Data Processing Agreement

[PARTY 1]

and

BOMAG Americas, Inc

THIS AGREEMENT IS MADE ON THE _____ DAY OF _____ 202[*]

Parties

(1) **[FULL COMPANY NAME]** incorporated and registered in United States and/or Canada with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (the **Customer**); and

(2) **BOMAG Americas** incorporated and registered in United States and Canada with company number 34-1603223 whose registered office is at Corporation Trust Center, 1209 Orange Street, Wilimington Delaware 19801 (the **Provider**).

Background

(A) The Customer and the Provider entered into licence agreement relating to 'BOMAP Connect' (**Licence Agreement**) that may require the Provider to process Personal Data on behalf of the Customer.

(B) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing services under the Licence Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Business Purposes means the services described in the Licence Agreement or any other purpose specifically identified in Appendix A.

Controller means either: (a) the meaning set forth in the relevant Data Protection Legislation; or (b) absent such a definition, the party that determines the means and purpose of the Processing of Personal Data. "Controller" includes a "business" under the CCPA or CPRA.

Data Protection Legislation means any applicable international, foreign, national, federal, state, or local, statutes, ordinances, regulations, rules, executive orders, supervisory requirements, directives, circulars, opinions, judgments, interpretive letters, official releases, and other pronouncements having the effect of law relating to Personal Data or collection, use, storage, disclosure, transfer, or other Processing of Personal Data of or by any government, or any authority, department, or agency thereof, or self-regulatory organization, including, without limitation: (a) the EU General Data Protection Regulation 2016/679 and the implementing acts of the foregoing by a member state of the European Union, a member of the

European Economic Area and/or Switzerland (the "**GDPR**"); (b) all data protection laws and regulations applicable to the United Kingdom including the Data Protection Act 2018 and The Data Protection, Privacy and Electronic Communications (EU Exit) Regulations 2019 (the "**UK Data Protection Law**s"); (c) the CCPA; (d) the CPRA (when in effect); and (e) the Virginia CDPA (when in effect). Data Protection Legislation includes any of the foregoing as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder. Data Protection Legislation includes any of the foregoing as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

Data Subject means an individual who is the subject of Personal Data.

Personal Data means: (a) any information relating to an identified or identifiable natural person, or (b) any information that applicable Data Protection Legislation otherwise defines as "personal information" or "personal data" or other similar definition, that is processed by the Provider as a result of, or in connection with, the provision of the services under the Licence Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processing, processes and process means either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.

Processor means either: (a) the meaning set forth in the relevant Data Protection Legislation; or (b) absent such a definition, the party that Processes the Personal Data on behalf of the Controller. A "Processor" includes a "service provider" or a "contractor" under the CCPA or CPRA.

Sale means selling, renting, releasing, disclosing, disseminating, making available, transferring, or communicating by other means any Personal Data in exchange for monetary or other valuable consideration.

Standard Contractual Clauses (SCC) means the applicable module(s) of the European Commission's standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of

the European Parliament and of the Council, as set out in the Annex to Commission Implementing Decision (EU) 2021/914.

UK Data Protection Legislation means all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

1.2 This Agreement is subject to the terms of the Licence Agreement and is incorporated into the Licence Agreement. Interpretations and defined terms set forth in the Licence Agreement apply to the interpretation of this Agreement.

1.3 The Appendices form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Appendices.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

1.5.1 any provision contained in the body of this Agreement and any provision contained in the Appendices, the provision in the body of this Agreement will prevail;

1.5.2 the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Appendices, the provision contained in the Appendices will prevail;

1.5.3 any of the provisions of this Agreement and the provisions of the Licence Agreement, the provisions of this Agreement will prevail; and

1.5.4 any of the provisions of this Agreement and any executed SCC, the provisions of the executed SCC will prevail.

2. Personal Data types and processing purposes

2.1 The Customer and the Provider acknowledge that for the purpose of the Data Protection Legislation, the Customer is the Controller and the Provider is the Processor.

2.2 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

2.3 Appendix A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Provider may process to fulfil the Business Purposes of the Licence Agreement.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Legislation.

