Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO // *Agreement in accordance with Sec. 28 GDPR for the commissioned processing of personal data*

Vereinbarung zwischen der //
Agreement between

Unternehmen, Straße Hausnummer, PLZ Ort

Company, Street, House number, Postcode, Town

Verantwortlicher // ***Controller***

nachstehend **Auftraggeber** genannt //
hereinafter referred to as ***Principal***

und der // *and*

Myra Security GmbH
Landsberger Straße 187
80687 München, Germany

Auftragsverarbeiter // ***Processor***

nachstehend **Auftragnehmer** genannt //
hereinafter referred to as ***Service Provider***

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Der Gegenstand des Vertrags zur Auftragsverarbeitung konkretisiert die datenschutzrechtlichen Vorgaben, die sich aus dem zwischen Verantwortlichem und Auftragsverarbeiter geschlossenen Vertrag ergeben.

(2) Dauer

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Vertrages / der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

1. Subject and duration of the commission

(1) Subject

☒ *The subject of the commission substantiates the data protection requirements resulting from the contract concluded between the Controller and the Processor.*

(2) Duration

☒ *The duration of this commission (term) corresponds to the term of the contract/service agreement*.

or (*especially if no service agreement regarding duration exists*)

☐ *The commission is issued for one-time execution.*

or

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von zwei Wochen zum Ende der Laufzeit gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

☐ *The duration of this commission (term) is limited until .....*

or

☐ *The commission is issued for an indefinite period and may be terminated by either party with two weeks' notice to the end of the term. The possibility of termination without notice remains unaffected.*

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Bereitstellung des IT-Sicherheitsdienstes EU-Captcha zur Erkennung automatisierter Zugriffe (Bot-Erkennung), Abwehr von Spam, Schutz vor Angriffen (z. B. Credential Stuffing) sowie zur Sicherstellung der Funktionsfähigkeit und Sicherheit der Webanwendungen des Auftraggebers. Die Verarbeitung erfolgt ausschließlich zu IT-Sicherheitszwecken.

(2) Art der Daten

☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

☐ Personenstammdaten

☐ Kommunikationsdaten (z.B. Telefon, E-Mail)

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ Planungs- und Steuerungsdaten

☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

2. Specification of the content of the commission

(1) *Nature and purpose of the intended processing of data*

☒ *Provision of the EU-Captcha IT security service for the detection of automated access (bot detection), the prevention of spam, protection against attacks (e.g. credential stuffing), and to ensure the functionality and security of the client's web applications. Data processing is carried out exclusively for IT security purposes.*

(2) Type of data

☒ *The following types/categories of data are the subject of the processing of personal data (list/description of data):*

☐ *Personal master data*

☐ *Communication data (e.g. telephone, e-mail)*

☐ *Contract master data (contractual relationship, product, or contractual interest)*

☐ *Customer history*

☐ *Contract billing and payment data*

☐ *Planning and controlling data*

☐ *Information (from third parties, e.g. credit agencies, or from public directories)*

☒ Session IDs und weitere Cookie- oder Cookie-ähnliche Daten

☐ Wallet-Adressen

☐ Benutzernamen

☒ Log-Daten (IP-Adresse, Zeitstempel, aufgerufene URL/Ressource, technische Verbindungsdaten)

☒ Gerätedaten (Browsertyp/-version, Betriebssystem, Gerätetyp)

☒ Interaktions- und Umgebungsdaten (technische Nutzungsparameter, ggf. Maus-/Interaktionssignale zur Bot-Erkennung)

(3) Kategorien betroffener Personen

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Ansprechpartner des Auftraggebers (Backend-Login, Rechnungslegung etc.)
- Nutzer der Web-Applikationen des Auftraggebers
- Besucher der Webseite des Auftraggebers

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt

☒ *Session IDs and other cookie or cookie-like data*

☐ Wallet addresses

☐ Usernames

☒ Log data (IP address, timestamp, URL/resource accessed, technical connection data)

☒ Device data (browser type/version, operating system, device type)

