

AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 DSGVO

Version 1.0 – Stand: 12.10.2026

zwischen dem Verantwortlichen

Der Kunde im Sinne der Allgemeinen Geschäftsbedingungen (AGB) des
Auftragnehmers, für den der jeweilige Workspace im Sinne von Ziffer 1.5 der AGB
eingerichtet wird

– nachfolgend „Auftraggeber“ genannt –

und dem Auftragsverarbeiter

Kunststoff Information GmbH

– nachfolgend „Auftragnehmer“ genannt –

– nachfolgend zusammen „Parteien“ genannt –

PRÄAMBEL

Dieser Auftragsverarbeitungsvertrag wird nicht als Individualvertrag abgeschlossen, sondern über die Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers einbezogen. Der Auftragnehmer betreibt eine SaaS-Plattform, auf der der Auftraggeber einen oder mehrere Workspaces im Sinne von Ziffer 1.5 der AGB einrichten kann. Der Vertrag kommt für jeden Workspace gesondert mit dessen Einrichtung zwischen dem Auftraggeber (Verantwortlicher) und dem Auftragnehmer (Auftragsverarbeiter) zustande. Der Beitritt weiterer Nutzer zu einem bestehenden Workspace, Einladungen, der Abschluss oder die Änderung eines Abonnements sowie die Buchung zusätzlicher Seats begründen keinen weiteren Auftragsverarbeitungsvertrag. Einer gesonderten Unterzeichnung bedarf es nicht.

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1. GEGENSTAND

- 1.1 Gegenstand dieses Auftragsverarbeitungsvertrags ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.
- 1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in der Anlage unter der Ziffer 1.

2. ORT DER DATENVERARBEITUNG

Die vertraglich vereinbarte Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern sich aus der Anlage nichts anderes ergibt. Vor Verlagerung der Verarbeitung in ein Drittland informiert der Auftragnehmer den Auftraggeber in Textform (bspw. per E-Mail). Der Auftraggeber kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch den Auftragnehmer in schriftlicher Form oder in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein begründeter Widerspruch vor, der vom Auftragnehmer nicht durch zumutbare Anpassung des Auftrages oder in sonstiger zumutbarer Form beseitigt werden kann, gilt Ziffer 11.6 entsprechend. Die Verlagerung der Verarbeitung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

3. LAUFZEIT

- 3.1 Dieser Vertrag wird als Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers für jeden Workspace gesondert mit dessen Einrichtung auf der SaaS-Plattform des Auftragnehmers wirksam. Er gilt, solange der betreffende Workspace besteht bzw. solange der Auftragnehmer im Rahmen der Nutzung dieses Workspace personenbezogene Daten des Auftraggebers verarbeitet. Mit Beendigung des Workspace endet auch dieser Vertrag. Die Regelungen zur Löschung und Rückgabe personenbezogener Daten sowie zur Vertraulichkeit gelten über das Vertragsende hinaus.
- 3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schwerwiegenden Verstoß dar.

4. WEISUNG

- 4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten. Als Weisung gilt auch die Nutzung der Funktionen der Plattform durch den Auftraggeber und seine Nutzer.
- 4.2 Falls Weisungen die unter Ziffer 1 der Anlage getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn die Parteien hierüber eine entsprechende neue Vereinbarung in Textform treffen.
- 4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für die Laufzeit dieses Vertrags und anschließend noch für drei Jahre aufzubewahren.
- 4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.
- 4.5 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Weisungsberechtigt auf Seiten des Auftraggebers sind der Workspace-Verantwortliche im Sinne von Ziffer 1.5 der AGB sowie

die vom Auftraggeber im jeweiligen Workspace als Administrator hinterlegten Nutzer. Der Auftraggeber verwaltet diese Berechtigungen eigenverantwortlich über die Plattform. Weisungsempfänger auf Seiten des Auftragnehmers ist datenschutz@ki.de. Der Auftragnehmer stellt sicher, dass nur befugte und zur Vertraulichkeit verpflichtete Mitarbeiter Zugriff auf dieses Postfach haben. Änderungen des Workspace-Verantwortlichen und der Administratoren nimmt der Auftraggeber selbst in der Anwendung vor; einer gesonderten Mitteilung bedarf es nicht.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

- 5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.
- 5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgenabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.
- 5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

- 6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage die zum Nachweis der Einhaltung der in diesem Vertrag und in Art. 28 DSGVO geregelten Pflichten erforderlichen Informationen zur Verfügung. Die Auskunft beschränkt sich auf Informationen, die die im Rahmen dieses Vertrages erfolgende Verarbeitung betreffen; ein Anspruch auf Offenlegung von Betriebs- und Geschäftsgeheimnissen, sicherheitsrelevanten Details, personenbezogenen Daten Dritter oder Informationen anderer Kunden des Auftragnehmers besteht nicht.
- 6.2 Der Auftragnehmer kann den Nachweis der Einhaltung seiner Pflichten nach Art. 28 DSGVO auch durch die Vorlage geeigneter Unterlagen führen, insbesondere durch aktuelle Testate, Berichte oder Auszüge von unabhängigen Stellen (z. B. Wirtschaftsprüfer, interne oder externe Datenschutzbeauftragte, Auditoren), durch eine geeignete Zertifizierung nach einem genehmigten Zertifizierungsverfahren i. S. v. Art. 42 DSGVO, durch die Einhaltung genehmigter Verhaltensregeln i. S. v. Art. 40 DSGVO oder durch sonstige geeignete Dokumentation des technisch-organisatorischen Sicherheitskonzepts. Der Auftraggeber wird vor einer Vor-Ort-Kontrolle prüfen, ob die nach Ziffer 6.1 und 6.2 vorgelegten Informationen und Nachweise ausreichen. Das Recht zur Vor-Ort-Kontrolle nach Ziffer 6.3 bleibt unberührt.

