BINDING CORPORATE RULES (“BCR”)

TABLE OF CONTENTS

1. INTRODUCTION

Hilti has a reputation for providing quality products and excellent customer service but is also committed to protecting customer and employee privacy in the offline and online sphere. Customer and employee privacy is important to Hilti; therefore, it has established a foundation for the protection of all Personal Data processed by all Hilti Entities to ensure a common ground applicable worldwide.

Hilti provides global procedures and program which define and set forth how it processes Personal Data globally. These measures hereto presented constitute the Binding Corporate Rules Policy ("BCR").

2. SCOPE OF BCR

Hilti protects Personal Data and enforces Data Subject Rights under the BCR within or outside the EEA and Switzerland. Hilti will not transfer Personal Data to any Hilti Entity located outside the EEA before such Hilti Entity is effectively bound by the Hilti BCR, and can deliver compliance with them, by signing the Joint Agreement and becoming a Hilti Entity.

a. Geographical scope

The BCR apply to the processing of Personal Data by Hilti.

Appendix 2 contains the list of all Hilti Entities and Hilti HQ to which the herewith BCR are applicable.

b. Material scope

The BCR cover all Personal Data processing activities of the following Data Subjects:

- Hilti customers, contact persons and suppliers
- Hilti candidates and job applicants, Hilti employees and their dependents

A detailed description of the material scope can be found in Appendix 3.

c. Duty to respect BCR

The same way Hilti ensures globally a high-level delivery of its products and services, Hilti undertakes to provide high standards for data protection throughout all the Hilti Entities by ensuring the legally binding nature of the herewith BCR.

This means that Hilti employees are bound by the BCR, regardless of the geographic location.

Any Hilti Entity wishing to be part of the BCR must sign the Joint Agreement, legally binding such Entity and their employees to comply with these BCR jointly with any other Hilti Entity and Hilti HQ.

Prior to becoming a Hilti Entity, a Hilti organization must implement the BCR within their own organization to fulfill their duty to respect the BCR.

This means that Hilti Entities must ensure that:

- Its employees are legally bound, understand, abide by and are trained on BCR
- Data Subject Rights including Third-Party beneficiary rights can be enforced
- There is a DSR handling process in place as provided in the BCR
- It will abide by and implement the related data protection policies established by Hilti HQ
- It will cooperate with Hilti HQ to ensure the effective and continuous implementation of the BCR over time

Hilti Entities' employees are bound to the present BCR by means of dedicated clauses in their employment contract, their general obligation of loyalty, general obligation to comply with Hilti's policies and also by the applicable code of conduct or charters.
Hilti employees also have by default an obligation of secrecy which applies to the processing of Personal Data.

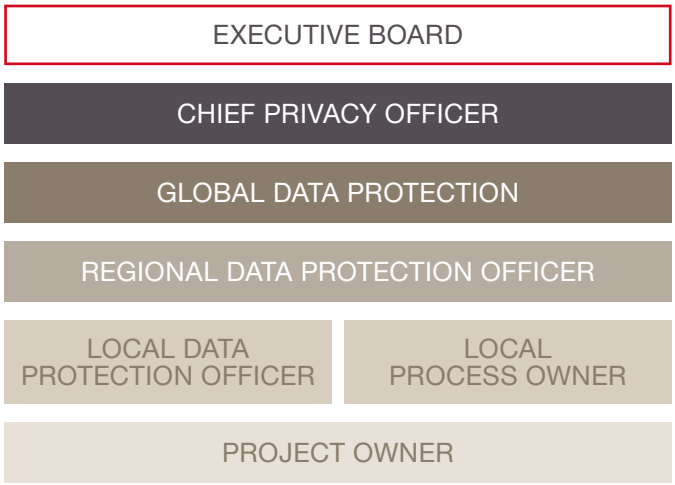
Hilti applies the highest data protection standards and provides Third-Party beneficiary rights to Data Subjects. These rights are enforceable no matter where Personal Data is processed by Hilti. Where additional rights can be granted to Data Subjects for example as per national data protection laws and regulations, Hilti undertakes to respond to such right.

Hilti provides an up-to-date list of Hilti Entities bound by the BCR available on: www.hilti.group.

3. DATA PROTECTION OFFICER

a. Purpose

Data Protection Officers ("DPO's") are a key role in the data protection accountability-based framework. Hilti has appointed a network of DPOs to ensure the implementation of compliance and internal privacy policies throughout the whole organization.



b. Roles and responsibilities

Chief Privacy Officer: Hilti has appointed a Chief Privacy Officer ("CPO") responsible for monitoring compliance with data protection laws and regulations and easily accessible from each Hilti Entity. CPO is the designated Data Protection Officer for Hilti, and its contact details are communicated to the Liechtenstein Data Protection Authority as per GDPR Article 37.

The CPO has been appointed based on his/her expert knowledge in the field of data protection and data privacy, as well as overall years of experience which attest their professional qualities required to fulfill the tasks of a CPO. The required skills are:

- Expertise and in-depth understanding of national, EEA, global data protection and privacy laws, regulations and practices
- Advanced knowledge of the business sector and Hilti internal organization

- Good understanding of processing activities and operations carried out by Hilti
- Integrity and high professional ethics
- Understanding of GDPR processes and principles
- Outstanding communication skills in order to train and work with various teams and business lines
- Ability to guarantee secrecy and high confidentiality during the performance of their duties

The role of CPO has been strictly assessed and Hilti ensures the independence of the CPO role which is free from any conflict of interest within Hilti.

The CPO operates from Hilti's Headquarters and reports to the highest management level.

The CPO undertakes to fulfill the following tasks:

- Regularly or where necessary, informs and advises the Executive Board
- Monitors compliance with data protection regulations and internal policies, including to protect Personal Data, assign responsibilities, raise awareness, and ensure the training of staff involved in processing operations and related audits
- Provides advice where requested with regards to Data Protection Impact Assessments and monitors their performance
- Cooperates with the Supervisory Authorities
- Acts as a contact point for the Supervisory Authorities on any issue relating to processing of Personal Data, including prior consultation where required and to consult where appropriate with regard to any other matter
- Provides guidance by evaluating the risks associated with all data processing activities including but not limited to the scope, nature, context, and purposes for the processing
- Monitors and annually reports on compliance at a global level to the executive board of directors
- Ensures the integration of data protection in overall compliance management, this includes but is not limited to the product and services development process as well as continued process reviews and enhancements
- Supervises the Global Team
- Informs the Executive Board or highest management level of any question or concern arising during the performance of his/her duties
- Decides on or requests audits on an ad hoc basis

Global Team: The Global Team ("Global Team") is composed of privacy professionals specializing in legal and technical implementation of data protection matters. The Global Team directly reports to the CPO and is involved at the earliest stage of Hilti operations to assess data protection.