☒ Interaction and environmental data (technical usage parameters, and, where applicable, mouse/interaction signals for bot detection)

(3) *Categories of data subjects*

☒ *The categories of data subjects concerned by the processing include:*

- *Contact persons of the Principal (back-end login, invoicing, etc.)*
- *Users of the web applications of the Principal*
- *Visitors to the Principal's website*

3. Technical and organizational measures

(1) Prior to the commissioning, the Service Provider shall document the implementation of the required technical and organizational measures set out in advance of the commissioning, in particular with regard to the actual execution of the commission and shall submit them to the Principal for review. If accepted by the Principal, the documented measures shall become the basis of the commission. If the Principal's review/audit reveals a need for adaptation, this shall be implemented by mutual agreement.

(2) The Service Provider shall establish security pursuant to Secs. 28 para. 3 lit. c, 32 GDPR, in connection with Sec. 5 para. 1, para. 2 GDPR. The measures to be taken are

handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

measures of data security and to ensure a level of protection appropriate to the risk regarding confidentiality, integrity, availability, and the resilience of the systems. In this regard, the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons within the meaning of Sec. 32 para. 1 GDPR must be considered [details in Annex 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Service Provider is permitted to implement alternative adequate measures. However, the security level of the specified measures must not deteriorate. Significant changes shall be documented.

4. Berichtigung, Einschränkung und Löschung von Daten

4. Correction, restriction and deletion of data

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(1) The Service Provider may not correct, delete or restrict the processing of data processed as part of the commission on its own authority, but only in accordance with documented instructions from the Principal. If a data subject contacts the Service Provider directly in this regard, the Service Provider shall forward this request to the Principal without delay.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Daten von Ansprechpartner des Auftraggebers werden für die Erbringung von Supportleistungen und für die Nachverfolgbarkeit der Supportvorgänge sowie aufgrund von gesetzlichen Vorgaben (bspw. HGB etc.) auch nach Beendigung der Zusammenarbeit weiter gespeichert.

(2) Insofar as included in the scope of services, the deletion concept, right to be forgotten, correction, data portability and information shall be ensured directly by the Service Provider in accordance with the documented instructions of the Principal. Data of contact persons of the Principal shall continue to be stored for the provision of support services and for the follow-up of support processes as well as due to legal requirements (e.g. German Commercial Code, etc.) even after termination of the cooperation.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt: Christian Volkmer, Projekt 29 GmbH & Co. KG, Ostengasse 14, 93047 Regensburg, Tel.: +49-941-298693-0, Fax: +49-941-298693-16, E-Mail: info@projekt29.de.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Europäischen Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 Satz 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer 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. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5. Quality Assurance and other duties of the Service Provider

In addition to complying with the provisions of this commission, the Service Provider shall have legal obligations pursuant to Secs. 28 to 33 GDPR; in this regard, the Service Provider shall in particular ensure compliance with the following requirements:

a) ☒ *Written appointment of a data protection officer who performs his duties in accordance with Secs. 38 and 39 GDPR.*

The data protection officer appointed by the Service Provider is: Christian Volkmer, Projekt 29 GmbH & Co. KG, Ostengasse 14, 93047 Regensburg, Germany, Tel.: +49-941-298693-0, Fax: +49-941-298693-16, E-mail: info@projekt29.de.

The Principal must be informed immediately of any change of data protection officer.

b) ☐ *The Service Provider is not obliged to appoint a data protection officer. Mr./Mrs. [enter: first name, last name, organizational unit, telephone, e-mail] shall be named as the contact person at the Service Provider.*

c) ☐ *As the Service Provider has its registered office outside the European Union, it shall appoint the following representative in accordance with Sec. 27 para. 1 GDPR in the Union: [Enter: first name, last name, organizational unit, telephone, e-mail].*

d) *Maintaining confidentiality in accordance with Secs. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the work, the Service Provider shall only use employees who have committed themselves to confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The Service Provider and any person subordinate to the Service Provider who has access to personal data may process such data solely in accordance with the Principal's instructions, including the powers granted in this agreement, unless they are required by law to process such data.*