6.3 Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Dritter sind berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO durch eine Inspektion in den Geschäftsräumen des Auftragnehmers zu überprüfen. Für solche Vor-Ort-Kontrollen gilt:

- a) Die Kontrolle ist mit angemessener Frist, in der Regel mindestens vier (4) Wochen im Voraus, schriftlich oder in Textform anzukündigen und im Einvernehmen mit dem Auftragnehmer terminlich abzustimmen;
- b) sie findet während der üblichen Geschäftszeiten und ohne vermeidbare Störung des Betriebsablaufs des Auftragnehmers statt;
- c) sie erfolgt grundsätzlich höchstens einmal je Kalenderjahr; darüber hinausgehende Kontrollen bei konkreten Anhaltspunkten für einen Verstoß oder aufgrund einer verbindlichen Anordnung einer Aufsichtsbehörde bleiben hiervon unberührt;
- d) der beauftragte Dritte darf kein Wettbewerber des Auftragnehmers sein und ist vor der Kontrolle zur Vertraulichkeit zu verpflichten;
- e) der Auftraggeber trägt die ihm durch die Kontrolle entstehenden Kosten selbst; der dem Auftragnehmer durch die Unterstützung entstehende angemessene Aufwand kann diesem nach seinen jeweils gültigen Sätzen vergütet werden, sofern die Kontrolle nicht einen vom Auftragnehmer zu vertretenden Verstoß aufdeckt;
- f) Zugang zu Daten, Systemen und Informationen anderer Kunden des Auftragnehmers sowie zu Betriebs- und Geschäftsgeheimnissen besteht nicht; erforderlichenfalls sind geeignete Schutzmaßnahmen (z. B. Anonymisierung, Begleitung durch Personal des Auftragnehmers) zu treffen.

Der Auftragnehmer ermöglicht die nach Maßgabe dieser Ziffer zulässigen Kontrollen und wirkt hieran im erforderlichen Umfang mit.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

Der Datenschutzbeauftragte des Auftragnehmers ist in der Anlage dieses Vertrags unter Ziffer 3 angeführt, soweit für den Auftragnehmer ein Datenschutzbeauftragter bestellt sein muss oder freiwillig bestellt ist.

8. VERTRAULICHKEIT

8.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.

8.2 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und

auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

- 8.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen.

9. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

- 9.1 Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Er gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und ein angemessenes Schutzniveau erreicht wird. Insbesondere hat der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen sicherzustellen.
- 9.2 Die in Ziffer 5 der Anlage beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.
- 9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage unter der Ziffer 5 vereinbarten Maßnahmen entsprechen. Wesentliche Änderungen bedürfen einer Vereinbarung nach Maßgabe von Ziffer 14.3.

10. INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS UND VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

- 10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personenbezogener Daten betreffen.
- 10.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.
- 10.3 Sollten die personenbezogenen Daten die unter dieser Vereinbarung verarbeitet werden beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Restrukturierungsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der

Auftragnehmer wird alle in diesem Zusammenhang relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

- 10.4 Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht festgestellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.
- 10.5 Diese Ziffer 10 gilt entsprechend für Vorkommnisse bei Prozessen, die von Unterauftragnehmern ausgeführt werden.

11. UNTERAUFTRAGNEHMER

- 11.1 Vor der Hinzuziehung oder Ersetzung von Unterauftragnehmern informiert der Auftragnehmer den Auftraggeber in Textform (bspw. per E-Mail). Der Auftraggeber kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch den Auftragnehmer in schriftlicher Form oder in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.
- 11.2 Der Auftragnehmer hat vertraglich sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Unterauftragnehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.
- 11.3 Eine Beauftragung von Unterauftragnehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- 11.4 Der Auftraggeber erteilt hiermit seine Zustimmung zur Beauftragung der in der Anlage unter der Ziffer 4 aufgeführten Unterauftragnehmer.
- 11.5 Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unterauftragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftragnehmer nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.
- 11.6 Liegt ein begründeter Widerspruch gegen einen neuen Unterauftragnehmer gem. Ziffer 11.1 vor, der vom Auftragnehmer nicht durch zumutbare Anpassung des Auftrages oder in sonstiger zumutbarer Form beseitigt werden kann, ist jeder Vertragspartner berechtigt, das bestehende Vertragsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist zu kündigen, insbesondere wenn ihm die Fortsetzung des Vertragsverhältnisses bis zur vereinbarten Beendigung oder bis zum Ablauf einer Kündigungsfrist nicht zumutbar ist.
- 11.7 Abweichend von Ziffer 11.1 kann der Auftragnehmer einen Unterauftragnehmer ohne vorherige Information ersetzen, wenn dies zur Abwehr einer unmittelbaren Gefahr für die Sicherheit oder Verfügbarkeit der Verarbeitung erforderlich ist, insbesondere bei einer

