Terms and Conditions for Hilti Trainings

These Terms and Conditions for Hilti Trainings govern the provision of trainings ("**Trainings**") by Hilti, Inc., or Hilti (Canada) Corporation ("**Hilti**"), for sales and deliveries in the United States or Canada, respectively to Customer, and to the extent not in conflict with the terms stated herein, incorporate the respective Hilti Terms and Conditions of Sale, available on Hilti Online under www.hilti.com (US) or www.hilti.ca (Canada), ("**Hilti Terms**").

1. Subject Matter of the Contract

1.1 These Terms and Conditions for Hilti Trainings are applicable to all Trainings offered by Hilti to Customers, including e-learnings, webinars and face-to-face Trainings. Prices, details and descriptions for the Trainings are provided on Hilti Online and the Hilti booking platform through which the Training was booked by the Customer. By booking a Training, Customer agrees to these Terms and Conditions for Hilti Trainings for the current as well as any future Trainings booked by the Customer. Additional Training program terms may apply to specific Trainings such as certified installer Trainings.

1.2 E-learnings

For Trainings provided in the form of e-learnings, Customer is either granted access to the e-learning directly at the end of the booking process or in case of bulk Trainings, Customer is awarded the relevant credits for Training units which Customer may allocate to Authorized Users, where "Authorized User" shall mean Customer or its employees. E-learnings cannot be forwarded or shared with other users. All certificates obtained will be kept on the learning management platform for 2 years unless otherwise specified in the training description.

1.3 Webinars

For Trainings provided in the form of webinars, Customer will be granted access to participate in the selected webinar on a training platform. If possible, Hilti makes recordings of webinars available for download, but only for the respective Authorized User having purchased the webinar.

1.4 Face-to-Face Trainings

Hilti offers face-to-face Trainings either as pre-scheduled Training with the Training date, content and location described on Hilti Online and/or the respective booking platform or as individually agreed Training where Training date, content and location is mutually agreed with the Customer.

2. Registration Process

2.1 In order to book Trainings and access the training platform for webinars and e-learnings prior registration by Customer on Hilti Online is required. Customer may subsequently book Trainings on Hilti Online and/or the available Hilti training platforms using the log-in credentials provided upon registration on Hilti Online.

2.2 Hilti reserves the right to reject registrations and/or bookings for any or no reason. Customer's booking of a Training will only be deemed accepted by Hilti on completion of the Hilti Online registration, payment of the Training fee, and Customer's receipt of a confirming email from Hilti.

3. Cancellation

3.1 E-learnings: e-learnings are allocated to the Customer directly at the end of the booking process and therefore cannot be cancelled or rescheduled.

3.2 Presence Trainings & Webinars: If not indicated otherwise in the confirmation e-mail received by Customer after booking, Customer may cancel Trainings up to 5 working days before the scheduled Training date and the Training fee will be refunded. Trainings can be cancelled by e-mail to the e-mail address indicated in the confirmation e-mail received by Customer after booking or directly on the booking platform. In case of cancellation after the above indicated date, Customer will not be granted any refund and the payment will be forfeited. Failure to participate in a scheduled Training will be treated as same-day cancellation and any payment will be forfeited. Rescheduling of Trainings is only possible with Hilti's written approval.

3.3 Hilti reserves the right to cancel Trainings up to five days prior to scheduled Training date for any or no reason. In this case Customer will be given the option of cancelling the Training for a full refund (if the Training has

already been paid), or scheduling for another Training date.

4. Training Fee

Training fees are due upon booking of the Training. The price stated for each Training participant includes all taxes and fees. Customer is responsible for any travel expenses, cost of accommodation and/or meals.

5. Participation in Face-to-Face Trainings

Hilti reserves the right to require any Training participants to leave if, in Hilti's sole opinion, they disrupt the Training. While in principle anyone may participate in the Training, Hilti reserves the right, but without obligation to do so, to not allow a participant to proceed who, in Hilti's sole opinion, may create a safety concern or is otherwise incapable of reasonably fulfilling the Training objectives. Hilti shall have no obligation to provide a reason for a rejection.

The Training shall be performed in the English language. Hilti cannot accommodate participants who are not proficient in reading, writing, speaking and understanding English.

