Vertrag zur Auftragsverarbeitung

über die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten
gemäß Art. 28 Datenschutzgrundverordnung (DS-GVO), Stand: 10.02.2022

Präambel

Der vorliegende Vertrag zur Auftragsverarbeitung adressiert zentrale Punkte, die mit der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten in Verbindung stehen. Die Vertragsparteien sind sich darüber einig, dass in diesem Vertrag nur datenschutzrechtliche Regelungen zur Auftragsverarbeitung getroffen werden.
Die beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Leistungsvertrag in Zusammenhang stehen und bei denen die Mitarbeitenden der Leistungserbringerin (IWOP GmbH, Albert-Einstein-Str. 1, 49076 Osnabrück, Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO) oder durch die Leistungserbringerin beauftragte Dritte mit personenbezogenen Daten der Leistungsnehmerin (Unternehmen, welches ein Nutzerkonto bei www.teamlove.app anlegt, Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO) in Berührung kommen können.

1. Gegenstand und Dauer des Auftrags (Art. 28, III S. 1 DS-GVO)

1.1. Gegenstand des Auftrags ist die Erhebung und Auswertung von Meinungsdaten von Mitarbeitenden, Kund:innen, Lieferant:innen oder Geschäftspartner:innen der Leistungsnehmerin durch die Leistungserbringerin im Rahmen der Nutzung des Teamfeedbacktools „Teamlove“ durch die Leistungsnehmerin.

1.2. Die Dauer des Auftrags (Laufzeit) beginnt mit der Einrichtung eines Nutzerkontos auf der Seite www.teamlove.app durch die Leistungsnehmerin und endet mit der Löschung des Nutzerkontos durch die Leistungsnehmerin oder die Leistungserbringerin aus in den AGB spezifizierten Gründen. Der Vertrag gilt unabhängig davon so lange, wie die Leistungserbringerin personenbezogene Daten der Leistungsnehmerin verarbeitet (einschließlich Backups).

2. Umfang und Art der Datenerhebung (Art. 28, III, S. 1 DS-GVO)

2.1. Um den Service von Teamlove anbieten zu können, benötigt die Leistungserbringerin Zugriff auf die unter 2.2. genannten Daten. Der Zugriff ist dabei insbesondere nötig für folgende Punkte: Anlegen eines Nutzerkontos für Mitarbeitende oder andere Personen, die am Teamfeedback teilnehmen sollen, Versendung von Einladungen via E-Mail-Adressen, um am Teamfeedback teilnehmen zu können, Zuordnung der Kontoinhaber:innen zu Teams, Unternehmen und Abteilungen oder Gruppen von Teams, Erhebung der Meinungsdaten der Teammitglieder, Unterstützung

bei der Auswertung des Feedbackergebnisses sowie der Erreichung von Zielen. Die Nutzung anonymisierter Daten für wissenschaftliche Forschung durch die Leistungserbringerin ist zulässig.

2.2. Im Rahmen der Nutzung von Teamlove durch die Leistungsnehmerin erhebt, verarbeitet und nutzt die Leistungserbringerin selbstdeklarierte Meinungsdaten (z. B. Einstellungen, Bewertungen, Einschätzungen), Kommunikationsdaten (z. B. E-Mail-Adressen für die Kommunikation und Einrichtung der Zugänge) sowie arbeitsbezogene Metadaten (diese können über die Vergabe von Labels von der Leistungsnehmerin selber festgelegt werden, z. B. Organisationseinheit, Standort) der Teilnehmenden. Notwendige Kommunikations- und Personalstammdaten zur Durchführung des Teamfeedbacktools werden durch die Leistungsnehmerin eigenständig erfasst und an die Leistungserbringerin zur Verarbeitung und Nutzung über Eingabemasken in der Teamlove-Nutzeroberfläche zur Verfügung gestellt.

2.3. Die durch den Umgang mit ihren Daten Betroffenen sind in der Regel Beschäftigte der Leistungsnehmerin, können aber je nach Zusammensetzung der durch die Leistungsnehmerin selbst angelegten Teams in Teamlove auch Kund:innen, Lieferant:innen oder Geschäftspartner:innen sein.