Verletzung des Schutzes personenbezogener Daten beim Unterauftragnehmer, dessen Insolvenz, der Einstellung seiner Leistungen oder dem Wegfall der Voraussetzungen nach Art. 28 oder Art. 44 ff. DSGVO. Der Auftragnehmer informiert den Auftraggeber hierüber unverzüglich in Textform. Die Frist für einen Widerspruch nach Ziffer 11.1 beginnt mit Zugang dieser Information; Ziffer 11.6 gilt entsprechend. Die Pflichten nach Ziffern 11.2, 11.3 und 11.5 bleiben unberührt.

- 11.8 Nicht als Unterauftragsverhältnisse im Sinne dieser Ziffer 11 gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt und bei denen kein Zugriff auf die im Auftrag verarbeiteten personenbezogenen Daten im Klartext vorgesehen ist, insbesondere Telekommunikations- und Netzdienstleistungen, reine Transport- und Zustelldienste sowie die Wartung von Hardware ohne Datenzugriff. Der Auftragnehmer trifft auch in diesen Fällen angemessene vertragliche Vereinbarungen und Kontrollmaßnahmen zum Schutz der Daten.
- 11.9 Die in Anlage Ziffer 4 aufgeführten Unterauftragnehmer setzen ihrerseits weitere Unterauftragsverarbeiter ein, die sie in eigenen, von ihnen bereitgestellten Verzeichnissen ausweisen. Die Genehmigung nach Ziffer 11.4 erstreckt sich auf diese weiteren Unterauftragsverarbeiter in der jeweils aktuellen Fassung dieser Verzeichnisse. Ziffer 11.1 findet auf Änderungen dieser Verzeichnisse keine Anwendung. Der Auftragnehmer stellt durch die Verträge mit seinen Unterauftragnehmern sicher, dass diese ihren weiteren Unterauftragsverarbeitern gleichwertige Datenschutzpflichten auferlegen; Ziffer 13 Satz 2 bleibt unberührt.

12. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

- 12.1 Maßgeblicher Zeitpunkt für die Beendigung der Verarbeitung ist die Beendigung des jeweiligen Workspace, nicht die Beendigung eines kostenpflichtigen Abonnements. Wird ein kostenpflichtiges Abonnement gekündigt, während der Workspace im Rahmen eines kostenlosen Tarifs fortbesteht, dauert die Auftragsverarbeitung fort. Nach Beendigung des Workspace ist der Auftragnehmer verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung verarbeitet hat, nach Maßgabe der nachfolgenden Absätze zu löschen oder herauszugeben. Die Pflicht zur Löschung oder Herausgabe besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten unverzüglich zu löschen, sobald die Pflicht zur Speicherung entfällt.
- 12.2 Der Auftraggeber kann die von ihm erstellten und hochgeladenen Inhalte innerhalb von 30 Tagen nach Beendigung des Workspace in Textform (bspw. per E-Mail) herausverlangen. Der Auftragnehmer stellt die Inhalte in diesem Fall innerhalb von 14 Tagen nach Zugang des Verlangens in einem gängigen, maschinenlesbaren Format bereit. Verlangt der Auftraggeber die Herausgabe nicht innerhalb der vorgenannten Frist, gilt die Löschung als gewählt.
- 12.3 Die Daten werden im Rahmen der laufenden Löschung aus produktiven Systemen entfernt. Der Auftragnehmer erstellt vollständige, verschlüsselte Snapshots der Anwendungsdatenbank mit rollierender Aufbewahrung (2 Jahre), die ausschließlich der Wiederherstellung nach

technischen Ausfällen, fehlerhaften Migrationen und Ransomware-Fällen dienen. Einzelne Datensätze lassen sich aus diesen Snapshots technisch nicht herauslösen, ohne die Integrität des Gesamtbestands zu zerstören. Bis zur endgültigen Löschung aus den Backups wird die Verarbeitung der betroffenen Daten eingeschränkt. Eine aktive Nutzung oder ein Zugriff auf diese Daten findet nicht statt.