The Global Team tasks are the following:

- Providing CPO and business lines with legal and technical assessments with regards to data protection
- Drafting internal policies and processes
- Providing business lines with guidance
- Conducting DPIA
- Promoting data protection by Design and by Default in the whole organization
- Regularly reviewing organization's governance in regard to data protection
- Providing regular guidance for regional and local DPOs and monitoring performance at a regional and local level
- Raising awareness in the organization
- Providing Regional and Local DPOs with training
- Supporting global corporate audit teams in the performance of audit program
- Updating the record of processing activities at a global level on behalf of the Controller (Hilti Entity or Hilti HQ)
- Drafting and reviewing data processing agreements for global contracts
- Handling Data Subject requests including assessment of Data Subject Rights

The Global Team works hand-in-hand with the CPO, performs in an independent manner and undertakes strict secrecy and confidentiality during the course of their duties.

Regional DPOs: Regional DPOs are appointed to coordinate data protection policies at a regional level according to Hilti's internal organization.

Regional DPOs are responsible for the following tasks:

- Ensuring a legal watch for the region and informing the Global Team for further assessment
- Communicating to Local DPOs action plans, roadmaps and insights provided by the Global Team or CPO
- Providing the Global Team with periodic reports on performance
- Seeking guidance from the Global Team or CPO
- Handling DSR and claims

Local DPOs and Local Process Owners: Local DPOs are responsible for monitoring data protection practices and processing activities in Hilti Entities.
Local DPOs are responsible for the following tasks:

- Locally implementing global and regional internal policies
- Evaluating local processing activities together with project owners
- Drafting data processing agreements with local vendors
- Ensuring a legal watch and reporting to Regional DPO, Head of Legal and Compliance or the Global Team
- Updating the record of processing activities at a local level and ensuring this is continuously updated and maintained
- Handling DSR and claims

Local Process Owners are responsible for assisting their respective Local DPO and informing them regarding the development of local activities. They are also responsible for assisting Local DPOs generally in the performance of their duties.

Project owners: All Project owners are responsible for working hand-in-hand with Local DPOs and Local Process Owners and inform the latter of projects prior to conducting any processing activity. Project owners gather all information required before the launch of any project and provide it to the Local DPOs and Local Process Owner for prior assessment. Project Owners report any risk, issue or question related to data protection to the Local DPOs and Local Process Owners before, during and after the project completion. Project Owners are trained and perform with respect to data protection by Design and by Default principles.

4. TRAINING PROGRAM FOR HILTI EMPLOYEES

Employees have permanent or regular access to and process Personal Data during the performance of their daily activities at Hilti. Therefore, to raise awareness within all departments, Hilti has taken measures for employees to better understand how to carry out their work duties generally, but also depending on their area of work in accordance with data protection practices.

5. APPLICABLE DATA PROTECTION PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

Hilti is determined to apply the data protection principles defined in the EEA to Personal Data worldwide. Such level of protection is enforced by Hilti to guarantee a proper processing of Personal Data, ensuring key elements such as the processing of Personal Data in accordance with the minimisation principle, data quality or default security practices.
Hilti has established an action plan to prevent and mitigate any Personal Data Breach and where applicable, to inform Data Subjects or the Supervisory Authorities.

Hilti enforces data protection principles, as explained in these BCR, irrespective of the applicable data protection law, unless it is providing more stringent requirements than those set up in the BCR. All of these principles are promoted and implemented within Hilti by means of data protection by Design and by Default policies and trainings in order to ensure overall Personal Data governance.

a. Transparency, fairness, and lawfulness principles

The principle of fairness and transparency requires that any information and communication relating to the processing of Personal Data is easily accessible and easy to understand, as well as drafted in a clear and plain language. Hilti will only process personal data in a lawfully, fairly, and transparent manner.
The principle of lawfulness means that the data processing is taking place according to a defined legal basis.

To ensure the application of these three main principles, Hilti has put in place various measures, these include:

- Transparency measures for the processing (as detailed under BCR Section 6). Definition of the legal basis for each processing activity.
- The applicable legal basis can either be:
  - Consent of the Data Subject
  - Contractual relationship or pre-contractual relationship with the Data Subject
  - Hilti's legal obligations
  - The protection of vital interests of the Data Subject as well as of another natural person or, where applicable
  - The legitimate interests (by conducting a balance of interest's assessment with Data Subjects' rights, freedoms, and expectations) pursued by the Controller or by a Third-Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child

The processing of special categories of Personal Data is lawful only where, in addition to the legal bases listed above, one of the following exemptions applies:

- Explicit consent of the Data Subject
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent
- Processing relates to Personal Data which are manifestly made public by the Data Subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy

In order to make sure that there is no oversight, Hilti has put in place tools (see BCR Section 7) and will inform Data Subjects on the applicable legal basis along with the information Data Subjects are entitled to (see BCR Section 6).

b. Purpose limitation

This principle means Personal Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Hilti ensures that Personal Data are processed only to fulfil its specific, clear, and legitimate purposes. Data Subjects are informed of such purposes which are defined before collecting Personal Data (see BCR Section 6).

Personal Data will not be further processed in a manner which is deemed incompatible with the defined purposes.

Hilti will only process Personal Data for a new purpose if and insofar as it has obtained consent from the Data Subject.

However, such consent collection is not carried out where the new purpose for processing can be reasonably expected from Data Subjects.

To determine whether a processing activity can be done for another purpose which is compatible with the initial purpose for which Personal Data is collected, Hilti takes into account:

- Any link between the purposes for which Personal Data have been collected and the purposes for the intended further processing

- The context in which Personal Data have been collected, especially with regards to the relationship between Hilti and Data Subjects
- The nature or sensitivity of the Personal Data collected
- The possible consequences of the intended further processing for Data Subjects, especially with regards to the rights and freedoms of Data Subjects
- The existence and implementation of appropriate safeguards or additional and required organizational and technical measures such as, but not limited to, encryption, pseudonymization or anonymization of Personal Data

c. Data minimization and accuracy

The minimisation principle means that Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The accuracy principle means that Personal Data must be accurate and kept up to date. Inaccurate Personal Data (based on the applicable purposes) must be erased or rectified.

Hilti must only collect and process Personal Data necessary to achieve the purposes defined beforehand. Hilti will inform Data Subjects of such purpose to give them the possibility to note that what Hilti collects is relevant and strictly necessary (see BCR Section 6).

Nonetheless, Personal Data changes with time and must be updated. For this reason, Hilti provides Data Subjects with clear methods for Data Subjects to update their Personal Data on the different Hilti websites or applications and Data Subjects are encouraged to inform Hilti of any change in their situation or inaccuracies relating to the Personal Data provided or collected.