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers 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 beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits 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 beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu

e) *The implementation of and compliance with all technical and organizational measures required for this commission pursuant to Secs. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in Annex 1].*

f) *Upon request, the Principal and the Service Provider shall cooperate with the supervisory authority in the performance of its duties.*

g) *The immediate information of the Principal about control actions and measures of the supervisory authority, as far as they relate to this commission. This shall also apply insofar as a competent authority investigates in the context of administrative offense or criminal proceedings regarding the processing of personal data during the commissioned processing at the Service Provider.*

h) In the event that the Principal is subject to control by the supervisory authority, administrative or criminal proceedings, a liability claim by a data subject or a third party, or any other claim in connection with the processing of the order by the Service Provider, the Service Provider shall support the Principal to the best of its ability.

i) In order to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and the protection of the rights of the data subject, the Service Provider shall regularly monitor the internal processes as well as the technical and organizational measures.

j) Verifiability of the technical and organizational measures taken vis-à-vis the Principal within the scope of its control powers pursuant to clause 7 of this agreement.

6. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision shall be understood to be those services which directly relate to the provision of the main service. This does not include ancillary services which the

gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikations-leistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Service Provider uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Service Provider is obliged to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Principal's data also in the case of outsourced ancillary services.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

☐ Eine Unterbeauftragung ist unzulässig.

☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

(2) The Service Provider may only engage subcontractors (further processors) with the prior express written or documented consent of the Principal.

☐ *Subcontracting is not permitted.*

☐ *The Principal consents to the commissioning of the following subcontractors subject to the condition of a contractual agreement in accordance with Sec. 28 paras. 2-4 GDPR:*

Unterauftragnehmer // *Subcontractor*	Leistung // *Service*

Die Myra Security GmbH setzt keine Unterauftragnehmer zur Verarbeitung von personenbezogenen Daten ein. Die Server der Myra Security GmbH stehen in Colocation-/Housing-Rechenzentren des umfangreich zertifizierten/testieren IT-Scopes.

In den Rechenzentren (RZ) werden nur Housing-Dienstleistungen (Anmietung von Racks sowie unterbrechungsfreie Stromversorgung, Klimatisierung, physische Sicherheit, Internetzugang usw.) genutzt. In

Myra Security GmbH does not use subcontractors for the processing of personal data. Myra Security GmbH's servers are located in colocation/housing data centres of the extensively certified and tested IT scope.

Only housing services (rental of racks, as well as uninterruptible power supply, air conditioning, physical security, internet access, etc.) are utilised in the data centres (DCs). Myra Security GmbH's own servers are located in the DCs. The DC service providers have no access to data on Myra

den RZ stehen die eigenen Server der Myra Security GmbH. Die RZ-Dienstleister haben keinen Zugriff auf Daten der Myra Security GmbH Server. Die Administration aller Daten erfolgt ausschließlich durch die IT-Administration der Myra Security GmbH 24/7/365.

Security GmbH's servers. All data is administered exclusively by Myra Security GmbH's IT administration team 24/7/365.

☐ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

☒ *The outsourcing to subcontractors or*

☒ *the change of the existing subcontractor is allowed, insofar as:*

- *the Service Provider notifies the Principal of such outsourcing to subcontractors a reasonable time in advance in writing or in text form, and*
- *the Principal does not object to the planned outsourcing in writing or in text form to the Service Provider by the time of the transfer of the data and*
- *a contractual agreement in accordance with Sec. 28 paras. 2-4 of the GDPR is used as a basis.*

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(3) The transfer of personal data of the Principal to the subcontractor and the subcontractor's first activity shall be permitted only after all requirements for subcontracting have been met.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Service Provider shall ensure that it is admissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

(5) Another outsourcing by the subcontractor

☐ *is not allowed;*

☐ *requires the express consent of the main principal (at least in text form);*

☐ *requires the express consent of the main service provider (at least in text form);*

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

All contractual provisions in the contractual chain must also be imposed on the further subcontractor.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen je nach Situation und Erfordernis durch:

- die Einhaltung genehmigter Verhaltens-regeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschut-zauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7. Control rights of the Principal

(1) The Principal shall be entitled to carry out inspections in consultation with the Service Provider or to have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Service Provider's compliance with this agreement in its business operations by means of spot checks, which must generally be notified in a timely manner.