- 12.4 Wird ein Backup gem. Ziffer 12.3 wiedereingespielt, das bereits zu löschende Daten gem. Ziffer 12 dieses Vertrags enthält, so werden die betroffenen Daten nach Abschluss der Wiederherstellung erneut gelöscht. Der Vorgang wird dokumentiert.
- 12.5 Soweit personenbezogene Daten nach Beendigung des Auftragsverhältnisses noch in Backups gemäß Ziffer 12.3 vorgehalten werden, gelten die Regelungen dieses Vertrags in Bezug auf diese Daten – insbesondere zu Vertraulichkeit, technischen und organisatorischen Maßnahmen, Weisungs- und Zweckbindung, Einschaltung von Unterauftragsverarbeitern sowie Kontroll- und Nachweisrechten – bis zur endgültigen Löschung der Daten aus den Backups fort.
- 12.6 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind; für Daten in Backups gemäß Ziffer 12.3 gilt dies spätestens mit Ablauf der Backup-Rotation.
- 12.7 Der Auftragnehmer wird dem Auftraggeber die Löschung in Textform bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren. Ziffer 6 dieses Vertrags gilt hierfür entsprechend.

13. HAFTUNG

Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diesen Vertrag entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer. Die Haftungsbeschränkungen gemäß Ziffer 11 der AGB gelten auch für die Haftung der Parteien untereinander aus oder im Zusammenhang mit diesem Vertrag. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt hiervon unberührt.

14. SCHLUSSBESTIMMUNGEN

- 14.1 Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten ausgeschlossen.
- 14.2 Die Anlage zu diesem Vertrag ist wesentlicher Bestandteil desselben.
- 14.3 Für Änderungen dieses Vertrags einschließlich seiner Anlage gilt Ziffer 12.3 der AGB mit der Maßgabe, dass die Zustimmungsfiktion nur für nicht wesentliche Änderungen gilt. Wesentliche Änderungen, insbesondere Änderungen der Festlegungen unter Ziffer 1 der Anlage und wesentliche Änderungen der technischen und organisatorischen Maßnahmen im Sinne von

Ziffer 9.3, bedürfen der ausdrücklichen Zustimmung des Auftraggebers in Textform. Die Widerspruchsverfahren nach Ziffer 2 und Ziffer 11.1 bleiben unberührt.

- 14.4 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht.
- 14.5 Dieser Vertrag einschließlich seiner Anlage wird in deutscher und englischer Sprache bereitgestellt. Maßgeblich ist die deutsche Fassung; bei Abweichungen zwischen den Sprachfassungen geht die deutsche Fassung vor.

ANLAGE ZUM AUFTRAGSVERARBEITUNGSVERTRAG

1. GEGENSTAND DES AUFTRAGS

1.1 Gegenstand des Auftrags:

Gegenstand des Auftrags ist die Bereitstellung und der Betrieb der SaaS-Plattform „pricenxt“ für den Auftraggeber. Dies umfasst insbesondere die Verwaltung der Mitgliedschaften, Rollen und Berechtigungen innerhalb des Workspace sowie das Speichern, Anzeigen und – nach Vorgabe des Auftraggebers – Teilen der von seinen Nutzern erstellten Inhalte innerhalb des jeweiligen Workspace. Nicht Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten im Zusammenhang mit Benutzerkonten, der Abrechnung und der Protokollierung; insoweit ist der Auftragnehmer eigener Verantwortlicher gemäß Ziffern 10.1 und 10.2 der AGB.

1.2 Art und Zweck der Datenverarbeitung:

Der Auftragnehmer verarbeitet die vom Auftraggeber bereitgestellten personenbezogenen Daten der vom Auftraggeber benannten Nutzer (Art der Daten siehe Ziff. 1.3) zum Zweck der Bereitstellung einer Preisinformations- und Marktintelligenz-Plattform für Rohstoff- und Werkstoffpreise. Dies umfasst insbesondere die individuelle Zusammenstellung und Darstellung von Preisreihen in einem persönlichen Dashboard, das Anlegen von Notizen, die Einladung weiterer Nutzer in den Workspace sowie – soweit vom Auftraggeber genutzt – den Upload eigener Preisdaten durch den Auftraggeber sowie – soweit vom Auftraggeber bzw. seinen Nutzern aufgerufen – KI-gestützte Funktionen zur Auswertung von Workspace-Inhalten (z. B. Berichte, Zusammenfassungen, Analysen).

1.3 Art der Daten:

Datenkategorie	Auflistung konkret verarbeiteter Daten
Berufliche Kontakt- und (Arbeits-) Organisationsdaten	Name, Vorname, geschäftliche E-Mail-Adresse, Anrede
Daten zu beruflichen Verhältnissen	Berufsbezeichnung
Workspace-Mitgliedschafts- und Berechtigungsdaten	Rolle, Einladungsstatus, zugewiesener Seat
Von Nutzern erstellte Inhalte	Notizen, Dashboard-Konfigurationen und individuell zusammengestellte Preisreihen
Hochgeladene eigene Preisdaten	Vom Auftraggeber optional hochgeladene eigene Preisdaten
KI-gestützte Auswertungsergebnisse	Aus KI-gestützten Funktionen erzeugte Ergebnisse (z. B. Berichte, Zusammenfassungen, Analysen)

Personenbezogene Daten Dritter	In den vorgenannten Inhalten ggf. enthaltene personenbezogene Daten Dritter (z. B. Namen von Geschäftskontakten)
--------------------------------	--