If Data Subjects inform Hilti, or if Hilti notices that Personal Data are either not entirely correct or no longer up-to-date, Hilti will make sure to update said and reflect such update across its systems and databases.

d. Limited retention periods

This principle means that Personal Data must be kept in a form which permits the identification of Data Subjects for no longer than necessary for the purposes for which Personal Data is processed.

Furthermore, Hilti ensures the application of a clear Personal Data retention policy.
Hilti retains Personal Data by using technical and organizational safeguards and processes Personal Data for as long as required to fulfil Hilti purposes defined by its business needs or as required by law.

The Personal Data retention period is defined in accordance with the processing activity by conducting the following assessment:

- Definition of the purpose for processing Personal Data and the business needs:
  - Purpose for Personal Data processing
  - Estimated data retention period to achieve such purpose
- Assessment of legal obligations
  - Review of data retention applicable legal and regulatory requirements
  - Duration of the processing activity
- Balancing the Data Subjects interests, rights and freedoms
  - Evaluating Data Subjects' interests and expectations
  - Assessing Hilti's interests (such as responding to a claim)

Hilti does not retain Personal Data longer than necessary, when such Personal Data is no longer needed.
Hilti will either:

- Dispose of Personal Data in a secure manner and in accordance with its TOMs and security guidelines; or
- Anonymize Personal Data in a manner by which Data Subjects cannot be identified – where Hilti requires to retain Personal Data in the future

e. Personal Data security and Data Processing Agreements

Technical And Organizational Measures (TOMs)

This principle means that Personal Data is processed in a manner that ensures appropriate TOMs, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate TOMs.

Hilti is dedicated to ensuring to the best of its capabilities the security of data without hindering their use within the normal conduct of business with Data Subjects or the experience of Data Subjects with Hilti's services. As a result, Hilti is striving to safeguard Personal Data against risks that may result from improper use, especially with regards to unauthorised or unlawful processing and against accidental loss, destruction or alteration of Personal Data.

Hilti is enforcing various organizational, physical and technical security measures along with protocols, controls, documented guidance, good practices, processes and policies. The TOMs are enforced as a minimum security-baseline. To implement TOMs appropriate to the risk, Hilti considers the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The appropriate measures implemented include:

- The pseudonymisation and encryption of Personal Data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing, and evaluating the effectiveness of TOMs for ensuring the security of the processing

Data Processing Agreements and contractual relationship with Processors

Controller instructs Processors to perform its processing activities. Controller conducts due diligence and assesses such processing activities to ensure that they meet Controller's standards. They are monitored periodically to ensure that they ensure continuous implementation of organizational and technical measures.

Controller ensures proper contractual safeguards are in place by means of a written agreement (DPA). Such agreement is signed before conducting any processing activity and includes all data protection legal requirements to govern the parties' contractual relationship.

Where processing is to be carried out on behalf of a Controller, the Controller shall use only Processors providing sufficient guarantees to implement appropriate TOMs in such a manner that processing will meet the requirements of the herewith BCR and ensure the protection of the Data Subjects' rights.

The DPA stipulates that Processor must and as provided by Article 28(3) GDPR:

- Process Personal Data solely under written instructions from Controller, including with regards to transfers of Personal Data to a non-EEA country or organization
- Ensure persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Ensure it has taken all appropriate TOMs
- Only engages another Processor (Sub-Processor) with prior specific or general written authorization of the Controller and apply the same data protection obligations as set out in the contract or other legal act between the Controller and the Processor
- Be held liable for any violation of its sub-Processors to the herewith BCR
- Assist Controller with Data Subject Rights and complaints processes
- Assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR considering the nature of processing and the information available to the Processor
- Either return or delete Personal Data processed in accordance with the Data Processing Agreement instructions
- Make available to Controller all necessary information in order to demonstrate compliance with the BCR as well as contributing to audits
- Immediately inform the Controller where an instruction may infringe GDPR or national data protection laws

Furthermore, DPAs contain at least the following information with regards to the processing activity:

- The subject-matter and duration of the processing
- The nature and purpose of the processing
- The type of Personal Data and categories of Data Subjects
- The obligations and rights of the Controller

Personal Data Breach management process

While Hilti processes Personal Data in accordance with state-of-the-art TOMs, it also ensures a proper legal framework and implements incident response guidelines. Hilti has established a Personal Data Breach process to anticipate incidents. This process allows Hilti to ensure that the risks or impacts for Data Subject rights and freedoms are mitigated as much as possible or entirely prevented.

Therefore, as soon as becoming aware of a Personal Data Breach, Hilti Entities have a duty to report it to the Hilti HQ without undue delay.

Hilti HQ will take applicable preventive measures and ensure that the relevant data protection, IT and security functions and bodies are involved to conduct investigations, mitigation measures and report adequately on the matter.

Throughout this event, Hilti HQ will assess the situation to ensure it meets its obligations of notification to the Supervisory Authorities. Hilti will notify the competent Supervisory Authority without undue delay, and where feasible no later than 72 hours after having become aware of the Personal Data Breach. Should the 72-hour period not be met, reason must be given for the delay. Hilti will also inform Data Subjects, should Hilti not be able to mitigate the consequences of a Personal Data Breach which is likely to result in a high risk for Data Subjects' rights and freedoms.

Any Personal Data breach is documented (comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken). Such documentation is made available to the Supervisory Authority on request.

Requirements in respect of transfers and onward transfers to Third-Parties not bound by the BCR

Any transfer or onward transfers of Personal Data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if all provisions in Chapter V GDPR are complied with.

A transfer or onward transfer may take place if a transfer mechanism as described in the following table applies:

#	Transfer mechanism	Description
1.	Transfers based on an adequacy decision	A transfer of Personal Data to a third country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
2.	Standard Data Protection Clauses adopted by the European Commission	Contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses – so-called standard contractual clauses (SCC) – that have been "pre-approved" by the European Commission.

#	Transfer mechanism	Description
3.	An approved Code of Conduct	Codes of Conduct taking account of the specific features of the various processing sectors and the specific needs of micro-, small-, and medium-sized enterprises.
4.	An Approved Certification Mechanism	To demonstrate compliance of processing operations by Controllers and Processors.
5.	Contractual clauses between the Controller or Processor and the Controller, Processor or the recipient of the Personal Data in the third country or international organisation	Subject to the authorisation from the competent Supervisory Authority, the appropriate safeguards may also be provided by contractual clauses.