3.2 The Provider must promptly comply with any Customer request or instruction requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Provider to process or disclose Personal Data, the Provider must first inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.5 The Provider must promptly notify the Customer of any changes to Data Protection Legislation that may adversely affect the Provider's performance of the Licence Agreement.

3.6 The Provider shall not engage in the Sale of Personal Data.

4. Provider's employees

4.1 The Provider will ensure that all employees:

4.1.1 are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

4.1.2 have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

4.1.3 are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

5. Security

5.1 The Provider must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Appendix B.

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

5.2.1 the pseudonymisation and encryption of personal data;

5.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. Personal Data Breach

6.1 The Provider will promptly and without undue delay notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Provider will restore such Personal Data at its own expense.

6.2 The Provider will, without undue delay, notify the Customer if it becomes aware of:

6.2.1 any accidental, unauthorised or unlawful processing of the Personal Data; or

6.2.2 any Personal Data Breach.

6.3 Where the Provider becomes aware of any event described in 6.1 and/or 6.2 above, it shall, without undue delay, also provide the Customer with the following information:

6.3.1 description of the nature of 6.1 and/or 6.2, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

6.3.2 the likely consequences;

6.3.3 description of the measures taken or proposed to be taken to address 6.1 and/or 6.2, including measures to mitigate its possible adverse effects;

6.3.4 any other information required under applicable Data Protection Legislation.

6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Provider will reasonably co-operate with the Customer in the Customer's handling of the matter, including:

6.4.1 assisting with any investigation;

6.4.2 making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

6.4.3 taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.5 The Provider will not inform any third party of any Personal Data Breach without first obtaining the Customer's prior written consent, except when required to do so by law.

6.6 The Provider agrees that the Customer has the sole right to determine whether:

6.6.1 to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

6.6.2 to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.7 Each party will cover all of its own reasonable expenses associated with the performance of the obligations under this clause 6, provided, however, that to the extent a Personal Data Breach arises out of or results from Provider’s breach of its security obligations or negligence or more culpable acts or omissions, Provider shall reimburse Customer for all actual reasonable costs incurred by Customer in responding to, and mitigating damages caused by, any Personal Data Breach, including all costs of notice and/or remediation pursuant to Section described in clause 6.6.

7. Cross-border transfers of Personal Data

7.1 The Provider shall not process the Personal Data outside the countries in the European Economic Area (**EEA**), the United States of America (**USA**), or the country or countries in which the Customer is established without obtaining the Customer's prior written consent.

7.2 Where such consent is granted, the Provider may only process, or permit the processing, of Personal Data outside the EEA or the country or countries of the Customer's seat of business under the following conditions:

7.2.1 the Provider is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. The Provider must identify in Appendix A the territory that is subject to such an adequacy finding; or

7.2.2 the Provider participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Provider (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation (*(EU) 2016/679*). The Provider must identify in Appendix A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Provider must immediately inform the Customer of any change to that status;

7.2.3 The Customer notifies Provider that Customer has obtained valid Data Subject consent to the transfer, or Provider has obtained such consent on Customer's behalf, each to the extent necessary or permitted under the Data Protection Legislation; or

7.2.4 the transfer otherwise complies with the Data Protection Legislation for the reasons set out in Appendix A.

7.3 If any Personal Data transfer between the Customer and the Provider requires execution of SCC in order to comply with the Data Protection Legislation (where the Customer is the entity exporting Personal Data to the Provider outside the EEA or the country of the Customer's seat of business), the parties will complete all relevant details in, and execute, the SCC, and take all other actions required to legitimise the transfer, including, if necessary: (a) cooperating to register the SCC with any supervisory authority in any EEA country; (b) procuring approval from any such supervisory authority; or (c) providing additional information about the transfer to such supervisory authority.

7.4 If the Customer consents to appointment by the Provider located within the EEA or the country of the Customer's seat of business of a subcontractor located outside the EEA or the country of the Customer's seat of business in compliance with the provisions of clause 8, then the Customer authorises

the Provider to enter into SCC with the subcontractor in the Customer's name and on its behalf. The Provider will make the executed SCC available to the Customer on request.

