Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen dem

Vertragspartner

nachstehend **„Verantwortlicher“**

und dem

PL Gutscheinsysteme GmbH
Ainmillerstraße 11
80801 München

nachstehend **“Auftragsverarbeiter“**

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Auftragsverhältnis im Sinne des Art. 28 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, **„DSGVO**“).

Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als **„Vereinbarung**“ bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem zugrundeliegenden Hauptleistungsvertrag zwischen den Parteien über die Nutzung des Produktes „Givve Lunch“ durch den Verantwortlichen (dieser Hauptleistungsvertrages nachfolgend gemeinsam als **„Hauptvertrag**“ bezeichnet). Sofern Bezug auf die Regelungen des Bundesdatenschutzgesetzes (nachfolgend **„BDSG**“) genommen wird, so ist damit das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 in der zum Zeitpunkt ab dem 25. Mai 2018 geltenden Fassung gemeint.

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen zur Erfüllung des Hauptvertrages und dieser Vereinbarung nach Maßgabe der folgenden Bestimmungen:

§ 1 Anwendungsbereich und Begriffsbestimmungen

(1) Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 DSGVO, die der Auftragsverarbeiter auf Grundlage des Hauptvertrages gegenüber dem Verantwortlichen erbringt.

(2) Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ von Daten benutzt wird, ist darunter allgemein die Verwendung von personenbezogenen Daten zu verstehen. Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) Auf die weiteren Begriffsbestimmungen in Art. 4 DSGVO wird verwiesen.

(4) Im Übrigen finden die Begriffsdefinitionen aus dem Hauptvertrag auf die in dieser Vereinbarung entsprechend Anwendung.

§ 2 Gegenstand und Dauer der Datenverarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.

(2) Gegenstand des Auftrags ist die Bereitstellung einer Software-Applikation („**App**“) durch den Auftragsverarbeiter zur Einreichung von dienstlichen Verpflegungsbelegen der Mitarbeiter der Verantwortlichen und der Nutzung dieser App durch den Verantwortlichen und dessen Arbeitnehmer im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs, gemäß dem Hauptvertrag.

(3) Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

§ 3 Art und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Dieser umfasst folgende Tätigkeit(en) und Zweck(e):

- Hochladen von Verpflegungsbelegen durch Arbeitnehmer des Verantwortlichen über die APP in Form von mit den Smartphones der Arbeitnehmer aufgenommenen Fotos dieser Belege;
- Prüfung der Erstattungsfähigkeit der auf den Belegen enthaltenen Rechnungsposten durch Mitarbeiter des Auftragsverarbeiters;
- Erstellung von Abrechnungsbelegen zu den erstattungsfähigen Rechnungsposten durch den Auftragsverarbeiter und Übersendung dieser Beleg an den Verantwortlichen.

§ 4 Kategorien betroffener Personen

Im Rahmen dieser Vereinbarung werden personenbezogene Daten von folgenden Kategorien betroffener Personen verarbeitet:

- Arbeitnehmer des Verantwortlichen

§ 5 Art der personenbezogenen Daten

Von der Auftragsverarbeitung sind folgende Datenarten betroffen:

- Personenstammdaten (Name, Anrede, Titel/akademischer Grad)
- Kontaktdaten (E-Mail-Adresse)
- Daten auf seitens der Arbeitnehmer des Verantwortlichen über die App hochgeladenen Verpflegungsbelegen (Datum, Zeit, Beschreibung der Ausgabe, Betrag der Ausgabe in Euro, Vertragspartner, Ort, verwendetes Zahlungsmittel)

§ 6 Rechte und Pflichten des Verantwortlichen

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig und somit für die Verarbeitung Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

(2) Der Verantwortliche ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragsverarbeiters unverzüglich vom Verantwortlichen schriftlich oder in Textform (z.B. per E-Mail) zu bestätigen.

(3) Soweit es der Verantwortliche für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Verantwortliche dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Verantwortlichen ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.

(4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter festgestellt werden.