1.4 Kreis der Betroffenen:

Betroffenengruppe	Beschreibung	Beispiele
Mitarbeiter des Auftraggebers/des Verantwortlichen	Eigene Mitarbeiter des Auftraggebers/ des Verantwortlichen	Arbeitnehmer, freie Mitarbeiter, sonstige vom Auftraggeber berechnigte Personen
Externe Nutzer	Vom Auftraggeber in den Workspace eingeladene externe Nutzer	Mitarbeiter anderer Gesellschaften, die der Auftraggeber für seinen Workspace freigeschaltet hat
Geschäftskontakte des Auftraggebers	Geschäftskontakte des Auftraggebers, soweit in Inhalten enthalten	Ansprechpartner bei Lieferanten oder Kunden

2. WEISUNGSBERECHTIGTE PERSONEN

2.1 Weisungsberechtigte Personen des Auftraggebers sind:

Der Workspace-Verantwortliche im Sinne von Ziffer 1.5 der AGB sowie die vom Auftraggeber im jeweiligen Workspace als Administrator hinterlegten Nutzer.

2.2 Weisungsempfänger beim Auftragnehmer sind:

datenschutz@ki.de

3. DATENSCHUTZBEAUFTRAGTER

3.1 Datenschutzbeauftragter des Auftragnehmers ist:

Proliance GmbH

www.proliance.ai

Datenschutzbeauftragter

Leopoldstr. 21

80802 München

E-Mail: datenschutzbeauftragter@proliance.ai

4. UNTERAUFTRAGNEHMER

Zum Kreis der genehmigten Unterauftragnehmer bei Abschluss dieses Vertrags gehören:

Nr.	Unterauftragnehmer (Name, Anschrift, Ansprechpartner)	Verarbeitete Datenkategorien	Beschreibung der Tätigkeit	Ort der Datenverarbeitung
1	Supabase Pte. Ltd., 65 Chulia Street #38- 02/03, OCBC Centre, Singapore 049513; Kontakt: legal@supabase.io	Datenkategorien gemäß Ziff. 1.3 der Anlage, insbesondere Workspace- Mitgliedschafts- und Berechtigungsdat en, von Nutzern erstellte Inhalte und hochgeladene Dateien	Hosting von Datenbank, Dateispeicher und serverseitigen Funktionen der Plattform	EU (AWS-Region Frankfurt). Vertragspartner mit Sitz in Singapur; Zugriffe von außerhalb der EU, insbesondere für Support und Administration, können nicht ausgeschlossen werden. Garantie: EU- Standardvertragsklauseln (Modul 3) gemäß Supabase-DPA.
2	Vercel Inc., 440 N Barranca Ave #4133, Covina, California 91723, USA; Kontakt: ar@vercel.com	Datenkategorien gemäß Ziff. 1.3 der Anlage, soweit sie in Anfragen und Antworten der Anwendung enthalten sind und über die Hosting- Infrastruktur durchlaufen	Hosting und Auslieferung der Webanwendung app.pricenxt.com	Primär EU; über das globale Edge-Netzwerk können je nach Zugriffsstandort auch Server außerhalb der EU beteiligt sein. US- Unternehmen. Garantie: EU-US Data Privacy Framework sowie EU- Standardvertragsklauseln (Modul 3) gemäß Vercel- DPA.
3	Lettermint B.V., Willemsvaart 16B, Unit 1.08, 8019 AB Zwolle, Niederlande (KvK 99337711); Kontakt: legal@lettermint.co	Name und E-Mail- Adresse der Nutzer und eingeladener Nutzer sowie der Inhalt der aus dem Workspace versendeten E- Mails (z. B. Name des Workspace und des Einladenden, Benachrichtigung en zu Workspace- Aktivitäten); dazu technische Versanddaten (Zustellstatus, Zeitstempel)	Versand von E- Mails aus dem Workspace (Einladungen, Benachrichtigung en zu Workspace- Aktivitäten) einschließlich Zustell- und Bounce- Verarbeitung	EU (Niederlande; Sicherungskopien in Deutschland). Keine Drittlandübermittlung.
4	Functional Software, Inc. (Sentry), 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Datenkategorien gemäß Ziff. 1.3 der Anlage, soweit sie in Fehlermeldungen	Erfassung und Analyse von Anwendungsfehl ern	EU (EU-Datenregion). US- Unternehmen; Zugriffe aus den USA können nicht ausgeschlossen werden. Garantie: EU-US Data