8. Subcontractors

8.1 The Provider may only authorise a third party (subcontractor) to process the Personal Data if:

8.1.1 the Customer is provided with an opportunity to object to the appointment of each subcontractor within fourteen (14) days after the Provider supplies the Customer with details regarding such subcontractor;

8.1.2 the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of such contracts;

8.1.3 the Provider maintains control over all Personal Data it entrusts to the subcontractor; and

8.1.4 the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

8.2 Those subcontractors approved as at the commencement of this Agreement are as set out in Appendix A.

8.3 Where the subcontractor fails to fulfil its obligations under such written agreement, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.4 The Parties consider the Provider to control any Personal Data controlled by or in the possession of its subcontractors.

8.5 On the Customer's written request, the Provider will audit a subcontractor's compliance with its obligations regarding the Customer's Personal Data and provide the Customer with the audit results.

9. Complaints, data subject requests and third-party rights

9.1 The Provider must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

9.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase

Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

9.1.2 information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.

9.2 The Provider must notify the Customer without undue delay if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Provider must notify the Customer within ten (10) working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 The Provider will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this Agreement or as required by law.

10. Term and termination

10.1 This Agreement will remain in full force and effect so long as:

10.1.1 the Licence Agreement remains in effect; or

10.1.2 the Provider retains any Personal Data related to the Licence Agreement in its possession or control (**Term**).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Licence Agreement in order to protect Personal Data will remain in full force and effect.

10.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Licence Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within four weeks, they may terminate the Licence Agreement on written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer a copy of or access to all or part of the Customer's Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Licence Agreement for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any Personal Data related to this Agreement in its possession or control, except for one copy that it may retain and use for twelve (12) months for audit purposes only.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents or materials that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 The Provider will certify in writing that it has destroyed the Personal Data within five (5) working days after it completes the destruction.

12. Records

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Customer, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of Personal Data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5.1 (**Records**).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this Agreement and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Provider must review the information listed in the Appendices to this Agreement once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audits

13.1 The Provider shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

13.2 On request, during the Term and within two (2) years after the expiration or earlier termination of this Agreement, the Customer may at its own expense audit the Provider’s Records using an independent and accredited third-party firm that is reasonably acceptable to the Provider as necessary to verify the Provider’s compliance with this Agreement and Data Protection Legislation. The Customer may conduct any audit under this Section 13.2 at any time during the Provider’s regular business hours on business days at the Provider’s principal place of business or at its data processing facilities and shall not unreasonably interfere with the Provider’s course of business; provided, however, that Customer may not exercise its audit right under this

Section 13.2 more than one (1) time in any twelve (12) month period. The Customer shall keep all information obtained during any audit confidential and must impose confidentiality obligations on the third-party accounting firm that are no less restrictive than the confidentiality obligations in the Licence Agreement.

14. Warranties

14.1 The Provider warrants and represents that:

14.1.1 its employees, subcontractors, agents and any other person or persons accessing Personal Data on its behalf have received the required training on the Data Protection Legislation relating to the Personal Data;

14.1.2 it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

14.1.3 as of the effective date of this Agreement, it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Licence Agreement's contracted services; and

14.1.4 considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

(b) the nature of the Personal Data protected; and

(c) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

14.2 The Customer warrants and represents to Provider that:

14.2.1 It complies with all applicable Data Protection Legislation;

14.2.2 All processing instructions shall at all times comply with applicable Data Protection Legislation; and

14.2.3 the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Notice

15.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

15.2 For the Customer: [CUSTOMER DATA PRIVACY CONTACT]

15.3 For the Provider: BOMAG GmbH, Data Protection Officer, Hellerwald, 56154 Boppard, Germany

15.4 Clause 15.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16. Indemnification; Limitations of Liability

16.1 In addition to any indemnification obligations set forth in the License Agreement, each party (as the **Indemnifying Party**) shall defend, indemnify and hold harmless the other party (as the **Indemnified Party**), the other party's Affiliates, and their respective officers, directors, employees, agents, contractors, licensors, suppliers, successors, and assigns from and against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees (collectively, **Losses**) incurred by the Indemnified Party arising out of or relating to any claim, suit, action, or proceeding by a third-party (each, an **Action**) that does or is alleged to arise out of or result from breach of any representation, warranty, covenant or obligation of Indemnifying Party under this Agreement.

