Data Processing Exhibit for EQS Cloud Services and Whistleblowing Solution (pursuant to Art 28 GDPR)
Based on Standard Contractual Clauses issued by EU Commission Implementation Decision (EU) 2021/915

1.   Purpose and scope

(a)   The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28 (4) of 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b)   The processors and subprocessors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28 (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c)   These Clauses apply to the processing of personal data as specified in Annex II.

(d)   Annexes I to III are an integral part of the Clauses.

(e)   These Clauses are without prejudice to obligations to which the processor is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f)   These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

2.   Invariability of the Clauses

(a)   The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b)   This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

3.   Interpretation

(a)   Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b)   These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c)   These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4.   Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

5.   Docking clause

(a)   Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a processor or a subprocessor by completing the Annexes and signing Annex I.

(b)   Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a processor or a subprocessor, in accordance with its designation in Annex I.

(c)   The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

6.   Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the processor, are specified in Annex II.

7.   Obligations of the Parties

7.1.   Instructions

(a)   The subprocessor shall process personal data only on documented instructions from the processor acting as a representative of its end customers (controller), unless required to do so by Union or Member State law to which the subprocessor is subject. In this case, the subprocessor shall inform the processor of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the processor throughout the duration of the processing of personal data. These instructions shall always be documented.

(b)   The subprocessor shall immediately inform the processor if, in the subprocessor's opinion, instructions given by the processor infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2.   Purpose limitation

The subprocessor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the processor.

7.3.   Duration of the processing of personal data

Processing by the subprocessor shall only take place for the duration specified in Annex II.

7.4.   Security of processing

(a)   The subprocessor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b)   The subprocessor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The subprocessor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5.   Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the subprocessor shall apply specific restrictions and/or additional safeguards.

7.6.   Documentation and compliance

(a)   The Parties shall be able to demonstrate compliance with these Clauses.

(b)   The subprocessor shall deal promptly and adequately with inquiries from the processor about the processing of data in accordance with these Clauses.

(c)   The subprocessor shall make available to the processor all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the Informa D&B end customer acting as a controller request or at processor's request, the subprocessor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Informa D&B end customer acting as a controller and the processor may take into account relevant certifications held by the subprocessor.

(d)   The Informa D&B end customer acting as a controller and the processor and the processor may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the subprocessor and shall, where appropriate, be carried out with reasonable notice.

(e)   The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7.   Use of sub-subprocessors

(a)   The subprocessor has the processor's general authorisation for the engagement of sub-subprocessors from an agreed list. The subprocessor shall specifically inform in writing the processor of any intended changes of that list through the addition or replacement of sub-subprocessors at least 30 days in advance, thereby giving the processor sufficient time to be able to object to such changes prior to the engagement of the concerned sub-subprocessor(s). The subprocessor shall provide the processor with the information necessary to enable the processor to exercise the right to object.

(b)   Where the subprocessor engages a sub-subprocessor for carrying out specific processing activities (on behalf of the processor), it shall do so by way of a contract which imposes on the sub-subprocessor, in substance, the same data protection obligations as the ones imposed on the data subprocessor in accordance with these Clauses. The subprocessor shall ensure that the sub-subprocessor complies with the obligations to which the subprocessor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c)   At the processor's request, the subprocessor shall provide a copy of such a sub-subprocessor agreement and any subsequent amendments to the processor. To the extent necessary to protect business secret or other confidential information, including personal data, the subprocessor may redact the text of the agreement prior to sharing the copy.

(d)   The subprocessor shall remain fully responsible to the processor for the performance of the sub-subprocessor's obligations in accordance with its contract with the subprocessor. The subprocessor shall notify the processor of any failure by the sub-subprocessor to fulfil its contractual obligations.

(e)   In the event the processor disappears, ceases to exist in law or has become insolvent - the Informa D&B end customer acting as a controller shall have the right to terminate the sub-subprocessor contract and to instruct the sub-subprocessor to erase or return the personal data.

7.8.   International transfers

(a)   Any transfer of data to a third country or an international organisation by the subprocessor shall be done only on the basis of documented instructions from the processor or in order to fulfil a specific requirement under Union or Member State law to which the subprocessor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The processor agrees that where the subprocessor engages a sub-subprocessor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the processor) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the subprocessor and the sub-subprocessor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

8. Assistance to the processor

(a) The subprocessor shall promptly notify the processor of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the processor.

(b) The subprocessor shall assist the processor in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the subprocessor shall comply with the processor's instructions.

(c) In addition to the subprocessor's obligation to assist the processor pursuant to Clause 8(b), the subprocessor shall furthermore assist the processor in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the subprocessor:

    (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a change to the Whistleblowing Solution occurs or/and a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, and to document it;

    (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the processor to mitigate the risk;

    (3) the obligation to ensure that personal data is accurate and up to date, by informing the processor without delay if the subprocessor becomes aware that the personal data it is processing is inaccurate or has become outdated;

    (4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the subprocessor is required to assist the processor in the application of this Clause as well as the scope and the extent of the assistance required.