6. Access Requirements

Access by Customer to the training platform for webinars and e-learnings may require certain system requirements as specified and updated from time to time at https://www.docebo.com/online-training-lms-system-requirements, where solely Customer shall be responsible to ensure that the system requirements are met.

7. Copyright and Rights of Use for the Customer

7.1 © Hilti Corporation 2019. Hilti Corporation, Feldkircherstrasse 100, 9494 Schaan, Liechtenstein, exclusively and unrestrictedly retains sole ownership, and reserves all rights, title and interest and all Intellectual Property Rights (as such term is defined in section 7.2) to the content and documentation provided on the Hilti training platform, in the Trainings and any recordings thereof ("**Training Content**"), unless explicitly otherwise stated in these Terms and Conditions for Trainings. Hilti is entitled by Hilti Corporation to grant to Customer rights to the Training Content according to the terms and conditions described herein.

7.2 "**Intellectual Property Rights**": means any and all common law, statutory and other industrial property rights and intellectual property rights, including copyrights, trademarks, trade secrets, patents and other proprietary rights issued, honored or enforceable under any applicable laws anywhere in the world, and all moral rights, related to the Training Content.

7.3 Subject to the limited rights expressly granted hereunder, no rights are granted to Customer hereunder other than as expressly set forth herein. Customer shall use the Training Content solely for its internal business purposes and shall not: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, offer, or otherwise make the Training Content available to any third party; (ii) use the Training Content in violation of applicable local, state, national and/or foreign law, treaties, and/or regulations applicable to a respective party; (iii) edit, reproduce, modify, copy or create any derivative works based on the Training Content; (iv) access the Training Content in order to build any commercially available product or service; (v) copy any features, functions, interfaces or graphics of the Training Content or any part thereof; or (vi) use the Training Content in any manner that exceeds the scope of use permitted herein. (iv) record any Training Content in audio or video or by means of screen shots.

7.4 Hilti grants to Customer a non-exclusive, at any time revocable, non-transferable right to use the Training Content in accordance with these Terms and Conditions for Hilti Trainings. This right of use encompasses the right to make available to and use the Training Content by Customer or to have it used by any Authorized User. Customer shall use reasonable efforts to prevent unauthorized access to, or use of, the Training Content by not authorized users (i.e. third parties, etc.) through its systems, and notify Hilti promptly of any such unauthorized access or use.

8. Important Notes

8.1 General

The content of Hilti Trainings is a partial list of the common instructional warnings that must be followed for safe engineering, handling and installing Hilti products. Further instructions can be found in the product-related Hilti Instructions for Use, in Hilti Technical Manuals or Hilti Technical Data Sheets, but also in national or international building codes, construction product regulations and approvals. Failure to follow these instructions can result in serious incidents, potentially leading to injury or death. Always read and understand all of the instructions in the above mentioned relevant regulations and documents before engineering, handling or installing Hilti products.

Hilti does not warrant the suitability of the information provided in any Hilti Trainings to fulfil any legal requirements or specific customer needs. The customer remains solely responsible for the definition and implementation of appropriate and legally required measures and compliance with applicable regulations.

8.2 Health and Safety ("**HSE**") Trainings

Hilti HSE Trainings do not provide a complete overview of all potential health and safety issues, but are only intended to review some of the more common health and safety issues associated with the relevant Training topic in typical jobsite conditions. Hilti HSE Trainings are under no circumstances meant to provide legal or medical advice and therefore do not replace the consultation of legal and / or medical specialists. Hilti does not warrant the suitability of the information provided in Hilti HSE Trainings to fulfil any legal and/or HSE requirements or specific customer needs. The customer remains solely responsible for the definition and implementation of appropriate and legally required HSE measures and compliance with applicable regulations. In any case, the general industry safety practices, regulations, job-specific requirements and applicable literature (e.g. product instructions-for-use and operator's manuals, Safety Data Sheets, product labels, etc) must always be followed.

9. Liability

For purposes of this Section 9, "Hilti" includes Hilti, Inc. or Hilti (Canada) Corporation respectively, its employees, directors, agents, and affiliates. Hilti's sole obligation for any claim in any way associated with the Training shall be as stated in these Terms and Conditions for Hilti Trainings, and if not otherwise addressed Hilti's liability shall in no event exceed the fee paid for the Training. Hilti shall in no event be liable for, and Customer agrees to indemnify Hilti against, any and all other claims and costs (including attorney's fees), including any claim for direct, indirect, special, consequential, or any other damages, regardless of the legal theory, and including any claim based on the negligence or intentional wrongdoing of Hilti.