16.2 Except for liability for indemnification, (a) in no event shall either party be liable under this Agreement to the other party or any third-party for consequential, indirect, incidental, special, exemplary, punitive or enhanced damages, lost profits or revenues or diminution in value, arising out of, or relating to, and/or in connection with any breach of this Agreement, regardless of (i) whether such damages were foreseeable; (ii) whether or not it was advised of the possibility of such damages; and (iii) the legal or equitable theory (contract, tort or otherwise) upon which the claim is based; and (b) in no event shall either party's aggregate liability arising out of or related to this Agreement, whether arising out of or related to breach of contract, tort (including negligence) or otherwise, exceed the total of the amounts paid to Provider pursuant to the License Agreement in the twelve (12) month period preceding the event giving rise to the claim.

This Agreement has been entered into on the date stated at the beginning of it.

Signed by [NAME]

for and on behalf of [NAME OF CUSTOMER]

_____

Signed by [NAME]

for and on behalf of **BOMAG Americas**

_____

APPENDIX A: Personal Data Processing Purposes and Details

Subject matter of processing:

Data processing for the purpose and in the course of providing the services agreed to in the Licence Agreement.

Duration of Processing:

Entire term of the Licence Agreement.

Nature of Processing:

Under the Licence Agreement, the Provider processes the following types of customer Personal Data:

1. Authorised users of the BOMAP Connect portal (backend):

   - Right of use granted by the customer
   - User names = e-mail addresses and passwords
   - E-mail address
   - Time / scope of the creation of the user, time of the use of the interface for the transmission of the login data to the added user, time of the use of the activation link.
   - Log data incl. IP address,
   - User calls in the backend with time stamp, request, response and status code
   - Time of login to the portal, failed login attempts
   - Search terms of the user (location determination/display) in the integrated Google Maps function
   - Projects created/edited by the user with recorded detailed data, e.g. project no., customer, time of creation of the project, CAD data uploaded by the user
   - Point of Interests created by the user in BOMAP Connect
   - Settings for scales
   - Tags
   - selected language version

- Selected mode (Day / Dark)
- Granted permissions / own permissions
- News internal / external
- retrieved data / exports together with times
- Archiving a project together with the time
- Notifications of malfunctions of the portal to the contractor by the user (content, time)

2. App users:

- Device ID of the mobile device on which the app was installed, app version, name of the mobile device, version of the operating system
- Right of use granted by the customer
- App user account: Username = email addresses and passwords
- E-mail address
- Time / scope of the creation of the user, time of the use of the interface for the transmission of the login data to the added user, time of the use of the activation link.
- Log data incl. IP address,
- Time of transmission of the compaction values / measured values to the Connect portal
- Type of machine, manufacturer, machine ID, drum width
- current project
- Machine location data incl. times / real-time transmission, direction of travel
- Recording of the mechanically processed zones (areas, number and times of the passes at a location, start / stop of the measurement with recording of the compaction measured value at the respective position, temperature, speed, selected amplitude, frequency, split spreader active yes/no)
- Machines used (with serial number, if applicable)
- Creation / display of points of interest

- Version Joblink interface of the machine

- Version of the machine software used

Business Purposes:

In order for the customer to be able to use the BOMAG Connect functionalities offered (software as a service), it is necessary to process the data recorded by the customer with the BOMAP app, cf. in this regard under I 2 above, in particular its storage and making accessible to the customer, as well as the data recorded in the portal (authorised users created, user actions), cf. in this regard under I 1 above. The Provider may require access to this data in order to check and rectify faults in BOMAG Connect and to support the customer in certain actions, e.g. setting up users in the portal, creating projects.

