Besondere Geschäftsbedingungen der Hilti Deutschland AG für Schulungen

Für die Erbringung von Schulungsleistungen der Hilti Deutschland AG („Hilti“) gelten ausschließlich diese Geschäftsbedingungen. Entgegenstehende, abweichende oder ergänzende Geschäftsbedingungen des Kunden werden hiermit zurückgewiesen und werden nicht Vertragsbestandteil, es sei denn, Hilti stimmt ihrer Geltung ausdrücklich und schriftlich zu. Durch den Abschluss eines Schulungsvertrages, spätestens jedoch mit Antritt einer Schulung erkennt der Kunde diese Geschäftsbedingungen für die aktuelle als auch für künftige vom Kunden gebuchte oder besuchte Schulungen an.

1. Vertragsgegenstand

1.1 Diese Geschäftsbedingungen für Hilti Schulungen gelten für Schulungen, die Hilti seinen Kunden anbietet, insbesondere für Präsenzschulungen (physisch, online oder hybrid). Preise, Details und Beschreibungen der Schulungen sind auf Hilti Online (www.hilti.de) zu finden.

1.2 Online-Schulungen

Für Schulungen, die online abgehalten werden (z.B. via MS Teams), erhält der Kunde vor Schulungsbeginn einen Einwahllink zur Teilnahme an der gewählten Schulung.

1.3 Präsenzschulungen

Hilti bietet Präsenzschulungen entweder als vorgeplante Schulung mit Schulungsdatum, -inhalt und -ort, wie im Online-Eventkalender beschrieben, oder als individuell vereinbarte Schulung, bei der Schulungsdatum, -inhalt und -ort im Einvernehmen mit dem Kunden festgelegt werden, an.

2. Anmeldung und Vertragsschluss; Warteliste

2.1 Anmeldung und Vertragsschluss

2.1.1 Online-Anmeldung

Bei Online-Anmeldungen kommt der Schulungsvertrag erst mit Zugang einer Anmeldebestätigung zustande. Um sich online zu Schulungen anzumelden, muss sich der Kunde mit seiner Hilti Kundennummer für eine Schulung im Online-Eventkalender (cvent Formular) registrieren.

2.1.2 Sonstige Anmeldungen

Für alle sonstigen Anmeldemöglichkeiten gilt: Angebote von Hilti sind freibleibend. Anmeldungen des Kunden müssen schriftlich (per E-Mail) erfolgen. Der Schulungsvertrag kommt erst mit Zugang einer Anmeldebestätigung zustande.

2.2 Warteliste

Bei ausgebuchten Schulungen besteht die Möglichkeit zur Wartelistenanmeldung. Beim Freiwerden von Schulungsplätzen kann Hilti eine Anmeldebestätigung zusenden, mit deren Zugang ein Schulungsvertrag zustande kommt.

3. Stornierung / Absage

3.1 Präsenzschulungen & Online-Schulungen: Falls nicht anders in der vom Kunden nach der Anmeldung erhaltenen Bestätigungs-E-Mail angegeben, kann der Kunde Schulungen bis 4 Werktage vor dem geplanten Schulungstermin stornieren, wobei die Schulungsgebühr rückerstattet wird, sofern diese bereits gezahlt wurde. Schulungen können per E-Mail an die in der vom Kunden erhaltenen Bestätigungs-E-Mail angeführte E-Mail-Adresse storniert werden. Im Fall einer Stornierung von weniger als 4 Werktagen vor dem geplanten Schulungstermin ist eine Rückerstattung an den Kunden ausgeschlossen und die Zahlung des Kunden verfällt bzw. bleibt die Schulungsgebühr sofern noch nicht gezahlt dennoch fällig. Die Nichtteilnahme an einer geplanten Schulung gilt als Stornierung am selben Tag und jegliche Zahlung verfällt bzw. bleibt die Schulungsgebühr sofern noch nicht gezahlt dennoch fällig.

3.2 Hilti behält sich das Recht vor, Schulungen aus jeglichem Grund bis vier Tage vor dem geplanten Schulungszeitpunkt abzusagen. In diesem Fall kann der Kunde wahlweise die Schulung unter Rückerstattung des vollen Betrages stornieren (falls die Schulung bereits bezahlt wurde) oder auf einen anderen

Schulungstermin umbuchen.

3.3 Keine Pflicht zur Durchführung der Schulung bei Verhinderung des Trainers

Für alle Formen von Schulungen gilt: Sofern der von Hilti für die vereinbarte Schulung vorgesehene Trainer zum vorgesehenen Zeitpunkt der Schulung krankheitsbedingt oder aus einem anderen triftigen Grund für die Schulung ausfällt, z.B. im Falle von Streiks, Stau, Unfall, Ableben von Angehörigen, muss Hilti die vereinbarte Schulung zum vorgesehenen Zeitpunkt nicht durchführen. Mangels Pflichtverletzung schuldet Hilti dem Kunden keinen Schadens- oder Aufwendungsersatz wegen der aus einem solchen Grund ausgefallenen Schulung. Hilti schuldet dem Kunden in diesem Fall ausschließlich eine unverzügliche Mitteilung, dass die vereinbarte Schulung zum vorgesehenen Zeitpunkt nicht stattfinden kann. Der Kunde und Hilti werden anschließend einvernehmlich einen Ersatztermin für die Schulung zu vereinbaren suchen. Kommen der Kunde und Hilti zu keiner Einigung, können beide Vertragspartner vom betroffenen Schulungsvertrag zurücktreten.

4. Schulungsgebühr

Schulungsgebühren werden mit Abschluss des Schulungsvertrages fällig, sofern nicht abweichend mit dem Kunden vereinbart. Zu den von Hilti angegebenen Preisen kommt die gesetzliche MwSt. hinzu. An/- Abreise, und Logis sind im Preis nicht enthalten. Bei Präsenzschulungen ist Verpflegung im Preis inkludiert.

5. Teilnahme an Präsenzschulungen

Hilti behält sich das Recht vor, einen Schulungsteilnehmer, der nach Ermessen von Hilti die Schulung stört, zum Verlassen der Schulung aufzufordern. Während grundsätzlich jede Person an der Schulung teilnehmen kann, behält sich Hilti das Recht vor, ist aber nicht dazu verpflichtet, einem Teilnehmer die weitere Teilnahme zu untersagen, wenn er nach Ermessen von Hilti ein Sicherheitsrisiko darstellt oder auf sonstige Weise nicht in der Lage ist, die Schulungsziele auf angemessene Weise zu erreichen. Hilti ist nicht verpflichtet, einen Grund für eine Ablehnung anzuführen.