10. Data Protection

Personal Data shall be processed in line with the Data Processing Agreement attached as Annex 1 to this Agreement.

11. Governing Law and Venue

11.1 The governing law and venue are regulated by the Hilti Terms.

Annex 1 - Data Processing Agreement (Controller to Processor)

This Data Processing Agreement ("**DPA"**) is entered into by and between:
(i) the Customer, acting as controller ("**Controller**"); and
(ii) Hilti, acting as processor ("**Processor**"),

each a "**Party"**, together the "**Parties"**.

The terms being used in this DPA shall have the same meaning as under the Agreement and as further specified herein.

PREAMBLE

WHEREAS, under the Terms and Conditions for Hilti Trainings ("**Agreement**") concluded between Processor and Controller, Processor agreed to provide the services as set forth in the Agreement and as further specified in Exhibit 1 to this DPA (the "**Services**");

WHEREAS, in rendering the Services, Processor may from time to time be provided with, or have access to information which may qualify as personal data within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR"**), and other applicable data protection laws and provisions;

WHEREAS, Controller engages Processor as a commissioned Processor acting on behalf of Controller as stipulated in Art. 28 GDPR;

NOW, **THEREFORE**, and in order to enable the parties to carry out their relationship in a manner that is compliant with law, the parties have entered into this DPA as follows:

1. Terminology
For the purposes of this DPA, the terminology and definitions as used by the GDPR shall apply. In addition to that,

"**Member State"**	Shall mean a country belonging to the European Union or to the European Economic Area;
"**Subprocessor"**	Shall mean any further processor, located within or outside of the EU/EEA, that is engaged by Processor as a sub-contractor for the performance of the Services or parts of the Services on behalf of Controller provided that such Subprocessor has access to the personal data of Controller exclusively for purposes of carrying out the subcontracted Services on behalf of Controller.
"Security Breach"	Shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which affects the personal data of the Controller covered by this DPA.

Further definitions are provided throughout this DPA.

2. Details of the processing
(a) The details of the processing operations provided by Processor to Controller as a commissioned data processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Exhibit 1 to this DPA.

3. Obligations and responsibilities of Controller
(a) The Controller is responsible that the processing activities relating to the personal data, as specified in the Agreement and this DPA, are lawful, fair and transparent in relation to the data subjects, as set out in Exhibit 1. The actual personal data being uploaded and/or being made available to Processor are solely steered and monitored by Customer and solely Customer is responsible to have obtained all necessary consents and permissions to conduct such processing in accordance with the applicable data protection laws. In case of any violations hereof, Customer shall indemnify and hold harmless Processor for any and all claims raised against the Processor.

(b) Notwithstanding anything to the contrary in this Agreement, the Controller shall serve as a single contact for the Processor and is solely responsible for the internal coordination, review and submission of instructions or request of other controllers to the Processor. The Processor shall be discharged of its obligation to inform or notify a controller when it has provided such information or notice to the Controller. The Processor is entitled to refuse any instructions provided directly by a controller that is not the Controller similarly. The Processor will serve as a single point of contact for the Controller and is solely responsible for the internal coordination, review and submission of instructions or requests from the Controller to the Processor subprocessor(s).

4. Instructions
(a) The Processor is obliged to process the personal data only on behalf of the Controller and in accordance with this DPA and the Agreement.

(b) The Controller's instructions are exhaustively set forth in this DPA and the Agreement.

5. Obligations of Processor
(a) The Processor shall use commercially reasonable efforts that persons authorized by the Processor to process the personal data on behalf of the Controller, in particular the Processor's employees as well as employees of any Subprocessors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that such persons who have access to the personal data process such personal data in compliance with this DPA.

(b) The Processor shall use commercially reasonable efforts to implement and maintain the technical and organizational measures as specified in Exhibit 2. The Processor may amend the technical and organizational measures from time to time, provided that the amended technical and organizational measures are in overall not less protective as those set out in Exhibit 2. Substantial amendments to the technical and organizational measures shall be notified to the Controller.