In absence of an Adequacy Decision (#1) or of appropriate safeguards (#2-5) a transfer or a set of transfers of Personal Data to a third country or an international organization shall take place only if the conditions as per Art. 49 GDPR are met, such as:

- The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards
- The transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent

Further, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a Controller or Processor to transfer or disclose Personal Data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to GDPR Chapter V.

Any transfer of Personal Data to a Third-Party not bound by GDPR is subject to a prior assessment as detailed under BCR Section 10.c.

BCR shall not permit onward transfers to a Third-Party made under the justification that Data Subjects have been given the opportunity to opt-out from such transfer of Personal Data.

6. TRANSPARENCY AND EASY ACCESS TO BCR

Hilti provides transparent communication to Data Subjects including by means of an accurate, up-to-date and detailed privacy notice covering all areas processing Personal Data as well as the herewith BCR and a detailed HR privacy notice for Hilti employees. Hilti BCR are published and easily accessible on a dedicated BCR webpage.

Hilti BCR are made publicly available and contain at least the following detailed sections in full:

- Definitions of the terms used in BCR (Appendix 1)
- Hilti Data protection office (BCR Section 3)
- Scope of BCR including material and geographical scope (BCR Section 2 and Appendix 3)
- Liability process and Hilti HQ burden of proof (BCR Section 9.g)
- Data Subject rights including Third-Party beneficiary rights and Data Subject request, complaint, and redress procedure (BCR Section 9)
- Applicable Data protection principles for the processing of Personal Data (BCR Section 5)
- Transparency and easy access to BCR (BCR Section 6)
- Cooperation with the Supervisory Authorities and national laws (BCR Section 10)
- Process for updating the BCR (BCR Section 11)

Other sections of the BCR will also be provided to Data Subjects in an abbreviated form. When Personal Data is **directly obtained from Data Subjects,** information is provided at the time when Personal Data are obtained directly from Data Subjects.

When Personal Data **are obtained from sources other than the Data Subject,** the information is provided:

- Within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed
- If the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject or
- If a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed

Hilti ensures that the right of the Data Subjects to be informed is respected and provides them with the following information as per the following table:

	Information provided to Data Subjects	When Hilti collects Personal Data directly from Data Subject	When Hilti collects Personal Data indirectly, from other sources
Who	Who is the Controller within Hilti, responsible for data processing and its contact details	■	■
Who	Who and to which Hilti Entity or Hilti HQ Data Subjects can contact for any query or to exercise Data Subjects rights with regards to the processing of Personal Data – such as a local DPO	■	■
Why	Why Hilti needs to process Personal Data (data processing purposes) and the applicable legal basis	■	■
Why	Where Hilti is processing Personal Data based on legitimate interests as a legal basis, further information regarding such interests	■	■
Right	Where Hilti is processing Personal Data based on Data Subjects' consent, information on how to withdraw consent at any time and as legally permitted under applicable data protection laws, such consent withdrawal shall be effective for further processing of Personal Data	■	■
What	The categories of Personal Data Hilti processes about Data Subjects (such as full name, e-mail address or company information)		■
How	How Hilti collected Personal Data and whether it was from publicly accessible sources		■
When	How long Hilti retains Personal Data, whether the fixed retention period or the reference basis used to determine such retention period	■	■
Who	The list of recipients which receive Personal Data	■	■
How	The list of Data Subject Rights regarding Personal Data in accordance with processing activities (access, rectification, erasure, restriction, portability and objection)	■	■
How	Right to lodge a complaint	■	■
How	Where Hilti intends to transfer Personal Data outside the EEA, measures Hilti takes to protect Personal Data before the transfer or giving access to the Personal Data to a Hilti Entity or recipient located outside the EEA and further details on such processing activity	■	■
Why	Where the collection of Personal Data stems either from a legal, pre-contractual or contractual requirement. Where such legal basis applies and Data Subjects are required to provide Personal Data, further details will be provided including regarding the possible consequences of not doing so	■	
Why	Where Personal Data is processed to make automated decisions without human action and causes legal effects or significantly affects Data Subject rights and freedoms, including profiling (evaluation or analysis of Data Subject personal aspects or prediction of behavior). Where such automated process is used, the logic involved, significance and the potential consequences of such decisions will be explained to Data Subjects	■	■

Where applicable, Hilti is not required to provide Data Subjects with such information if:

- Data Subjects already have access to relevant information
- Hilti complies with a legal obligation preventing such disclosure as per GDPR Article 23

7. ACCOUNTABILITY

Hilti undertakes to act in accordance with data protection principles. Therefore, Hilti HQ is bound by the herewith BCR and takes responsibility for developing processes and demonstrating compliance with the BCR.

8. AUDIT OF BCR

Hilti establishes internal data protection rules and policies to ensure proper safeguards for processing Personal Data. As part of this, Hilti has implemented a data protection audit program.
The purpose of audits is to assess Hilti's compliance against the BCR, where both Hilti Group and its Entities implement data protection policies on an ongoing basis in accordance with BCR.

9. INDIVIDUAL RIGHTS AND COMPLAINT HANDLING PROCEDURE

a. Purpose

This section details Hilti's procedures for handling rights requests of individuals under these BCR. It covers Data Subject Rights as well as data protection claims and complaints. Both Data Subject Rights and Data Subject complaints are defined as request rights. This section does not cover or govern other rights individuals are granted by other laws, which are managed separately.

b. Data Subject Rights and Third-Party beneficiary rights

Data Subjects are entitled to exercise the following Data Subject Rights including Third-Party beneficiary rights as follows:

Right of access: Data Subjects have the right to obtain from the Controller confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, access to the Personal Data and the following information:

- The purposes of the processing
- The categories of Personal Data processed
- The recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations
- Where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where the Personal Data are not collected from the Data Subject, any available information as to their source
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subjects
- Where Personal Data are transferred to a third country or to an international organisation, the Data Subjects shall have the right to be informed of the appropriate safeguards relating to the transfer

Right to rectification: Data Subjects shall have the right to obtain from the Controller without undue delay the rectification of inaccurate Personal Data concerning him or her. Data Subjects shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement reflecting the purposes of the processing.

Right to erasure: Data Subjects shall have the right to obtain from the Controller the erasure of Personal Data concerning him or her without undue delay and the Controller shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies:

- The Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- Data Subjects withdraw consent on which the processing is based and where there is no other legal ground for the processing
- Data Subjects object to the processing and there are no overriding legitimate grounds for the processing, or Data Subjects object to the processing of their Personal Data for direct marketing purposes
- The Personal Data have been unlawfully processed
- The Personal Data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject
- The Personal Data have been collected in relation to the offer of information society services

Where the Controller has made the Personal Data public and is obliged to erase the Personal Data, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform Controllers which are processing the Personal Data that Data Subjects have requested the erasure by such Controllers of any links to, or copy or replication of, those Personal Data.

