Verian Group Supplier Data Processing Agreement

This Data Protection Agreement (DPA) shall amend and apply to all agreements for Services provided by Verian Group to Client that reference and incorporate this DPA (Agreement) and to the extent that Supplier Processes Customer Personal Data (as defined below). The parties agree that from the effective date of the Agreement, or if later, the effective date on which the Parties amend the Agreement to add this DPA, these terms will supplement existing privacy and data protection terms contained in the Agreement, however this DPA shall prevail to the extent set out below.

NOW, THEREFORE, the Parties agree as follows:

1. DEFINITIONS
Capitalised terms not otherwise defined herein shall have the meaning and interpretations given to them in the Agreement. In this DPA, the following terms shall have the meanings and interpretations set out below unless the context otherwise requires:

1.1 **Affiliate** means, in respect of Verian Group, any entity (excluding Europanel) which, from time to time both: (i) directly or indirectly through one or more intermediaries, Controls, or is Controlled by, or is under common Control of, Verian Group; and (ii) is trading as Verian Group (and Verian Group Affiliate shall be construed accordingly); and, in respect of Supplier, any entity, which is Controlled by Supplier (and Supplier Affiliate shall be construed accordingly)

1.2 **Customer Personal Data** means any Personal Data Processed by Supplier or a Sub-processor (as a Processor) on behalf of Customer (as Controller or as a Processor for one of Customer's end client(s)) pursuant to the Agreement

1.3 **Control** means, in respect of any entity: (i) possession, direct or indirect through one or more intermediaries, of the power to direct the management or policies of such entity, whether through ownership of voting securities, by contract relating to voting rights, or otherwise; or (ii) ownership, direct or indirect through one or more intermediaries, of more than 50% percent of the outstanding voting securities or other ownership interest of such entity (and Controls and Controlled shall be construed accordingly)

1.4 **Data Processing Particulars** means such template attached in Annex 1 that describes the Processing carried out in connection with the Agreement. The Data Processing Particulars will be completed and annexed to the relevant SOW

1.5 **Data Protection Laws** means EU Data Protection Laws and UK Data Protection Laws including any applicable delegated acts adopted by the European Commission and any applicable national legislation made under or otherwise adopted by Member States of the European Economic Area pursuant to specific rights or powers contained within the GDPR, together with any replacement legislation or any equivalent legislation of any other applicable jurisdiction and all other applicable laws and regulations in any relevant jurisdiction relating to the Processing of Personal Data and privacy

1.6 **EU Data Protection Laws** means the GDPR and laws implementing or supplementing the GDPR, the Privacy and Electronic Communications Directive 2002/58/EC and any other Applicable Laws relating to the Processing of personal data and privacy, including where

applicable the guidance and codes of practice issued by a relevant regulator in relation to such applicable laws in each case as amended, repealed or replaced from time to time

1.7 **GDPR** means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council 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

1.8 **Independent Auditor** means an auditor from PWC, Deloitte, KPMG or Ernst & Young or another mutually agreeable internationally recognized auditing firm that is not employed on a contingency basis

1.9 **International Data Transfer Agreement or UK IDTA** means the Restricted International Transfer Agreement required for new Processing arrangements entered into from 21 March 2022 (and a separate UK Addendum) when Customer requires to transfer Customer Personal Data from the UK to processors established in Third Countries (as amended or replaced from time to time)

1.10 **Personnel** means either Party's stakeholders, directors, employees, agents, consultants, subcontractors, or other persons authorized by (i) either Party (ii) their Affiliates (iii) their subcontractors engaged in the provision of Services

1.11 **Restricted International Transfer** means a transfer of personal data between parties established in: (i) a country that is deemed adequate (by the European Commission or any other competent body for the purposes of Data Protection Laws) and Third Countries, (ii) any Third Country to another Third Country

1.12 **Restricted International Transfer Agreement** means the relevant standard contractual clauses (such as the Standard Contractual Clauses or the International Data Transfer Agreement) or any other standard or non-standard contractual clauses required under Data Protection Laws (as amended or replaced from time to time)

1.13 **SOW** means a statement of work entered into by the Parties (or any of their respective Affiliates) to document their agreement in respect of any services, which is more specifically defined in the Agreement

1.14 **Standard Contractual Clauses** means the standard contractual clauses (adopting the appropriate module as per the relationship of the Parties) approved by European Commission decision 2021/914 on standard contractual clauses for the transfer of Personal Data to processors established in Third Countries, as amended or replaced from time to time