§ 7 Pflichten des Auftragsverarbeiters

(1) Datenverarbeitung

Der Auftragsverarbeiter wird personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden

Hauptvertrages sowie nach den Weisungen des Verantwortlichen zu verarbeiten.

(2) Betroffenenrechte

(a) Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Sollte der Auftragsverarbeiter die in § 5 dieser Vereinbarung genannten personenbezogenen Daten im Auftrag des Verantwortlichen verarbeiten und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität gem. Art. 20 DSGVO, wird der Auftragsverarbeiter dem Verantwortlichen den betreffenden Datensatz innerhalb einer angemessen gesetzten Frist, im Übrigen innerhalb von sieben Arbeitstagen, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

(b) Der Auftragsverarbeiter hat auf Weisung des Verantwortlichen die in § 5 dieser Vereinbarung genannten personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Das Gleiche gilt, wenn diese Vereinbarung eine Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten vorsieht.

(c) Soweit sich eine betroffene Person unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung der in § 5 dieser Vereinbarung genannten personenbezogenen Daten wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich nach Erhalt an den Verantwortlichen weiterleiten.

(3) Kontrollpflichten

(a) Der Auftragsverarbeiter stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden.

(b) Der Auftragsverarbeiter wird sein Unternehmen und seine Betriebsabläufe so gestalten, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(c) Der Auftragsverarbeiter bestätigt, dass er gem. Art. 37 DSGVO und, sofern anwendbar, gemäß § 38 BDSG einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht. Datenschutzbeauftragter des Auftragsverarbeiters ist derzeit:

Felix Bonstein
ISiCO Datenschutz GmbH
Am Hamburger Bahnhof 4
10557 Berlin

(4) Informationspflichten

(a) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine von dem Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

(b) Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen.

(5) Ort der Datenverarbeitung

Die Verarbeitung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(6) Löschung der personenbezogenen Daten nach Auftragsbeendigung

Nach Beendigung des Hauptvertrages wird der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder

zurückgeben, sofern der Löschung dieser Daten keine gesetzlichen Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen. Die datenschutzgerechte Löschung ist zu dokumentieren und gegenüber dem Verantwortlichen auf Anforderung zu bestätigen.

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche ist berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters oder Gefährdung der Sicherheitsmaßnahmen für andere Verantwortliche und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Auftragsverarbeiters aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte durchgeführt werden. Der Auftragsverarbeiter wird die notwendige Unterstützung zur Durchführung der Kontrollen anbieten.

(2) Der Auftragsverarbeiter wird den Verantwortlichen über die Durchführung von Kontrollmaßnahmen der Aufsichtsbehörde informieren, soweit die Maßnahmen oder Datenverarbeitungen betreffen können, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

§ 9 Unterauftragsverhältnisse

(1) Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Auftragsverarbeiter gemäß den nachfolgenden Absätzen in § 9 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. Art. 28 Abs. 2 DSGVO dar.

(2) Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den in der Anlage 2 benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

(3) Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragsverarbeiter wird den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Änderung Einspruch erheben.

(4) Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragsverarbeiter zu erheben. Im Fall des Einspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragsverarbeiter nicht zumutbar ist – etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für den Auftragsverarbeiter – oder die Abstimmung eines weiteren Auftragsverarbeiters fehlschlägt, können der Verantwortliche und der Auftragsverarbeiter diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.

(5) Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich.

§ 10 Vertraulichkeit

(1) Der Auftragsverarbeiter ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit verpflichtet.

(2) Der Auftragsverarbeiter verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Die

Vornahme der Verpflichtungen wird der Auftragsverarbeiter dem Verantwortlichen auf Nachfrage nachweisen.

(3) Sofern der Verantwortliche anderweitigen Geheimnisschutzregeln unterliegt, wird er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird seine Mitarbeiter entsprechend den Anforderungen des Verantwortlichen auf diese Geheimnisschutzregeln verpflichten.

§ 11 Technische und organisatorische Maßnahmen

(1) Die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Der Auftragsverarbeiter kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.