3. Umsetzung und Einhaltung technisch-organisatorischer Maßnahmen

3.1. Die Leistungserbringerin ergreift in ihrem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt der Leistungsnehmerin die Dokumentation dieser Maßnahmen zur Prüfung [Anlage 1]. Die dokumentierten Maßnahmen werden Grundlage dieses Vertrags.

3.2. Soweit die Prüfung/ein Audit der Leistungsnehmerin einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen oder die Nutzung von Teamlove durch die Leistungsnehmerin einzustellen.

3.3. Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Leistungserbringerin zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch die Leistungserbringerin zu dokumentieren sind, ist die Leistungsnehmerin unverzüglich in Kenntnis zu setzten.

4. Rechte und Anfragen von betroffenen Personen

4.1. Die Verantwortung für die Wahrung der Rechte der durch die Datenspeicherung bei der Leistungserbringerin betroffenen Personen (insbesondere bei Anfragen zur Berichtigung, Löschung, Sperrung und Auskunftserteilung) liegt bei der Leistungsnehmerin. Die Leistungserbringerin unterstützt die Leistungsnehmerin in ihrem Verantwortungsbereich und soweit möglich bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte.

4.2. Die Leistungserbringerin darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach vertraglicher Vereinbarung oder Weisung der Leistungsnehmerin beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken.

4.3. Soweit eine betroffene Person sich diesbezüglich ohne bestehende Vereinbarungen oder Weisung der Leistungsnehmerin unmittelbar an die Leistungserbringerin wendet, wird die Leistungserbringerin dieses Ersuchen unverzüglich an die Leistungsnehmerin weiterleiten.

4.4. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung der Leistungsnehmerin unmittelbar durch die Leistungserbringerin sicherzustellen.

5. Pflichten der Leistungserbringerin (Art. 28, III DS-GVO)

5.1. Die Leistungserbringerin hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet sie insbesondere die Einhaltung folgender Vorgaben:

5.1.1. Schriftliche Benennung einer/eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt, soweit dies gesetzlich vorgeschrieben ist. Dessen Kontaktdaten lauten: Heiko Beemers, TopZert GmbH, Stader Landstr. 27a, 21762 Otterndorf, Tel.: +49 4751 999 54 69, datenschutz@topzert.eu. Ein Wechsel des Datenschutzbeauftragten wird der Leistungsnehmerin zeitnah mitgeteilt.

5.1.2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Die Leistungserbringerin setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Leistungserbringerin und jede der Leistungserbringerin unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung der Leistungsnehmerin verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.1.3. Die Leistungsnehmerin und die Leistungserbringerin arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.1.4. Die unverzügliche Information der Leistungsnehmerin über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei der Leistungserbringerin ermittelt.

5.1.5. Soweit die Leistungsnehmerin ihrerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei der Leistungserbringerin ausgesetzt ist, hat sie die Leistungserbringerin nach besten Kräften zu unterstützen.

5.1.6. Die Leistungserbringerin kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

5.1.7. Nachweis der getroffenen technischen und organisatorischen Maßnahmen gegenüber der Leistungsnehmerin im Rahmen ihrer Kontrollbefugnisse.

6. Unterauftragsverhältnisse

6.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erhebung und Auswertung der Daten beziehen. Hierzu gehören nicht Nebenleistungen, die die Leistungserbringerin in Anspruch nimmt, wie z. B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice, Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Leistungserbringerin ist jedoch dazu

verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten der Leistungsnehmerin auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2. Die Leistungserbringerin darf zur Erfüllung der vertraglichen Vereinbarungen sorgfältig ausgewählte Unterauftragnehmende beauftragen. Sie hat bei der Beauftragung die Anforderungen gemäß Art. 28 Abs. 2-4 DS-GVO zu beachten und die Verträge so zu gestalten, dass sie den in dieser Vereinbarung beschriebenen Rahmenbedingungen gerecht werden.

6.3. Die Leistungsnehmerin stimmt den unter 15. bezeichneten Unterauftragnehmenden unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit den Unterauftragnehmenden zu. Änderungen werden gemäß 13.1 mit einer Frist von mindestens 30 Tagen angekündigt.

6.4. Widerspricht die Leistungsnehmerin der Begründung eines Unterauftragsverhältnisses, steht ihr ein Sonderkündigungsrecht zu. Sie kann ihr Nutzerkonto auf Teamlove zu jederzeit löschen und somit die Auftragsverarbeitung beenden. Das Sonderkündigungsrecht hat Vorrang gegenüber anderen Vereinbarungen über Laufzeiten und Kündigungsrechte.

6.5. Die Weitergabe von personenbezogenen Daten der Leistungsnehmerin an Unterauftragnehmende und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7. Kontrollrechte der Leistungsnehmerin

7.1. Die Leistungsnehmerin hat das Recht, im Einvernehmen mit der Leistungserbringerin Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfende durchführen zu lassen. Die Leistungsnehmerin hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch die Leistungserbringerin in deren Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

7.2. Die Leistungserbringerin stellt sicher, dass sich die Leistungsnehmerin von der Einhaltung der Pflichten der Leistungserbringerin nach Art. 28 DS-GVO überzeugen kann. Die Leistungserbringerin verpflichtet sich der Leistungsnehmerin auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8. Unterstützung durch die Leistungserbringerin

8.1. Die Leistungserbringerin unterstützt die Leistungsnehmerin bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.:

8.1.1. Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

8.1.2. Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an die Leistungsnehmerin zu melden.

8.1.3. Die Verpflichtung, die Leistungsnehmerin im Rahmen ihrer Informationspflicht gegenüber den Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

8.1.4. Die Unterstützung der Leistungsnehmerin für deren Datenschutz-Folgenabschätzung.

8.1.5. Die Unterstützung der Leistungsnehmerin im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9. Weisungsbefugnisse der Leistungsnehmerin (Art. 28, III S. 2 lit. a DS-GVO)

9.1. Mündliche Weisungen bestätigt die Leistungsnehmerin unverzüglich schriftlich oder per E-Mail (in Textform).

9.2. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung der Leistungsnehmerin. Die Leistungsnehmerin behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass sie durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf die Leistungserbringerin nur nach vorheriger schriftlicher Zustimmung durch die Leistungsnehmerin erteilen.

9.3. Die Leistungserbringerin hat die Leistungsnehmerin unverzüglich zu informieren, wenn sie der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Die Leistungserbringerin ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch die Leistungsnehmerin bestätigt oder geändert wird.

9.4. Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre durch die Leistungsnehmerin aufzubewahren.

9.5. Die Leistungsnehmerin informiert die Leistungserbringerin unverzüglich, wenn Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse festgestellt werden.

10. Löschung von Daten und Rückgabe überlassener Datenträger (Art. 28, III S. 2 lit. g DS-GVO)

10.1. Die Leistungserbringerin verwendet die Daten für keine anderen als in diesem Dokument beschriebenen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien oder Duplikate der Daten werden ohne Wissen der Leistungsnehmerin nicht erstellt. Hiervon ausgenommen sind (Sicherheits-)Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2. Die Löschung von personenbezogenen Daten wird durch die Mitarbeitenden der Leistungsnehmerin durch die Löschung der von ihnen zuvor selbst angelegten Nutzerkonten veranlasst. Die Löschung von Unternehmensdaten erfolgt durch die Löschung des Unternehmenskontos durch Mitarbeitende der Leistungsnehmerin.

10.3. Alternativ kann die Löschung von Daten durch die Leistungserbringerin initiiert werden, entweder nach Aufforderung (schriftlich oder in Textform) durch die Leistungsnehmerin oder im Falle einer einseitigen Kündigung des Vertragsverhältnisses durch die Leistungserbringerin aufgrund der in den AGB aufgeführten Ausnahmefälle.

10.4. Der Austausch von Datenträgern ist nicht vorgesehen. Im Ausnahmefall werden die überlassenen Datenträger an die Leistungsnehmerin zurückgegeben.

11. Vergütung

11.1. Die Leistungserbringerin hat einen Vergütungsanspruch für Leistungen, die über Pflichten zur Einhaltung der DS-GVO hinausgehen und die nicht auf ihr Verschulden zurückzuführen sind, sondern von der Leistungsnehmerin in Auftrag gegeben worden sind. Die Leistungserbringerin wird die Leistungsnehmerin vorab in Textform (z. B. E-Mail) über die Kostenpflichtigkeit und soweit möglich über den geschätzten Aufwand informieren. Die Kosten werden nach dem im Leistungsvertrag vereinbarten Tagessatz abgerechnet.