Die Schulung wird in deutscher Sprache durchgeführt. Hilti kann Teilnehmer, die des Lesens, Schreibens, Sprechens und Verstehens der deutschen Sprache nicht mächtig sind, nicht in Schulungen aufnehmen.

6. Urheberrecht und Nutzungsrecht des Kunden

6.1 ©2023 Sämtliche Rechte vorbehalte. Die in den Schulungen zur Verfügung gestellten Inhalte und Unterlagen sowie jegliche Aufzeichnungen davon („**Schulungsinhalt**“) verbleiben ohne Einschränkungen im alleinigen Eigentum der Hilti Aktiengesellschaft, Feldkircherstraße 100, 9494 Schaan, Liechtenstein, und diese behält sich, sofern in diesen Geschäftsbedingungen für Schulungen nicht ausdrücklich anders angegeben, sämtliche Rechte, Ansprüche und Beteiligungen sowie sämtliche Rechte am geistigen Eigentum gemäß Definition dieses Begriffs in Abschnitt 6.2) vor. Hilti wird von der Hilti Aktiengesellschaft ermächtigt, dem Kunden gemäß den hierin beschriebenen Geschäftsbedingungen Rechte am Schulungsinhalt zu gewähren.

6.2 „**Rechte am geistigen Eigentum**“: bezeichnet sämtliche gewohnheitsrechtlichen, gesetzlichen und sonstigen gewerblichen Schutzrechte und geistigen Eigentumsrechte, einschließlich Urheberrechte, Schutzmarken, Geschäftsgeheimnisse, Patente und sonstige Schutzrechte, die gemäß geltenden Gesetzen irgendwo auf der Welt erteilt, anerkannt oder durchsetzbar sind, sowie alle Urheberpersönlichkeitsrechte im Zusammenhang mit dem Schulungsinhalt.

6.3 Vorbehaltlich der ausdrücklich gemäß diesen Bedingungen gewährten eingeschränkten Rechte werden dem Kunden keine anderen als die ausdrücklich hierin angeführten Rechte gewährt. Der Kunde verwendet den Schulungsinhalt nur für seine internen Geschäftszwecke und ist nicht berechtigt: (i) Lizenzen oder Unterlizenzen für den Schulungsinhalt zu gewähren oder diesen zu verkaufen, wiederzuverkaufen, zu vermieten, zu verpachten, zu übertragen, abzutreten, zu verteilen, im Rahmen eines Timesharing-Konzeptes zu vergeben, anzubieten oder auf sonstige Weise Dritten zur Verfügung zu stellen; (ii) den Schulungsinhalt so zu verwenden, dass lokale, einzelstaatliche, nationale bzw. ausländische Gesetze, Verträge bzw. Vorschriften, die für eine bestimmte Partei gelten, verletzt werden; (iii) den Schulungsinhalt zu bearbeiten, zu vervielfältigen, abzuändern, zu kopieren oder davon abgeleitete Werke herzustellen; (iv) auf den Schulungsinhalt zuzugreifen, um handelsübliche Produkte oder Dienstleistungen zu erstellen; (v) Features, Funktionen, Schnittstellen oder Grafiken des Schulungsinhalts ganz oder teilweise zu kopieren; oder (vi) den Schulungsinhalt auf eine Weise einzusetzen, die den gemäß diesen Bedingungen zulässigen Verwendungszweck überschreitet; (vi) Ton- oder Videoaufzeichnungen bzw. Screenshots des Schulungsinhalts anzufertigen.

6.4 Hilti gewährt dem Kunden ein nicht-exklusives, jederzeit widerrufbares, nicht übertragbares Nutzungsrecht am Schulungsinhalt gemäß diesen Geschäftsbedingungen für Hilti Schulungen. Dieses Nutzungsrecht umfasst das Recht, den Schulungsinhalt dem Kunden zur Verfügung zu stellen und dessen Verwendung durch den Kunden bzw. dessen Verwendung durch einen autorisierten Nutzer zu gestatten. Der Kunde wird sich angemessen bemühen, den unbefugten Zugang zum Schulungsinhalt bzw. dessen unbefugte Verwendung durch nicht autorisierte Benutzer (d.h. Dritte, usw.) durch seine Systeme zu unterbinden und Hilti unverzüglich von einem solchen unbefugten Zugang bzw. einer unbefugten Verwendung in Kenntnis setzen.

7. Wichtige Hinweise

7.1 Allgemeines

Der Inhalt von Hilti Schulungen ist eine unvollständige Liste allgemeiner bedienungstechnischer Warnhinweise, die für die sichere technische Umsetzung, Handhabung und Installation von Hilti-Produkten befolgt werden müssen. Weitere Anweisungen finden sich in den produktrelevanten Gebrauchsanleitungen von Hilti, in technischen Handbüchern von Hilti oder technischen Datenblättern von Hilti, aber auch in nationalen oder internationalen Bauvorschriften, Bauprodukteverordnungen und Zulassungen. Die Nichtbefolgung dieser Anweisungen kann schwerwiegende Zwischenfälle nach sich ziehen, die auch zu Personenschäden oder zum Tod führen können. Bitte lesen Sie daher alle Anweisungen in den oben genannten relevanten Vorschriften und Unterlagen sorgfältig und aufmerksam durch und stellen Sie – insbesondere in Ihrem eigenen Interesse - sicher, dass Sie diese verstanden haben, bevor Sie Hilti-Produkte technisch umsetzen, installieren oder mit ihnen hantieren.

Hilti gewährleistet und haftet insbesondere nicht für die Eignung der im Rahmen von Hilti Schulungen bereitgestellten Informationen, um rechtliche Anforderungen oder spezifische Kundenbedürfnisse zu erfüllen. Der Kunde bleibt für die Festlegung und Umsetzung geeigneter und gesetzlich erforderlicher Maßnahmen und für die Einhaltung der geltenden Vorschriften allein verantwortlich.