1.15 **Subcontractor** means any third party (excluding any Supplier Affiliate) to whom Supplier has delegated any function or obligation to provide the Services

1.16 **Sub-processor** means any Subcontractor appointed as set out in Clause 6 (Sub-processors) to Process Customer Personal Data on behalf of Customer in connection with the Agreement

1.17 **UK Addendum** means a separate UK addendum to be used in conjunction with the Standard Contractual Clauses if there is also a Restricted International Transfer under Standard Contractual Clauses that includes the UK

1.18 **UK Data Protection Laws** means the GDPR as transposed into United Kingdom domestic law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (UK GDPR), together with the Data Protection Act 2018, the Privacy and

Electronic Communications (EC Directive) Regulations 2003 (as amended) and other data protection or privacy legislation in the United Kingdom in each case as amended, repealed or replaced from time to time

1.19 The terms, **Binding Corporate Rules Commission, Controller, Data Subject, Member State, Personal Data, Processing, Processor, Third Country and Supervisory Authority** shall have the same meaning as in Data Protection Laws, and their cognate terms shall be construed accordingly.

1.20 For the purposes of this DPA:

1.20.1 any reference to **Parties** shall be to Verian Group, Supplier and the relevant parties to the relevant SOW (and Party shall mean any one of them);

1.20.2 any references to **Customer** shall mean Verian Group and the relevant Verian Group Affiliate that is a party to that SOW; and

1.20.3 any references to **Supplier** shall mean Supplier and, in respect of any SOW, the relevant Supplier Affiliate that is a party to that SOW.

2. SUPPLIER PROCESSING AS AN INDEPENDENT CONTROLLER

2.1 The parties acknowledge that with regard to the Customer Personal Data, Supplier may act as an independent Controller of Customer Personal Data and if acting as an Independent Controller shall only Process Customer Personal Data in accordance with Data Protection Laws and, for the following purposes, Processing: (i) for the purpose of providing the Services business contact details to carry out administrative functions for the provision of the Services; (ii) initiated by Data Subjects in their use of the Services; (iii) to comply with other documented reasonable written instructions provided by Customer (including via email); and (iv) as required by applicable law and regulatory obligations.

2.2 To the extent that Supplier acts as an independent Controller, the duration of the processing, the nature and purpose of its processing, the types of Customer Personal Data and categories of Data Subjects shall be set out in each SOW; and

2.3 Customer confirms that it has and will fulfil its obligations required under the Data Protection Laws, that it has the authority to provide Customer Personal Data to the Supplier in connection with the performance of the Services and that any Customer Personal Data provided to the Supplier has and will be Processed in accordance with the Data Protection Laws.

2.4 Where the Supplier acts as an independent Controller, the Parties agree that:

2.4.1 Clause 4 (Technical and organisational measures);

2.4.2 Clause 5 (Rights of Data Subjects); and

2.4.3 Clause 8 (Data Incident Management Notification),
shall apply to this Clause 2.

2.5 Supplier warrants that any Restricted International Transfers are subject to Clause 12 (Restricted International Transfers and Processing in Third Countries).

2.6 Upon request, each party shall provide the other with information relating to its processing

of the Customer Personal Data as reasonably required for the other to satisfy its obligations under Data Protection Laws.

3. SUPPLIER PROCESSING AS A PROCESSOR

3.1 The parties acknowledge that with regard to the Customer Personal Data, Supplier may act as a Processor of Customer Personal Data and agree that the terms of Clauses 3 (Supplier Processing as a Processor) to clause 12 (Restricted International Transfers and Processing in Third Countries) (inclusive) shall apply.

3.2 Supplier shall Process Customer Personal Data on behalf of the Customer in compliance with the Customer's lawful instructions for the purposes described in Annex 1 (Data Processing Particulars) (Permitted Purposes).

3.3 If such other Processing is required by local applicable law (including local laws in the relevant Sub-processor country), Supplier shall inform Customer of that legal requirement before such Processing, unless that law prohibits this on important grounds of public interest. Notwithstanding the foregoing, Supplier shall not carry out such Processing (including transfer of Customer Personal Data to a public authority) unless there is a legal mandate between the Customer country and the relevant local country for Customer to carry out such Processing.

4. TECHNICAL AND ORGANISATIONAL MEASURES

4.1 A description of the technical and organisational security measures implemented by Supplier is set out in Annex 2.

4.2 Supplier shall provide and maintain appropriate technical and organisational measures that are commensurate with the Services.