(2) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art. 32 i.V.m Art. 5 Abs. 1 DSGVO. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird der Auftragsverarbeiter die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

§ 12 Haftung/ Freistellung

(1) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Eine Ersatzpflicht des Auftragsverarbeiters besteht nicht, sofern der Auftragsverarbeiter nachweist, dass er die ihm überlassenen Daten des Verantwortlichen ausschließlich nach den Weisungen des Verantwortlichen verarbeitet und seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nachgekommen ist.

§ 13 Sonstiges

(1) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung. Mündliche Nebenabreden bestehen nicht und sich auch für künftige Änderungen dieser Vereinbarung ausgeschlossen.

(3) Diese Vereinbarung unterliegt deutschem Recht.

(4) Sofern der Zugriff auf die Daten, die der Verantwortliche dem Auftragsverarbeiter zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich hierüber zu benachrichtigen.

Anlagenverzeichnis

Anlage 1: Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Anlage 2: Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Anlage 1

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung der Pseudonymisierung:

Soweit ein Personenbezug bzw. -beziehbarkeit aufgrund des Zwecks der Datenverarbeitung erforderlich und eine Aonymisierung der verarbeiteten personenbezogenen Daten nicht möglich ist, erfolgt eine Pseudonymisierung bzw. eine Verarbeitung von pseudonymisierten oder pseudonymen Daten. Eine Verarbeitung von nicht-pseudonymisierten Klardaten erfolgt nur dort, wo der Verarbeitungszweck nicht mit der Verarbeitung von pseudonymen bzw. pseudonymisierten Daten erreicht werden kann.

B. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

- Symmetrische / Asymmetrische Verschlüsselung
- Blockalgorithmen (z. B. AES, 3DES)
- Stromchiffrierungen (A5-Algorithmus)

Der Cloud Provider „Google LLC" hat folgende Maßnahmen ergriffen:

"Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough"

C. Maßnahmen zur Sicherung der Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Beschreibung des Zutrittskontrollsystems:

Das Büro der PL Gutscheinsysteme GmbH wird durch eine abgesperrte Bürotür oder über einen codegesicherten Aufzug betreten. Zugang zu dem Büro hat jeder Mitarbeiter sowie das Reinigungspersonal.

Der Cloud Provider **„Google LLC"** hat folgende Maßnahmen für die Datenzentren ergriffen:

„On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they

wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity."

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- Kennworte werden als gesalteter kryptographischer Hash gespeichert
- Kennwortstärke wird durch ein unteres Limit an Entropie-Bits gewährleistet
- Kennworte für Nutzer mit besonderen Rechten die über Kundenrechte hinausgehen haben eine begrenzte Lebenszeit
- Begrenzte Zahl an Mitarbeitern haben direkten Zugriff auf Produkte von Dienstleistern die Einblick in geschützte Daten erlauben
- Sofern Dienstleister für ihre Produkte ein Anmeldeverfahren mit MFA anbieten wird diese genutzt.
- Individuelles Benutzerkontensystem: Für den Zugriff ist die Eingabe von individualisierten Nutzernamen und Kennwort erforderlich.

3. Zugriffskontrolle

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

Beschreibung des Zugriffskontrollsystems:

- Berechtigungskonzepte (Profile, Rollen, etc.) und deren Dokumentation
- Protokollierung von Zugriffen und Missbrauchsversuchen

4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Trennung von Test und Produktivsystem
- Mandantentrennung durch Berechtigungskonzepte mit Gruppenzugehörigkeiten und Rollensystem. Abfragen von Daten einzelner Gruppen ist nur Mitgliedern dieser Gruppen möglich.
  Datenzugriff innerhalb von Gruppen wird anhand von Rollen gesteuert, welche der Gruppenmitgliedschaft des durchführenden Benutzers zugeordnet sind

D. Maßnahmen zur Sicherung der Integrität

1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität:

- Einspielen neuer Releases und Patches mit Release-/Patchmanagement
- Funktionstest bei Installation und Releases/Patches durch IT-Abteilung
- Prüfen von übertragenen Daten soweit möglich auf syntaktische und semantische Korrektheit

Der Cloud Provider „Google LLC" hat folgende Maßnahmen ergriffen:

"Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems."

2. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

Beschreibung der Übertragungskontrolle:

- Bei einem Datenzugriff ist eine Autorisierung erforderlich. Der Datenzugriff ist abhängig von der Rollen- und Gruppenzugehörigkeit des ausführenden Benutzers.

Der Cloud Provider „Google LLC" hat folgende Maßnahmen ergriffen:

"Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols."

3. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Beschreibung der Transportkontrolle:

- Jede Datenverbindung von oder zu Endpunkten, die sich nicht innerhalb unserer gesicherten Netzwerke befinden, werden nur über kryptographisch verschlüsselte Netzwerkverbindungen durchgeführt.
- Die Konfiguration der Verschlüsselung entspricht zeitgemäßen "Best Practices".

Der Cloud Provider „Google LLC" hat folgende Maßnahmen ergriffen:

"Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough"

4. Eingabekontrolle

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

Beschreibung des Eingabekontrollvorgangs:

- Auditlog: Zu jeder durchgeführten Aktion werden ausführender Benutzer, Zeitpunkt, Quell-IP und Ergebnis der Aktion (erfolgreich, nicht erfolgreich) festgehalten.

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

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

Beschreibung des Verfügbarkeitskontrollsystems:

- Datensicherungsverfahren
- Automatische Skalierung der Serverumgebung abhängig von den erforderlichen Kapazitäten

Der Cloud Provider „Google LLC" hat folgende Maßnahmen ergriffen:

"Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs."

2. Rasche Wiederherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Wiederherstellbarkeit:

- Datensicherung

3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

- Automatisiertes Prüfen der Verfügbarkeit und Performance von Datenbank und Servern

Der Cloud Provider „Google LLC" hat folgende Maßnahmen ergriffen:

„Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. tightly controlling the size and make-up of Google's attack surface through preventative measures;
2. employing intelligent detection controls at data entry points; and
3. employing technologies that automatically remedy certain dangerous situations.
Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents."

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Jährliches Überprüfen der AVV unserer Sub-Auftragsverarbeiter auf Änderungen
- Regelmäßiges, internes Überprüfen unserer Prozesse im Hinblick auf die Implementierung der hier genannten TOM durch eigens dafür vorgesehene Mitarbeiter.

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Beschreibung der Maßnahmen zur Auftragskontrolle:

- Eindeutige Vertragsgestaltung, die die Weisungen des Auftraggebers dokumentiert
- Formalisiertes Auftragsmanagement
- Ticket-System: Anfragen werden automatisch als Ticket erfasst, wodurch Weisungen stets protokolliert werden.

Anlage 2

Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

1. Google LLC

Name/Firma: Google LLC
Funktion/Tätigkeit: Cloud Provider / Server & Infrastruktur Hosting
Sitz [Stadt, Land]: Mountain View, California 94043, USA

2. MongoDB Limited

Name/Firma: MongoDB Limited
Funktion/Tätigkeit: Datenbank Hosting
Sitz [Stadt, Land]: Dublin, Ireland

3. New Relic, Inc.

Name/Firma: New Relic Inc
Funktion/Tätigkeit: Performance Metriken
Sitz [Stadt, Land]: San Francisco, CA 94105, USA

4. Functional Software, Inc.

Name/Firma: Functional Software, Inc.
Funktion/Tätigkeit: Exception Handling
Sitz [Stadt, Land]: San Francisco, CA 94107, USA

5. Help Scout, Inc.

Name/Firma: Help Scout Inc.
Funktion/Tätigkeit: Helpdesk-System
Sitz [Stadt, Land]: Boston, MA 02108, USA

6. Quopio KG

Name/Firma: Quopio KG
Funktion/Tätigkeit: Callcenter
Sitz [Stadt, Land]: Hagen, Deutschland