Data Subject Types:

Employees of the customer

Employees of third companies whose employer has formed a consortium (working group) with the customer on the occasion of a specific project / tender.

Personal Data Categories (& related risk assessment):

The parties have examined the risks of the data subjects affected by the processing of the principal's data and have come to the following conclusion:

Due to the aspects explained below, it is not necessary to take additional technical and organisational protective measures beyond the average level.

The need for protection of the processed data of the data subjects is to be classified as low - medium. A possible misuse would have no or no significant impact on the data subjects.

The species concerned were the following groups, classified as follows:

Data type	**Risk**	**Justification**
User name	Low	These do not have to/should not contain clear names, but rather information such as "User001" etc. It is then not possible to assign the usernames to a person concerned.
Contact details of the portal users	Low - medium	By providing contact details, it may be possible to identify a user; this depends on the contact details provided (telephone extension or central call number/type of e-mail address provided, etc.); the contact details are almost exclusively professional/business contact details, some of which are publicly accessible, e.g. trade register, customer websites; any

		risk in the event of loss/disclosure of this data is therefore only of minor significance for the data subjects.
Portal user usage data (log data, time of login, etc.)	Low - medium	From this, it may be possible to analyse from which location (IP address) and at what times which person has used the portal, if the user is identifiable; since the use of the portal is also almost exclusively professional/business, only the professional/business sphere of the person concerned would be affected if there were a data protection breach.
Projects, exports	Low - medium	The pure project data contains the name of the customer's customer and participating companies (consortiums); this is usually not Personal Data; moreover, this is business data and its need for protection is therefore low under data protection law. Insofar as the project data contains individual details that can be traced back to the machine operators, this would be Personal Data (employee data). Since this data is work related/occupationally related, there are also no significant risks for the persons concerned (reputational risk/consequential damage due to unauthorised use of this data or similar). Data concerning the time and type of export of the projects (recipients) also almost exclusively concern persons (senders/recipients) who are active in their professional/business environment. In the event of a breach of protection, no major personal risks are apparent in this respect.
News	Low - medium	Any message content exchanged via the portal or between portal user and user concerns the use of the portal/the project(s) in question. These are almost exclusively business transactions; no major risks for the persons involved are apparent.
App user (mobile device ID, device data)	Low - medium	The app is used almost exclusively for business/professional purposes. These are the mobile end devices provided to the user by the customer. It is possible that an identifiable user name is assigned to the app user. This would make it possible to determine when the user opens/closes the app and initiates processes via it. The risks for the data subjects in the event of a data breach are likely to be low.

App users, location data, summarisation data	Low - medium	The app records the current location of the mobile end device and thus also of the operator (app user), who is also usually the machine operator, by means of the GPS/location recording released by the app user. In addition, with regard to the activated project in which the compaction data (machine data) is recorded, the operating number or similar assigned to the machine is also recorded. From this, when the app user is identified (if he is in the machine), it is clear when the app user was where. There is no significant risk to the freedoms / rights of the data subject, as the data relates to the app user's professional activity.

Approved Subcontractors:

Other processors of the Provider are:

Company, address	Type of processing	Purpose	Type of data	Categories of data subjects
Telekom Germany GmbH	Hosting, Cloud Service	Storage of customer data, making the software accessible	See Appendix B	See above
BOMAG GmbH	Access to user data on the occasion of the provision of services	Setting up of the services for the Customer, provision of support services, monitoring	See Appendix B	See above
Fayat Bomag GmbH & Co. Unternehmensführungs KG	Access to user data on the occasion of the provision of services	Services for the provision of data processing infrastructure	See Appendix B	See above

m2Xpert GmbH & Co KG Alfred-Bozi Strasse 21/22 33602 Bielefeld	Access to user data on the occasion of the provision of services	Software services, support	See Appendix B	See above

APPENDIX B- Security Measures

1. Explanation

The Provider offers the "BOMAP Connect" service and must comply with the requirements of Article 32 of the GDPR.

Appropriate technical and organisational measures shall be taken to ensure a level of protection appropriate to the risk, taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons.

