMEN GEMÄß BSI-GRUNDSCHUTZ (APP, CON, OPS, NET, SYS)

Kryptografische Absicherung: Kommunikation ausschließlich über HTTPS mit TLS 1.2 / 1.3. Adminzugänge ausschließlich über SSH (Ed25519 oder RSA-Schlüssel, keine Generalschlüssel). Verschlüsselung der Speichermedien mit AES-XTS. Interne Systemkommunikation mit AES256-CBC und RSAES-OAEP verschlüsselt. **Backup-Strategie:** Tägliche automatische Cloud-Backups. Monatliche manuelle Offline-Sicherungen. Quartalsweise Prüfung der Wiederherstellbarkeit. **Zugriffsmanagement:** Zugriff auf Webapplikation via OAuth 2.0. Optionale Zwei-Faktor-Authentifizierung für Standardnutzer, verpflichtend für Admins. Datenbankzugriff verschlüsselt via SCRAM-SHA256. Rollenbasierter Zugriff auf Datenmandanten und Module. **Patch- und Update-Management:** Sicherheitsupdates: automatische Installation innerhalb von 24 Stunden. Manuelle Updates: innerhalb von 72 Stunden. Permanentes Monitoring auf sicherheitsrelevante Schwachstellen. **Systemschutz und Bedrohungserkennung:** Firewall-Schutz durch restriktive Portfreigaben. OWASP-10-konforme Absicherung der Webschnittstellen. Verhaltensbasierte Angriffsabwehr durch Threat Detection Engine.

C) MONITORING, AUDITS UND OPERATIVE SICHERHEITSMAßNAHMEN

Systemmonitoring: Laufende Überwachung von Ressourcen (CPU, Speicher, Speicherplatz), Status von Updates und Backups. **Logfile-Analyse:** Automatisierte Auswertung sicherheitsrelevanter Logs. **Software-Lieferkette:** Monatlicher Audit von verwendeten Bibliotheken und Containern (inkl. CVE-Abgleich). **Systemaudit:** Halbjährliches Audit des Gesamtsystems inkl. Abgleich mit dem BSI-Grundschutzkompendium. **Penetrationstests & Recon:** Durchführung von Tests zur Schwachstellenidentifikation **Entwicklung nach Security-by-Design:** Integration von Datenschutz-Folgeabschätzungen, Threat Modeling und Sicherheitsreviews bei Weiterentwicklungen.