7.2 Gesundheit und Sicherheit – HSE-Schulungen

Hilti HSE-Schulungen liefern keine abschließende Übersicht über alle potentiellen Gesundheits- und Sicherheitsthemen, sondern sollen lediglich einige der häufigeren Gesundheits- und Sicherheitsthemen im Zusammenhang mit dem relevanten Schulungsthema unter den üblichen Bedingungen am Arbeitsplatz (exemplarisch) darstellen. Hilti HSE-Schulungen sind unter keinen Umständen als rechtliche oder ärztliche Beratung gedacht und ersetzen daher keinesfalls die Beratung durch Rechtsexperten und/oder medizinische Fachkräfte. Hilti gewährleistet und haftet insbesondere nicht für die Eignung der im Rahmen von Hilti-Schulungen bereitgestellten Informationen, um rechtliche bzw. HSE-Anforderungen oder spezifische Kundenbedürfnisse zu erfüllen. Der Kunde bleibt für die Festlegung und Umsetzung geeigneter und gesetzlich erforderlicher HSE-Maßnahmen und für die Einhaltung der geltenden Vorschriften allein verantwortlich. In jedem Fall sind die allgemeinen Praktiken, Vorschriften, funktionsspezifischen Anforderungen im Hinblick auf Arbeitsschutz sowie die jeweils geltenden Unterlagen (z.B. Produktgebrauchsanweisungen und Bedienungshandbücher, Sicherheitsdatenblätter, Produktkennzeichnungen usw.) stets einzuhalten.

7.3 Hilti ist nicht verpflichtet den Lernerfolg der Teilnehmer zu überwachen und wird keine Lernerfolgsüberwachung durchführen, sofern dies nicht im Einzelfall für Präsenzseminare oder präsenzäquivalente Online-Schulungen abweichend vereinbart wird.

8. Haftung

Im Sinne dieses Abschnitts 8 umfasst „Hilti“ das Unternehmen Hilti, dessen MitarbeiterInnen, Führungskräfte, Handlungsbevollmächtigte und verbundene Unternehmen.

Die Haftung von Hilti gleich aus welchem vertraglichen oder gesetzlichen Rechtsgrund, ist für sämtliche Schäden ausgeschlossen, es sei denn, der jeweilige Schaden beruht auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung oder auf einer einfach fahrlässigen Verletzung wesentlicher Vertragspflichten (das sind Pflichten, auf deren Erfüllung der Kunde zur ordnungsgemäßen Durchführung des Vertrages regelmäßig vertraut und vertrauen darf). Bei einer einfach fahrlässigen Verletzung wesentlicher Vertragspflichten ist die Haftung von Hilti auf den vorhersehbaren, typischerweise eintretenden Schaden begrenzt. Diese Haftungsausschlüsse gelten nicht im Falle der Haftung wegen schuldhafter Verletzungen des Lebens, des Körpers sowie der Gesundheit, nicht im Falle der Haftung wegen Nichterfüllung einer Garantie, nicht im Falle der Haftung wegen arglistigen Verschweigens eines Mangels. Für etwaige Schäden, die dem Kunden bei der Anwendung der bei der jeweiligen Schulung erworbenen Kenntnisse entstehen, haftet Hilti

nicht. Der Kunde verpflichtet sich, Hilti diesbezüglich schad- und klaglos zu halten.

9. Datenschutz

Datenverarbeitungsvereinbarung

Hilti wird personenbezogene Daten nach Maßgabe der anwendbaren datenschutzrechtlichen Bestimmungen und im Einklang mit der diesem Dokument als Anhang 1 beiliegenden Datenverarbeitungsvereinbarung verarbeiten.

10. Geltendes Recht und Gerichtsstand

Für die vertraglichen Beziehungen gilt ausschließlich deutsches Recht unter Ausschluss internationalen Privatrechts, das zur Anwendung des Rechts eines anderen Staates führen würde. Gerichtsstand ist München, es sei denn, dass der Besteller seinen Sitz im Bezirk des Amtsgerichts Landsberg a.L. hat. Hilti ist jedoch auch berechtigt, ein anderes, für den Kunden zuständiges Gericht anzurufen.

11. Sonstiges

11.1 Teilnahmebescheinigung

Den Teilnehmern wird nach erfolgter Schulung eine Teilnahmebescheinigung ausgestellt. Ein Anspruch auf Ausstellung darüberhinausgehender Bescheinigungen oder Zertifikate besteht nicht, sofern es nicht schriftlich im Einzelfall abweichend vereinbart wird.

11.2 AGB

Nachrangig und ergänzend gelten die Allgemeinen Geschäftsbedingungen, Verkaufs- und Leistungsbedingungen von Hilti, die auf Hilti Online unter https://www.hilti.de/content/hilti/E3/DE/de/company/corporate-information/agb-overview/agb.html verfügbar sind („Hilti Bedingungen“) in ihrer zum Zeitpunkt des Vertragsschlusses gültigen Fassung.

Anhang 1 - Datenverarbeitungsvereinbarung
(Verantwortlicher an Auftragsverarbeiter)

Anhang 1 zum Vertrag über die Durchführungen von Schulungen („Vertrag“)

Vereinbarung zur Auftragsverarbeitung („AVV“)

Der vorliegende Auftragsverarbeitungsvertrag („AVV“) wird geschlossen von und zwischen:

i. dem Kunden als Datenverantwortlicher („Verantwortlicher“); und
ii. dem Serviceanbieter als Auftragsverarbeiter („Auftragsverarbeiter“),

jeweils „Vertragspartei“ und gemeinsam „Vertragsparteien“.

1. Gegenstand dieser AVV

Im Rahmen der Erbringung der vertragsgegenständlichen Leistungen verarbeitet der Auftragsverarbeiter personenbezogene Daten, für die der Kunde im Sinne des geltenden Datenschutzrechts als Verantwortlicher anzusehen ist (nachfolgend „personenbezogene Kundendaten“ genannt). Diese AVV legt die Datenschutzrechte und -pflichten der Parteien im Zusammenhang mit den Aktivitäten des Auftragsverarbeiters zur Verarbeitung personenbezogener Kundendaten fest.

2. **Umfang der Verarbeitung**

2.1. Die Parteien vereinbaren, dass der Kunde der Verantwortliche im Sinne des Art. 4 Abs. 7 DSGVO und der Serviceanbieter der Auftragsverarbeiter im Sinne des Art. 4 Abs. 8 DSGVO ist. Der Auftragsverarbeiter verarbeitet die personenbezogenen Kundendaten im Namen und nach den Weisungen des Verantwortlichen im Sinne des Art. 28 DSGVO.

