TRILUX LMS/DIGITAL SERVICES ANLAGE ZUR AUFTRAGSDATENVERABEITUNG

Diese Anlage konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus den Allgemeinen bzw. ergänzenden Geschäftsbedingungen der TRILUX GmbH & Co. KG, Heidestraße 4, 59759 Arnsberg (nachfolgend "TRILUX" oder "Auftragnehmer") für Lichtmanagementsysteme und Digital Services „LMS-AGB“ und der dazugehörigen Leistungsbeschreibung einsehbar unter www.trilux.com/AGB ergeben. Sie findet Anwendung auf alle Tätigkeiten, die damit in Zusammenhang stehen und bei denen Beschäftigte der TRILUX oder durch TRILUX Beauftragte personenbezogene Daten verarbeiten oder mit personenbezogenen Daten des Auftraggebers (nachfolgend "Kunde") in Berührung kommen können.

1. Gegenstand und Dauer der Vereinbarung

1.1. TRILUX verarbeitet personenbezogene Daten im Auftrag des Kunden. Dies umfasst alle Tätigkeiten, die TRILUX gemäß der Leistungsbeschreibung und den LMS-AGB gegenüber dem Kunden erbringt und die eine Auftragsverarbeitung darstellen.

1.2. Die Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art.44 ff. DSGVO erfüllt sind.

1.3. Die Verarbeitung erfolgt zeitlich unbefristet, sofern dies nicht anders vertraglich vereinbart ist.

1.4. Der Kunde kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von TRILUX gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, TRILUX eine Weisung des Kunden nicht ausführen kann oder will oder TRILUX Kontrollrechte des Kunden vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art.28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

2.1. Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne des Art.4 Nr.2 DSGVO.

2.2. Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung erforderlichen und alle in Ziffern 12. dieser Vereinbarung zur Auftragsverarbeitung und der Leistungsbeschreibung vereinbarten weiteren Vertragszwecke.

2.3. TRILUX verarbeitet folgende Daten aus den Leuchten bei Energy Monitoring:

– Energieverbrauch,

– Betriebszeit und -dauer,

– Schaltstatus an/aus,

– variable DALI-Kennziffern sowie

– Seriennummern der durch den Kunden eingesetzten TRILUX Leuchten,

– Informationen zu den Räumen, in denen die Leuchten installiert sind.

Bei Light Monitoring kommen hinzu:

– Dimmlevel,

– Fehler aus den DALI Vorschaltgeräten und LiveLink-Lichtmanagementsystem,

– Temperatur im Vorschaltgerät in der Leuchte.

2.4. Betroffene Personen können die Mitarbeiter und regelmäßig tätige Mitarbeiter von Drittdienstleistern sein, sofern die Raumaufteilung und Raumnutzung in Verbindung mit den TRILUX Digital Services Rückschlüsse auf bestimmbare Personen und / oder deren Nutzungsverhalten im Hinblick TRILUX Leuchten zulässt.

3. Hinweise zur Fernwartung:

3.1. Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

3.2. Für den Fall, dass der Kunde einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung

nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Kunden auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

3.3. Wenn der Kunde bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

3.4. Falls im Rahmen der Wartung Daten beim Auftragnehmer gespeichert wurden, sind diese nach Abschluss der Arbeiten sorgfältig wieder zu löschen.

4. Rechte und Pflichten sowie Weisungsbefugnisse des Kunden

4.1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art.6 Abs.1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art.12 bis 22 DSGVO ist allein der Kunde verantwortlich („Verantwortlicher“ im Sinne des Art.4 Nr.7 DSGVO). Gleichwohl ist TRILUX verpflichtet, alle Anfragen, sofern sie erkennbar ausschließlich an den Kunden gerichtet sind, unverzüglich an diesen weiterzuleiten.

4.2. Der Kunde nennt TRILUX bei Bedarf den Ansprechpartner für im Rahmen dieser Vereinbarung zur Auftragsverarbeitung anfallende Datenschutzfragen.

4.3. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen den Parteien abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Kunde erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

4.4. Der Kunde ist berechtigt, sich wie vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der TRILUX getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Kunde informiert TRILUX unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

5. Weisungsberechtigte des Kunden, Weisungsempfänger der TRILUX

Die Weisungsberechtigten Personen des Kunden, die Weisungsempfänger bei TRILUX und die für die Weisung zu nutzenden Kommunikationskanäle sind zwischen den Parteien gesondert vereinbart. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

6. Pflichten der TRILUX

6.1. TRILUX verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Kunden, sofern TRILUX nicht zu einer anderen Verarbeitung durch anwendbare Rechtsvorschriften hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt TRILUX dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verboten ist.