(2) The Service Provider shall ensure that the Principal can satisfy itself of the Service Provider's compliance with its obligations pursuant to Sec. 28 of the GDPR. The Service Provider undertakes to provide the Principal with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.

(3) The proof of such measures, which do not only concern the concrete order, can take place depending upon situation and requirement by:

- *compliance with approved codes of conduct in accordance with Sec. 40 GDPR;*
- *certification in accordance with a data protection certification mechanism in accordance with Sec. 42 GDPR;*
- *current attestations, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors);*
- *suitable certification by IT security or data protection audit (e.g. according to BSI-Grundschutz).*

8. Mitteilung bei Verstößen des Auftragnehmers

8. Notification of violations by the Service Provider

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

(1) The Service Provider shall support the Principal in complying with the obligations set out in Secs. 32 to 36 of the GDPR regarding the security of personal data, data breach notification obligations, data protection impact assessments and prior consultations. This includes, among other things

a) 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

a) Ensuring an adequate level of security through technical and organizational measures that consider the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a potential security breach, and allow for the immediate detection of relevant breach events

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

b) The obligation to report personal data breaches to the Principal without delay

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

c) the obligation to support the Principal within the scope of his duty to inform the data subject and to provide him with all relevant information in this context without delay

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

d) the support of the Principal for its data protection impact assessment

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

e) the support of the Principal within the framework of prior consultations with the supervisory authority

9. Weisungsbefugnis des Auftraggebers

9. Authority of the Principal to issue instructions

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(1) The Principal shall confirm verbal instructions without delay (at least in text form).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(2) The Service Provider shall inform the Principal without delay if it is of the opinion that an instruction violates data protection regulations. The Service Provider shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Principal.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Daten-bestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Daten-verarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Access-Logs inklusive IP-Adressen werden für eine maximale Dauer von zehn Tagen aufbewahrt. Darunter sind diese Logs zu verstehen, welche die Aufrufe auf die jeweilige URL des Verantwortlichen loggen.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be made without the knowledge of the Principal. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data that is required regarding compliance with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Principal - at the latest upon termination of the service agreement - the Service Provider shall hand over to the Principal all documents, created processing and usage results as well as data files related to the contractual relationship that have come into its possession or, after prior consent, destroy them in accordance with data protection regulations. The same shall apply to test and reject material. The protocol of the deletion shall be submitted upon request.

(3) Documentation that serves as proof of the orderly and proper data processing shall be retained by the Service Provider beyond the end of the contract in accordance with the respective retention periods. He may hand them over to the Principal for his discharge at the end of the contract.

(4) Access logs, including IP addresses, are stored for a maximum period of ten days. These logs are understood to be those that log visits to the respective URL of the Principal.

11. Haftung

Auf Art. 82 DSGVO wird verwiesen.

11. Liability

Reference is made to Sec. 82 GDPR.

12. Anlagen

Folgende Anlagen sind Bestandteil dieser Vereinbarung:

Anlage 1: Technische und Organisatorische Maßnahmen (TOM)

12. Annexes

The following annexes are part of this agreement:

Annex 1: Technical and Organizational Measures (TOM)

13. Maßgebliche Sprache

Bei Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung, insbesondere über deren Auslegung, ist allein die deutsche Fassung maßgeblich.

13. Authoritative Language

In the case of any dispute arising out of or in connection with this agreement, in particular regarding its interpretation, the German version alone shall be authoritative.

