Verpflichtungserklärung der ista Luxembourg S.à r.l. zur Auftragsverarbeitung

Wir, die ista Luxembourg S.à r.l., 23,rue des Bruyères, L-1274 Howald verarbeiten aufgrund des zwischen Ihnen und uns bestehenden Vertragsverhältnisses für Sie personenbezogene Daten. Um den datenschutzkonformen Umgang mit diesen personenbezogenen Daten sicherzustellen, geben wir folgende Verpflichtungserklärung zur Auftragsdatenverarbeitung gemäß Artikel 28 der Datenschutz-Grundverordnung (DS-GVO) (nachfolgend „Verpflichtungserklärung“ genannt) ab:

1. Gegenstand und Dauer der Verpflichtungserklärung

(1) Gegenstand

Der Gegenstand der Verpflichtungserklärung und Ihre Kontaktdaten ergeben sich aus dem jeweiligen mit Ihnen bestehenden Auftrag bzw. Rahmenvertrag, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2)Dauer

Die Dauer dieser Verpflichtungserklärung (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung, unbeschadet der in dieser Erklärung längeren gesetzlichen Aufbewahrungsfrist.

2. Konkretisierung des Inhalts der Verpflichtungserklärung

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten Art und Zweck der Verarbeitung personenbezogener Daten durch uns für Sie sind konkret beschrieben in der Leistungsvereinbarung.

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 Ihrer vorherigen Zustimmung und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2)Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Daten- arten/-kategorien:

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Mieter-/Wohnungseigentümerdaten (z. B. Name, Anschrift, Umlageschlüssel, Verbrauchsdaten)

(3)Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- ista Servicepartner (Ableser, Monteure)
- Beschäftigte
- Lieferanten
- Ansprechpartner
- Mieter, Wohnungseigentümer

3. Technisch-organisatorische Maßnahmen

(1) Wir setzen die technischen und organisatorischen Maßnahmen, die in Anlage 1 benannt sind, um. Die dokumentierten Maßnahmen sind Grundlage der Verpflichtungserklärung. Soweit eine Prüfung/ein Audit durch Sie einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2)Wir haben die Sicherheit gem. Art. 28 Abs. 3 lit. c und Art. 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1 und 2 DS-GVO 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 DS-GVO zu berücksichtigen (Einzelheiten in Anlage 1).

(3)Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es uns 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) Wir dürfen die Daten, die von uns in Ihrem Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung von Ihnen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an uns wendet, werden wir dieses Ersuchen unverzüglich an Sie weiterleiten.

(2)Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung von Ihnen unmittelbar durch uns sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten der ista Luxembourg S.à r.l. als Auftragnehmer

Wir haben zusätzlich zu der Einhaltung der Regelungen dieser Verpflichtungserklärung weitere gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleisten wir insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
Kontaktdaten zum Zweck der direkten Kontaktaufnahme:
ista Luxembourg S.à r.l.
Datenschutzbeauftragter
23, rue des Bruyères
L-1274 Howald
E-Mail: GDPR_DPO@ista.lu

06/2018

Verpflichtungserklärung der ista Luxembourg S.à r.l. zur Auftragsverarbeitung

b) Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, Art. 29 und Art. 32 Abs. 4 DS-GVO. Wir setzen 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. Wir und jede uns unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend Ihrer Weisung verarbeiten, was auch hinsichtlich der in dieser Verpflichtungserklärung eingeräumten Befugnisse gilt, es sei denn, dass wir gesetzlich zur Verarbeitung verpflichtet sind.

c) Umsetzung und Einhaltung aller für diese Verpflichtungserklärung erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c und Art. 32 DS-GVO (Einzelheiten in Anlage 1).

d) Wir und Sie arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung Ihrer Aufgaben zusammen.

e) Ihre unverzügliche Information über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Verpflichtungserklärung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei uns ermittelt.

f) Soweit Sie Ihrerseits 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 bei uns ausgesetzt ist, haben wir Sie jeweils zu unterstützen.

g) Wir kontrollieren regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in unserem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen Ihnen gegenüber im Rahmen Ihrer Kontrollbefugnisse nach Ziffer 7 dieser Verpflichtungserklärung.

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 wir in Anspruch nehmen (z. B. 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). Wir sind jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wir dürfen weitere Auftragsbearbeiter auf Grundlage der hier allgemein erteilten schriftlichen Einwilligung einsetzen. Wir informieren Sie über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung solcher Auftragsbearbeiter, indem die jeweils aktuelle Liste der Auftragsbearbeiter unter der Internetadresse av.ista.de zur Verfügung gestellt wird. Sie stellen durch mindestens monatlichen Abruf (z. B. durch geeignete technische Vorkehrungen) sicher, dass Sie stets über den aktuellen Stand der aufgelisteten Auftragsbearbeiter informiert sind.