The risk identified for the persons affected by the data processing was assessed as low - medium in accordance with Appendix A.

The technical and organisational measures are to be aligned with this.

The following concept presents in detail the selection of technical and organisational measures suitable for the identified risk, taking into account the protection goals according to the state of the art and with special consideration of the IT systems and processing procedures used.

The BOMAP Connect web application and the user and content data are provided and processed for the Provider by BOMAG GmbH using the cloud service of Telekom Deutschland GmbH, Bonn, Germany. In addition, BOMAG GmbH is supported in the operation of BOMAP Connect by the IT service providers named in Appendix A.

The following description of the technical and organisational measures is therefore based on the aforementioned structure.

2. Organisational and possible technical measures

Organisational measures to ensure the special requirements of data protection include, in particular, measures such as the appointment of a data protection officer, service instructions or company agreements, training, obligations, documentation, specifications for the implementation of technical and other measures, the establishment of an authorisation system, review of access control, etc. This also includes the design of internal organisation in such a way that it meets the special requirements of data protection. This also includes the design of the internal organisation in such a way that it meets the special requirements of data protection. To ensure this, BOMAG GmbH has procedures in place to regularly review, assess and evaluate the effectiveness of the technical and organisational measures.

Ultimately, organisational and technical measures cannot always be separated from each other. Therefore, the following description of the implemented measures is based on the protection goals of Article 32 (1) of the GDPR as well as on the different IT systems or acting companies.

A. Cloud service of Telekom Deutschland GmbH

1. Description

Telekom Deutschland GmbH provides BOMAG GmbH with the server infrastructure for BOMAP Connect in the form of virtual servers with an operating system. Furthermore, Telekom Deutschland GmbH provides an internet connection, a firewall and a backup system. Therefore, Telekom Deutschland GmbH also has access to the cloud and the Personal Data processed there as well as any additional information provided by the customer within the scope of support.

The cloud service is provided in the form of "IaaS" (Infrastructure as a Service) by Telekom Deutschland GmbH in Germany and Hungary. Telekom Deutschland GmbH is certified/audited according to the following standards:

https://open-telekom-cloud.com/de/sicherheit/datenschutz-compliance

2. Measures

The following technical and organisational security measures, among others, have been agreed with Telekom Deutschland GmbH, compare, among others, the Annex to the Supplementary Terms and Conditions for Commissioned Data Processing of Personal Data for Open Telekom Cloud:

a) Confidentiality (Art. 32)

- Access control

  No unauthorised access to data processing systems, e.g.: Magnetic or chip cards, keys, electric door openers, factory security or gatekeepers, alarm systems, video systems;

- Access control

  No unauthorised system use, e.g.: (secure) passwords, automatic locking mechanisms, two factor authentication, encryption of data media;

- Access control

  No unauthorised reading, copying, modification or removal within the system, e.g.: Authorisation concepts and needs-based access rights, logging of accesses;

- Separation control

- Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing;

b) Integrity (Art. 32)

- Transfer control

  No unauthorised reading, copying, modification or removal during electronic transmission or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature,

- Input control

  Determining whether and by whom Personal Data have been entered into, changed or removed from data processing systems, e.g.: Logging, document management;

c) Availability and resilience (Art. 32)

- Availability control

Protection against accidental or deliberate destruction or loss, e.g.: Backup strategy (online/offline, on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans;

- Rapid recoverability (Art. 32 (12) (c) GDPR)

d) Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

- Data protection management;

- Incident response management;

- Data protection-friendly default settings (Art. 25 (2) GDPR);

- Order control

No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the customer, e.g.: Clear contract design, formalised order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.