12. Verhältnis zu den Allgemeinen Geschäftsbedingungen (AGB)

12.1. Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen der AGB der Leistungserbringerin.

12.2. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus den AGB, gehen die Regelungen aus diesem Vertrag vor.

13. Schlussbestimmungen

13.1. Über Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen der Leistungserbringerin und Änderungen an Unterauftragsverhältnissen oder den Technisch-organisatorischen Maßnahmen – informiert die Leistungserbringerin in Textform per E-Mail oder im Nutzerkonto mit einer Frist von mindestens 30 Tagen und mit einem ausdrücklichen Hinweis darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.

13.2. Sollten einzelne Teile dieses Vertrages unwirksam sein oder werden, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht. Der unwirksame Teil soll einvernehmlich durch eine solche Bestimmung ersetzt werden, welche der ursprünglichen Absicht der Parteien wirtschaftlich und datenschutzrechtlich so weit wie möglich gleichkommt.

13.3. Im Falle von Regelungslücken werden die Parteien eine Regelung treffen, die sie getroffen hätten, wenn sie den betreffenden Punkt bei Abschluss der Vereinbarung bedacht hätten.

13.4. Gerichtsstand und anzuwendendes Recht sind in den AGB geregelt.

14. Haftung

14.1. Leistungsnehmerin und Leistungserbringerin haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

15. Liste an Unterauftragnehmenden

Für das Hosting von Teamlove kommen folgende Unternehmen zum Einsatz (Webserver sind in der EU lokalisiert):
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland
Salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 München, Deutschland

Für den Versand von System-Mails nutzen wir die folgenden Anbieter:
Sinch AB (publ.), Lindhagensgatan 74 HQ, 112 18 Stockholm, Sweden
Google Commerce Limited, Gordon House, Barrow Street, Dublin 4, Ireland

Technische und organisatorische Maßnahmen

gem. Art. 32, I DSGVO

Datum: 04. Juli 2022 **Datum der letzten Änderung:** 09. Aug 2022

1. Allgemeine Rahmenbedingungen

Die Leistungserbringerin weist darauf hin, dass die nachfolgend technisch-organisatorischen Maßnahmen dem technischen Fortschritt und Weiterentwicklungen unterliegen und dass auch alternative adäquate Maßnahmen zur Anwendung kommen können, wobei wesentliche Änderungen kommuniziert und dokumentiert werden.

2. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Vertraulichkeit als Teil der Informationssicherheit – geeignete Maßnahmen, welche sicherstellen, dass Informationen nur einem bestimmten Empfängerkreis zugänglich sind.

2.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Leistungserbringerin betreibt keine eigenen Rechenzentren, sondern mietet Webserver zum Zwecke der Durchführung und automatisierten Auswertung von Umfragen bei sorgfältig ausgewählten Drittanbietern an. Durch die Natur der Dienstleistung wird für die Zutrittskontrolle insbesondere auf die Rechenzentrumsbetreiber verwiesen. Diese sind grundsätzlich nach ISO/IEC 27001 zertifiziert und stellen den angemieteten Server in einem europäischen Rechenzentrum zur Verfügung.

Die Zutrittskontrolle zu den Geschäftsräumen der Leistungserbringerin ist für die Bereitstellung von Teamlove grundsätzlich unerheblich, da hier keine Daten gespeichert werden oder gesonderte Zugriffsmöglichkeiten auf die Daten bestehen. Zur Vollständigkeit wird sie dennoch nachfolgend beschrieben: Das ICO, in dem die Leistungserbringerin ihren Unternehmenssitz hat, ist folgendermaßen von außen und innen gesichert: Im Gebäude sind nicht vollständig zu öffnende Dreifachfenster vorhanden. Lichtschächte oder Lüftungsöffnungen, über die sich Unbefugte eventuell Zutritt zu den Büroräumen verschaffen könnten, existieren nicht. Eine Videoüberwachung findet nicht statt. In den öffentlich zugänglichen Flurbereichen befinden sich Bewegungsmelder.

