Änderungen NEU in Gelb markiert!

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO mit Geltung ab dem 25.05.2018

Vereinbarung zwischen dem Lizenznehmer von oHA (=Verantwortlicher), nachstehend Auftraggeber genannt

und der

LuxActive KG
Media Quarter Marx 3.2,
Maria Jacobi Gasse 1
1030 Wien
(= Auftragsverarbeiter), nachstehend Auftragnehmer genannt.

§ 1 Gegenstand und Dauer des Auftrags

1. Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Lizenzvertrag zwischen Auftragnehmer und Auftraggeber auf den hier verwiesen wird (im Folgenden Lizenzvertrag). Der Lizenzvertrag ist in den **AGBs von LuxActive** geregelt (siehe https://www.luxactive.com/agb/) und wurde vom Auftraggeber akzeptiert .

2. Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Lizenzvertrages.

§ 2 Konkretisierung des Auftragsinhalts

Weitere Einzelheiten zu Art und Zweck der vorgesehenen Verarbeitung oder Nutzung sind unter Buchstabe A. der Anlage 1 zu dieser Vereinbarung aufgeführt.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

- wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

Die Art der personenbezogenen Daten sind unter Buchstabe B. der Anlage 1 aufgeführt.
Personenbezogene Daten dürfen nur im Rahmen des Hauptvertrages oder auf dokumentierte Weisung des Auftraggebers verarbeitet werden.
Der Kreis der Betroffenen ist unter den Buchstabe C. der Anlage 1 aufgeführt.

§ 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 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].

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.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

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.

2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 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:

1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Christoph Hrdinka, LuxActive KG, Telefon: +43 680 2438573 Mail: christoph.hrdinka@luxactive.com, benannt.

2. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 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.

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

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

5. 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.

6. 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.

7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 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 gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, 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.

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

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

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Universität Wien	Universitätsring 1 1010 Wien Österreich	Statistische Auswertungen

Firma Unterauftragnehmer	Anschrift/Land	Leistung

SWISDATA GmbH	Maria Jacobi Gasse 1, 1030 Wien Österreich	Statistische Auswertungen

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.

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.

5. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

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

§ 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 durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

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.

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

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

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

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

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

2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 9 Weisungsbefugnis des Auftraggebers

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

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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, 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 Lizenzvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, 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 Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage 1: A. Zu § 2 Ergänzungen zu Art und Zweck der Datenverarbeitung
B. Zu § 2 Art der personenbezogenen Daten
C. Zu § 2 Kreis der Betroffenen
Anlage 2: Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Anlage 1:
A. Zu § 2 Ergänzungen zu Art und Zweck der Datenverarbeitung
Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung sind:

B. Zu § 2 Art der personenbezogenen Daten
(maßgebliche Datenarten sind aufgelistet)

- Adressdaten
- Kontaktdaten
- Vertragsdaten
- Bankverbindungsdaten
- Kontodaten
- Abrechnungsdaten
- Leistungsdaten
- Finanzdaten
- Angebotsdaten
- Gesprächshistorie
- Transaktionsdaten

- Auskünfte
- Mitarbeiterdaten
- Gesundheitsdaten, die nur bei aktiviertem Modul der Kinderbetreuung in oHA gespeichert und verarbeitet werden

C. Zu § 2 Kreis der Betroffenen
(maßgebliche Personengruppen sind aufgelistet)

- Mitarbeiter
- Kunden
- Lieferanten/Dienstleister
- Gesellschafter

Anlage 2: Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO
Dokumentation der nach 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen [1].

1.	**Pseudonymisierung** Wie wird die Pseudonymisierung der Daten gewährleistet? Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.	○ Personenbezogene Daten werden durch Zufallscodes ersetzt ○ Data Masking
2.	**Verschlüsselung** Wie wird die Verschlüsselung gewährleistet? Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die	○ Nutzung von kryptografischen Tools ○ Data Hashing ○ Verschlüsselung von Speichermedien

	"Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.	○ Verschlüsselung der Kommunikation
3.	**Fähigkeit der Vertraulichkeit** Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	○ Elektronisches Zutrittskontrollsystem ○ Sicherheitstüren und/oder -fenster ○ Gitter vor Fenstern und Türen ○ Werkschutz, Pförtner ○ Alarmanlage ○ Videoüberwachung ○ Spezielle Schutzvorkehrungen für den Serverraum ○ Individueller Log-In und Kennwortverfahren ○ Zusätzlicher Log-In für bestimmte Anwendungen ○ Automatische Sperrung der Clients (Zeitablauf) ○ Verwaltung von Berechtigungen ○ Dokumentation von Berechtigungen ○ Verschlüsselung von Systemen ○ Verschlüsselung der Kommunikation ○ Verschlüsselung von Datenträgern ○ VPN (Virtual Private Network) ○ Gesichertes WLAN ○ SSL-Verschlüsselung bei Web-Access

4.	**Fähigkeit der Integrität** Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet? Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.	○ Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern ○ Verwendung von Zugriffsrechten ○ Systemseitige Protokollierungen ○ Funktionelle Verantwortlichkeiten
5.	**Fähigkeit der Verfügbarkeit** Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet? Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	○ Back-Up Verfahren ○ Spiegeln von Festplatten ○ Unterbrechungsfreie Stromversorgung (USV) ○ Virenschutz /Firewall ○ Notfallplan ○ Klimaanlagen ○ Brand- und Löschwasserschutz ○ Alarmanlage
6.	**Fähigkeit der Belastbarkeit** Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet? Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.	○ Penetrationstest
7.	**Wiederherstellbarkeit der Verfügbarkeit und des Zugangs** Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?	○ Back-Up Verfahren ○ Unterbrechungsfreie Stromversorgung (USV) ○ Notfallplan

8.	**Verfahren zur regelmäßigen Überprüfung*** Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?	○ Es existiert eine festgelegte Prüfroutine ○ Prüfberichte werden evaluiert ○ Implementierung von Verbesserungsvorschlägen
9.	**Unrechtmäßiger Zugang zu personenbezogenen Daten** Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?	○ Individueller Log-In und Kennwortverfahren ○ Zusätzlicher Log-In für bestimmte Anwendungen ○ Automatische Sperrung der Clients (Zeitablauf) ○ Verwaltung von Berechtigungen Dokumentation von Berechtigungen ○ Verschlüsselung von Systemen
10.	**Verarbeitung personenbezogener Daten nur nach Anweisung** Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden? 0 Mitarbeiter sind zu Verhaltensregeln verpflichtet	○ Implementierung unternehmensinterner Datenschutz-Richtlinien ○ Verpflichtung der Mitarbeiter auf das Datengeheimnis ○ Schulungen aller zugriffsberechtigten Mitarbeiter ○ Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag

[1] Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine allgemeine Beschreibung darstellen, die es ermöglicht, vorläufig zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem Auftraggeber bei wesentlichen Änderungen und im Übrigen jährlich zur Durchführung der Auftragskontrolle vorzulegen.