Details of sub-processors / services / processing locations:

Separate authorisation: Telekom intends to use the following sub-processors for the following services / at the following processing locations:

- T-Systems International GmbH

  60528 Frankfurt am Main, Hahnstraße 43 d

  Services: Cloud provider

Processing location: Germany, Netherlands

- Deutsche Telekom Regional Solutions & Products GmbH

  53113 Bonn, Friedrich-Ebert-Allee 71-77

  Services: 1st & 1.5 Level Support

  Processing location: Germany

- IT Services Hungary

  H-1097 Budapest, Toth Kalman u 2/B

  Services: Operation, 1st and 2nd Level Support

  Processing location: Hungary

- Deutsche Telekom IT GmbH

  53227 Bonn, Landgrabenweg 151

  Service: MyWorkplace

  Processing location: Germany

- STRATO AG

  10587 Berlin, Pascalstraße 10

  Services: Service Desk

  Processing location: Germany

- Axivas Germany GmbH

  68723 Schwetzingen, Carl-Benz-Straße 9-11

  Services: Service Desk

  Processing location: Germany, Netherlands

- Deutsche Telekom Individual Solutions & Products GmbH

  53113 Bonn, Friedrich-Ebert-Allee 70

  Services: Hardware maintenance and installation

Processing location: Germany, Netherlands

- GULP Solutions Services GmbH & Co.KG

  50667 Cologne, Breite Straße 137-139

  Service: Service desk

  Processing location: Germany, Magdeburg

  Used by Deutsche Telekom Individual Solutions & Products GmbH

- I.T.E.N.O.S. International Telecom Network Operation Services GmbH

  53119 Bonn, Lievelingsweg 125

  Service: Hardware maintenance and installation

  Processing location: Germany, Bonn

  Used by: Deutsche Telekom Individual Solutions & Products GmbH

B. BOMAG GmbH and FAYAT BOMAG GmbH & Co. Unternehmensführungs KG

1. Description of the services provided by BOMAG GmbH and FAYAT BOMAG GmbH & Co. Unternehmensführungs KG

BOMAG GmbH is a company affiliated with the Provider and supports the Provider in the provision to the Customer of the services required to fulfil the respective customer contract, in particular by establishing access to the cloud (setting up the service for the customer, providing support services for the customer, monitoring).

FAYAT BOMAG GmbH & Co. Unternehmensführungs KG is an affiliated company of BOMAG GmbH and provides services to BOMAG GmbH in connection with the provision of the data processing infrastructure used for the execution of the BOMAP Connect customer contracts.

Here, employees of both companies can see the data of the portal users as well as the project data stored by the customer and the information transmitted via app.

Access is via secure web access (https and user authentication, administrative SSH access).

The following IT systems, among others, are used for this purpose:

- Mobile devices

- Non-mobile devices

- Firewalls

- LAN/WAN/WLAN (encrypted) Infrastructure

- VPN

2. Measures

BOMAG GmbH and FAYAT BOMAG GmbH & Co. Unternehmensführungs KG use the following technical and organisational security measures, among others:

a) Confidentiality (Art. 32)

- Access control

    - The contractor's building is protected by security measures against unauthorised entry.

    - the premises can only be entered outside business hours via an access control system (ZKS) or locking system.

    - Access to the office spaces is controlled by the ZKS at all times. The doors are equipped with motor locks and are kept locked at all times.

    - individual offices and server rooms are only accessible via the ZKS.

    - In addition to the ZKS, the building floor doors are equipped with a cylinder locking system.

    - The ZKS contains an automatic access logging system limited in number.

    - Access to the server rooms is only possible for authorised persons.

    - Role-based access authorisation (ZKS) according to access concept (documentation of access rights)

    - Visitors/third parties must register at reception and will be accompanied by staff.

    - Authorised third parties have access to the server rooms only when accompanied by IT staff.

    - The building and office space entrances are video-monitored.

- Access control

    - Access to the Contractor's IT systems is protected by passwords.

- There is only password-protected access at both operating system and application level (applications with Personal Data).

- Passwords comply with an internal password policy in line with the current state of security.

- Access to IT systems is automatically blocked if the wrong password is entered several times.

- Access is enabled either only for the employee entrusted with processing the data or for a group created according to a role concept.

- The network structure is divided into several network segments for the different tasks (WAN, LAN, DMZ) via a hardware firewall.

- External access to BOMAG's internal network or to the operating system level of the hosted systems at a subcontractor (in the case of a hosting contract) is only possible via an encrypted VPN connection.