Zutritt zum ICO haben grundsätzlich nur berechtigte Personen. Werktags ist die Haupteingangstür von ca. 07:30 bis 18:00 Uhr auch für Besucher:innen geöffnet. Am Abend wird die Schließung der Türen durch einen Sicherheitsdienst kontrolliert. Die Reinigungskräfte haben grundsätzlich Zutritt zu den Räumlichkeiten, haben hierfür aber eine entsprechende Erklärung unterzeichnet, die bei Bedarf beim ICO eingesehen werden kann. Im ICO Gebäude kommt ein Transponder-System als Schlüssel zum Einsatz. Die Transponder sind der Art, dass sie nicht einfach unbefugt dupliziert werden können. Die Daten des Zugangs zu jeder Tür werden für die jeweils letzten 200 Zugänge gespeichert. Die Zugänge zur Haupteingangstür außerhalb der Hauptöffnungszeiten werden grundsätzlich aufgezeichnet.

Die Büroräume im Zentrum von Osnabrück sind folgendermaßen von außen und innen gesichert: Der Zugang zu den Büroräumen ist durch verschließbare Sicherheits- und Stahltüren geschützt. Dabei kann die Tür zum Außenbereich von außen nur per

Schlüssel geöffnet werden. Die Klingelanlage hat eine Gegensprechfunktion. Zudem kann der Zugang durch ein abschließbares Rolltor zusätzlich gesichert werden. Die Dreifachfenster der Büroräume sind manuell oder elektronisch verschließbar und durch die Lage zum Innenhof wenig einsehbar. Im Außenbereich und in den Büroräumen kommen Bewegungsmelder zum Einsatz. Eine Videoüberwachung findet weder im Außenbereich noch in den Büroräumen statt. Falls Betriebsfremde Zutritt zu den Büroräumen benötigen, werden diese ständig durch Beschäftigte der IWOP GmbH begleitet. In den Büroräumen befinden sich Rauchmelder und Feuerlöscher.

Sämtliche Schlüssel zu Büroräumen der IWOP GmbH sind in einem Übersichtsdokument aufgeführt. Sowohl die Schlüsselausgabe als auch die Schlüsselrücknahme werden quittiert. Die Schlüssel von ausgeschiedenen Mitarbeitenden werden unverzüglich eingezogen. Überzählige Schlüssel werden in einem Tresor deponiert.

2.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Nach der Anlage von Teilnehmendendaten durch die Leistungsnehmerin in der Nutzeroberfläche von Teamlove werden personenbezogene Daten nur auf dem Webserver dauerhaft gespeichert. Diese verbleiben bis zur Löschung auf dem Webserver und werden auf diesem automatisiert ausgewertet. Weitere Datenträger im eigentlichen Sinne werden nicht benutzt. Durch diese Prozessarchitektur werden die Möglichkeiten zum Datenzugriff eingeschränkt und leichter kontrollierbar. Für die Gewährleistung der Zugangskontrolle ist der Serverschutz maßgebend. Dieser erfolgt über eine Secure-Shell in Kombination mit Public-Key-Authentifizierung. Uneingeschränkter Zugriff auf die Serverdatenbank ist nur nach Anmeldung auf dem Server möglich. Der Schutz des Datenbankzugangs erfolgt im zweiten Schritt durch eine Benutzername- /Passwort-Kombination. Der Schutz von anderen nicht öffentlichen Diensten erfolgt mittels Authentifizierung durch Benutzername und Passwort. Im Rahmen des Datenschutzes und der IT-Sicherheit der Leistungserbringerin existiert eine Passwortrichtlinie für die sichere Verwendung von Passwörtern nach dem Stand der Technik. Die Verwaltung von Passwörtern erfolgt in einer verschlüsselten Passwortdatei (256-Bit AES in Kombination mit einer Passphrase). Zur weiteren Sicherung des Webservers kommen Firewall-, Intrusion-Prevention-Systeme und Anti-Malware bzw. Anti-Virensoftware zum Einsatz. Die Dokumentation erfolgt über ein internes Wiki und Ticketsystem.

