­­­

**Vereinbarung zur Auftragsverarbeitung personenbezogener Daten**

|  |  |
| --- | --- |
| zwischen | und |
|  | **plazz AG**  Bahnhofstr. 5a, 99084 Erfurt |
| *vertreten durch* | *vertreten durch*  Jürgen Mayer (CEO) |
|  |  |
| im Folgenden: **Auftraggeber** | im Folgenden: **Auftragnehmer** |

# Einleitung, Geltungsbereich, Definitionen

1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

# Gegenstand und Dauer der Verarbeitung

## Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

Verarbeitung von Daten im Rahmen einer Mobile App zum Einsatz bei Veranstaltungen.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsauftrag vom XYZ (im Folgenden „Hauptvertrag“).

## Dauer

Die Verarbeitung beginnt am [DATUM] und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

# Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

## Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Die Verarbeitung dient folgendem Zweck: Bereitstellung von Veranstaltungsinformationen und Interaktionsmöglichkeiten im Zusammenhang mit den besuchten Veranstaltungen.

## Art der Daten

Es werden folgende Daten verarbeitet:

* Profildaten (z.B. ID, Vorname, Nachname, E-Mail Adresse, Firma, Position, Stadt, Profilbild, sonstige Beschreibungstexte, Gruppenzugehörigkeiten)
* Eigener User Generated Content (z.B. Favoriten, Notizen)
* Geteilter User Generated Content (z.B. Umfrageergebnisse, gestellte Fragen, Abgegebene Bewertungen, Erfasste Leads, Chatnachrichten, (in der App hinterlegte) Termine, Gamification-Ranking, Posts und Likes auf Wall-of-Ideas)
* Tracking-Daten (Opt-Out verfügbar, z.B. App-Abstürze, Empfang von iBeacons, sofern vom Auftraggeber gewünscht)

Von der Verarbeitung betroffen sind:

* Projektbeteiligte
* Teilnehmer der Veranstaltungen

# Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
8. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
9. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
10. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

# Technische und organisatorische Maßnahmen

1. Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
6. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig für die Laufzeit des Vertrags von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

# Regelungen zur Berichtigung, Löschung und Sperrung von Daten

1. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Beschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart.

# Unterauftragsverhältnisse

1. Die zukünftige Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragsverarbeiter ohne gesonderte Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.
2. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
3. Zurzeit sind für den Auftragsverarbeiter die in der Anlage 2 dokumentierten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit der Beauftragung der in Anlage 2 genannten Subunternehmer erklärt sich der Auftraggeber einverstanden.
4. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
5. Auf schriftliche Aufforderung des Auftraggebers hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmer zu erteilen.

# Rechte und Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
4. Dem Auftragnehmer steht es frei, die hinreichende Umsetzung der Pflichten aus diesem AVV-Vertrag, insbesondere der technisch-organisatorischen Maßnahmen (§ 7) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch folgende Nachweise zu belegen:

* die Einhaltung genehmigter Verhaltensregeln;
* die Zertifizierung nach einem genehmigten Zertifizierungsverfahren;
* aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision);
* eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit;
* Eigenerklärung des Auftragnehmers.

1. Der Auftraggeber kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in diesem AVV-Vertrag niedergelegten Pflichten durch die Einholung von Auskünften und Abfrage der unter (4) angeführten Nachweise beim Auftragnehmer in Hinblick auf die ihn betreffende Verarbeitung kontrollieren. Der Auftraggeber wird vorrangig prüfen, ob die in Satz 1 dieses Absatzes eingeräumte Möglichkeit der Überprüfung ausreicht. Der Auftraggeber kann darüber hinaus auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz vor Ort kontrollieren. Der Auftraggeber kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Vom Auftraggebern mit der Kontrolle betraute Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Die vom Auftraggebern mit der Kontrolle betrauten Personen oder Dritte werden dem Auftragnehmer in angemessener Form vorangekündigt und in die Lage versetzt, ihre Legitimation zur Durchführung der Kontrollen nachzuweisen. Dritte im Sinne dieses Absatzes dürfen keine Vertreter von Wettbewerbern des Auftragnehmers sein. Der Auftraggeber wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen.

# Mitteilungspflichten

1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen.
2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.
5. Die Mitteilung erfolgt an den in der Anlage festgelegte weisungsberechtigte Person seitens des Auftraggebers.

# Weisungen

1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.
3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
5. Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

# Beendigung des Auftrags

1. Bei Beendigung des Auftragsverhältnisses hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach seiner Wahl entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.
2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.
5. Die Kosten für die Vernichtung bzw. Herausgabe trägt der Auftraggeber.

# Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nur, soweit ausdrücklich geregelt.