2.2. Die Verarbeitung personenbezogener Kundendaten durch den Auftragsverarbeiter erfolgt in der Art und Weise, dem Umfang und zu dem Zweck, und bezieht sich auf die Arten personenbezogener Daten und Kategorien betroffener Personen und umfasst die Verarbeitungsvorgänge, die in der Anlage 1 angegeben sind.

2.3. Die Dauer der Verarbeitung ist ebenfalls im der Anlage 1 festgelegt.

2.4. Der Auftragsverarbeiter behält sich das Recht vor, die personenbezogenen Kundendaten so zu anonymisieren oder zu aggregieren, dass es nicht mehr möglich ist, einzelne betroffene Personen zu identifizieren und sie in dieser Form für die im Vertrag genannten Zwecke zu verwenden. Die Parteien sind sich einig, dass anonymisierte und gemäß der oben genannten Anforderung aggregierte personenbezogene Kundendaten nicht mehr als personenbezogene Kundendaten für die Zwecke dieser AVV betrachtet werden.

2.5. Die Verarbeitung personenbezogener Kundendaten durch den Auftragsverarbeiter erfolgt grundsätzlich im Land des Auftragsverarbeiters oder innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Europäischen Wirtschaftsraums (EWR) oder eines vergleichbaren Landes. Der Auftragsverarbeiter ist jedoch berechtigt, personenbezogene Kundendaten gemäß den Bestimmungen dieser AVV außerhalb des EWR zu verarbeiten, wenn er dem Verantwortlicher vorab über den Ort der Datenverarbeitung informiert und die Anforderungen des Kapitels V der DSGVO erfüllt sind. Wenn personenbezogene Kundendaten von einem Unterauftragsverarbeiter verarbeitet werden, dessen Verarbeitung der personenbezogenen Kundendaten nicht der DSGVO unterliegt, gilt Ziffer 7.4 dieser AVV.

3. Weisungen des Verantwortlichen

3.1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Kundendaten in Übereinstimmung mit den dokumentierten Weisungen des Verantwortlichen im Sinne des Art. 28 DSGVO, es sei denn, der Auftragsverarbeiter ist nach geltendem Recht dazu verpflichtet, anders zu verfahren. In diesem Fall hat der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über diese gesetzliche Anforderung zu unterrichten, es sei denn, ein solcher Hinweis ist aus wichtigen Gründen des öffentlichen Interesses gesetzlich verboten.

3.2. Die Weisungen des Verantwortlichen sind in dieser AVV grundsätzlich abschließend festgelegt und dokumentiert. Abweichende Einzelanweisungen oder Weisungen, die zusätzliche Anforderungen stellen, sind vorab mit dem Auftragsverarbeiter abzustimmen, um die Durchführbarkeit zu beurteilen und daraus folgende Kosten einschätzen zu können. Etwaige Mehrkosten, die dem Auftragsverarbeiter durch abweichende Einzelanweisungen oder Weisungen entstehen, die zusätzliche Anforderungen stellen, sind vom Verantwortlichen zu tragen.

3.3. Ungeachtet gegenteiliger Bestimmungen in dieser AVV ist der Verantwortliche zentraler Ansprechpartner für den Auftragsverarbeiter und ist alleinig für die interne Koordination, Überprüfung und Übermittlung von Weisungen oder Anfragen anderer Verantwortlicher (die zur Unternehmensgruppe des Verantwortlichen gehören) an den Auftragsverarbeiter verantwortlich. Der Auftragsverarbeiter ist von seiner Verpflichtung zur Information oder Benachrichtigung eines Verantwortlichen entbunden, wenn er dem Verantwortlichen nach dieser AVV die entsprechenden Informationen oder Benachrichtigungen übermittelt hat. Ebenso ist der Auftragsverarbeiter berechtigt, Weisungen, die direkt von einem Verantwortlichen, der nicht der Verantwortliche nach dieser AVV ist, übermittelt werden, abzulehnen. Der Auftragsverarbeiter dient als zentraler Ansprechpartner für den Verantwortlichen und ist allein verantwortlich für die interne Koordination, Überprüfung und Übermittlung von Weisungen oder Anfragen des Verantwortlichen an den/die Unterauftragsverarbeiter des Auftragsverarbeiters.

3.4. Wenn der Auftragsverarbeiter der Meinung ist, dass eine Weisung des Verantwortlichen gegen diese AVV oder gegen

geltendes Datenschutzrecht verstößt, ist der Auftragsverarbeiter nach entsprechender Benachrichtigung des Verantwortlichen berechtigt, aber nicht verpflichtet, die Ausführung der Weisung auszusetzen, bis der Verantwortliche die Weisung bestätigt hat. Die Parteien vereinbaren, dass die alleinige Verantwortung für die Rechtmäßigkeit der Verarbeitung (gemäß Art. 6 DSGVO) der personenbezogenen Kundendaten beim Verantwortlichen liegt.

4. Rechtliche Verantwortung des Verantwortlichen

4.1. Der Verantwortliche ist im Verhältnis zwischen den Parteien allein verantwortlich für die Zulässigkeit der Verarbeitung der personenbezogenen Kundendaten und für die Wahrung der Rechte der betroffenen Personen (gemäß Art. 12 bis 22 DSGVO).

4.2. Der Verantwortliche stellt dem Auftragsverarbeiter die personenbezogenen Kundendaten rechtzeitig für die Erbringung der Dienstleistungen zur Verfügung und ist für die Qualität der personenbezogenen Kundendaten verantwortlich. Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu unterrichten, wenn er bei der Prüfung der Ergebnisse des Auftragsverarbeiters Fehler oder Unregelmäßigkeiten im Hinblick auf das Datenschutzrecht oder seine Weisungen feststellt.

4.3. Auf Verlangen stellt der Verantwortliche dem Auftragsverarbeiter die in Art. 30 Abs. 2 DSGVO genannten Informationen zur Verfügung, sofern diese dem Auftragsverarbeiter nicht selbst zur Verfügung stehen.

4.4. Wenn der Auftragsverarbeiter aufgrund eines zwingenden Gesetzes oder einer Aufforderung verpflichtet ist, einer staatlichen Stelle oder Person Auskunft über die Verarbeitung der personenbezogenen Kundendaten zu erteilen oder in sonstiger Weise mit diesen Stellen zusammenzuarbeiten, unterstützt der Verantwortlicher den Auftragsverarbeiter auf erstes Anfordern bei der Bereitstellung solcher Informationen und bei der Erfüllung anderer Mitwirkungspflichten. Angemessene Kosten, die hierbei entstehen, werden durch den Verantwortlichen getragen.