2.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Alle von der Leistungsnehmerin zur Verfügung gestellten Daten sowie alle im Rahmen der Befragung erhobenen Daten werden vertraulich behandelt. Dies wird mit einem Berechtigungskonzept sichergestellt: Die Anzahl von Administrator:innen sowie von Zugriffsberechtigten wird auf das Notwendigste reduziert. Zugangsberechtigungen von Mitarbeitenden sind auf die an der Softwareentwicklung oder -administration beteiligten Personen begrenzt und werden bei Bedarf (etwa zum Vertragsende eines Mitarbeitenden) durch die Systemadministrator:innen umgehend gesperrt oder gelöscht. Datenbankzugriffe wie die Eingabe, Änderung oder Löschung von Einträgen werden protokolliert. Die Löschung von Datenträgern geschieht bei Rootservern durch mehrfaches Überschreiben und die anschließende Außerdienststellung des Servers. Sollten sonstige zu vernichtende Unterlagen oder Datenträger existieren, werden diese in verschlossenen Behältern zu einem sorgfältig ausgewählten, zertifizierten und schriftlich auf Datenschutz verpflichteten Entsorgungsunternehmen transportiert und dort datenschutzkonform entsorgt.

2.4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Leistungserbringerin betreibt getrennte Systeme zur Entwicklung und zum Produktiveinsatz, eine logische Mandantentrennung besteht nicht. Datensätze sind mit Zweckattributen versehen, um eine korrekte Zuordnung der Daten zu gewährleisten.

Kommunikations- und Meinungsdaten werden in unabhängigen Datenbanktabellen gespeichert. Um die Anonymität im Feedbackverfahren zu gewährleisten, werden Feedbackergebnisse nie mit Personenbezug berichtet. Innerhalb der Teams werden die eingegebenen offenen Kommentare jedoch im Klartext berichtet und können eventuell Rückschlüsse auf einzelne Personen ermöglichen. Dieses Vorgehen ist zur Arbeit mit den Ergebnissen zwingend erforderlich. Auf Unternehmensebene werden keine Kommentare individueller Personen dargestellt, sondern nur durch Teams gemeinsam definierte Problem- und Handlungsfelder.

3. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Integrität als Teil der Informationssicherheit – geeignete Maßnahmen, welche die Korrektheit/ Unversehrtheit von Daten und die korrekte Funktionsweise von Systemen gewährleistet.

3.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Transportsicherheit der Daten wird mittels Transport Layer Security (TLS, früher SSL) sichergestellt. Bei der Erstellung und Einbindung der Verschlüsselungszertifikate kommen zur Herstellung der höchstmöglichen Sicherheit bei gleichzeitiger Sicherstellung einer hohen Kompatibilität mit Client-Systemen die von der Mozilla-Corporation empfohlenen Konfigurationsparameter für „Intermediate compatibility“ zur Anwendung. Eine Liste erlaubter Algorithmen kann zur Verfügung gestellt werden.

Der Austausch personenbezogener Daten geschieht immer in verschlüsselter Form über den Teamlove-Server. Ein Datenaustausch mittels Transportes über physische, elektronische Datenträger zwischen Leistungserbringerin und Leistungsnehmerin erfolgt in der Regel nicht.

3.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Eingabe von Meinungsdaten im Rahmen des Feedbackprozesses wird nur von den Betroffenen selbst durchgeführt. Die Eingaben können innerhalb eines Feedbackzyklus revidiert werden, danach ist eine Änderung nicht mehr möglich. Die Eingabe von personenbezogenen Daten im Rahmen der Erstellung von Teams inklusive den Teamadministrator:innen wird durch die Leistungsnehmerin selbst durchgeführt. Änderungen sind durch die Leistungsnehmerin zu dokumentieren und werden nicht im System protokolliert. Die Eingabe von personenbezogenen Daten im Rahmen der Einladung von Teammitgliedern wird durch die Teamadministrator:innen der Leistungsnehmerin durchgeführt. Änderungen sind durch Teamadministrator:innen zu dokumentieren und werden nicht im System protokolliert.