(c) The Processor shall use commercially reasonable efforts to make available to the Controller any information necessary to demonstrate compliance with the obligations of Processor laid down in Art. 28 GDPR and in this DPA.

(d) The Processor shall use commercially reasonable efforts to provide an independent third-party audit report upon Controller`s request, where such audit report shall only be requested once per calendar year and at Controller`s costs.

(e) The Processor is obliged to notify the Controller within 48 hours:

- about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; and
- about any complaints and requests received directly from a data subject (e.g., regarding access, rectification, erasure, restriction of processing, data portability, objection to processing of data, automated decision-making) without responding to that request, unless the Processor has been otherwise authorized by the Controller to do so, or (ii) in case of a Security breach the Processor is becoming aware of.

(f) The Processor shall use commercially reasonable efforts to assist the Controller with its obligation to carry out a data protection impact assessment as may be required by Art. 35 GDPR and prior consultation as may be required by Art. 36 GDPR that relates to the Services provided by the Processor to the Controller under this DPA by means of providing the necessary and available information to the Controller, where any extraordinary costs hereto shall be beard by Customer.

(g) The Processor shall use commercially reasonable efforts to not further process the personal data, after the end of the provision of Services, and delete any existing copies unless European Union or Member State law requires the Processor to retain such personal data.

6. Data subject rights

(a) The Controller is primarily responsible for handling and responding to requests made by data subjects.

(b) The Processor shall use commercially reasonable efforts to assist the Controller with any appropriate and possible technical and organizational measures to respond to requests for exercising the data subjects' rights which are laid down in Chapter III of the GDPR, where Controller herewith confirms to consider the technical and organizational measures being set forth in Exhibit 2 to be sufficient

(c) The Controller is obliged to determine whether or not a data subject has a right to exercise any such data subject rights as set out in this Section 6 and to give specifications to the Processor to what extent the assistance specified in Section 6 (b) is required.

7. Subprocessing

(a) Processors may subcontract its obligations under this DPA in compliance with the requirements as set forth herin to Processors' affiliated companies and/or third parties ("Subprocessors"). A list of the Subprocessors engaged with Processors as of the Effective Date of the Agreement is available at https://tos.docebo.com/Docebo-sub-processors-list.pdf and Customer herewith agrees to the engagement of such Subprocessors.

(b) During the Term, Processors will provide at least four (4) weeks prior notice ("Subprocessor Change Notification") to the Customer before authorizing any new Subprocessor ("Subprocessor Change Effective Date"). If Customer disapproves of the engagement of such new Subprocessor, Customer may terminate the Agreement with two (2) weeks written notice, including an explanation of the reasonable grounds for disapproval of the Subprocessor, to the Subprocessor Change Effective Date. If the Customer does not object to the Subprocessor Change Notification in accordance with the foregoing, this shall be deemed as the Customer's acceptance of the new Subprocessor. Processors remain responsible for any Subprocessors' compliance with the obligations of this DPA.

(c) In case a Subprocessor is located outside the EU/EEA in a country that is not recognized as providing an adequate level of data protection, the Processor will (i) enter into a data processing agreement based on EU Model Clauses (Processor to Processor), or (ii) provide the Controller with information on the Subprocessor's certification under the Privacy Shield program and re-confirms that the Subprocessor's certification under the Privacy Shield program is still valid upon Controller`s request, or (iii) provide the Controller, upon Controller`s request, with other information and relevant documentation on the mechanism for international data transfer pursuant to Art. 46 GDPR that is used to lawfully disclose the Controller's personal data to the Subprocessor.

10. Term and termination

The term of this DPA is identical with the term of the Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Agreement.

11. Miscellaneous

(a) The Parties are required to comply with those obligations under the GDPR and under any other applicable data protection laws that apply, as applicable, to the Controller in its role as data controller or to the Processor in its role as data processor.

(b) If and to the extent necessary to comply with mandatory provisions regarding the commissioning and performance of the Processor under the laws applicable to the Controller, the Controller may require any necessary changes (including amendments) to the provisions of this DPA and its annexes. If the Controller and the Processor are not able to agree upon changes required to meet mandatory legal requirements within thirty (30) days of the Processor's receiving written notice of the mandatory changes, either Party shall have the right to terminate this DPA with thirty (30) days' notice in writing.