4.3 Supplier agrees that it shall ensure that any changes made to the technical and organisational measures result in a level of protection for the Customer Personal Data that is the same as or greater than that which applied as at the at the date of this DPA.

4.4 Supplier shall:

4.4.1 only involve Supplier Personnel to Process Customer Personal Data under the Agreement who have had appropriate training pertinent to the care and handling of Personal Data;

4.4.2 only authorise Supplier Personnel to Process Customer Personal Data if such person is subject to a duty of confidentiality (whether a contractual duty or a statutory duty or otherwise); and

4.4.3 ensure the reliability of Supplier Personnel to whom Supplier has provided access to Customer Personal Data.

4.5 Customer shall comply with and will continue to comply with Data Protection Laws and Supplier shall inform Customer if, in the Supplier opinion, instructions given by Customer infringe Data Protection Laws.

5. RIGHTS OF DATA SUBJECTS

5.1 Supplier shall to the extent legally permitted, immediately notify Customer if Supplier receives a request from a Data Subject, third parties, relevant data protection authorities in the

relevant local jurisdiction, or any other law enforcement authority, to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (right to be forgotten), data portability, right to object to the Processing, or its right not to be subject to automated individual decision making (Data Subject Request).

5.2 Taking into account the nature of the Processing, Supplier shall in accordance with Customer's reasonable instructions, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws.

5.3 If Customer does not have the ability to address a Data Subject Request, Supplier shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Supplier is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws.

5.4 Neither Supplier nor relevant Sub-processor shall respond to a Data Subject Request unless authorised to do so by the Customer.

6. SUB-PROCESSORS

6.1 Supplier will not share, transfer, disclose, make available or otherwise provide access to any Customer Personal Data to any third party (including Supplier Affiliates), or contract any of its rights or obligations concerning Customer Personal Data performed on behalf of Customer pursuant to this DPA to a Sub-processor without the specific written consent of Customer. For the avoidance of doubt, Customer's prior written consent must be obtained for each and any change of Sub-processor no later than 60 calendar days prior to such change.

6.2 Supplier represents and warrants that such Sub-processor has entered into binding written agreements with the Supplier that are substantially the same and no less onerous as those imposed on the Supplier pursuant to this DPA.

6.3 Supplier shall provide Customer with the necessary information to help it verify the Sub-processor's compliance with its data protection obligations pursuant to this DPA and Data Protection Laws.

6.4 Supplier shall remain fully liable towards Customer for the performance of any and all Sub-processors obligations under this DPA and all Data Protection Laws.

7. AUDIT

7.1 In addition to any audit rights within the Agreement and upon request by Customer and subject to Customer's reasonable discretion, Supplier allows Customer (either on its own or on behalf of its end client(s) as Controller) or an Independent Auditor instructed by Customer to audit and review the Supplier, and the Sub-processor's, information security program, data processing facilities and data protection compliance program in order to verify compliance with this DPA, Data Protection Laws and Customer or Customer's own obligations to its end client(s), (Data Protection and Security Audit).

7.2 Such Data Protection and Security Audit may include tests designed to breach the Supplier's, or Sub-processor's, information security program and associated security measures (including security penetration testing) and shall be conducted with no less than 10 days' prior written notice.

7.3 If Customer reasonably believes that the results of a Data Protection and Security Audit identifies a weakness in the security measures adopted by the Supplier, or the Sub-processor, the Supplier shall evaluate such weakness and provide a suitable solution to Customer (or its end client(s)) satisfaction within timescales agreed by the Customer.

7.4 The Supplier acknowledges that any regulator or its agent may from time to time audit the Supplier, or any approved Sub-processors, and that any such audit shall not be subject to any of the restrictions set out in this Clause 7.

7.5 The Supplier shall maintain a continuous record of its Processing activities conducted for and on behalf of Customer. This record shall be made available to Customer within 48 hours of the Customer making a request.

8. DATA INCIDENT MANAGEMENT AND NOTIFICATION

8.1 In addition to compliance with the relevant technical and organisational measures, Supplier will maintain security incident management policies and procedures and shall notify Customer without undue delay (and in any event within 24 hours) after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data, transmitted, stored or otherwise Processed by Supplier or its Sub-processors which results in any actual loss or misuse of Customer Personal Data (a Data Incident).