6.2. TRILUX verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Kunden nicht erstellt.

6.3. TRILUX sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

6.4. Bei der Erfüllung der Rechte der betroffenen Personen nach Art.12 bis 22 DSGVO durch den Kunden, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten hat die TRILUX im notwendigen Umfang mitzuwirken und den Kunden - soweit möglich - angemessen zu unterstützen.

6.5. TRILUX wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. TRILUX ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Kunden nach Überprüfung bestätigt oder geändert wird.

6.6. TRILUX hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Kunde dies mittels einer Weisung verlangt und berechtigte Interessen von TRILUX dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf TRILUX nur nach vorheriger Weisung oder Zustimmung durch den Kunden erteilen.

6.7. TRILUX erklärt sich damit einverstanden, dass der Kunde - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Kunde beauftragte Dritte zu kontrollieren. Dieses kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort erfolgen, sofern dabei Arbeits- und Organisationsprozesse bei TRILUX nicht beeinträchtigt werden. TRILUX wird bei diesen Kontrollen unterstützend mitwirken.

6.8. TRILUX sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet wurden. TRILUX überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Betrieb.

6.9. Bei TRILUX ist als Beauftragter für den Datenschutz SAFE-PORT Consulting GmbH, Hülshoff-Straße 7, D-59469 Ense | Datenschutz | privacy@trilux.com bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Kunden unverzüglich mitzuteilen.

7. Mitteilungspflichten von TRILUX bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

TRILUX teilt dem Kunden unverzüglich Störungen, Verstöße gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Kunden. TRILUX sichert zu, den Kunden erforderlichenfalls bei seinen Pflichten nach Art.33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art.33 oder 34 DSGVO für den Kunden darf TRILUX nur nach vorheriger Weisung durchführen.

8. Unterauftragsverhältnisse mit Subunternehmern / Weitere Auftragsverarbeiter

8.1. Der Kunde erteilt TRILUX die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art.28 DSGVO in Anspruch zu nehmen.

8.2. TRILUX informiert den Kunden, wenn eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt ist. Ein Einspruch gegen die beabsichtigte Änderung ist innerhalb von 4 Wochen nach Zugang der Information über die Änderung gegenüber TRILUX zu erheben. Im Fall des Einspruchs kann TRILUX nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung TRILUX nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Kunde innerhalb von 4 Wochen nach Zugang des Einspruchs kündigen.

8.3. Erteilt TRILUX Aufträge an weitere Auftragsverarbeiter, so obliegt es TRILUX, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.

8.4. Eine aktuelle Liste der eingesetzten Subunternehmen ist einsehbar unter www.trilux.com/AGB.

9. Technische und organisatorische Maßnahmen nach Art.32 DSGVO (Art.28 Abs.3 S.2 c) DSGVO)

9.1. Die jeweils aktuell geltenden technischen und organisatorischen Maßnahmen kann der Kunde unter www.trilux.com/AGB einsehen.

9.2. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art.32 Abs.1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen potentielle Risiken auf Dauer eingedämmt werden.

Der Kunde informiert sich vor Abschluss der Vereinbarung zur Auftragsverarbeitung und anschließend in regelmäßigen Abständen über diese technischen und organisatorischen Maßnahmen.

Der Kunde trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt TRILUX vorbehalten, sofern das Schutzniveau nach DSGVO und die vereinbarten Standards nicht unterschritten werden.

10. Verpflichtungen von TRILUX nach Beendigung des Auftrags

10.1. Nach Abschluss der vertraglichen Leistungen wird TRILUX sämtliche in ihrem Besitz sowie an Subunternehmen gelangte personenbezogene Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht löschen bzw. vernichten.

10.2. Die Löschung bzw. Vernichtung wird von der TRILUX auf Wunsch des Kunden mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format bestätigt.

11. Gegenseitige Unterstützung

Im Fall des Art.82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

12. Vereinbarung weiterer Vertragszwecke

12.1. TRILUX ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten

a) für die Fehlerbehebung in dem bereitgestellten Service, in dem die Daten gespeichert sind,

b) zum Zweck der Qualitätssicherung für den bereitgestellten Service bzw. für eine neuere Version des Services

c) zum Zweck der Entwicklung neuer oder Weiterentwicklung bestehender TRILUX-Services in einer angemessen gesicherten Umgebung zu verarbeiten.

12.2. TRILUX ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zu verarbeiten,

a) soweit dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist,

b) soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit dem vereinbarten Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.

Dies umfasst insbesondere auch, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern ("Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren