MDP PRIVACY AND SECURITY TERMS AND CONDITIONS

Version 2025-1

Article 1. Introduction

These MDP Privacy and Security Terms outlines the specific obligations and responsibilities of the Parties with regard to the protection of personal data, security and Customer's digital operational resilience in relation to the provision and use of any products and services under the Agreement. The purpose of these MDP Privacy and Security Terms is to ensure that the agreed obligations and responsibilities are in line with the applicable regulatory requirements including the GDPR, DORA and the NIS2 Directive (where applicable). These MDP Privacy and Security Terms are an addition to and an integral part of the Agreement, the terms of which fully apply, except where these MDP Privacy and Security Terms explicitly deviate.

Article 2. Definitions

The meaning of the definitions used in these MDP Privacy and Security Terms shall be equal to the meaning given to them in the Market Data Platform Terms and Conditions. Additional definitions, used in these MDP Privacy and Security Terms, shall have the following meaning:

Controller	means controller as defined in Article 4 of the GDPR.
Customer Personal Data	means the Personal Data, received by BIQH from Customer, Customer's Affiliates and other parties authorized by Customer to use the MDP Services.
Data Processing	means any Processing, performed in the performance of the Agreement.
Data Subject	means a data subject as defined in Article 4 of the GDPR.
DORA	means Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector.
Exit Plan	means an exit plan as described in section 19.3 of the MDP Terms and Conditions.
Incident Reporting Policy	means BIQH's policy on Incident reporting obligations, available in the Documentation.
ISMS	means Information Security Management System.

ISO27001	means the standard for information security management systems (ISMS), issued by the International Organization for Standardization.
MDP Privacy and Security Terms	means this document 'MDP Privacy and Security Terms and Conditions.
MDP Privacy Statement	means the statement, containing information as set forth in article 13 and 14 of the GDPR, available at https://www.biqh.com/privacy-statement, or any updated version thereof.
NIS2 Directive	means Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Customer Personal Data.
Processes, Processing	means to process or the processing of Personal Data as defined in Article 4 of the GDPR.
Processor	means a natural or legal person, public authority, agency or other body which Processes personal data on behalf of the Controller.
SCC's	means the Standard Contractual Clauses, adopted by the European Commission on 4 June 2021.
Service Level Agreement or SLA	means the document 'MDP Service Level Agreement', or any updated version thereof.
Subcontracting Arrangement	means an arrangement made with a Subcontractor on Critical Services subcontracted.
Sub Processor	means a subcontractor, engaged by BIQH to carry out, on BIQH's behalf, specific processing activities in relation to the Data Processing.

Article 3. Personal Data protection

3.1 Roles

In the performance of the Agreement, BIQH may act in the capacity of Controller or Processor, depending on whether BIQH or Customer determines the purpose and means of a specific Data Processing activity. Customer, Customer Affiliates and other parties, authorized by Customer to use the MDP Services may qualify as Controller under the Agreement. Customer accepts liability for the

performance of any Controller obligations under the Agreement, for itself and any such other (joint) Controllers. Customer warrants that it is authorized to accept such liability on behalf of such other (joint) Controller.

3.2 Personal Data transfer

The Parties shall, where the Agreement entails the transfer of Personal Data to a third country or to an international organization, comply with the obligations in Chapter V of the GDPR. Where the transfer cannot be based on the legal basis stated in Article 45 or Article 46, subsections 2, (a) or (b) the Parties agree that the legal basis of the transfer will be the SCC's. The Parties will consult with each other whether the SCC's apply, which version applies to which Processing activity ('Controller-Controller' or 'Controller-Processor') and perform the obligations under the SCC's, that shall apply to the Processing in addition to the obligations under these MDP Privacy and Security Terms.

3.3 Controller obligations

With regard to the Data Processing each Party commits to, in its capacity as a Controller, comply with the obligations arising from the GDPR, GDPR implementation laws and other privacy laws applying to it. Where BIQH acts, in its performance of the Agreement, as Controller, information on the Data Processing is provided by BIQH in the MDP Privacy Statement.

3.4 Details of the Data Processing

Where BIQH acts, in the performance of the Agreement, as a Processor, the Parties will determine the details of the Data Processing and document such details in the MDP Order Form or another Written document. Such details will include, without limitation: the subject-matter and duration of the Data Processing, the nature and purpose of the Data Processing, the type of Customer Personal Data and categories of Data Subjects.

3.5 Processor Obligations

The following provisions apply to the Data Processing, performed by BIQH in its capacity as a Processor:

(a) BIQH shall process the Customer Personal Data only on documented instructions from Expert Users, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which BIQH is subject; in such a case, BIQH shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) BIQH ensures that persons, authorised to process the Customer Personal Data are subject to obligations of confidentiality as set forth in section 5.2 of the MDP Terms and Conditions;

(c) BIQH shall take all measures required pursuant to Article 32 of the GDPR, as specified under Article 4 of these MDP Privacy and Security Terms;

(d) BIQH shall carefully select Sub-Processors, enter into an agreement within the meaning of Article 28/2 of the GDPR with Sub-Processors, list any Sub-Processors that it has

engaged and locations of storage in the SLA or Customer Appendix, notify Customer in advance of any intended changes to such Sub-Processors, to which change the Customer can object;

(e) assist Customer with the fulfilment of its obligation to respond to requests for exercising Customer Data Subject's rights laid down in Chapter III of the GDPR;

(f) assist Customer, with ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR;

(g) assist Customer, with executing a Data Protection Impact Assessment within the meaning of Article 35 of the GDPR;

(h) assist Customer, with answering any requests in relation to an investigation by a data protection supervisory authority and cooperate, in accordance with Article 16 of the MDP Terms and Conditions, with any audit, performed by Customer to investigate compliance with these MDP Privacy and Security Terms;

(i) at the choice of Customer, delete or return all the Customer Personal Data to Customer after the end of the Agreement, and delete existing copies unless Union or Member State law requires storage of the Customer Personal Data;

(j) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this section 3.5, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

3.6 Customer obligations

Customer shall authorize an Expert User to give instructions as referred to under section 3.5 (a) of these MDP Privacy and Security Terms. Customer will refrain from giving any instructions that do not comply with the GDPR, GDPR implementation laws or any other data protection laws applicable to it. BIQH may rely on the instructions, given by the Customer and will not be liable for following up on any non-complying instructions. Customer agrees that where BIQH provides assistance as set forth under section 3.5 under (e), (f), (g) and (h), such assistance will be provided as Professional Services and Customer will compensate BIQH for such assistance by payment of the related Professional Services Fee.

Article 4. Security

4.1 Security general

BIQH has implemented an ISMS that is ISO27001 and SOCII Type 1 certified. Further, BIQH has implemented organizational and technical security measures to manage the risks posed to the security of the MDP and to prevent or minimize the impact of Incidents on recipients of its services. As part of the Plan-Do-Check-Act cycle of the ISMS, the security measures are continuously evaluated and, if necessary, amended. The categories of measures are listed under section 4.2. Further explanation on the security measures listed is provided in the Documentation and any specific information will be provided to an Expert User by the MDP Support Desk, at its request.

4.2 Technical and organizational security measures

The measures referred to under section 4.1 include, without limitation, measures in the following categories:

(a) policies on risk analysis and information system security;
(b) incident handling;
(c) business continuity, such as backup management and disaster recovery, and crisis management;
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure, threat-led penetration testing (TLPT) (for which the process is available in the Documentation);
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
(g) cyber hygiene practices and cybersecurity training;
(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
(i) human resources security, access control policies and asset management;
(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

4.3 Incident reporting

If an Incident occurs, BIQH and/or Customer may be subject to security breach reporting obligations under applicable laws and regulations, such as the NIS2 Directive implementation law, DORA and (in the event of a breach with regard to Customer Personal Data) the GDPR. BIQH has implemented procedures to ensure that Incidents are correctly classified and, depending on their classification, reported, by BIQH or Customer (as applicable) in accordance with the requirements ensuing from the applicable laws and regulations. The procedures are available in the Documentation.