# Haftung

1. Der Auftragnehmer ist für die Implementierung der in diesem Vertrag festgelegten Maßnahmen verantwortlich. Der Auftragnehmer haftet nicht für den Fall, dass diese Maßnahmen sich als unzureichend erweisen. Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen Dritter, insbesondere durch Behörden, in Bezug auf die Verarbeitung von personenbezogenen Daten nach diesem Vertrag frei. Art. 82 Abs. 5 DS-GVO bleibt hiervon unberührt.
2. Jegliche Haftung des Auftragnehmers aufgrund zurechenbaren Ausfalls der Ausführung dieses Vertrages oder aus jeglichem anderen Grund, untersteht der im Hauptvertrag vereinbarten Haftungsbegrenzung.

# Sonderkündigungsrecht

1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
4. Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

# Sonstiges

1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
2. Für Nebenabreden ist die Schriftform erforderlich.
3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

**Unterschriften**

Ort, Datum Ort,Datum

Auftraggeber Auftragnehmer

##### Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

**Hinweis:** Die Maßnahmen müssen im Interesse beider Parteien so konkret wie möglich beschrieben werden! Sie sind Maßstab für Kontrollen durch den Auftraggeber und auch für die Frage entscheidend, ob möglicherweise ein Pflichtverstoß vorliegt. In dieser Anlage wird ganz maßgeblich festgelegt, was der Auftragnehmer zu leisten und nachzuweisen hat und was nicht. Unklare oder interpretationsfähige Umschreibungen sind dringend zu vermeiden!

**1 Vertraulichkeit**

**1.1 Zutrittskontrolle**

Das Hosting der Software-Plattform von plazz AG erfolgt in einem Rechenzentrum von Google (Google Cloud Plattform) in Frankfurt(EU-West 03).

Eine ausführliche Dokumentation der von Google getroffenen technischen und organisatorischen Maßnahmen der Datensicherheit und der Zertifizierungen von Google aus dem Bereich der Informationssicherheit (einschließlich ISO 27001) findet sich hier: <https://cloud.google.com/terms/data-processing-terms-20180313>.

Die Büroräume der plazz AG befinden sich in einem Bürohaus in Erfurt. Die Zugänge zum Bürohaus und auch zu den Büroräumen von plazz AG sind Tag und Nacht verschlossen. Es kommt ein elektronisches Schließsystem zum Einsatz. Die Personalabteilung von plazz AG verwaltet die Schlüssel/Transponder und erteilt und entzieht die jeweiligen Zutrittsrechte. Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu dem Bürohaus und dann den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet. Jeder Besucher wird in einer Besucherliste protokolliert und dann von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Die Eingänge und Fenster des Bürohauses und auch der Büroräume sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Unabhängig davon wird die Alarmanlage täglich jedoch stets am Abend automatisch aktiviert.

**1.2 Zugangskontrolle**

Um Zugang zur Software-Plattform von plazz AG und generell zu den IT-Systemen von plazz AG zu erhalten, müssen Nutzer/innen über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Zugangsberechtigungen von Administrator/innen vergeben. Zugangsberechtigungen werden nur erteilt, wenn dies von der/dem jeweiligen Vorgesetzten beantragt wurde.

Nutzer/innen erhalten einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss. Eine Passworthistorie ist hinterlegt, so wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 10-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Accounts.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

Remote-Zugriffe auf IT-Systeme erfolgen stets über verschlüsselte Verbindungen.

Auf den Servern ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeitenden sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

**1.3 Zugriffskontrolle**

Zugriffsberechtigungen im Rahmen der Software-Plattform von plazz AG und generell für IT-Systeme und Applikationen von plazz AG werden ausschließlich von Administratoren eingerichtet.

Zugriffsberechtigungen können flexibel und granular gesetzt werden und werden grundsätzlich nach dem „Need to Know“-Prinzip auf „Least Privilege“-Basis vergeben. Es erhalten demnach nur die Mitarbeitenden Zugriffsrechte auf Daten, Datenbanken und/oder Applikationen, die diese Daten, Datenbanken und/oder Applikationen warten und pflegen bzw. in der Entwicklung tätig sind und die einen solchen Zugriff im Rahmen ihrer Tätigkeit zwingend benötigen. Voraussetzung ist eine entsprechende Anforderung der Zugriffsberechtigung für eine/n Mitarbeitende/n durch eine/n Vorgesetzte/n.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Mitarbeitende abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Die Vergabe von Admin-Rechten wird äußerst restriktiv gehandhabt.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.

Alle Mitarbeitenden sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

Mitarbeitenden ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen von plazz AG zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheitsupdates aktualisiert.