9. Notification of personal data breach

In the event of a personal data breach, the subprocessor shall cooperate with and assist the processor for the processor to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the subprocessor.

9.1 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the subprocessor shall assist the processor:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the processor has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the processor's notification, and must at least include:

    (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    (2) the likely consequences of the personal data breach;

    (3) the measures taken or proposed to be taken by the processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the subprocessor

In the event of a personal data breach concerning data processed by the subprocessor, the subprocessor shall notify the processor without undue delay after the subprocessor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the subprocessor when assisting the processor in the compliance with the processor's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

10. Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the subprocessor is in breach of its obligations under these Clauses, the processor may instruct the subprocessor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The subprocessor shall promptly inform the processor in case it is unable to comply with these Clauses, for whatever reason.

(b) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

    (1) the processing of personal data by the subprocessor has been suspended by the processor pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

    (2) the subprocessor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

    (3) the subprocessor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The subprocessor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the processor that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the processor insists on compliance with the instructions.

(d) Following termination of the contract, the subprocessor shall, at the choice of the processor, delete all personal data processed on behalf of the processor and certify to the processor that it has done so, or, return all the personal data to the processor and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the subprocessor shall continue to ensure compliance with these Clauses.

11. Miscellaneous

(a) Prior to the commencement of any audit, the Informa D&B end customer acting as a controller, processor and subprocessor shall jointly agree the scope, time, duration of the audit and the remuneration to be paid by the controller as well as conclude an appropriate confidentiality agreement. The processor shall inform subprocessor immediately of any infringements found during an audit.

(b) The agreed list of subprocessor's sub-subprocessors as set out in Clause 7.7 can be found at www.eqs.com/subsubprocessor. Any changes to this agreed list may be notified in text form or on a website.

If the processor objects to a new sub-subprocessor within the 30 day notice period, subprocessor will make reasonable efforts,

    (1) to make available to the processor a change in the affected Cloud Service, or

    (2) recommend a commercially reasonable change in the processor's configuration or use of the Cloud Service to avoid the processing of personal data by the rejected new sub-subprocessor without unreasonably burdening the processor.

If subprocessor is unable to make available such a change within the notice period, the processor may terminate the applicable Cloud Service which cannot be provided by subprocessor without the use of the objected-to new sub-subprocessor, by providing written notice to subprocessor. The processor shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Cloud Service.

    (3) Subprocessor may charge processor for any assistance provided under these Clauses per subprocessor's standard hourly rates. However, subprocessor shall not be entitled to a fee in connection with:

(c) personal data breaches of processor as set out in Clause 9.2, and

(d) inquiries and inspections conducted by a responsible supervisory authority.

ANNEX I

List of parties

Please see the parties listed in the applicable underlying Agreement. INFORMA D&B being the processor acting on behalf of its end customers and EQS Group being the subprocessor.

─────

ANNEX II

Description of the processing

1. Categories of data subjects whose personal data is processed

    a) clients

    b) employees

    c) interested parties

    d) subscribers

    e) contact person with details

    f) For whistleblowing solution: reporters and other involved persons

2. Categories of personal data processed

    a) Personal (first name, surname, organizational data)

    b) Communication data (e.g. telephone, e-mail, address)

    c) For whistleblowing solution: information on (potential) criminal offences or suspicion thereof as well as other reporting data

3. Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

    a) For whistleblowing solution: possible

4. Nature of the processing

    The nature of the processing of personal data by subprocessor on behalf of the processor are set out in this Exhibit and in the Agreement.

5. Purpose(s) for which the personal data is processed on behalf of the processor

    The purpose of the processing of personal data by subprocessor on behalf of the processor are set out in this Exhibit and in the Agreement.

    The personal data are processed for purposes related to the Integrity Line and the provision hosting services. INFORMA D&B in the quality of Reseller and acting as a processor makes available to its end Customers a Whistleblowing platform called Integrity Line, developed by EQS. The platform is based on a cloud solution that hosts the data processed in the scope of the Integrity Line, data related with the whistleblowing hotlines are also processed.

6. Duration of the processing

    During the term of the Agreement

7. For processing by (sub-) subprocessors, also specify subject matter, nature and duration of the processing

    The subject matter of the processing of personal data by subsubprocessors are set out in the list of subsubprocessors.

    The nature and purpose of the processing of personal data by subsubprocessor are set out in this Exhibit and in the Agreement.

─────

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

The technical and organizational measures are described in subprocessors Technical and Organizational Measures for EQS Cloud Services document, available on www.eqs.com. The technical and organizational measures are subject to further development and subprocessor is permitted to implement alternative adequate measures, subject to keeping an equal or improved security level. Subprocessor agrees to remain ISO 27001 certified.