Right to restriction of processing: Data Subjects shall have the right to obtain from the Controller restriction of processing where one of the following applies:

- The accuracy of the Personal Data is contested by Data Subjects, for a period enabling the Controller to verify the accuracy of the Personal Data
- The processing is unlawful, and Data Subjects oppose the erasure of the Personal Data and requests the restriction of their use instead
- The Controller no longer needs the Personal Data for the purposes of the processing, but they are required by Data Subjects for the establishment, exercise, or defence of legal claims
- The Data Subject has objected to processing pursuant to the right to object (see below) pending the verification whether the legitimate grounds of the controller override those of the Data Subject

Right to data portability: Data Subjects shall have the right to receive the Personal Data concerning them, which they have provided to a Controller, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the Personal Data have been provided, where:

- The processing is based on consent or on a contract and
- The processing is carried out by automated means

In exercising their right to data portability Data Subjects shall have the right to have the Personal Data transmitted directly from one Controller to another, where technically feasible.

Right to object: The Data Subjects shall have the right to object, on grounds relating to their situation, at any time to processing of Personal Data concerning them which is based on the Controller or Third-Party legitimate interests as per Section 5.a (by conducting a balance of interest's assessment with Data Subjects' rights, freedoms, and expectations) including profiling based on those provisions.

The Controller shall no longer process the Personal Data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of Data Subjects or for the establishment, exercise, or defense of legal claims.

Where Personal Data are processed for direct marketing purposes, Data Subjects shall have the right to object at any time to processing of Personal Data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where Data Subjects object to processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

Automated individual decision-making, including profiling: Data Subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Third-Party beneficiary rights

Hilti BCR confer Third-Party beneficiary rights to Data Subjects by which Data Subjects may enforce principles as detailed in the herewith BCR such as described hereafter:

- Applicable Data protection principles for the processing of Personal Data (BCR Section 5)
- Transparency and easy access to the BCR (BCR Section 6)
- Data Subject Rights and Third-Party beneficiary rights (BCR Section 9.b)
- The need to be transparent where the national legislation prevents Hilti or one of its Entities from complying with the BCR (BCR Section 10.b)
- Cooperation duties with Supervisory Authorities with regards to Personal Data related to the Data Subject (BCR Section 10)
- Liability (BCR Section 9.g)
- The duty to inform Data Subjects about any update of the BCR and of the list of group members bound by the BCR (BCR Section 11)
- Right to bring a claim, complain and redress (BCR Section 9.c, 9.d and 9.e)

c. Data Subject request, complaint, and redress procedure

Data Subjects have the possibility to report any concern or issue with regards to data processing by Hilti. Data Subjects are entitled to ask for information or documentation regarding data protection including the BCR. Data Subjects have the following possibilities to make use of the rights detailed in Section 9.b:

Data Subject Requests (DSR): In compliance with data protection laws, Data Subjects are entitled to exercise rights including Third-Party beneficiary rights as provided by data protection regulations and as detailed in Section 9.b. DSR allow Data Subjects to file complaints and claims with Hilti itself. Prior to lodging a complaint to a Supervisory Authority or a court, it is preferable to submit any request or raise any concern in writing directly for the attention of Hilti CPO who is the appropriate point of contact for any data protection matter (See BCR Section 3 – Data Protection Office). Further detailed information on DSR in BCR Section 9.e.

Data subjects can lodge a complaint to a Supervisory Authority: Hilti works closely with the Liechtenstein Supervisory Authority where Hilti has its headquarters. Data Subjects have the right to lodge a complaint with the Supervisory Authority of Liechtenstein or to the local supervisory authorities in any EEA member state, e.g., Data Subject's place of habitual residence, place of work or the place in which the alleged infringement took place. Data Subjects can easily find the list of the relevant National Data Protection Supervisory Authorities.

Data Subjects can bring a claim to courts: Data Subjects also have the right to file a claim before competent courts subject to local laws of their habitual residence or where the relevant Hilti Entity has an establishment. The competent courts are those recognized as being in the Member States of the European Economic Area. In cases where the alleged infringement is caused by a non-EEA Entity, Data Subjects can bring a claim to the court of the EEA Member State where Hilti HQ is established or the competent court of the EEA Member State of the Data Subject`s habitual permanent residence.

Such rights do not extend to matters relating to internal mechanisms implemented by Hilti such as details of training or audit programs, compliance network, and mechanism for updating rules and measures.

Upon closing a request and following the DPOs assessment, Hilti keeps a record of Data Subject's input where further action is required and updates policies and processes accordingly where applicable and necessary. Such corrective actions are included in the report. The report is communicated to Hilti CPO and other internal data protection teams where deemed necessary.

d. Conditions for making a request

Request criteria: When a Data Subject sends a DSR, Hilti assesses it with regards to the different Data Subject Rights and their respective grounds for making a request. If there is no applicable ground for the DSR, Hilti informs the Data Subject the reason as to why it cannot execute the request.

Request type: Data Subjects can submit several requests (e.g., various types of DSR) or questions at a time, or in several requests by indicating their identity and context for the requests.

Request format: Requests can be made orally as well as face-to-face at Hilti offices, Hilti stores or when in contact with the salesforce and Customer Service team (for example, to opt-out from marketing communications). However, Hilti's designated, and preferred method is in writing and electronically.

The Hilti HR Privacy Notice ensures employees are informed on the processes for DSR and can directly contact their local Human Resources department, Legal Counsel and DPO. Data Subjects can contact Hilti through the following methods:

- Dedicated local and global DPO e-mail addresses as stated in the Privacy Policy
- Directly use the DSR form on the Hilti websites, where Data Subjects can easily contact the local and global DPO team
- In writing by post to a Hilti Office, by addressing the letter to the Hilti "Data Protection Officer" or "Legal Department" to ensure the letter reaches the relevant team
- On the phone, through customer service numbers available on the Hilti websites or Hilti Stores

Identity verification: When Hilti has reasonable doubts with regards to the identity of Data Subjects, Data Subjects can be asked to provide a proof of identity. The requirements can be:

- Full name of Data Subject
- E-mail address
- Hilti ID – where applicable
- Telephone number (business)
- Company address or country of residence

Content of the DSR: Data Subjects can provide the following details in their DSR such as:

- Identity information (see "identity verification")
- Information regarding the request, such as:
  - Type of Request (see "definition") including questions or requesting further information
  - Type of Personal Data concerned (either category of Personal Data or specific Personal Data)
  - Preferred response method (communication through e-mails is the default method)

Data Subjects may also provide additional information with regards to DSR purpose, motivation, or ground for such request.