(c) In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations.

Exhibit 1 to the DPA
(processing details)

A) The following **categories of data subjects** are being processed while offering the Services:

☐ Hilti customer`s employees and Hilti customer's former employees	☐ Hilti employees (for testing purposes)

B) The following **categories of personal data** are being processed by Processor on behalf of Controller while offering the Services:

☐ Mandatory: Business or personal email, User ID, Full name
☐ Optional: Date of birth, role/job function, business or personal address, interests, learning preferences, Trade
☐ Technical data: Subscription date, Hilti account number, email validation status, user status expiration, connection data (IP address, protocols, etc.)

C) Special categories of personal data
The Services are not intended to process special categories of personal data.

D) Subject-matter of the processing

Processing activity	**Processing time**
Collection or registration of data	limited to purpose
Organization or structuring of data	limited to purpose
Hosting or storage of the data	limited to purpose
Adaptation or modification of the data	limited to purpose
Extraction or consultation of data	limited to purpose
Limitation (blocking) of data	limited to purpose
Usage of data	limited to purpose
Deletion or destruction of data	limited to purpose (all certificates obtained after completion of a course will be kept 2 years unless otherwise specified in the training description)
Support and maintenance of data	limited to purpose

Exhibit 2 to the DPA
(technical and organizational measures)

Description of the technical and organizational measures implemented by Processor as verified and confirmed by Controller:

Access Control to Processing Areas

- Data Importer implements suitable measures in order to prevent unauthorized persons from gaining physical access to the data processing equipment where Personal Data is processed or used, in particular:
    - Site access is tracked and documented.
    - Site access is supervised and secured by an appropriate security system and/or security organization.
    - Visitors will be continuously escorted.

Access Control to Data Processing Systems

- Data Importer implements suitable measures to prevent the data processing systems used for the processing of Personal Data from being used or logically accessed by unauthorized persons, in particular:
    - User identification and user authentication methods are in place to grant controlled access to the processing system.
    - Access control and authorizations are defined according to a 'need to have' principle.
    - Data Importer's internal endpoints used to support the software service are protected to prevent unwanted access to the systems and to avoid infiltration of malicious software. This covers technologies as firewalls, antivirus detection, malware detection, intrusion detection and prevention and others. These technologies will be adjusted to new levels based on the overall development in these areas.

Access Control to Use Specific Areas of Data Processing Systems

- Data Importer implements suitable measures within the applications so that the persons entitled to use the data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that personal data cannot be read, copied or modified or removed without proper authorization, in particular:
    - For Data Importer personnel policies are in place and trained related to the access to personal data.
    - Data Importer informs its personnel about relevant security procedures including possible consequences of breaching the security rules and procedures.
    - For training purposes Data Importer will only use anonymous data.
    - Access to the data is either done from a controlled location or via a controlled network access.
    - End devices used to access the data are protected by up to date client protection mechanisms.

Transmission Control

- Data Importer implements suitable measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission can be established and verified (data transfer control), in particular:
    - Control of data transfer between Data Exporter and the Data Importer supplied software service:
        - Data Importer's software services use encryption to ensure confidentiality and integrity/authenticity when transferring data from the Data Exporter to the software service.
    - Control of data transfers between Data Importer and Sub Processors:
        - In addition to the contractual agreed areas, data retrieval is only allowed for dedicated support activities and only for authorized support staff.
        - The authorization process for Data Importer support staff performing data transfers is regulated through a defined process.
        - If data has to be copied to specific media for transport to a 3rd party, these media will be treated with discernment in accordance with the sensitivity of the data.
        - Documented procedures for the secure transfer of Personal Data are established.

Input Control, Processing Control and Separation for different purposes

- Data Importer implements suitable measures to ensure that Personal Data is processed safe and solely in accordance with the Data Exporter's instructions, in particular:
    - Access to data is separated through application security for the appropriate users.
    - The application supports the identification and authentication of users.
    - Application roles and resulting access is based on roles based on the function to be executed within the application.
    - When reasonable and feasible, Data Importer may implement in their software controls to validate data input and/or to track usage or modification of data.