- Up-to-date virus protection is installed on all clients.

- The data carriers of the notebooks are completely encrypted.

- Access control

  - Individual access rights are set centrally using a documented role concept.

  - The data carriers of the notebooks are completely encrypted.

- User control

  - An identity and access management system is used.

  - For non-AD systems, application authentication is used.

  - There is a password policy that is binding for all employees and corresponds to the current state of security.

  - If technically feasible, the complexity requirements for the password are stored in the applications (e.g. Active Directory).

  - If the number of possible failed attempts is exceeded, the user account is blocked for a specified time or permanently.

  - If technically possible, there is a requirement to change the password periodically.

  - Each employee has a personal password known only to him or her.

- Data carrier control

    - Data carriers are securely deleted before they are used for any other purpose on the basis of a data deletion concept.

    - Disposal of electronic data carriers with data only to certified disposal companies (subcontractors) with reference to the necessary security level for destruction.

- Transmission control

    - If required, the Contractor shall provide FTP access with optional encryption for the Client.

- Transport control

    - Web access to systems containing Personal Data is encrypted.

- Separation control

    - Production and test systems are separated.

- Pseudonymisation and encryption (Art. 32 para; Art. 25)

    - All login data from our own online portals are transmitted in encrypted form (webshop, partner & support portal, ...).

    - Data carriers in notebooks are encrypted.

b) Integrity (Art. 32)

- Transfer control

    - The procedures for the transmission of Personal Data are documented in the procedural descriptions.

    - Visitors do not have access to the company LAN/WLAN.

- Input control

    - There are differentiated permissions that allow only authorised users/user groups to save a data set.

- Data integrity

    - The ERP software is only used via protocols defined by the manufacturer.

- Regular restoration of random samples from backup copies is carried out and logged.

c) Availability and resilience (Art. 32)

- Availability control
  - All systems required for data processing are monitored. In the event of an error, the IT staff is notified.
  - Up-to-date virus protection is installed on all clients.
  - Security-relevant updates are installed regularly and promptly.
  - For hosting contracts: Server systems of the subcontractor "Telekom AG".
  - To protect against accidental destruction or loss, the subcontractor shall perform a daily data backup of the entire server system to a physically separate backup infrastructure.
- Reliability
  - Active service contracts are in place for all important hardware and software systems with response times appropriate to the system task.
- Recoverability (Art. 32)
  - The systems are backed up using a defined data backup concept.
  - Backing up entire virtual machines ensures faster recovery.

d) Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

- A data protection officer exists.
- Regular data protection training is provided for all employees.
- Order control
- Subcontractors have been carefully selected and agreements have been concluded with them in accordance with Art. 28.

C. m2Xpert GmbH & Co KG

1. Description of the services of m2Xpert GmbH & Co KG

The company m2Xpert GmbH & Co KG, Bielefeld, Germany, assists BOMAG GmbH with support, troubleshooting and further development of BOMAP Connect. m2Xpert carries out service work on the software it has developed, which is operated by BOMAG. For this purpose, m2Xpert accesses internal databases and log data of the system in case of errors. m2Xpert also imports new software versions into the system. m2Xpert has no direct contact with customers.

Access is via secure web access (https) and administrative SSH access.

The following IT systems, among others, are used for this purpose:

- Mobile devices

- Non-mobile devices

- Firewalls

- LAN/WAN infrastructure

2. Measures

The following technical and organisational security measures, among others, have been agreed with m2Xpert GmbH & Co KG; compare, among other things, the annex to the commissioned processing of Personal Data for BOMAP Connect:

a) Confidentiality (Art. 3)

- Access control

No unauthorised access to data processing systems, e.g.: Keys, alarm systems, video systems;

- Access control

No unauthorised system use, e.g.: (secure) passwords;

- Access control

No unauthorised reading, copying, modification or removal within the system, e.g.: Authorisation concepts and needs-based access rights;

b) Integrity (Art. 32 para. 1)

- Transfer control

No unauthorised reading, copying, modification or removal during electronic transmission or transport, e.g.: Encryption, Virtual Private Networks (VPN);