8.2 Supplier shall provide Customer with sufficient information to allow Customer to meet any obligations to assess and report a Data Incident under the Data Protection Laws, which may be provided in stages as it becomes available to Supplier and shall include the following:

8.2.1 a description of the nature of the Data Incident, including details of any Sub-processors involved, the categories and numbers of Data Subjects concerned, and the categories and numbers of Customer Personal Data records concerned;

8.2.2 the name and contact details of Supplier's or the relevant Supplier Affiliate's data protection officer or other relevant contact from whom more information may be obtained;

8.2.3 the likely consequences of the Data Incident; and

8.2.4 the measures taken or proposed to be taken to address the Data Incident.

8.3 Supplier shall make all reasonable efforts to identify the cause of such Data Incident and take those steps as Customer deems necessary and reasonable in order to remediate the cause of such a Data Incident to the extent that the remediation is within Supplier's reasonable control.

8.4 Supplier shall be liable for all costs arising from a Data Incident caused by a breach of this clause 8 including but not limited to any fines or payments to third party required to be paid by the Customer and the reasonable legal costs of the Customer in defending any claims or legal proceedings brought against the Customer as a result of the Data Incident.

8.5 In the event of a Data Incident, Customer (subject to any obligations Customer has to its end client(s)) shall be responsible for notifying Data Subjects and or Supervisory Authorities. Before any such notification is made, Customer shall, where possible, consult with and provide Supplier an opportunity to comment on any notification made in connection with a Data Incident.

verian

9. RETURN AND DELETION OF CUSTOMER PERSONAL DATA

Supplier shall, and shall procure that Sub-processors shall, at any time on Customer's request, delete or return all Customer Personal Data except that this requirement shall not apply to the extent that: (i) Supplier or Sub-processors are required to retain Customer Personal Data for compliance with applicable laws or regulatory requirements; (ii) Customer Personal Data is archived on back-up systems, provided that such copies are kept confidential and secure in accordance with the relevant Agreement terms.

10. LIMITATION OF LIABILITY

Save as set out in clause 8.4 above, each Party and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to a breach of its obligations under this DPA, whether in contract, tort or under any other theory of liability is subject to the liability terms in the Agreement, and any reference in such terms to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement.

11. DATA PROTECTION IMPACT ASSESSMENT

11.1 Upon Customer's request, Supplier shall, and shall procure that Sub-processors shall, provide Customer with reasonable cooperation and assistance, at Customer's cost, needed to fulfil Customer's obligation to carry out a data protection impact assessment (DPIA) including but not limited to where a type of Processing is likely to result in a high risk to the rights and freedoms of Data Subjects, to allow the Customer to comply with its obligations as a Controller in relation to data security, DPIA and any related consultations under Data Protection Laws.

11.2 The Supplier and each Sub-processor shall comply with its obligation to consult the relevant Supervisory Authority prior to Processing where a DPIA indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk.

12. RESTRICTED INTERNATIONAL TRANSFERS AND PROCESSING IN THIRD COUNTRIES

12.1 Supplier represents and warrants that it has entered into relevant Restricted International Transfer Agreements with its Sub-processors in respect to any Restricted International Transfers, or that Restricted International Transfers will be covered at the time of the transfer by Binding Corporate Rules.

12.2 The Restricted International Transfer Agreement terms shall be incorporated by reference into this DPA and shall apply on commencement, and to the extent, of any Restricted International Transfer or Binding Corporate Rules as the case may be.

12.3 The Parties options for the Standard Contractual Clauses (or equivalent options) are set out in paragraph 1 (Options (from EU SCCs) and equivalent terms) in Annex 3.

12.4 The Parties shall cooperate with each other to carry out the Supplementary Security Measures set out in paragraph 2 (Supplementary Security Measures) of Annex 3.

verian

13. GOVERNING LAW
The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity, and this DPA and is governed by the laws of the country or territory stipulated for this purpose in the Agreement.

ANNEX 1

DETAILS OF PROCESSING OF CLIENT PERSONAL DATA
This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data
The subject matter and duration of the Processing of the Customer Personal Data are set out in the [MSA] and this Addendum.

The nature and purpose of the Processing of Customer Personal Data

[Include description here]

The types of Customer Personal Data to be Processed

[Include list of data types here]

The categories of Data Subject to whom the Customer Personal Data relates

[Include categories of data subjects here]

The obligations and rights of Customer and Customer Affiliates

The obligations and rights of Customer and Customer Affiliates are set out in the [MSA] and this Statement of Work.