Other "self-service" methods: Digital platform users are able to rectify or delete their Personal Data and manage their communication preferences directly through their Preference Center. It is also possible to manage cookie settings through the dedicated cookie banner.

e. Request management

This section details the procedure for managing DSR and other questions related to data protection.

Responsible owners:

- Global Data Team, with regards to the global processing activities
- Local data protection teams including Regional and Local DPOs, with regards to their respective local processing activities
- Global and Local process experts

Upon request: DPOs receive the DSR or request from the Data Subject through the designated methods (see "Request format"), either directly from the Data Subject, or through other internal departments. The DPO replies with an acknowledgement e-mail to the Data Subject to inform them their request is being assessed. When receiving the request, the DPO may then ask the Data Subject for further information (see "identity verification" and "content of the DSR"). The DPO then proceeds with the request assessment and determines whether legal grounds apply as well as the efforts associated with the request (see "Request criteria"). Hilti ensures to answer to the enquiry without undue delay, starting from the date the request is received.

Refusal of request: Following DPO assessment and in the absence of legal grounds for the request or where Hilti must abide by legal requirements which are in accordance with GDPR Article 23 and retain Personal Data Hilti is entitled to refuse to execute such request.

Inquiry action: Once the assessment has been done by the DPOs, one or several local process expert(s) will provide support in searching for the relevant elements the Data Subject is requesting. The latter will provide DPOs with the information and Personal Data found regarding the Data Subject, in accordance with his initial request (see "content of the DSR").

Timeline: Hilti ensures to answer Data Subjects without undue delay and in any event within one month. Considering the complexity and number of requests and where requests require further investigation efforts, the timeframe can be expanded by 2 months. In this case, the DPOs will inform the Data Subject before the time limit of one month, explaining the reason for the delay.

Record keeping: Hilti keeps a record of all DSR including the outcome of DSR and legal grounds for refusal where applicable.

f. Response management

After DPOs and process experts have assessed and dealt with the DSR, they will proceed with the response to the Data Subject, as follows:

Access requests: Hilti provides the Data Subject with the Personal Data it holds about them by considering the initial request (see "content of the DSR"). Hilti will provide the Data Subject their Personal Data in a secure, easy, and readable format. The Data Subject can also request a different format for the response, but the electronic format is always preferred.

Rectification, erasure and restriction: Where the legal grounds are applicable, the Data Subject can request for the erasure and the restriction of the processing of their Personal Data. Process owners ensure that the data is rectified in a timely manner. If applicable, process owners will then rectify or delete the data accordingly. Data Subjects can also easily modify or delete their data through the Hilti digital platforms (see "Other self-service methods").

Data portability requests: Where legal grounds are applicable, Data Subjects can request Hilti to be provided with their processed data to be reused for their own purposes to different services. Hilti ensures to transfer or copy data from one IT environment to another by the use of secured transfer mechanisms without affecting its usability. Data is transferred or processed and provided to the Data Subjects in a structured, commonly used, and machine-readable format such as, but not limited to, "JSON".

Right to object: Where a Data Subject exercises their right to object to further processing of Personal Data, based on grounds relating to their particular situation, including profiling, Hilti will no longer process their Personal Data unless Hilti demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims. Data Subjects are informed of their right to object in the Hilti communications and can easily object at any time to processing of Personal Data for direct marketing purposes by accessing the Hilti Preference Center through the Hilti Online platform.

Outcome of automated decisions: Where Data Subject has requested an investigation with regards to an automated decision, Hilti will provide Data Subject with an explanation of the decision which has been made, and where applicable the possibility to discuss and contest the outcome of this decision with a responsible Hilti employee.

g. Liability

Hilti HQ bears the sole responsibility for actions of any non-EEA Hilti Entity, including payment of compensation to Data Subjects for any damage suffered resulting from a violation of this BCR by any non-EEA Hilti Entity and to agree to take the necessary actions to remedy the breaches of the herewith BCR.

Hilti HQ is committed to bear the burden of proof, meaning that Hilti HQ will be responsible for proving that either the non-EEA Hilti Entity is not responsible for the event giving rise to Data Subject complaints or that no violation occurred, should Hilti be willing to discharge itself from any responsibility.

10. COOPERATION WITH THE SUPERVISORY AUTHORITIES AND NATIONAL LAWS

a. Purpose and cooperation principle

Hilti has the duty to cooperate with the Supervisory Authorities to ensure proper exchange of information and Supervisory Authorities' shall undertake inspection of Hilti Entities where applicable.

Hilti shall abide by the data protection laws applicable and abide with the Supervisory Authorities' guidance, decisions and advice regarding the implementation and execution of the BCR. Hilti internally assesses the Supervisory Authorities' advice and the ability for Hilti to respond to such advice or recommendation based on local factors, internal resources, timeframes for progress to ensure Hilti effectively implements the Supervisory Authorities' measures.

Hilti accepts to be subject to Supervisory Authorities' inspections and audits with regards to the BCR implementation.

In the case where Hilti updates the BCR (where for example there are changes in the Entity list), Hilti shall notify all Hilti Entities as well as Supervisory Authority. New Hilti Entities added to the list must sign the Joint Agreement by which they undertake to comply with this BCR and continuously implement such measures accordingly.

b. Transparency where national legislation prevents Hilti from complying with BCR

Where a Hilti Entity must abide by national laws and respond to Personal Data disclosure requests from state security bodies or public authorities, it undertakes to report such requests to the Global Team as well as the CPO. Both the Global Team together with CPO inform the relevant Supervisory Authority with at least the information listed below.

Where a Hilti Entity is unable to provide such information and has to abide by criminal laws which prevent the Hilti Entity from disclosing Personal Data to security state bodies or public authorities based on confidentiality provisions (for example in the event of a law enforcement investigation), the Hilti Entity must use its best efforts to provide the Supervisory Authority with the relevant list of information or if despite such efforts the Hilti Entity is nonetheless unable to provide such efforts, undertake to keep an updated annual record listing all the DSR including the listed information. Such record must be annually provided to the relevant Supervisory Authority.

In addition, transfers of Personal Data by a Hilti Entity bound by the herewith BCR to any public authority cannot be excessive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Where a Hilti Entity bound by BCR considers that a national or local legislation might prevent it from enforcing the BCR or fulfilling its obligations under BCR, it will promptly alert Hilti HQ and CPO, except where such information is prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement inspection or investigation.

Hilti Entities undertake to communicate to the competent Supervisory Authority any legal obligation or requirement they are subject to in a third country which could lead to an adverse impact on the guarantees provided by BCR.