		und Stacktraces enthalten sind (z. B. Board- oder Notizinhalt)		Privacy Framework, hilfsweise EU-Standardvertragsklauseln (Modul 3) gemäß Sentry-DPA.
5	Acronis International GmbH, Rheinweg 9, 8200 Schaffhausen, Schweiz	Datenkategorien gemäß Ziff. 1.3 der Anlage als Bestandteil verschlüsselter Sicherungskopien	Backup und Wiederherstellung (Ziff. 12.3 des Vertrags)	EU (EU-Datenregion). Vertragspartner mit Sitz in der Schweiz; Zugriffe aus der Schweiz, insbesondere für Support und Administration, können nicht ausgeschlossen werden. Übermittlung auf Grundlage des Angemessenheitsbeschlusses der EU-Kommission für die Schweiz.
6	Wasabi Technologies, LLC, 75 Arlington Street, Suite 810, Boston, MA 02116, USA; Kontakt: support@wasabi.com	Datenkategorien gemäß Ziff. 1.3 der Anlage als Bestandteil verschlüsselter Sicherungskopien	Objektspeicher für Sicherungskopien (Ziff. 12.3 des Vertrags)	EU (vom Auftragnehmer gewählte EU-Speicherregion). US-Unternehmen; nach dem Wasabi-DPA sind Zugriffe von außerhalb der gewählten Region möglich. Garantie: EU-Standardvertragsklauseln (Modul 3) gemäß Wasabi-DPA.
7	Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland; Kontakt: support@anthropic.com; Konzernmutter Anthropic, PBC, San Francisco, USA	Datenkategorien gemäß Ziff. 1.3 der Anlage, soweit sie bei Nutzung der KI-gestützten Funktionen an das Sprachmodell übermittelt werden (z. B. Notizen, Preisreihen, hochgeladene Preisdaten und daraus erzeugte Ergebnisse)	Bereitstellung des KI-Sprachmodells (Claude) für die KI-gestützten Funktionen nach Ziff. 1.2 der Anlage; keine Nutzung der Daten zum Training von KI-Modellen	Vertragspartner in der EU (Irland). Verarbeitung auch in den USA durch Anthropic, PBC und weitere Unterauftragsverarbeiter von Anthropic. Garantie für die Weiterübermittlung: EU-Standardvertragsklauseln (Modul 3) gemäß Anthropic-DPA.

5. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

5.1 Technische und organisatorische Maßnahmen im Einzelnen

5.1.1 Zutrittskontrolle für Räumlichkeiten und Einrichtungen, in denen Daten verarbeitet werden

Beschreibung: Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Der Auftragsverarbeiter hat im Rahmen der Zutrittskontrolle folgende Maßnahmen ergriffen:

- Zutrittskontrollsysteme für das Betriebsgelände, für das Gebäude und auch für einzelne Räume/Räumlichkeiten, in denen die Datenverarbeitung stattfindet (z.B. Ausweisleser, Magnetkarte, Chipkarte, Schlüssel)
- Türsicherung (Sicherheitsschlösser, elektrische Türöffner, manuelles/automatisches/biometrisches Transponder Schließsystem usw.)
- Standort des Servers, z.B. in Raum, Schrank, ausgelagert
- Sicherung des Serverraums vor Zutritt unberechtigter Personen
- Anzahl der Personen, die Zugang zum Serverraum haben, auf das Notwendigste begrenzt
- Kontrollierte, dokumentierte Schlüsselvergabe, nicht duplizierbare Schlüssel, sichere Verwahrung von zusätzlichen Schlüsseln, Zutrittskarten etc.
- Server außerhalb des Unternehmens ausgelagert
- Zutrittsregelungen für freie Mitarbeiter/Besucher/Dienstleister (z.B. Besucher gelangen zuerst zu einem Empfang und betreten das restliche Gebäude nur in Begleitung)

5.1.2 Zugangs- und Zugriffskontrolle

Beschreibung: Das Eindringen Unbefugter in die Datenverarbeitungs(DV)-Systeme (IT-Systeme) ist zu verhindern. Ebenso sind Tätigkeiten in DV-Systemen (IT-Systemen) außerhalb eingeräumter Berechtigungen sowie unerlaubte Zugriffe auf das System von außen zu verhindern.

Der Auftragsverarbeiter hat im Rahmen der Zugangs- und Zugriffskontrolle (zu IT-Systemen) folgende Maßnahmen ergriffen:

- Dokumentation der Ausgabe von Hardware an Mitarbeiter
- Personalisierte Accounts (eindeutige Benutzer-ID/Benutzer-Zuordnung), kein „Account-Sharing“ (Nutzung eines Accounts durch mehrere Personen)
- Individuelle Einrichtung von Zugangsrechten (Zugangsrechte sind für die Mitarbeiter auf die Programme beschränkt, die sie auch verwenden müssen)
- Anzahl der Systemadministratoren auf das Notwendigste begrenzt
- Login mit Benutzerkennung und Passwort
- Kennwortverfahren/Passwortregelungen (u.a. Sonderzeichen, Mindestlänge); Passworrichtlinie
- Einrichtung jeweils nur eines Benutzerstammsatzes pro User/getrennte Benutzerstammsätze