Ort, Datum *Place, date*	Ort, Datum *Place, date*
Unterschrift Auftraggeber *Signature Principal*	Unterschrift Auftragnehmer *Signature Service Provider*

Anlage 1 – Technische und organisatorische Maßnahmen // *Annex 1 – Technical and Organizational Measures (TOM)*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
0	**Organisation**		***0***	***Organization***	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutz-beauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem BDSG (neu DSGVO) eingesetzt.		*How is the implementation of data protection organized?*	*An external data protection officer is appointed to perform the advisory and control functions arising from the German "Federal Data Protection Act" (hereafter "BDSG") (new GDPR).*
	Namen und Kontaktdaten des Datenschutzbeauftragten.	Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg Tel.: +49-941-298693-0 Fax: +49-941-298693-16 E-Mail: info@projekt29.de		*Name and contact details of the data protection officer.*	*Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg, Germany Tel.: +49-941-298693-0 Fax: +49-941-298693-16 E-mail: info@projekt29.de*
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit als auch eine konstante Sensibilisierung durch monatliche Datenschutz Newsletter, fachbezogene Sondertermine und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.		*In what form are employees trained on the implementation of the agreed technical and organizational measures that apply to this processing?*	*The training concept includes data protection instruction at the beginning of the job as well as constant sensitisation through monthly data protection newsletters, special subject-related appointments and personal sensitisation by the external data protection officer.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
		Zusätzlich ist ein E-Learning Tool für regelmäßige Security Awareness Trainings im Einsatz.			*In addition, an e-learning tool is used for regular security awareness training.*
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Im Rahmen des internen Verfahrensverzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach BDSG nachgewiesen. Eventuell notwendige Vorabkontrollen werden im Planungsstadium integriert.		*Are the processing operations documented with regard to their permissibility under data protection law?*	*As part of the internal records of processing activities, the data flows are documented, and the permissibility of processing and use is proven in accordance with the BDSG. Any necessary prior checks are integrated at the planning stage.*
1.	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**		***1.***	***Confidentiality (Sec. 32 para. 1 lit. b GDPR)***	
1.1.	**Zutrittskontrolle**		***1.1.***	***Entry control***	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gebäude ist mit einer Sicherheits-Schließanlage ausgerüstet. Weiterhin verfügt das Gebäude über einen Wachschutz von 06 bis 22 Uhr und komplette Videoüberwachung.		*How are the buildings in which processing takes place secured against unauthorized entry?*	*The building is equipped with a security locking system. Furthermore, the building has a security guard from 06:00 am to 10:00 pm and complete video surveillance.*
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räume werden ebenfalls durch das Gebäude-Sicherheitssystem geschützt. Zusätzlich ist für die Büroräume ein eigenes Authentifizierungssystem eingerichtet. Der Zutritt zu den Büroräumen ist nur möglich mittels		*How are the rooms / offices in which processing takes place secured against unauthorized entry?*	*The rooms are also protected by the building security system. In addition, a separate authentication system is set up for the offices. Access to the offices is only possible by means of a locking system and personal*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
		Schließanlage und personenbezogene Token und Zugriffsrechte, die Eingangstüren zu unseren Büroräumlichkeiten werden zusätzlich videoüberwacht.			*tokens and access rights; the entrance doors to our offices are also video-monitored.*
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Die Systeme zur Datenverarbeitung sind in zwei Gruppen geteilt: 1. Server: Der Zugriff auf die Server erfolgt ausschließlich über ein Jump-Server-System mittels Nutzung von Private-Keys und SSH. 2. Clients: Diese Gruppe stellt Notebooks und stationäre Computer dar. Der Zugriff auf diese Systeme ist über ein Passwort-Management und Rollensystem gesteuert. Nur diejenigen Benutzer, die für Ihre Leistungserbringung zwingend nötig Zugriff auf IP-Adressen haben müssen, können diese verarbeiten.		*How are processing facilities protected from unauthorized access?*	*The systems for data processing are divided into two groups:* *1. Server: The servers are accessed exclusively through a jump server system by using private keys and SSH.* *2. Clients: This group represents notebooks and stationary computers. Access to these systems is controlled by a password management and role system. Only those users who absolutely need to have access to IP addresses for their service provision can process them.*
