Crownpeak DORA Addendum

Preamble:

This DORA Addendum is between the Crownpeak legal entity ("Crownpeak") and the customer legal entity ("Customer") each as identified on the Order Form to which this Addendum is attached.

The Digital Operational Resilience Act (Regulation (EU) 2022/2554), "DORA", is an European Union regulation that creates a binding, comprehensive information and communication technology risk management framework for the EU financial sector. DORA establishes technical standards that financial entities and their critical third-party technology service providers must implement in their ICT systems. It helps to strengthen the European financial market against cyber risks and incidents in information and communication technology (ICT).

ICT services are "digital and data services that are provided on a continuing basis to one or more internal or external users by means of ICT systems, including hardware as a service and hardware services, which includes technical support provided by the hardware provider by means of software or firmware updates, but excluding traditional analog telephone services".

Crownpeak and its affiliates ensure compliance with DORA and assist their customers in cyber security, ICT risks and digital operational resilience.

As such, Crownpeak notes the following DORA requirements and the Crownpeak contractual agreements adhering to those requirements,

§ 1 Description of Functions of the ICT Service Provider

A clear and complete description of all the functions and ICT services to be provided by Crownpeak is included in the **Software Description**.

§ 2 Location of Services and Data Storage (Art. 30 para. 2 b) DORA)

The locations (regions or countries) where the agreed or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, are specified in the **Data Processing Agreement** and **Sub Processor List**.

§ 3 Provisions regarding availability, authenticity, integrity and confidentiality in relation to data protection, including the protection of personal data (Art. 30 para. 2 c) DORA)

Provisions for ensuring access to personal and non-personal data processed by Crownpeak in the event of the insolvency, liquidation, cessation of business activities of Crownpeak or termination of the contractual agreements are included in the **Master Services Agreement** and the **Data Processing Agreement**.

§ 4 Service level descriptions, including updates and revisions (Art. 30 para. 2 e) DORA)

Complete descriptions of the service levels, including updates and revisions, with precise quantitative and qualitative performance targets within the agreed service level, to enable effective monitoring of the ICT services, are included in the **Service Level Agreement**.

§ 5 Support in the event of an ICT incident related to the ICT service provided (Art. 30 Para. 2 f) DORA)

The Supplier is obliged to provide support to the Customer in the event of an ICT incident related to the ICT service provided to the Customer. Crownpeak's obligation to support the Customer in the event of an ICT incident related to the ICT service provided to the Customer, at no additional cost or at a predetermined cost, is included in the **Data Processing Agreement**.

§ 6 Cooperation with Supervisory Authorities (Art. 30 Para. 2 g) DORA)

Crownpeak is obliged to fully cooperate with the authorities responsible for the Customer, in particular with the supervisory and processing authorities, including other persons named by them.

Crownpeak's obligation to fully cooperate with the authorities responsible for the Customer, including the persons named by them, is set out in the **Data Processing Agreement**.

§ 7 Termination Rights and Notice Periods (Art. 30 Para. 2 h) DORA)

The parties agree that the Customer is entitled to extraordinary termination in the event of the following circumstances in accordance with Art. 28 Para 7 DORA:

a) significant breach by Crownpeak of applicable laws, regulations or contractual terms;

b) circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of Crownpeak;

c) Crownpeak’s evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data;

d) where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement. For the avoidance of doubt, this circumstance shall only be deemed to exist if the authority demands a termination of the contractual agreement or an amendment that the parties cannot agree on.

Termination rights and minimum notice periods for the termination of the contractual agreements in line with the expectations of the relevant authorities are listed in the **Master Services Agreement and Data Processing Agreement**. Crownpeak’s notice periods and reporting obligations, including notification of any developments that could have a material impact on Crownpeak's ability to effectively provide the agreed service levels, are specified in the above-mentioned contracts.

§ 8 Participation in IT Security Training (Art. 30 Para. 2 i) DORA)

The terms and conditions for Crownpeak to participate in ICT security awareness programs and digital operational resilience training are set out in the **Data Processing Agreement**.

§ 9 Incident Reporting in Accordance with Art. 3 No. 8 DORA

Crownpeak shall report ICT-related incidents within the meaning of Art. 3 No. 8 DORA to the Customer if these may affect the ICT services owed. Likewise, Crownpeak shall report significant cyber threats within the meaning of Art. 3 No. 13 DORA if these may pose a threat to the ICT services owed. Crownpeak is obliged to report ICT-related incidents to the Customer immediately, but no later than 24 hours after their discovery.

§ 10 Definitions

All defined terms, words, expressions, and abbreviations shall have the meaning given in the Master Services Agreement and the Digital Operational Resilience Act (Regulation (EU) 2022/2554).