**1.4 Trennung**

Alle im Rahmen der Software-Plattform von plazz AG eingesetzten IT-Systeme sind mandantenfähig, die logische Trennung von Daten ist stets gewährleistet.

Die Produktivumgebung ist streng von der Testumgebung getrennt.

**1.5 Verschlüsselung & Pseudonymisierung**

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen. Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.

Bei einer Pseudonymisierung personenbezogener Daten erfolgt eine strikte Trennung der Zuordnungsdaten von den pseudonymisierten Daten.

Die Mitarbeitenden sind angewiesen, stets die Möglichkeit einer Pseudonymisierung oder Anonymisierung personenbezogener Daten zu prüfen und gegebenenfalls umzusetzen.

**2 Integrität**

**2.1 Eingabekontrolle**

Die Eingabe, Änderung und Löschung von (personenbezogenen) Daten wird grundsätzlich protokolliert. Die Protokollierung wird regelmäßig kontrolliert.

Mitarbeitende sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Accounts dürfen nicht mit anderen Mitarbeitenden geteilt bzw. gemeinsam genutzt werden. Es ist dementsprechend stets nachvollziehbar, wer Daten eingegeben, geändert oder gelöscht hat.

**2.2 Weitergabekontrolle**

Eine Weitergabe von personenbezogenen Daten erfolgt jeweils nur in dem Umfang, in dem dies zur Erbringung der jeweiligen vertraglichen Leistungen erforderlich ist.

Alle Mitarbeitenden werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Sämtliche Übermittlungen sind umfassend dokumentiert und es gibt detaillierte Datenflussübersichten und Aufbewahrungs- und Löschkonzepte.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern für betriebliche Zwecke ist den Mitarbeitenden untersagt.

**3 Verfügbarkeit und Belastbarkeit**

Daten auf Serversystemen werden mindestens täglich inkrementell und wöchentlich voll gesichert. Die Sicherungsmedien sind verschlüsselt. Das Einspielen von Backups wird regelmäßig getestet.

Alle relevanten IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Rechenzentrum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es besteht ein Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

**4 Informationssicherheits- und Datenschutzmanagementsystem**

**4.1 Informationssicherheits- und Datenschutzmanagementsystem**

Bei plazz AG ist ein umfassendes Informationssicherheits- und Datenschutzmanagementsystem implementiert. Die Verantwortlichkeiten in den Bereichen Informationssicherheit und Datenschutz sind eindeutig zugewiesen und dokumentiert.

Es bestehen Richtlinien zu Informationssicherheit und Datenschutz, mit denen die Umsetzung der Ziele des Informationssicherheits- und Datenschutzmanagementsystems gewährleistet wird. Die Wirksamkeit des Managementsystems und entsprechend der Richtlinien wird regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und es werden, wenn erforderlich, Anpassungen vorgenommen.

Es ist ein fachkundiger Datenschutzbeauftragter benannt und es ist zudem ein Informationssicherheits- und Datenschutzteam eingerichtet, das sämtliche Maßnahmen in den Bereichen Informationssicherheit und Datenschutz plant, umsetzt, evaluiert und Anpassungen vornimmt. Das Informationssicherheits- und Datenschutzteam berichtet direkt an die Geschäftsführung.

**4.2 Schulung und Verpflichtung der Mitarbeitenden**

Alle Mitarbeitenden bei plazz AG werden regelmäßig zu Datenschutz und Informationssicherheit geschult. Es werden regelmäßig ergänzende Awarenessmaßnahmen durchgeführt.

Alle Mitarbeitenden sind zudem auf Datenschutz und Vertraulichkeit verpflichtet. Die Verpflichtung gilt über das Ende der Tätigkeit bei plazz AG hinaus.

**4.3 Transparenz der Datenverarbeitung**

Die Transparenz der Datenverarbeitung ist vor dem Hintergrund des Geschäftsmodells von plazz AG von entscheidender Bedeutung. Plazz AG ist sich dieser Bedeutung unbedingt bewusst und legt großen Wert auf eine umfassende und klar verständliche Information der Betroffenen. Es besteht eine umfassende Dokumentation der Datenverarbeitung und die Datenschutzinformationen werden regelmäßig geprüft und erforderlichenfalls aktualisiert. Es besteht ein formalisierter Prozess zur Bearbeitung und Beantwortung von Betroffenenanfragen, die Einhaltung der entsprechenden Fristen wird stets gewährleistet.