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.		*How are the implemented entry control measures checked for suitability?*	*The entry control measures are also checked as part of the checks by the external data protection officer.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
1.2.	**Zugangskontrolle**		***1.2.***	***Account control***	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden nur sehr selektiv und nur nach Genehmigung durch die IT-Abteilung vergeben. Rechtevergabe und Änderung sind dokumentiert. Zugriff auf kaufmännische Dokumente und Kommunikationsinformationen sind durch Passwörter geschützt.		*How are user accounts assigned?*	*User accounts are only granted very selectively and only after approval by the IT department. Assignment of rights and changes are documented. Access to commercial documents and communication information are protected by passwords.*
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Eine regelmäßige Revision der vergebenen Rechte ist Teil der Prüfungen der Maßnahmen und wird zusammen mit dem IT-Sicherheitsbeauftragten durchgeführt und von diesem dokumentiert.		*How is the validity of user accounts checked?*	*A regular audit of the assigned rights is part of the checks of the measures and is carried out together with the IT security officer and documented by him.*
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Die Anlage und Veränderung von Benutzerzugängen werden im firmeneigenen Projektmanagement-System dokumentiert.		*How are user accounts documented, including application, approval procedures, etc.?*	*The creation and modification of user accesses are documented in the company's own project management system.*
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, Datenvermeidung und Datensparsamkeit, weniger ist hier oft mehr.		*How is it ensured that the number of administrative accounts is reduced exclusively to the necessary number and that only technically and*	*Decisions on the allocation of rights strictly adhere to the corresponding specifications, data minimization and data economy, less is often more here.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
	und persönlich geeignetes Personal hierfür eingesetzt wird?			*personally suitable personnel are deployed for this purpose?*	
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Der Zugriff auf die Server erfolgt ausschließlich über ein Jump-Server-System mittels Nutzung von Private-Keys und SSH unter gleichzeitigem Einsatz eines VPNs. Die Zugriffe sind zusätzlich per Whitelisting beschränkt.		*Is it possible to access the systems / applications from outside the company (home workstations, service providers, etc.) and how is access designed?*	*Access to the servers is exclusively via a jump server system using private keys and SSH, with simultaneous use of a VPN. Access is additionally restricted by whitelisting.*
1.3.	**Zugriffskontrolle**		***1.3.***	***Access control***	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden nicht gespeichert.		*How is it achieved that passwords are only known to the respective user?*	*Passwords are assigned by the respective employees themselves. The strict system default settings force a high password complexity. Passwords are not stored.*
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben Empfehlungen des BSI dienen als Vorbild für die o.g. Systemeinstellungen		*What are the requirements for the complexity of passwords?*	*The specifications Recommendations of the Federal Office for Information Security ("BSI") serve as a model for the above-mentioned system settings.*
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Systemeinstellungen der Betriebssysteme.		*How is it guaranteed that the user can / must change his password regularly?*	*System settings of the operating systems.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulung und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten. Hinweise im Mitarbeiterhandbuch.		*What organizational precautions are taken to prevent unauthorized access to personal data at the workplace?*	*Training and sensitization of employees.* *Briefings and regular training on the devices used.* *Notes in the employee handbook.*
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch Punkt Vergabe von Benutzerzugängen, Punkt 1.2; die IT-Abteilung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur		*How is it ensured that access authorizations are assigned according to requirements and limited in time?*	*See also allocation of user accounts, item 1.2; the IT department checks the rights and user structure at regular intervals.*
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Dokumentationen liegen im firmeneigenen Collaboration-Tool vor.		*How is the documentation of access permissions done?*	*Documentation is available in the company's own collaboration tool.*
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Regelmäßige Durchsicht der Systemprotokolle durch die IT-Abteilung.		*How is it ensured that access authorizations are not misused?*	*Regular review of system logs by the IT department.*