List of information to be provided: Hilti Entities or Hilti HQ together with CPO notify the competent Supervisory Authority where a legally binding request is made by a state security body or authority. The Hilti Entity informs the competent Supervisory Authority about at least:

- The nature and ground or legal basis for the request (except where such communication is otherwise prohibited under criminal law to uphold the confidentiality of a law enforcement investigation)
- Information regarding the categories of Personal Data Subject to disclosure
- Identity of the state security body or authority

If in specific cases the suspension and/or notification are prohibited by applicable criminal laws or state security bodies or authorities, the requested Hilti Entity will use its

best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so.

If despite using its best efforts a Hilti Entity or Hilti HQ is unable to notify the competent Supervisory Authority, it undertakes to at least annually provide the Supervisory Authority with information related to the requests received by the national security state bodies or authorities and at least the information listed above.

The transfers of Personal Data from a Hilti Entity to national security state bodies or authorities shall never be done in an excessive, disproportionate, and indiscriminate manner which would go beyond what is necessary in a democratic society.

c. Relationship between national laws and BCR

Hilti bound by the BCR implements very protective measures for the rights and freedoms of Data Subjects. The application of the highest data protection standards in all Hilti internal processes ensures that it develops its products and services in accordance with the principles set out in the BCR.

Nevertheless, and in accordance with the provisions of European data protection laws and regulations, there are situations in which national laws and regulations may be more protective than the principles set forth and applied in the Hilti BCR or provide specific requirements. Where such local legislation requires a higher level of protection for Personal Data than those set forth in the BCR, it will take precedence over the BCR. Where local legislation requires a lower level of protection for Personal Data, the BCR will take precedence.

Such protective or additional provisions are assessed with respect to the principles relating to the processing of Personal Data.

As a consequence, any Hilti Entity undertakes to comply with the applicable national or local provisions whenever these have additional and protective effects for Data Subjects or provide specific provisions applicable in the country. Each Hilti Entity is responsible for taking additional actions where deemed necessary in accordance with the national laws in which it is based. Such provisions include:

- Right for Data Subjects to decide on the fate of their Personal Data after death including exercising of rights by heirs or designated persons
- Processing of Personal Data in the field of employment, social security, or social protection law
- Application of Data Subject rights
- Conducting Data Protection Impact Assessments (DPIA) in accordance with specific local requirements
- Exercise DPO tasks in accordance with local requirements (e.g., secrecy obligation)

Hilti Entities communicate to and provide the Regional Data Protection Officer, the Global Team and CPO with a copy of such local or national laws and applicable requirements.

Where a Hilti Entity is taking actions, such as developing local processes or policies, it must provide the Global Team and CPO with a copy and details of such procedure or policy.

It has to be noted that such national laws do not override BCR and are to be considered to be additional requirements applicable in the country or state where the Hilti Entity is based. In the event such new provisions are applicable in one or several Hilti Entities, the latter must act and train the relevant employees to ensure that such provisions are implemented in existing processes or create new ones.

Furthermore, there are cases where Hilti needs to assess national requirements which may affect Personal Data transfers.

In such case, Hilti will conduct an assessment prior to any transfer of Personal Data to a third country.

This analysis is conducted by the exporting entity with assistance of the importing entity to determine the conditions and circumstances by which the transfer can take place, such as the categories of Personal Data transferred, categories of Data Subjects, type of processing activity, dataflow, evaluation of TOM's as well as legislations, statutes, court orders or mandatory standards applicable to such transfer of Personal Data and/or such importing entity.

Where the result of such assessment prevents the exporting entity from fulfilling its obligations under the herewith BCR, such exporting entity will either:

- Not start any transfer of Personal Data to the importing entity or
- For existing processing activities, discontinue any transfer of Personal Data or
- Implement supplementary measures in order to maintain the highest data protection standards as defined in the herewith BCR and in accordance with the latest EEA/ EDPB guidance

In the event no supplementary measures can be put in place, the exporting entity will either not start the processing activity or suspend any transfer of Personal Data.

The assessment can take the form of a DPIA with specific information relating to the supplementary measures. The documentation is made available to Supervisory Authorities upon request.

11. UPDATE OF BCR

Hilti has put in place the necessary measures to ensure a regular review and update of the BCR.

Hilti has appointed a CPO to manage the overall compliance with data protection laws and regulations.

The CPO is supported by the Global Team in charge of maintaining the BCR and ensuring they are amended when required in order to:

- reflect regulatory changes, modification of the Hilti group structure or any other applicable changes (e.g., administrative changes)
- maintain a fully updated list of Hilti Entities
- keep track of and record any updates to these BCR, and
- provide the necessary information to Data Subjects or the Supervisory Authorities

During the updating process, Hilti addresses all the legal and regulatory requirements at a national level with a detailed approach and develops a continuous plan to ensure consistency and effective watch over the BCR as shown hereafter:

Hilti HQ will ensure to inform all the Hilti Entities of any change in the BCR without undue delay.

In addition, Hilti HQ will inform the Lead Supervisory Authority at least once a year regarding any change in the BCR or in the list of Hilti Entities bound by BCR with a brief explanation for such amendment.

Where significant changes to the BCR are foreseen and could possibly affect the level of protection provided by the BCR or significantly affect the BCR, Hilti will promptly communicate to the Lead Supervisory Authority any changes.

Hilti HQ will update and make the updated BCR easily available to the Data Subjects.

Where the list of Hilti Entities is amended, Hilti will not transfer any Personal Data to a new Hilti Entity prior to the latter signing the Joint Agreement in order to be effectively bound by the BCR and until it has implemented the applicable compliance measures accordingly.

Hilti HQ keeps a record of the latest review dates and an explanation of changes undertaken.

12. APPENDIX 1 / DEFINITIONS

Binding Corporate Rules/Controller's Policy ("BCR"):
BCR (Binding Corporate Rules) are an EU mechanism to allow international transfers of Personal Data across Hilti Group worldwide Entities and organization. BCR are legally binding and approved by the EU data protection regulators. Hilti Entities sign the herewith BCR and Joint Agreement to comply with the same level of data protection and internal rules for processing Personal Data.

Chief Privacy Officer ("CPO"):
CPO means the Hilti Chief Privacy Officer. The CPO is responsible for reviewing and monitoring Hilti's data protection compliance and reporting to the highest level of management.

Controller:
Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Such Controller can be Hilti HQ, a Hilti Entity, or a Third Party.

Data Protection Officers ("DPO"):
DPO means privacy professionals specialized in legal and technical implementation of data protection matters. DPO's are part of the Hilti data protection network.

Data Processing Agreement ("DPA"):
A data processing agreement means a written agreement determining the obligations for both parties for the processing of Personal Data.

Data Protection Impact Assessment ("DPIA"):
A DPIA means a data protection impact assessment carried out to assess the likelihood, severity and risk arising from a processing activity, taking into account the nature, scope, context and purposes of the processing and the sources of the risk.