**4.4 Dienstleistermanagement (Auftragskontrolle)**

Bei der Beauftragung von Auftragsverarbeitern wird initial und anschließend regelmäßig ein Audit durchgeführt und es wird entsprechend den datenschutzrechtlichen Vorgaben eine Vereinbarung Auftragsverarbeitung abgeschlossen. Auftragsverarbeiter werden sorgfältig ausgewählt, insbesondere hinsichtlich der Gewährleistung eines angemessenen Niveaus an Informationssicherheit und Datenschutz.

Alle Auftragsverarbeiter sind verpflichtet, personenbezogene Daten stets auf Weisung des Verantwortlichen und spätestens bei Vertragsbeendigung zu löschen. Es ist gewährleistet, dass das Aufbewahrungs- und Löschkonzept von plazz AG auch bei Auftragsverarbeitern entsprechend umgesetzt wird.

**4.5 Umgang mit Informationssicherheits- und Datenschutzvorfällen**

Plazz AG hat eine Richtlinie für den Umgang mit Informationssicherheits- und/oder Datenschutzvorfällen implementiert, in der standardisierte Prozesse für den Umgang mit potenziellen Informationssicherheits- und/oder Datenschutzvorfällen definiert werden. Informationssicherheitsbeauftragter und Datenschutzbeauftragter werden stets informiert und eingebunden. Sämtlichen potenziellen Informationssicherheits- und/oder Datenschutzvorfälle werden dokumentiert und jeder Vorfall wird dahingehend analysiert, ob und welche Maßnahmen ergriffen werden können, um zukünftig ähnliche Vorfälle auszuschließen.

Es werden Firewalls und Spamfilter eingesetzt und laufend aktualisiert.

Alle Mitarbeitenden werden dahingehend instruiert, potenzielle Vorfälle auch beim geringsten Verdacht an das Informationssicherheits- und Datenschutzteam zu melden. Plazz AG gewährleistet stets die fristgerechte Meldung, sofern bei einem Informationssicherheits- und/oder Datenschutzvorfall gesetzliche Meldepflichten bestehen.

**4.6 Privacy by Design und Privacy by Default**

Bereits bei der Entwicklung bzw. Weiterentwicklung sowohl des Geschäftsmodells generell wie auch der Software-Plattform von plazz AG wird Sorge dafür getragen, dass den Grundsätzen der Datensparsamkeit und Datenminimierung Rechnung getragen wird.

Es werden stets nur die personenbezogenen Daten erhoben, die für den jeweiligen Zweck zwingend erforderlich sind. Es wird bei jedem Verarbeitungsvorgang kontinuierlich geprüft, ob eine Erforderlichkeit der Verarbeitung personenbezogener Daten besteht oder ob eine Anonymisierung vorgenommen werden kann.

##### Anlage 2 – Zugelassene Subdienstleister

|  |  |
| --- | --- |
| Name und Anschrift des Subunternehmers | Beschreibung der Teilleistungen |
| Neue Medien Münnich (ALL-INKL.COM) Hauptstraße 68  D-02742 Friedersdorf  Deutschland | Hosting der Anwendung und des Backends (Rechenzentrum Dresden) |
| Keyweb AG  Neuwerkstraße 45/46  D-99084 Erfurt  Deutschland | Hosting der Tracking-Tools  (Rechenzentrum Erfurt) |
| Microsoft Ireland Operations Limited  70 Sir John Rogerson's Quay  Dublin 2  Irland | Datenverarbeitung auf der Office 365 Plattform  Backups  (Rechenzentrum Amsterdam & Dublin) |
| Google Commerce Limited  Gordon House  Barrow Street  Dublin 4  Ireland | Hosting der Anwendung und des Backends bei Nutzung des Cloud Deployments  Backups  (Rechenzentrum Frankfurt) |
| Mailjet SAS  13-13 bis, Rue de l'Aubrac  75012 Paris  France | Email Verarbeitung und Auslieferung  (Rechenzentrum EU) |
| Freshworks GmbH  Alte Jakobstraße 85/86  10179 Berlin  Deutschland | Ticketsystem und IT Helpdesk  (Rechenzentrum EU – Frankfurt a. M.) |
| 3Q GmbH  Kurfürstendamm 102  10711 Berlin  Deutschland | Streaming und Hosting von Mediendaten  Rechenzentrum EU |

##### Anlage 3 – Weisungsberechtige Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Stefan Benischke – Technischer Leiter

Stefan Heinz – Leiter Productboard

Nicole Sauter – Customer Support

Berra Eksen – Sales

##### Anlage 4 – Kontaktdaten des Datenschutzbeauftragten

Datenschutzbeauftragte

Jonas Jöck & Julia Pudenz extern von Juno

E-Mail: [datenschutz@plazz.ag](mailto:datenschutz@plazz.ag)

Telefon: +49 361 55899161