5. Vertraulichkeitsverpflichtung

Der Auftragsverarbeiter verpflichtet alle Mitarbeiter, die mit personenbezogenen Kundendaten umgehen, zur Vertraulichkeit.

6. Sicherheit der Verarbeitung

6.1. Gemäß Art. 32 DSGVO ergreift der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung personenbezogener Kundendaten sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen, erforderliche und angemessene technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für die personenbezogenen Daten des Kunden zu gewährleisten.

6.2. Die derzeit geltenden technischen und organisatorischen Maßnahmen sind in Anlage 2 aufgeführt.

6.3. Der Auftragsverarbeiter hat das Recht, die technischen und organisatorischen Maßnahmen während der Laufzeit dieser AVV zu ändern, solange sie die gesetzlichen Anforderungen erfüllen.

7. Beauftragung von Unterauftragsverarbeitern

7.1. Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, Unterauftragsverarbeiter in Bezug auf die Verarbeitung personenbezogener Kundendaten zu beauftragen. Unterauftragsverarbeiter, die zum Zeitpunkt des Abschlusses des Vertrages beauftragt wurden, sind in der **Anlage 1** aufgeführt.

7.2. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über alle beabsichtigten Änderungen im Zusammenhang mit der Beauftragung oder dem Austausch von Unterauftragsverarbeitern per E-Mail. Der Verantwortliche hat das Recht, der Beauftragung eines potenziellen Unterauftragsverarbeiters zu widersprechen. Bei der Erhebung eines solchen Widerspruches hat der Verantwortliche seinen Widerspruch zu begründen. Widerspricht der Verantwortliche nicht innerhalb von vierzehn (14) Kalendertagen nach einer Benachrichtigung durch den Auftragsverarbeiter, erlischt sein Recht, der entsprechenden Beauftragung zu widersprechen. Wenn der Verantwortlicher einen solchen Widerspruch erhebt, ist der Auftragsverarbeiter berechtigt, den Vertrag und diese AVV mit einer Frist von fünf (5) Werktagen gemäß den Bedingungen im Vertrag zu kündigen.

7.3. Der Vertrag zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter muss dem Unterauftragsverarbeiter muss ein Schutzniveau gemäß dieser AVV vorsehen bzw. dem Unterauftragsverarbeiter die Pflichten im Sinne des Art. 28 Abs. 3 DSGVO auferlegen. Die Parteien vereinbaren ferner, dass diese Anforderung im Hinblick auf Cloud-Dienstleister, die Plattformen, Infrastrukturen oder "Software as a Service" bereitstellen, durch den Abschluss von Standard-Datenverarbeitungsvereinbarungen erfüllt werden kann, sofern diese die Anforderungen im Sinne des Art. 28 DSGVO erfüllen.

7.4. Vorbehaltlich der Einhaltung der Anforderungen von Ziffer 2.4 dieser AVV gelten die Bestimmungen dieser Ziffer 7 dieser AVV auch im Fall einer Beauftragung eines Unterauftragsverarbeiters, dessen Verarbeitung personenbezogener Kundendaten nicht der DSGVO unterliegt. In einem solchen Fall ist der Auftragsverarbeiter berechtigt und – soweit die Anforderungen der Ziffer 2.4 dieser AVV nicht anderweitig erfüllt werden – verpflichtet, einen Vertrag mit dem Unterauftragsverarbeiter abzuschließen, der die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates in Übereinstimmung mit dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 enthält, der das Modul 3 (Übertragung von Auftragsverarbeitern auf Auftragsverarbeiter) enthält. Wenn und soweit dies für ein angemessenes Schutzniveau in dem betreffenden Drittland erforderlich ist, muss ein solcher Vertrag zusätzliche Schutzvorkehrungen vorsehen, die zur Erreichung dieses Zwecks erforderlich sind. Die Parteien vereinbaren, dass ein solcher Vertrag auch die Anforderungen

gemäß Ziffer 7.3 dieser AVV erfüllt. Der Verantwortliche erklärt sich bereit, bei der Erfüllung der Ausnahmeregelungen im Sinne des Art. 49 DSGVO mitzuwirken, soweit dies erforderlich ist.

8. Rechte der betroffenen Personen

8.1. Der Auftragsverarbeiter unterstützt den Verantwortlichen, soweit dies möglich ist, im Sinne des Art. 28 Abs. 3 lit. e DSGVO durch technische und organisatorische Maßnahmen bei der Erfüllung seiner Verpflichtung zur Beantwortung von Anträgen, die in Ausübung der Rechte der betroffenen Person ergehen.

8.2. Soweit eine betroffene Person einen Antrag zur Ausübung ihrer Rechte direkt an den Auftragsverarbeiter stellt, leitet der Auftragsverarbeiter diese Anfrage zeitnah an den Verantwortlichen weiter, wenn der Auftragsverarbeiter die betroffene Person identifizieren kann und eine Zuordnung zum Verantwortlichen mit angemessenen Anstrengungen möglich ist.

8.3. Der Auftragsverarbeiter hat dem Verantwortlichen im Rahmen des Zumutbaren und Notwendigen, gegen die Erstattung der ihm dadurch entstandenen und nachzuweisenden Aufwendungen und Kosten, die Berichtigung, Löschung, Sperrung oder Einschränkung der weiteren Verarbeitung personenbezogener Kundendaten zu ermöglichen oder personenbezogene Kundendaten auf Weisung des Verantwortlichen selbst zu korrigieren, zu löschen, zu sperren oder die weitere Verarbeitung einzuschränken, wenn und soweit dies für den Verantwortlichen nicht möglich ist.

9. Benachrichtigungs- und Unterstützungspflichten des Auftragsverarbeiters

9.1. Soweit der Verantwortliche einer gesetzlichen Meldepflicht wegen einer Verletzung der Sicherheit von personenbezogenen Kundendaten (insbesondere im Sinne von Art. 33, 34 DSGVO) unterliegt, hat der Auftragsverarbeiter den Verantwortlichen rechtzeitig über alle meldepflichtigen Ereignisse in seinem Verantwortungsbereich zu unterrichten.