Article 5. DORA Compliance

5.1 Contractual arrangements under section 30/2 DORA

The below obligations of BIQH apply if Customer is a financial entity within the meaning of Article 2(2) of DORA and reflect the applicability, to the Agreement, of section 30/2 of DORA:

(a) the MDP is described in the Documentation, the Implementation Plan and (if applicable) MDP Order Forms, the MDP Services and Managed Services are described in the SLA, respectively the Customer Appendix;
(b) the locations where the contracted or subcontracted components of the MDP Services and Managed Services are provided and where data is processed, including the storage location, and the process to notify the Customer in advance if BIQH envisages changing

such locations are stated in the SLA, MDP Order Form or Customer Appendix (as applicable);

(c) provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data are set forth under section 4 of these MDP Privacy and Security Terms and further elaborated in the Documentation;

(d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by Customer in the event of the insolvency, resolution or discontinuation of the business operations of BIQH or in the event of the termination of the contractual arrangements are set forth in section 19.6 of the MDP Service Terms and Conditions and will be further set forth in the Exit Plan;

(e) service level descriptions regarding the MDP Services, including updates and revisions thereof are set forth in the SLA;

(f) if an Incident occurs, BIQH shall provide Incident Management as part of the MDP Service and in accordance with the SLA. Such service will be provided at no additional cost, except where the Incident is caused by Customer. If the Incident is caused by Customer, BIQH shall provide the assistance as Professional Services, against reasonable Professional Services Fees at the rates set forth in the MDP Order Form;

(g) BIQH shall fully cooperate with the competent authorities and the competent resolution authorities (as defined under Dutch law in the 'Wet herstel en afwikkeling van banken en beleggingsondernemingen', which implements the Bank Recovery and Resolution Directive (Directive 2014/59/EU) or any update or replacement thereof), including persons appointed by them;

(h) termination rights and related minimum notice periods for the termination of the Agreement are set forth in Articles 18 and 19 of the MDP Service Terms and Conditions, subject to any guidelines or orders of competent authorities and resolution authorities;

(i) BIQH offers, as Professional Services, participation in Customer's security awareness programs and digital operational resilience training in accordance with Article 13(6) of DORA.

5.2 Contractual arrangements under section 30/3 DORA

The below obligations of BIQH apply if the Customer is a financial entity within the meaning of Article 2(2) of DORA and to the extent the MDP Services or Managed Services qualify as Critical Services and reflect the additional applicability to the Agreement of section 30/2 of DORA.

(a) service level descriptions for the Critical Services, including updates and revisions thereof, with quantitative and qualitative performance targets within the agreed service levels, to allow monitoring by Customer of the Critical Service, and corrective actions to be taken by BIQH when agreed service levels are not met are set forth in the SLA and Customer Appendix;

(b) notice periods and reporting obligations of BIQH to Customer, including notification of any development that might have a material impact on BIQH's ability to effectively provide the Critical Services in line with agreed service levels are set forth in the SLA and Customer Appendix;

(c) BIQH has implemented and tests a business contingency plan and ICT security measures, tools and policies as set forth in Article 4 of these MDP Privacy and Security Terms and further elaborated in the Documentation;
(d) BIQH shall participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27 of DORA;
(e) Customer's right to monitor, on an ongoing basis, BIQH's performance is set forth in Article 16 of the MDP Terms and Conditions;
(f) exit strategies, in particular the establishment of a mandatory adequate transition period are set forth in sections 19.3 up to and including 19.6 of the MDP Terms and Conditions and in the Exit Plan.

5.3 Subcontracting

With regard to any Subcontractor that BIQH contracts to perform Critical Services or material parts thereof, this section 5.3 up to and including section 5.6 apply.

(a) BIQH shall provide to Customer all relevant information with regard to the subcontractor that Customer requests, to enable Customer to assess the operational and financial abilities of the potential Subcontractor to provide the services;
(b) BIQH shall identify, notify and inform the Customer of any Subcontractors in the chain of subcontracting (providing ICT services supporting Critical Services or material parts thereof), provide all relevant information that may be necessary for the assessment referred to under (a) and shall ensure that the identification of the chain remains up-to-date over time in order to allow for the Customer to discharge its obligation to maintain and update the register of information in accordance with Article 28(3) and (9) of DORA;
(c) BIQH ensures that the contractual arrangements with the Subcontractors allow the Customer to comply with its own obligations stemming from DORA and all other applicable legal and regulatory requirements, and grant Customer and competent and resolution authorities the same contractual rights of access, inspection and audit along the chain of Subcontractors as those granted to Customer;
(d) BIQH has established adequate abilities, expertise, financial, human and technical resources and applies appropriate information security standards, and has an appropriate organisational structure, including risk management and internal controls, incidents reporting and responses, to monitor its subcontractors;
(e) BIQH shall monitor all subcontracted Critical Services to ensure that its contractual obligations with the Customer are continuously met and periodically report to Customer on the subcontracted Critical Services;
(f) BIQH has assessed, and shall assess with regard to any new Subcontractor, all risks associated with the location of the current or potential Subcontractors, and their parent companies and the location where the service is provided from;
(g) the location of data processed or stored by the Subcontractor is, where relevant, specified in the MDP Order Form or Customer Appendix;
(i) BIQH shall ensure the continuity of the services throughout the chain of Subcontractors in case of failure by a Subcontractor to meet its contractual obligations, and its

contractual agreement with the Subcontractor includes the requirements on business contingency plans as set out under section 5.2 (c) of these MDP Privacy and Security Terms, and defines the service levels to be met by the Subcontractors in relation to these plans;

(j) BIQH shall specify, in its written contractual agreement with the Subcontractor, the ICT security standards and any additional security requirements, where relevant, that shall be met by the Subcontractors in line with section 5.2 (c) of these MDP Privacy and Security Terms;

(k) BIQH shall specify, in its written contractual agreement with the Subcontractor, that the Subcontractor is required to grant, to the Customer and relevant competent and resolution authorities, the same monitoring rights as granted to the Customer and relevant competent and resolution authorities by BIQH as set forth in Article 16 of the MDP Terms and Conditions, and collaborate with the Customer to enable the Customer to assess whether and how the potentially long or complex chain of Subcontractors Critical Services or material parts thereof may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect;

(m) BIQH shall allow the Customer to obtain information on contractual documentation between BIQH and its Subcontractors and on relevant performance indicators, considering the monitoring rights as set forth in Article 16 of the MDP Terms and Conditions.

5.4 **Changes to Subcontracting Arrangements**

BIQH shall notify Customer of material changes to Subcontracting Arrangements, observing a notice period sufficient for the Customer to assess the impact on the risks it is or might be exposed to, as well as whether such changes might affect the ability of BIQH to meet its obligations under section 5.3. BIQH shall implement the material changes only after the Customer has either explicitly approved or not objected to the changes by the end of the notice period.

5.5 **Objection to changes to Subcontracting Arrangements**

If the Customer objects to the changes referred to under 5.4 it shall, before the end of the notice period:

(a) inform BIQH of its risk assessment results as referred to in section 5.4; and,

(b) object to the changes and request modifications to the proposed subcontracting changes before their implementation.

5.6 **Right to terminate**

Without prejudice to the rights of Customer set forth in section 18.2 of the MDP Terms and Conditions, the Customer has a right to terminate the Agreement in each of the following cases:

(a) when BIQH implements material changes to Subcontracting Arrangements, despite the objection and request for modifications to the changes by Customer as referred to in section 5.5;
(b) when BIQH implements material changes to Subcontracting Arrangements before the end of the notice period without explicit approval by the financial entity, as referred to in section 5.4;
(c) when BIQH subcontracts a Critical Service not explicitly permitted to be subcontracted by the Agreement.