(3)Die Weitergabe Ihrer personenbezogenen Daten 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, stellen wir 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 Ihrer ausdrücklichen Zustimmung (mindestens Textform); sämtliche von uns übernommenen Datenschutzpflichten aus dieser Verpflichtungserklärung sind – soweit für das Unterauftragsverhältnis relevant – auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Ihre Kontrollrechte

(1) Sie haben das Recht, sich durch Stichprobenkontrollen, die mit einem Vorlauf von mindestens vier Wochen anzumelden sind, von der Einhaltung dieser Vereinbarung durch uns und in unserem Geschäftsbetrieb zu überzeugen. Von Ihnen dafür eingesetzte Personen müssen sich uns gegenüber zur Geheimhaltung verpflichten. Die Geheimhaltungsverpflichtung muss hohen Sicherheitsanforderungen genügen. Die eingesetzten Personen dürfen in keiner Beziehung zu einem unserer Wettbewerber stehen.

(2)Wir stellen sicher, dass Sie sich von der Einhaltung unserer Pflichten nach Art. 28 DS-GVO überzeugen können. Wir verpflichten uns, Ihnen 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 die konkrete Leistungsvereinbarung betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revisionsstellen, Datenschutzbeauftragte, IT-Sicherheitsabteilungen, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung im Rahmen von IT-Sicherheits- oder Datenschutzaudits (z. B. nach BSI-Grundschutz).

Verpflichtungserklärung der ista Luxembourg S.à r.l. zur Auftragsverarbeitung

8. Vergütung von datenschutzbezogenen Leistungen

Wir sind berechtigt, für Unterstützungsleistungen insbesondere nach Ziffer 7, 10 und 11 eine angemessene Vergütung nach Zeit- und Materialaufwand zu verlangen, sofern sie nicht in der Leistungsvereinbarung enthalten und nicht auf unser Fehlverhalten zurückzuführen sind sowie nicht ausschließlich in der Erfüllung unserer sich unmittelbar aus der DS-GVO bzw. dem BDSG ergebenden Pflichten bestehen.

Vorbehaltlich einer anderen Vereinbarung mit Ihnen gilt für die Vergütung unserer Fachkräfte ein Stundensatz i.H.v. 150,00 Euro zzgl. der gesetzlichen Umsatzsteuer. Materialaufwand und Reisekosten rechnen wir Ihnen gegenüber in der tatsächlich entstandenen Höhe ab.

9. Mitteilung bei Verstößen durch uns

Wir unterstützen Sie bei der Einhaltung der in Artt. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten sowie der Meldepflichten bei Datenpannen, bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen. Hierzu gehören:

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 des Schutzes personenbezogener Daten u. a. unverzüglich an Sie zu melden
c) die Verpflichtung, Sie im Rahmen Ihrer Informationspflicht gegenüber dem Betroffenen zu unterstützen und Ihnen in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

a) Unsere Unterstützung für Ihre Datenschutz-Folgenabschätzung

b) unsere Unterstützung im Rahmen Ihrer Konsultationen mit der Aufsichtsbehörde

10. Ihre Weisungsbefugnisse

(1) Mündliche Weisungen an uns bestätigen Sie unverzüglich (mindestens in Textform).

(2)Wir haben Sie unverzüglich zu informieren, wenn wir der Meinung sind, eine Weisung von Ihnen verstoße gegen Datenschutzvorschriften. Wir sind berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch Sie bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Ihr Wissen nicht erstellt. Hiervon ausgenommen sind Kopien, soweit sie zur Erfüllung der Leistungsvereinbarung und zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, für die nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung besteht.

(2)Nach Abschluss der aufgrund der Leistungsvereinbarung von uns zu erbringenden Arbeiten oder früher nach Aufforderung durch Sie – spätestens mit Beendigung der Leistungsvereinbarung – haben wir Ihnen sämtliche in unseren Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Leistungsvereinbarung stehen, auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3)Von den Lösch- und Rückgabepflichten sind solche Daten ausgenommen, für die nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung besteht (z. B. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch uns entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren).

ista Luxembourg S.à r.l.