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte, Bsp.: Begrenzung des Zugriffs auf Ordner nach dem „need-to-know“ Prinzip)
- Ordnungsgemäße Vernichtung/Löschung von Datenträgern
- Schadsoftwareschutz für den Server
- Firewall/Virenschutz für Rechner/Geräte
- Incident Response Management
- Clean-Desk-Policy
- Einsatz von Passwortmanagern zum Generieren und Teilen von Passwörtern
- Passwortverschlüsselung (auch Administratoren sollten Passwörter nicht einsehen können)
- Berechtigungskonzept
- Zweifaktorauthentifizierung für Administratoren
- Schutz von Schnittstellen gegen unbefugtes Eindringen von außen (z.B. WLAN, USB, Netzwerksteckdosen)
- Automatische Sperrung eines Benutzers, wenn er das Passwort mehrmals falsch eingibt und Maßnahmen, die in diesem Fall getroffen werden
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung (Timeout)/Bildschirmersperrung)
- Organisatorische Vorkehrungen zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz (z.B. Richtlinien)
- Schulung von Mitarbeitern, Awareness-Training
- Auswertungen / Reports
- VPN Technologie
- Verschlüsselung von Datenträgern
- Absicherung von Fernwartungszugängen, Servern und Endgeräten, externen Schnittstellen (z.B. USB)

5.1.3 Eingabekontrolle

Beschreibung: Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

Der Auftragsverarbeiter hat im Rahmen der Eingabekontrolle folgende Maßnahmen ergriffen:

- Login- und Logout-Protokollierung
- Protokollierungen der Aktivitäten des IT-Systems selbst sowie der Aktivitäten der IT-Administratorentätigkeiten
- Protokollierung hinsichtlich der Benutzeraktivitäten

- Dokumentation von durchgeführten Wartungs-, Fernwartungs- oder Reparaturarbeiten am IT-System
- Sicherstellung der Integrität neuer Programme und Updates, z.B. durch einen Prozess zur Sicherstellung, dass Mitarbeiter nicht selbst Programme herunterladen oder installieren können
- Schadsoftwarecheck für erhaltene und auszuliefernde Datenträger
- Komplette Sicherung der betroffenen Systeme vor größeren Wartungs-/Fernwartungs- oder Reparaturarbeiten

5.1.4 Auftragskontrolle

Beschreibung: Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Eine Datenverarbeitung durch Dritte (vgl. Art. 28 DSGVO) ist gemäß den Anweisungen des Auftraggebers/Datenexporteurs erlaubt. Maßnahmen (technisch und organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber/Datenexporteur und Auftragnehmer/Datenimporteur.

Der Auftragsverarbeiter hat im Rahmen der Auftragskontrolle folgende Maßnahmen ergriffen:

- Kriterien zur sorgfältigen Auswahl der Unterauftragnehmer
- Eindeutige Vertragsgestaltung, schriftliche Festlegung der Weisungen
- Maßnahmen, die gewährleisten, dass die Verarbeitung personenbezogener Daten im Auftrag entsprechend den Weisungen des Auftraggebers erfolgen, z.B. schriftliche Weisungen, Dokumentation der Weisungen, Angebot und Auftragsbestätigung, Sicherstellung der Verpflichtung der Mitarbeiter des Auftragnehmers auf die datenschutzrechtliche Vertraulichkeit, vertraglich festgelegte Verantwortlichkeiten (Weisungsberechtigte und Weisungsempfänger), regelmäßige Kontrollen im Unternehmen
- Auftragsverarbeitungsverträge
- Verzeichnis aller Auftragsverarbeitungsverträge
- Konzept für die Löschung der Daten nach Ende des Vertragsverhältnisses

Angaben zu ausgelagerten/fremdgehosteten Servern:

- Hoster:
Vercel und Supabase (jeweils virtuelle Server in deren Cloud-Infrastruktur).
- Serverstandort und Drittlandübermittlung:
Supabase: Projekt-Region ist EU (AWS-Region Frankfurt); da der Vertragspartner seinen Sitz in Singapur hat, können Zugriffe außerhalb der EU (insbesondere Support und Administration) nicht ausgeschlossen werden. Diese sind durch die im Supabase-DPA enthaltenen EU-Standardvertragsklauseln (Modul 3) abgesichert. Vercel ist ein US-Unternehmen mit einem globalen Edge-Netzwerk; die Anfrage wird jeweils vom geografisch nächstgelegenen Server

beantwortet, sodass je nach Zugriffsstandort des Nutzers auch Server außerhalb der EU beteiligt sein können. Soweit hierdurch Drittlandübermittlungen vorliegen, sind die Voraussetzungen nach Art. 44 ff. DSGVO durch das EU-US Data Privacy Framework sowie die im Vercel-DPA enthaltenen EU-Standardvertragsklauseln (Modul 3) abgesichert.

- Sicherheitsnachweise der Hoster:
Für beide Anbieter liegen Data Processing Agreements (DPA) vor. Für Vercel und Supabase liegen SOC-2-Type-II-Prüfberichte vor.
- Absicherung der Verbindung zu den Servern:
Sämtliche Verbindungen erfolgen ausschließlich verschlüsselt über TLS (HTTPS); der Zugriff auf die APIs der Hoster erfolgt über individuelle, nach dem Prinzip der geringsten Rechte vergebene API-Schlüssel/Zugangsdaten.

5.1.5 Getrennte Verarbeitung von Daten/Trennungskontrolle

Beschreibung: Die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke erhoben wurden, muss sichergestellt werden. Maßnahmen zur getrennten Verarbeitung der Daten unterschiedlicher Auftraggeber sind zu gewährleisten.