9.2. Der Auftragsverarbeiter unterstützt den Verantwortlichen auf dessen Verlangen, gegen die Erstattung der Aufwendungen und Kosten, die dem Auftragsverarbeiter dadurch nachweislich entstehen, bei der Erfüllung der Meldepflichten, soweit dies unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen angemessen und erforderlich ist.

9.3. Soweit der Verantwortliche einer rechtlichen oder behördlichen Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung (insbesondere im Sinne von Art. 35, 36 DSGVO) oder einer vergleichbaren Prüfung unterliegt, wird der Auftragsverarbeiter den Verantwortlichen auf dessen Verlangen bei der Erfüllung dieser Verpflichtung gegen Erstattung der dem Auftragsverarbeiter dadurch entstehenden und nachzuweisenden Aufwendungen und Kosten unterstützen, soweit dies unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen angemessen und erforderlich ist.

10. Laufzeit, Beendigung, Löschung und Rückgabe personenbezogener Kundendaten

10.1. Diese AVV tritt an dem Datum des Inkrafttretens des Vertrags in Kraft und endet mit deren Kündigung, spätestens jedoch mit dem Zeitpunkt, zu dem der Auftraggeber alle unter dieser AVV verarbeiteten personenbezogenen Kundendaten gelöscht oder gemäß den Anforderungen der Ziffer 2.4 dieser AVV anonymisiert bzw. aggregiert hat. Bei Konflikten zwischen dieser AVV und anderen Vereinbarungen zwischen den Parteien, insbesondere dem Vertrag, gehen die Bestimmungen dieser AVV vor.

10.2. Die im Vertrag festgelegten Kündigungsbestimmungen gelten auch für diese AVV.

10.3. Der Auftragsverarbeiter löscht die personenbezogenen Kundendaten unverzüglich nach Beendigung dieser AVV, es sei denn, der Auftragsverarbeiter ist nach geltendem Recht verpflichtet, die personenbezogenen Kundendaten weiter zu verwahren. Wenn der Verantwortlicher es vorziehen sollte, dass die personenbezogenen Kundedaten vor der Löschung zurückgegeben werden, muss der Verantwortliche den Auftragsverarbeiter unverzüglich hierüber informieren.

10.4. Der Auftragsverarbeiter kann auch nach der Beendigung der AVV solche Dokumentationen aufbewahren, die zum Nachweis einer ordnungsgemäßen und korrekten Verarbeitung von personenbezogenen Kundendaten dienen.

11. Nachweise und Audits

11.1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen alle erforderlichen und dem Auftragsverarbeiter verfügbaren Informationen bereit, um die Einhaltung seiner Verpflichtungen aus dieser AVV nachzuweisen.

11.2. Der Verantwortliche ist berechtigt, den Auftragsverarbeiter hinsichtlich der Einhaltung der Bestimmungen dieser AVV, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen. Dieses Recht umfasst, das Audit durch einen zertifizierten unabhängigen Dritten im Namen des Verantwortlichen durchführen zu lassen.

11.3. Zur Durchführung von Audits nach Ziffer 11.2 dieser AVV ist der Verantwortliche nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 dieser AVV auf eigene Kosten dazu berechtigt, innerhalb der üblichen Geschäftszeiten (montags bis freitags von 10:00 bis 16:00 Uhr Ortszeit) die Geschäftsräume des Auftragsverarbeiters zu betreten, in denen personenbezogene Kundendaten verarbeitet werden. Dabei darf der gewöhnliche Geschäftsgang des Auftragsverarbeiters nicht unterbrochen werden und der Verantwortliche verpflichtet sich schriftlich, die Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters unter allen Umständen zu wahren.

11.4. Der Auftragsverarbeiter ist berechtigt, nach eigenem Ermessen und unter Berücksichtigung der gesetzlichen Verpflichtungen des Verantwortlichen, Informationen nicht offenzulegen, die für die Geschäftstätigkeit des Auftragsverarbeiters sensibel sind oder wenn der Auftragsverarbeiter aufgrund seiner Offenlegung gegen gesetzliche oder sonstige vertragliche Bestimmungen verstoßen würde. Der Verantwortliche hat keinen Anspruch auf Zugang zu Daten oder Informationen über andere Kunden des Auftragsverarbeiters, Kosteninformationen, Berichten zur Qualitätskontrolle

und Vertragsverwaltung oder andere vertrauliche Daten des Auftragsverarbeiters, die für die vereinbarten Auditzwecke nicht unmittelbar relevant sind.

11.5. Der Verantwortliche hat den Auftragsverarbeiter rechtzeitig (in der Regel mindestens dreißig (30) Kalendertage im Voraus) über alle Umstände im Zusammenhang mit der Durchführung des Audits zu unterrichten. Der Verantwortlicher darf pro Kalenderjahr nur ein Audit gegen Erstattung der Kosten durchführen.

11.6. Wenn der Verantwortliche eine dritte Partei mit der Durchführung des Audits beauftragt, verpflichtet der Verantwortlicher die dritte Partei schriftlich auf die gleiche Weise, wie der Verantwortliche gegenüber dem Auftragsverarbeiter gemäß dieser Ziffer 11 dieser AVV verpflichtet ist. Darüber hinaus verpflichtet der Verantwortliche den Dritten schriftlich zur Verschwiegenheit und Geheimhaltung, es sei denn, der Dritte unterliegt einer beruflichen Verschwiegenheitspflicht. Auf Verlangen des Auftragsverarbeiters hat der Verantwortliche dem Auftragsverarbeiter unverzüglich die Verpflichtungsvereinbarungen, die mit dem Dritten abgeschlossen wurden, vorzulegen. Der Verantwortliche darf keine Wettbewerber des Auftragsverarbeiters mit der Durchführung des Audits beauftragen.

11.7. Nach Ermessen des Auftragsverarbeiters kann anstelle eines Audits ein Nachweis über die Einhaltung der Verpflichtungen aus dieser AVV erbracht werden, indem ein geeigneter, aktueller, unabhängiger Audit-Bericht von Drittanbietern oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit – z. B. nach ISO 27001, dem IT-Basisschutz des Bundesamtes für Sicherheit in der Informationstechnik (*BSI-Grundschutz*) oder eines vergleichbaren Standards ("**Audit Report**") – vorgelegt wird. Der Audit Report muss es dem Verantwortlichen in angemessener Weise ermöglichen, sich von der Einhaltung der vertraglichen Verpflichtungen zu überzeugen.