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Datensicherung/Protokollierung ist aktiv unter Berücksichtigung der gegebenen Aufbewahrungsfristen und rechtlichen Anforderungen. Access-Logs inklusive IP-Adressen werden für eine maximale Dauer von zehn Tagen aufbewahrt. Darunter sind diese Logs zu verstehen, welche die Aufrufe auf die jeweilige URL des Verantwortlichen loggen.		*How long are logs kept?* *Who has access to the logs and how often are they evaluated?*	*Data backup/logging is active, taking into account the given retention periods and legal requirements.* *Access logs, including IP addresses, are stored for a maximum period of ten days. These logs are understood to be those that log visits to the respective URL of the Principal.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
		Myras eigene System-Logs müssen laut PCI DSS für mindestens ein Jahr gespeichert/aufbewahrt werden. Wenn Daten von automatisierten täglichen Analysetools erzeugt werden, müssen diese ebenfalls mindestens ein Jahr lang gespeichert/aufbewahrt werden. Diese Logs sind nicht Teil der Auftragsverarbeitung, sondern lediglich Teil Myras technischer Maßnahmen. Sicherung der Inhalte der Myra Kundendatenbank erfolgt in Abhängigkeit von Geschäftsprozessen der Myra Security, sowie gegebenen Aufbewahrungsfristen und rechtlichen Anforderungen. Zugriff hat ausschließlich die Geschäftsführung und die IT-Administration. Es erfolgt eine regelmäßige Auswertung der Protokolle.			*Myra's own system logs must be stored/retained for at least one year in accordance with PCI DSS. If data is generated by automated daily analysis tools, it must also be stored/retained for at least one year. These logs are not part of the processing on behalf of the controller, but merely part of Myra's technical controls.* *The content of the Myra customer database is backed up in accordance with Myra Security's business processes, retention periods and legal requirements.* *Only the management and IT administration have access. The logs are evaluated on a regular basis.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
1.4.	**Trennungskontrolle**		***1.4.***	***Control of separation***	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Die Erhebung der IP-Adressen erfolgt stets zum gleichen Zweck. Separate Logdateien für alle Kundendaten, die auch nur in separaten Zugängen für die Kunden erreichbar sind.		*How is it ensured that data collected for different purposes are processed separately?*	*IP addresses are always collected for the same purpose.* *Separate log files for all customer data, which can also only be accessed by customers in separate accesses.*
1.5.	**Pseudonymisierung**		***1.5.***	***Pseudonymization***	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.		*What organizational measures have been taken to ensure that the processing of personal data complies with the law?*	*All persons entrusted with the processing of personal data have been obligated accordingly. A data protection concept is used in the company and has been made known to all employees. The training concept includes data protection instruction at the start of employment as well as constant sensitization through monthly data protection newsletters, specialist web training and personal sensitization by the external data protection officer.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
	Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?	Myra verfügt nicht über die technischen und rechtlichen Möglichkeiten, IP-Adressen natürlichen Personen zuzuordnen.		*How is personal data processed/stored so that it cannot be attributed to the data subjects?*	*Myra does not have the technical and legal means to attribute IP to natural persons.*
2.	**Integrität (Art. 32 Abs. 1 lit. b DSGVO)**		***2.***	***Integrity (Sec. 32 para. 1 lit. b GDPR)***	
2.1.	**Weitergabekontrolle**		***2.1.***	***Control of sharing***	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Es werden keine personenbezogenen Daten der Auftragnehmer weitergegeben.		*How do you ensure integrity and confidentiality when sharing personal data?*	*No personal data of service providers is shared.*
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	n/a		*Are encryption systems used when sharing personal data and if so, which ones?*	*n/a*
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	n/a		*How is the sharing of personal data documented?*	*n/a*
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.		*How are technical measures used to limit the unauthorized outflow of personal data?*	*Strict assignment of rights secures the data against unauthorized access.*
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von	Dies wird im Rahmen der Kontrollen unter Punkt 1 mit geprüft.		*Is a control system in place that can detect unauthorized outflow of personal data?*	*This is also checked as part of the controls under point 1.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
	personenbezogenen Daten aufdecken kann?				
2.2.	**Eingabekontrolle**		***2.2.***	***Input control***	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Sämtliche Zugriffe und Änderungen am System werden protokolliert.		*What measures are taken to track who has accessed applications when and for how long?*	*All accesses and changes to the system are logged.*