Data Subject:
Data Subject means identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

European Economic Area ("EEA"):
The EEA includes the EU countries as well as Iceland, Liechtenstein and Norway allowing them to be part of the EU's single market.

European Union ("EU"):
The EU is comprised of twenty-seven countries known as Member States which govern common political, economic, social and security policies. A list of the EU countries is available here.

General Data Protection Regulation ("GDPR"):
GDPR means REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data. GDPR is the main data protection EU regulation applicable in the EEA also addressing transfer of Personal Data. GDPR provides the herewith BCR as an adequate legal mechanism for Personal Data transfers.

Hilti Entity:
Hilti Entity means a Hilti Entity acting as Controller (including Hilti HQ as per the definition hereafter) or Processor bound by the herewith BCR by signing the joint agreement. The list of Hilti Entities is available by clicking here.

Hilti Group ("Hilti"):
Hilti means a group of undertakings comprised of a controlling undertaking and its controlled undertakings, whereby the controlling undertaking exerts a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have Personal Data protection rules implemented. An undertaking which controls the processing of Personal Data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings. Hilti means for the purpose of the herewith BCR Hilti Entities and Hilti HQ which are bound by BCR.

Hilti Headquarters ("Hilti HQ"):
Hilti HQ means Hilti Corporation, with its registered seat in Liechtenstein, exercising its statutory rights related to Hilti entities establishing data processing governance for Hilti entities. Hilti HQ is responsible for non-EEA Hilti entities and ensures for enforcing BCR through Hilti.

Human Resources Privacy Notice ("HR PRIVACY NOTICE"):
HR Privacy Notice means an internal Hilti document providing Hilti employees with specific details on the processing of Personal Data by Hilti, including with regards to sensitive information.

Joint Agreement:
The Joint Agreement means the undertaking entered by Hilti Group and a Hilti Entity by which the latter agrees to comply with the herewith BCR and its principles. The Joint Agreement defines the legally binding effects of the BCR and obligations for the parties.

Lead Supervisory Authority:
Lead Supervisory Authority means the independent public authority to be responsible for monitoring of the herewith BCR application for Hilti. Hilti liaises with the Lead Supervisory Authority to ensure reporting on a regular basis or as defined hereafter.

Personal Data:
Personal Data means any information relating to an identified or identifiable natural person (Data Subject).

Personal Data Breach ("DATA BREACH"):
Data Breach means 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.

Processing:
Processing of Personal Data means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor:
Processor means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller. Such Processor can be a Hilti Entity, Hilti HQ, or a Third-Party.

Supervisory Authority:
Supervisory Authority means an independent public authority which is established by an EEA Member State. Supervisory Authorities are responsible for monitoring the application of data protection laws and regulations, in order to protect the fundamental rights and freedoms of natural persons in relation to processing.

Technical And Organizational Measures ("TOMs"):
TOMs are internal measures and policies applicable to the processing of Personal Data by Hilti. TOMs consider the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing of Personal Data. TOMs are considered where Hilti develops, designs, selects, and uses Personal Data to fulfil their tasks, product, services, or applications with due regard to the state of the art.

Third-Party:
Third-Party means a natural or legal person, public authority, agency, or body other than the Data Subject, Controller, Processor, and persons who, under the direct authority of the Controller or Processor, are authorized to process Personal Data.

13. APPENDIX 2 – HILTI ENTITIES

The Hilti Entities bound to the present BCR are the ones necessary for Hilti to perform the data processing activities mentioned in Appendix 3, following the entity list and distinction provided for in Hilti financial reporting (available here). Also, as defined in section 11, the CPO is in charge of maintaining a fully updated list of such Hilti entities, which can be communicated upon request.

14. APPENDIX 3 – BINDING CORPORATE RULES MATERIAL SCOPE

This Appendix details the processing of Personal Data which takes place within Hilti:.

Purpose of the processing	Categories of Data Subjects	Categories of Personal Data	Third country destinations
• To provide, maintain, protect, and improve our services, websites, and apps, to develop new ones, and to protect Hilti and our customers. • Order and Logistics management • Tool management • Procurement activities	• Customers • Contact persons • Suppliers	• Contact Details • Payment Information • Marketing Information • Order Information • Authentication information	• Hilti maintains central data repositories exclusively within EU based systems or EU cloud solutions tenants for all customer data. Exceptions apply for Russian and Chinese data sets according to local laws • Access is granted on a need-to-know basis. The regional HUB`s can see their regional organizations data: Asia and Oceania, Central & South America and the Caribbean, Middle-East and Africa, North America, within the EU there are 5 regions accessing data for their markets only • Cross market access is limited to need-to-know basis and support roles and has different roles regarding visible attributes
• Talent pool management	• Candidates • Job applicants	• Contact details • Education, CV, and background data • Passport/ID information • Personal characteristics	• Hilti maintains central data repositories exclusively within EU based systems or EU cloud solutions tenants for all employee data • The talent pool can be accessed by all Hilti entities HR representatives. The visible information varies depending on the setting the candidates and employees chose for their profiles • Access for HR colleagues is granted based on a need-to-know basis and has different roles regarding visible attributes
• Human Resources Management	• Current and former Employees • Employee's dependents (e.g., partner, spouse, children) in the field of insurance, pension, social security benefits allowance and Employee mobility purposes	• Contact details • Passport or ID information • Sensitive information • Work, Education, CV, and background information • HR data • Dependent data (e.g., full name, date of birth, nationality)	• Hilti maintains central data repositories exclusively within EU based systems or EU cloud solutions tenants for all employee data • Access is granted on a need-to-know basis. The regional HUB`s can see their regional organizations data: Asia and Oceania, Central & South America and the Caribbean, Middle-East and Africa, North America, within the EU there are 5 regions accessing data for their markets only • Cross market access is limited to need-to-know basis and support roles and has different roles regarding visible attributes

The data flows from all market organizations to central data repositories exclusively hosted within EU based systems or EU cloud solutions tenants except for Russia and China. Service and maintenance access is limited to the extent possible to EU support, detailed information can be found in Hilti`s Privacy Policy and such on our country specific websites affecting local Data Subjects.

Customer data and data processed on behalf of customers can only be accessed from the respective markets and HUB`s, cross market access is limited to need-to-know basis and support roles and has different roles regarding visible attributes. Employee data is managed by employees and candidates based on individual settings on Data Subject side regarding their visibility within the organizations and cross market organizations. Beside that HR talent pools are visible to HR representatives and hiring managers on a need-to-know basis in HUB`s and globally. Hilti HQ access from EEA – Liechtenstein – follows the same logic for both customer and employee data.

A list of the HUB markets is visible on the website.