12. Schlussbestimmungen

12.1. Sollten einzelne Bestimmungen dieser AVV unwirksam sein oder unwirksam werden oder eine Lücke enthalten, bleiben die übrigen Bestimmungen davon unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine rechtlich zulässige Bestimmung zu ersetzen, die dem Zweck der unwirksamen Bestimmung am nächsten kommt und damit den Anforderungen im Sinne des Art. 28 DSGVO genügt.

Anlage 1 zur AVV (Details zur Verarbeitung)

a) Gegenstand und **Dauer** der Verarbeitung:
Gegenstand der Verarbeitung ist die Erbringung der Leistungen gemäß dem Vertrag.
Die Daten werden für 3 Jahre nach Durchführung der Schulung verarbeitet.

b) Die folgenden **Kategorien von Daten** sind betroffen, die über die angebotenen Dienste verarbeitet werden:
Beschäftigte und ehemalige Beschäftigte des Verantwortlichen

c) Die folgenden **Kategorien personenbezogener Daten** werden vom Auftragsverarbeiter verarbeitet:
Vorname, Nachname, Geburtsdatum, E-Mailadresse, Firma und Anschrift des Verantwortlichen, Name/Art der besuchten Schulung, Datum der besuchten Schulung, Schulung bestanden Ja/Nein (ohne konkretes Ergebnis).

d) Besondere Kategorien personenbezogener Daten:
Die Erbringung der Leistungen gemäß dem Vertrag sind nicht dazu bestimmt, besondere Kategorien personenbezogener Daten zu verarbeiten. Der Verantwortliche wird davon absehen, solche besonderen Kategorien personenbezogener Daten an den Auftragsverarbeiter zu übermitteln.

e) Art und **Zweck** der Verarbeitung:
Die Art der Verarbeitung umfasst die Erhebung, Speicherung, Verwendung (z.B. Bereitstellung, Übermittlung, usw.), Änderung/Korrektur und Löschung (einschließlich Anonymisierung oder Aggregierung).
Die Zwecke der Verarbeitung sind die Organisation von Schulungen, die Erstellung von Teilnahmebescheinigungen und die erneute Erstellung von Teilnahmebescheinigungen für einen vereinbarten Zeitraum nach Durchführung einer Schulung.

f) Unterverarbeiter:
Die vom Auftragsverarbeiter beauftragten Unterverarbeiter sind:

Subverarbeiter	**Verarbeitungstätigkeiten**	**Kategorien personenbezogener Daten**	**Ort der Verarbeitung**
Cvent [Cvent Deutschland GmbH c/o TMF Steuerberatung GmbH WPG Maximilianstr. 54 80538 München Germany	Speicherung der Daten für Verwaltungszwecke, Schulungsorganisation, Erstellen und Versenden von Teilnahmebescheinigungen, Kommunikation an den Kunden/Schulungsteilnehmer (mit wichtigen Informationen zur bevorstehenden oder bereits absolvierten Schulung) ➔ Cvent wird als Software/Plattform für alle Bereiche der Veranstaltungsorganisation genutzt. Es werden über Templates E-Mails an den Kunden versendet, die Schulungstermine inkl. Registrierungsmöglichkeit werden dem Kunden über Cvent zur Verfügung gestellt u.v.m.	Wie Auftragsverarbeiter	EU/EWR USA

Anlage 2 zur AVV

(Technische und organisatorische Maßnahmen)

This Document sets forth the technical and organizational security measures and procedures that Hilti undertakes, as a minimum, to maintain and to protect the security of personal data created, collected, received, used, stored or archived, disclosed by transmission, erased or otherwise processed. Hilti will keep documentation of technical and organizational measures identified below to facilitate audits, the conservation of evidence and to ensure compliance with the provisions of applicable data protection laws.

I. Confidentiality

i. Site Access Control

Hilti implements suitable measures in order to prevent unauthorized persons from gaining physical access to the data processing systems where personal data is processed.

a) The equipment on which the personal data is processed is placed within a physically protected site secured against accidents or hazards such as fire and flooding, attacks and physical access by unauthorized and/or uncontrolled individuals.

b) Secured doors are in place to access the physical sites. Access to the site is tracked. The doors are equipped with a spring-operated door shutter, that automatically closes the door.

c) Access authorizations are established for staff and third parties to the physical sites. The list of entitled individuals is reviewed periodically to reflect fluctuations and changes in roles and responsibility. This access list is under control of IT management.

d) The physical site is only entered when individuals justify the necessity to be granted access on site.

e) The site access is supervised and secured by an appropriate security system and/or security organization using a video control system.

f) Access to the site is controlled by an access card, a code lock or scanned biometric information.

ii. System Access Control

Hilti implements suitable measures to prevent its data processing systems from being used or logically accessed by unauthorized persons.

a) User identification and authentication methods to grant access to the processing systems are in place. Unique user IDs are used.

b) Authorizations are assigned according to a ‘need to have’ principle, approved and regularly reviewed by business owners.

c) Access rights revocation procedures are in place.

d) Privileged accounts are reserved for administrative IT functions and are not used outside of the required need of usage. These account owners with their specific areas covered are listed and regularly reviewed.

e) Access control mechanisms as password rules, lockouts or automatic timeouts are in place in accordance with defined overall standards.

f) Internet or end user facing endpoints are protected to prevent unwanted access to the systems and to avoid infiltration of malicious software. This covers areas as firewalls, malware detection, and others and is adjusted to new technologies based on the overall development.

iii. Data Access Control

Hilti commits to implement measures, which guarantee that the personnel authorized to use a data processing system can only access personal data of data subjects in accordance to the access authorization granted. Personal data cannot be read, copied, altered, deleted or otherwise processed without authorization during the processing, use or after storage.

a) Authorization mechanism that allows for precise definition of roles of authorized persons are in place. To ensure that staff will only access personal data and resources required to perform their job duties, staff is informed about their obligations and the consequences of any violations of such obligations.

b) Network shares with access only for authorized users / user groups.

c) Standard access, alteration and deletion logging is done with the base methods available on the OS, DB, network and application areas. Enhanced logging can be done on request and with special efforts based on the available functionalities of the implemented technologies and applications. Event logs recording user activities are regularly reviewed.

d) Depending on the level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons , additional dedicated confidentiality agreements are put in place with all persons accessing this information.

e) Specific encryption technologies are implemented for confidential data.

f) Mandatory authorization assignment procedure

g) Mandatory procedure for restoring data from backups (restored by IT department at request)

h) The assignment of authorization is only granted after the respective approval. The approvers are specified role owners (from business) and the assigners are the help desk (IT department).

i) Backup protected by appropriate authorization mechanisms (only authorized employees may access the backup).

iv. Separation Control

Hilti implements suitable measures to ensure that data collected for different purposes is processed separately.

a) Access to data is separated through application security for the appropriate users.

b) User roles and resulting access is based on function to be done.

v. Pseudonymisation

Hilti implements suitable measures that personal data shall be processed in such a way that the data can no longer be assigned to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures.