ANNEX 2

SUPPLIER TECHNICAL AND ORGANISATIONAL MEASURES

ANNEX 3

RESTRICTED INTERNATIONAL TRANSFER AGREEMENT TEMPLATES

UK Controller to Processor and Processor to Processor Restricted International Transfer Agreement: https://ico.org.uk/media/for-organisations/documents/4019536/idta.docx

UK Addendum: international-data-transfer-addendum.docx (live.com)

EU Controller to Processor and Processor to Processor Restricted International Transfer Agreement: https://iapp.org/media/resource_center/EU_SCCs_Controller_To_Processor_June2021.docx
https://iapp.org/media/resource_center/EU_SCCs_Processor_To_Processor_June2021.docx

EU Processor to Controller and Controller to Controller Restricted International Transfer Agreement: https://iapp.org/media/resource_center/EU_SCCs_Processor_To_Controller_June2021.docx
https://iapp.org/media/resource_center/EU_SCCs_Controller_To_Controller_June2021.docx

1. Options (from EU SCCs) and equivalent terms

1.1 The Parties hereby make the following options (from the Standard Contractual Clauses) and equivalent terms shall apply in each Restricted International Transfer Agreement entered into between the relevant parties in each Third Country as when such parties enter into this DPA.

1.2 **Clause 7 (Docking clause)** shall apply with regards to each Data Importer.

1.3 **Clause 9 (Use of Sub-processors).** Option 1 shall apply. The time period shall be 60 days.

1.4 **Clause 13(a) (Supervision**) means the Supervisory Authority in the Data Exporter country.

1.5 **Clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction).** Option 2 shall apply. The governing law and courts in the Data Exporter country shall apply.

1.6 **Annex I** of the Restricted International Transfer Agreements shall be deemed to be pre-populated with the relevant sections of Annex 1 to this DPA.

1.7 **Annex II** of the Restricted International Transfer Agreements shall be deemed to be pre-populated with the relevant sections of Annex 2 to this DPA.

2. Supplementary Security Measures

2.1 The Parties shall cooperate with each other to carry out these Supplementary Security Measures in response to a public / private / regulatory authority order to access Customer Personal Data or surveillance order (Order).

2.2 Supplier / Sub-processor in a Third Country shall notify Customer without undue delay of any Order.

2.3 Supplier / Sub-processor will not attempt to respond in detail to such a request without the relevant Controller's prior written consent. Supplier / Sub-processor may, however, provide generic information (not including Customer Personal Data) to public / private / regulatory authority as part of its obligations to cooperate without consulting or obtaining the prior consent of the relevant Controller.

2.4 If the Parties establish that there is a legal basis to comply with the Order, the Parties shall arrange for the Supplier / Sub-processor to provide information they have resolved to provide.

2.5 The Parties shall:

2.5.1 assist Data Subjects in exercising their rights in connection and Order

2.5.2 cooperate to notify relevant Data Subjects and assist Data Subjects in exercising their rights in connection with the Order by email prior to disclosing the content of the Order to them, however the Data Subject will not be notified if the Order legally prohibits Supplier / Sub-processor from doing so, or if there is an emergency

2.5.3 in any case notify the Data Subject as soon as it is legally permitted to do so or when the emergency (if any) has passed

2.6 Supplier / Sub-processor shall:

2.5.4 not without notifying Customer beforehand, create back doors or similar programming in its systems (used for Processing Customer Personal Data), that could be used by public / private / regulatory authorities to access Customer Personal Data and Supplier / Sub-processor will provide certification that it has not purposefully created such access to Customer Personal Data

2.5.5 not purposefully create or change its business Processes in a manner that facilitates access to Customer Personal Data

2.5.6 promptly inform Customer of any change in local law that requires Supplier / Sub-processor to comply with Orders that negatively affect the security of Customer Personal Data

2.5.7 in accordance with clause 7 (Audit) permit Customer (or its end client(s) as Controller) to conduct an audit or inspection of the relevant Processing facilities to verify if unauthorized transfers of Customer Personal Data have been made to public / private / regulatory authorities

2.5.8 regularly publish a cryptographically signed message informing Customer that as of a certain date and time it has received no Order. The absence of an update of this notification will indicate to Customer that the Supplier / Sub-processor may have received an Order in which case Customer may suspend Processing activities until the Supplier / Sub-processor has complied with its obligations in this clause. Supplier shall be liable to the Customer for Supplier / Sub-processor's failure to meet its Processing obligations as a result of such failure.