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Rollen-/Rechtekonzepte mit unterschiedlichen Berechtigungskonzepten.		*How is it possible to trace which activities were carried out on the corresponding applications?*	*Role/rights concepts with different authorization concepts.*
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/Rechte-konzepts zur ordnungsgemäßen Daten-verarbeitung und Speicherung.		*What measures are taken to ensure that processing by employees can only take place in accordance with the customer's instructions?*	*Access control based on the role/rights concept for proper data processing and storage.*
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Myra setzt keine Unterauftragnehmer zur Verarbeitung von personenbezogenen Daten ein.		*What measures are taken to ensure that subcontractors also only process the customer's personal data to the agreed extent?*	*Myra does not use subcontractors to process personal data.*
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Myra setzt keine Unterauftragnehmer zur Verarbeitung von personenbezogenen Daten ein.		*How is the deletion / blocking of personal data at the end of the retention period ensured for subcontractors?*	*Myra does not use subcontractors to process personal data.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
3.	**Verfügbarkeit und Belastbarkeit**		***3.***	***Availability and resilience***	
3.1.	**Verfügbarkeitskontrolle**		***3.1.***	***Availability control***	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Gesicherte Daten sind räumlich getrennt von Produktivdaten; ältere Bänder werden gesichert verwahrt. Die verwendeten Rechenzentren verfügen über marktübliche Systeme zur Abwehr von Elementareinflüssen.		*How is it ensured that data carriers are protected from elementary influences (fire, water, electromagnetic radiation, etc.)?*	*Secured data is physically separated from productive data; older tapes are stored securely. The data centers used have commercially available systems to protect against elemental influences.*
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig upgedatet.		*What protective measures are used to combat malware and how is their up-to-dateness ensured?*	*Constantly updated virus scanners and spam filters are used. The systems are updated on a regular basis.*
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung.		*How is it ensured that data carrier that are no longer needed or defective are disposed of properly?*	*Physical erasure of functional data media and mechanical destruction of defective data media prior to disposal.*
3.2.	**Wiederherstellbarkeit**		***3.2.***	***Recoverability***	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?	Eingerichtetes Backup-Verfahren mit Wiederherstellung der Datenstände auf Zuruf; Sicherung älterer Datenstände durch Einspielen von Bändern.		*What organizational and technical measures are taken to ensure the availability of data and systems as quickly as possible, even in the event of damage?*	*Backup procedure implemented including the restoration of data statuses on demand; backup of older data statuses by importing tapes.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
	(rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DSGVO)			*(rapid recoverability in accordance with Sec. 32 para. 1 lit. c GDPR)*	
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)**		***4.***	***Procedures for regularly testing, assessing, and evaluating (Sec. 32 para. 1 lit. d GDPR, Sec. 25 para. 1 GDPR)***	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.		*What procedures are in place for regular assessment/review to ensure the security of data processing (data protection management)?*	*The external data protection officer regularly checks compliance with the technical and organizational measures, in some cases also unannounced.*
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Einsatz eines Ticketsystems - dreistufig (1st, 2nd und 3rd-Level); zusätzlich Telefonhotline und automatisiertes Überwachungs- und Alarmierungssystem.		*How are requests and problems responded to (incident response management)?*	*Use of a ticket system with three levels (1st, 2nd, and 3rd level); ticketadditional telephone hotline and automated monitoring and alarm system.*
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DSGVO)?	Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen.		*What data protection-friendly default settings are there (Sec. 25 para. 2 GDPR)?*	*No preassignment by checkmarks; no preassignments are made when logging in to the system; user must enter the logon information in each case.*

Nr.	Gebiet	Beschreibung	*Nr.*	*Area*	*Description*
4.1.	**Auftragskontrolle**		***4.1.***	***Order control***	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte sowie der IT-Sicherheitsbeauftragte nehmen entsprechende Beratungs- und Kontrollpflichten wahr.		*What processes exist for the instruction or handling of commissioned data processing (data protection management)?*	*The contract has been designed in accordance with the new guidelines on commissioned data processing. The external data protection officer and the IT security officer perform corresponding advisory and monitoring duties.*