II. Integrity

i. Transmission Control

Hilti implements suitable measures to ensure that personal data cannot be read, copied, altered, removed or otherwise processed without authorization during electronic transmission, during transport or storage on data carriers, and that it can be verified and established at which points transfer of personal data by data transmission devices is permitted.

a) If data has to be copied to mobile devices, these mobile devices will be treated in accordance with the sensitivity of the data.

b) Authentication information which is being transferred within the public network is always encrypted. When accessed via the Internet encrypted transfer for all other data is used.

c) State-of-the-art network and network access protection technologies are used.

d) Monitoring of the completeness and correctness of the data transfer is supported by using network protocols with error correction features.

ii. Input Control

Hilti implements suitable measures to ensure that it can be subsequently verified and established whether and by whom personal data have been entered, modified, removed or otherwise processed from data processing systems.

a) If required for an adequate protection application functionalities are activated to automatically log users' information when data is created, modified, deleted or otherwise processed and protects the resulting protocol data against manipulation.

b) An authorization policy for the input of data, as well as for the reading, alteration and deletion of stored data is in place as described in the Data Access Control section hereafter.

c) If required for an adequate protection a role-based access control is put in place supporting the segregation of duty concept. Decision on the application of these concepts is based on an overall risk based approach.

III. Availability and Resilience

i. Availability Control

Hilti implements suitable measures to ensure that personal data is protected from accidental or unlawful destruction or loss.

a) Technical Backups are implemented, executed and tested based on a predefined policy to guarantee data and application recovery in accordance with the overall backup policy. This backup covers technical failures or operator errors of technical staff and implements data copies with short retention times. These backup copies are securely stored at a specifically protected site, separated from the site where the primary data resides. Backups are taken based on a defined service definition (backup frequency and retention) and also establish a target recovery time objective to get the backup restored to the primary location in case of loss of the primary data.

b) Availability is managed and designed based on an overall service level concept.

c) The physical site where the data processing equipment is located is protected against general environmental hazards and unauthorized access. It is protected with specific measures against power loss through UPS and Diesel engines. IT monitors and controls temperature and humidity at the site and alerts when reaching limits.

d) Availability of the network access to the site is enhanced through WAN based redundancies, network access redundancies to the site and onsite facilities through redundant datacenterbased networks.

e) Redundancies of the Infrastructure components itself (server and storage arrays) are in place in accordance with the agreed and predefined service levels.

f) The redundancy measures are checked on a regular basis. The results are documented accordingly.

g) State of the art functionalities are used on DB level to target for a minimum loss of transactional information in case of a technical failure by using DB features sup-porting minimal loss of transaction information where applicable..

h) In line with the service levels defined, additional availability features on DB level or at application level are in place.

i) Proactive infrastructure maintenance is set up to reduce unexpected unavailability.This maintenance work is planned based on a predefined monthly schedule. During these maintenance windows proactive tasks are executed to keep the infrastructure on a steady level aligned with the providers of the infrastructure components.

j) After the occurrence of a high-risk security incident,a structured After-Action Review is conducted to achieve mitigating actions and proactive measures to undertake.

k) Technical and application related changes are done according to change management processes, supported as far as possible by several stakeholders where changes are applied first before being applied to the production environment.

l) Long-term business-related archiving is done.

m) Where storage media has become obsolete and has to be decommissioned, specific destruction mechanism will be used to securely delete the stored data.

n) A disaster recovery plan is set out and regular emergency tests are carried out.

o) Risk analysis are conducted to derive security measures including documentation.

p) Personal data can be deleted where applicable in particular where an individual can exercise their right to erasure.

IV. Continuous Improvement (Procedure for Regular Review, Assessment and Evaluation)

i. Data Protection Management

a) Process owners are responsible for the periodic reviewing of data processing activities regarding data processed in their respective departments.

b) Should there be a change in data processing, such as additional personal data processed or changes regarding data storage, the CPO (Chief Privacy Officer) is immediately informed.

c) The CPO is responsible for the assessment of data processing activities and conducting a PIA or DPIA where necessary. PIA are incorporated into system, process and product life cycles.

ii. Incident Response Management

a) Documentation of the incident occurs simultaneous to incident analysis and response. It includes timestamps of significant events such as discovery, breach timing if possible, and resolution actions. The incidence documentation includes the description of the nature of the breach, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned where applicable. Documentation also includes the likely consequences of the personal data breach determined by IT security department together with CPO.

b) Following the discovery of a potential breach, including unauthorized access to user data or unauthorized access to the technology stack, we apply mitigating measures immediately, launch an investigation, conduct risk assessments and proceed to notify users where there is a high risk affecting their rights and freedom. The CPO conducts a risk assessment to establish the likelihood and severity resulting from the breach and notifies the relevant Supervisory Authority within 72 hours of becoming aware of breach, when deemed necessary.

c) A thorough analysis of each breach incident and handling process will be conducted by the security team in conjunction with our technical engineers. Security breach responses will be shared with relevant staff and organizational departments and taken into account in order to build more robust security systems.

d) Incidents (breaches, complaints, enquiries) are documented.

iii. Privacy by Design and Privacy by Default

Default settings ensure that personal data is only processed with the highest privacy protection at the earliest stages of the design of processing operations.
We undertake to comply with the Privacy by Design and Privacy by Default principles.

a) We include data protection and data privacy in our projects, IT systems and ensure that privacy is built for the whole lifecycle process.

b) We will collect the least amount of personal data from data subjects and privacy settings apply by default.

c) To ensure the minimization principle, pseudonymization and anonymization are used to reduce the risk of harm to data subjects.