4. Gewährleistung der Verfügbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeit als Teil der Informationssicherheit – geeignete Maßnahmen, welche sicherstellen, dass IT-Systeme innerhalb der erwarteten Zeit die an sie gestellten Anforderungen erfüllen.

4.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Verfügbarkeit der Daten wird grundsätzlich durch die Auswahl von nach ISO/IEC 27001 zertifizierten Rechenzentrumsbetreibern gewährleistet. Diese bieten Schutz vor Feuer-, Rauch-, Blitz-, Gas- und Wasserschäden. Die Rechenzentrumsräume sind klimatisiert und mit einer Notstromversorgung ausgestattet. Zur Datenspeicherung kommen ausschließlich redundant ausgelegte Speichersysteme zum Einsatz. Diese ermöglichen den Austausch einzelner schadhafter Speichermedien ohne Datenverlust im laufenden Betrieb. Zusätzlich zu diesen Maßnahmen werden täglich Datenbank-Back-ups erstellt.

5. Gewährleistung der Belastbarkeit der Systeme

Beschreibung von Maßnahmen, welche die Widerstandsfähigkeit, Unempfindlichkeit und Abwehr der Systeme gegen Software-Mängel, extreme Anzahl von Anfragen, Viren, Hackerangriffe etc. sicherstellen.

Durch die eingesetzte Systemarchitektur findet der gesamte Prozess der Datenerhebung und Datenauswertung auf dem Server statt. Grundsätzlich wird die Serverkapazität an die Anforderungen des Projektes angepasst. Der Server wird sowohl manuell als auch über automatisierte Administratorenbenachrichtigungen auf den Zustand von wichtigen Leistungsdaten wie Erreichbarkeit/ Latenz und CPU-, Festplatten- und Arbeitsspeicherauslastung überwacht. Sollte dennoch ein Ressourcenengpass auftreten, stehen uns verschiedene Optionen zum Load-Balancing sowie der zusätzlichen Allokation von Serverleistung zur Verfügung. Zur Sicherung des Webservers kommen außerdem Firewall-, Intrusion-Prevention-Systeme und Anti-Malware bzw. Anti-Virensoftware zum Einsatz.

6. Wiederherstellung der Verfügbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Beschreibung der Maßnahmen, welche die Wiederherstellung der Funktionsfähigkeit der IT-Systeme innerhalb einer angemessenen Zeit nach einem Systemausfall sicherstellen.

Die Installation und Einrichtung des Umfrageservers finden über ein automatisiertes Konfigurations- und Software-Management-Tool statt. Selbst nach einem kompletten Ausfall des Produktivsystems kann so eine neue Serverkonfiguration inklusive aller sicherheits- und leistungsrelevanten Einstellungen schnellstmöglich aufgesetzt, ein Back-up der Datenbank eingespielt und das System damit in den ursprünglichen Zustand versetzt werden. Erste Ansprechperson auch bei technischen Problemen sollte grundsätzlich der Kundenservice von Teamlove sein.

7. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch-organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Beschreibung der dokumentierten Regelungen der regelmäßigen Prüfung und Aktualisierung der Informationssicherheit.

7.1. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Leistungsempfängerin verarbeitet werden können.

Der Umgang mit personenbezogenen Daten erfolgt nach den gesetzlichen Richtlinien und nach Weisung der Leistungsnehmerin, die rechtskonforme (DS-GVO, BDSG-neu und weitere anwendbare Datenschutzbestimmungen) Änderungen an Art, Umfang und Verfahren der Datenverarbeitung anregen kann. Die Mitarbeitenden der Leistungserbringerin werden auf das Datengeheimnis verpflichtet und unterzeichnen entsprechende Belehrungen. Unterauftragnehmende werden sorgfältig ausgewählt. Dabei werden Prüfungen vor Ort oder mittels zur Verfügung gestellter Unterlagen wie Zertifikaten oder Urkunden durchgeführt. Für die Durchführung der Projekte in Kooperation mit anderen Partner:innen oder Unterauftragnehmenden werden die Zuständigkeiten klar geregelt.

Die Monitoring-, Firewall-, Intrusion-Prevention- und Anti-Malware-Systeme protokollieren relevante Ereignisse und werden regelmäßig in Bezug auf den Status der Informationssicherheit ausgewertet.