Der Auftragsverarbeiter hat im Rahmen der Trennungskontrolle folgende Maßnahmen ergriffen:

- Trennung von Daten, die verschiedene Kunden/Auftraggeber betreffen
- Trennung von Daten, die zu verschiedenen Zwecken verarbeitet werden
- Nutzung von unterschiedlichen, kundenspezifischen bzw. mandantenfähigen Systemen
- Funktionstrennung (Produktion/Test)
- Einhaltung verschiedener Löschfristen wird gewährleistet

5.1.6 Weitergabekontrolle

Beschreibung: Aspekte der Weitergabe personenbezogener Daten sind zu regeln (elektronische Übertragung, Datentransport, Übermittlungskontrolle usw.), um einen Verlust, eine Veränderung oder eine unbefugte Veröffentlichung zu verhindern. Maßnahmen zu Transport, Übertragung, Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie zur nachträglichen Überprüfung sind zu treffen.

Der Auftragsverarbeiter hat im Rahmen der Weitergabekontrolle folgende Maßnahmen ergriffen:

- WLAN-Zugänge gesichert
- Sicherung von Daten bei Übertragung auf dem elektronischen Weg
- E-Mail-Verschlüsselung (SSL, TLS usw.)
- Transportsicherung (z.B. Kurier, verschlossene Behälter)

- Sichere Vernichtung nicht mehr benötigter Datenträger
- Fachgerechte Entsorgung nicht mehr benötigter Papierakten
- Tunnelverbindung (VPN = Virtual Private Network)
- Verschlüsselte Plattformen zur Weitergabe von Daten

5.1.7 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Beschreibung: Die Daten sind gegen zufällige Zerstörung und Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch/logisch).

Der Auftragsverarbeiter hat im Rahmen der Kontrolle zur Verfügbarkeit und Belastbarkeit folgende Maßnahmen ergriffen:

- Regelmäßige Datensicherungen/Backup-Verfahren, Widerstandsfähigkeit (Resilience) von IT-Systemen
- Maßnahmen zur Sicherung des (eigenen) Serverraums und der IT-Infrastruktur
- Notfallplan für einen IT-Notfall (Disaster Recovery Plan) und für Datenschutzverletzungen
- Klare Meldewege für IT-Notfälle und Datenschutzverletzungen
- Virenschutz, Firewall, Anti-Spy-Software, Spam-Filter, IDS oder IPS-Systeme
- Feuermeldesystem

5.1.8 Organisationskontrolle

Beschreibung: Wie wird die reibungslose Organisation des Datenschutzes und der Sicherheit der Daten im Unternehmen sichergestellt?

Der Auftragsverarbeiter hat im Rahmen der Organisationskontrolle folgende Maßnahmen ergriffen

- Schriftliche Verpflichtung aller Mitarbeiter auf die datenschutzrechtliche Vertraulichkeit
- Verfahren zur Risikoabschätzung und zum Risikomanagement etabliert und dokumentiert
- Richtlinie zur Nutzung des betrieblichen Internetzugangs und des betrieblichen E-Mail-Accounts
- Regelmäßige Sensibilisierung/Schulung der Mitarbeiter, Richtlinien / Handbücher für die Mitarbeiter
- Organisation der Umsetzung des Datenschutzes (z.B. Bestellung eines Datenschutzbeauftragten; interne Mitarbeiter, die den Datenschutzbeauftragten unterstützen)
- Aufstellung eines Datenschutzkonzeptes
- Vorliegen eines IT-Sicherheitskonzeptes

- Richtlinie/Arbeitsanweisung zum Umgang mit personenbezogenen Daten im Homeoffice/ Mobile Office

5.1.9 Privacy by Default und Privacy by Design

Beschreibung:

Privacy by Default bedeutet übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Das heißt, bereits die Werkseinstellungen sollen datenschutzfreundlich ausgestaltet werden. Hierdurch sollen vor allem die Nutzer geschützt werden.

Privacy by Design bedeutet „Datenschutz durch Technikgestaltung“. Das heißt, dass bereits bei der Entwicklung oder dem Einkauf von Software auf eine datenschutzfreundliche Gestaltung geachtet werden soll.

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

Privacy by Default:

- Transparente Einstellungen und Optionen für den Nutzer zum Wählen der Einstellungen.
- Voreinstellungen, bei denen die Software nur die nötigsten Daten sammelt.

Privacy by Design:

- Bei der Entwicklung oder beim Kauf von Software wird darauf geachtet, dass die Software so wenige Daten wie möglich für die Verarbeitung anfordert/benötigt

5.1.10 Wirksamkeitskontrolle

Beschreibung: Alle Handlungen, die zu einem Nachweis führen, dass die eingesetzten Maßnahmen funktionieren.

Der Auftragsverarbeiter hat im Rahmen der Wirksamkeitskontrolle folgende Maßnahmen ergriffen:

- Regelmäßige Kontrollen der Wirksamkeit der eingesetzten technischen und organisatorischen Maßnahmen
- Regelmäßige Kontrolle der Funktionstüchtigkeit der Anti-Viren-Software und der Firewall