Ista Luxembourg S.à r.l. 23, rue des Bruyères 1274 Howald

Tel. 49 52 52 -45 Billing@ista.lu www.ista.lu

Verpflichtungserklärung der ista Luxembourg S.à r.l. zur Auftragsverarbeitung

Anlage 1 – Technisch-organisatorische Maßnahmen 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrollmaßnahmen
  - Physische Zugangsbeschränkungen für Unbefugte zu den Rechenzentren sowie den Servern in den Niederlassungen
  - Berechtigungsprüfung des Zutritts zu sensiblen Bereichen der Rechenzentren durch Ausweiskontrolle und Abgleich mit Listen von autorisierten Personen
  - Physische und organisatorische Sicherheitsmaßnahmen (Chipkartenlesegeräte, Empfang zur Registrierung) sind für nicht-öffentliche Bereiche implementiert
  - Besucher der Firmenzentrale erhalten sichtbar zu tragende Besucherausweise und dürfen die nicht-öffentlichen Bereiche nur in Begleitung betreten
  - Führen eines Schlüsselverzeichnisses für die Firmenzentrale
  - Implementierte
  - Einbruchschutzmaßnahmen(Videoüberwachung, Türsicherungen, Alarmanlage mit Sicherheitsdienst)
  - Protokollierung der Besuche in der Firmenzentrale und in den Niederlassungen
- Zugangskontrollmaßnahmen
  - Der Zugang zu Systemen ist nur mit individuellen Benutzernamen und Kennwörtern möglich
  - Der Zugang zu den Systemen ist nur einem definierten Kreis von Zugangsberechtigten möglich
  - Die Vergabe von Zugangsrechten erfolgt nach einem definierten Freigabeprozess
  - Es erfolgt eine Protokollierung der Benutzeranmeldungen und der jeweiligen Zeitpunkte
- Zugriffskontrollmaßnahmen
  - Berechtigungsprüfungen erfolgen auf Basis eines Berechtigungskonzepts Die Berechtigungsvergabe basiert auf dem Prinzip des „need-to-know“
  - Personenbezogene Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden
  - Eine Verwendung fortlaufend aktualisierter Virenschutzsoftware ist technisch sichergestellt
  - Eingehender E-Mail-Verkehr wird durch ein zentrales Virenschutz- und Spamfiltersystem auf Viren und Spam überprüft
  - Schutz der IT-Infrastruktur durch Firewalls
  - Passwortschutz (mindestens acht Stellen, Kombination von Buchstaben, Zahlen und Sonderzeichen, erzwungener Wechsel nach 90 Tagen)
  - Eine im Berechtigungskonzept umgesetzte Trennung von Abrechnungs- und Kundenstammdaten
  - Protokollierung von Datenänderungen
- Maßnahmen zur Trennungskontrolle
  - Test- und Freigabeverfahren für Softwareprodukte
  - Trennung der Produktiv- von der Test- und Entwicklungsumgebung
  - Logische Trennung der Dreisystemlandschaft gemäß Berechtigungskonzept Änderungsmanagement mit differenziertem Freigabeverfahren
- Maßnahmen zur Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  - Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten in den unterschiedlichen Systemen nicht ohne Hinzuziehung zusätzlicher Informationen einer spezifischen betroffenen Person zugeordnet werden können, sofern dies möglich und sinnvoll ist

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Maßnahmen zur Weitergabekontrolle
  - Verschlüsselung/Nutzung von VPN-Tunneln bei Übertragungen
  - SSL-Verschlüsselung bei Web-Access
  - Regelung des Systemkommunikationsverkehrs (zentrale Firewall, exklusive WAN-Verbindungen mit Zugriffskontrollen), Protokollierung (Userauthentifizierung, Zeitpunkt)
- Maßnahmen zur Eingabekontrolle
  - Systemseitig umgesetzte Plausibilitätskontrollen
  - Es kann nachträglich festgestellt werden, ob und von wem Kundenstammdaten in DV-Systeme eingegeben, verändert oder entfernt worden sind (Protokollierung)
  - Berechtigungskonzept

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DS-GVO)

- Personenbezogene Daten sind ständig verfügbar und durch regelmäßige Datensicherungen gegen zufällige Zerstörung oder Verlust geschützt
- Datensicherungskonzept (regelmäßige Back-ups: täglich, wöchentlich, monatlich), Aufbewahrungsmodalitäten der Back-ups (Safe, getrennte Brandabschnitte)
- Besonders geschützte Rechenzentrumsabschnitte (bauliche Trennung, getrennte Zutrittskontrollsysteme, Brandschutzwände für alle RZ-Bereiche, Stromversorgung über zwei geographisch getrennte Anbindungen, zwei getrennte Brandfrühwarnsysteme mit Anbindung an Feuerwehrleitstelle)
- Brandschutzvorrichtungen in der Firmenzentrale und in den Niederlassungen
- Unterbrechungsfreie Stromversorgung Redundante Stromzuführungen
- Überwachungs- und Meldesysteme

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-/Datensicherheitskonzept

- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle
- Verarbeitung nur entsprechend den dokumentierten Weisungen des Auftraggebers
- Weisungen erfolgen zwischen dafür ausdrücklich bestimmten Kontaktpersonen
- Konkrete Vorgaben für die Verpackung und den Versand von Dokumenten/ Gegenständen, die relevante Daten enthalten
- Eingesetzte Personen sind über datenschutzrechtliche Anforderungen informiert und schriftlich auf die Vertraulichkeit nach Artt. 24, 29 und 32 Abs. 4 DS-GVO verpflichtet
- Unterauftragnehmer werden sorgfältig im Hinblick auf die Eignung zur Einhaltung der maßgeblichen Sicherungsvorkehrungen geprüft und schriftlich zur Einhaltung der jeweils anzuwendenden datenschutzrechtlichen Vorgaben verpflichtet