DATA PROCESSING AGREEMENT

Upon being presented to you or with effect from any other date agreed by the Parties ("**Effective Date**"), this Data Processing Agreement ("**Agreement**") applies to the "**Services**" provided pursuant to, and defined under, one or more service agreements (each a “**Services Agreement**”) between either **Checkmarx, Ltd** or any relevant affiliate which is party to the Service Agreement as processor (the relevant party referred to as “**Checkmarx**”) and you as data controller (“**Customer**”), each a "**Party**". The Parties have agreed that this Agreement shall apply in order to address the compliance obligations imposed upon the Customer under Data Protection Legislation. This Agreement shall be incorporated in any such Service Agreement by reference.

BY CONTINUING TO PROVIDE OR RECEIVE THE SERVICES, AS APPLICABLE, THE PARTIES AGREE AND ACCEPT FROM THE EFFECTIVE DATE TO BE BOUND BY (I) THIS AGREEMENT AND ALL ITS PARTS INCLUDING (II) THE SCCS TO THE EXTENT APPLICABLE.

In exchange of mutual promises the value of which is hereby acknowledged, **IT IS AGREED AS FOLLOWS:**

1. DEFINITIONS AND INTERPRETATION

1.1 Unless the context otherwise requires, capitalised words in this Agreement shall have the meaning as defined below or elsewhere in this Agreement:

Business Day means a business day in England, Portugal and Israel when banks in London, Lisbon and Tel Aviv are open for business.

Customer Personal Data means any Customer personal data which Checkmarx processes, receives or otherwise has access to on behalf of Customer as a result of or in connection with the provision of the Services.

Data Protection Legislation means all applicable data protection and data privacy legislation including, as the case may be, the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**") and the Privacy and Electronic Communications Directive 2002/58/EC and, where applicable, the GDPR as adopted in the UK ("**UK GDPR**"), the UK Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), and any other applicable data protection and data privacy laws in any jurisdiction, each as amended or superseded from time to time.

SCCs or Standard Contractual Clauses means an international data transfer agreement mandated under Data Protection Legislation as set out in SCHEDULE 4.

Term has the meaning given to it in Clause 10.1.

1.2 All data protection terms used in this Agreement, including 'transfer', 'personal data', 'process', 'controller', 'processor', 'data subject', 'personal data breach' and 'supervisory authority' shall have the meaning ascribed to them in the Data Protection Legislation.

1.3 Interpretations and defined terms set forth in the Services Agreement apply to the interpretation of this Agreement.

1.4 The Schedules 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 Schedules.

1.5 A reference to "writing" or "written" includes email.

1.6 In the case of conflict or ambiguity between:

1.6.1 any of the provisions of this Agreement and the provisions of the Services Agreement, the provisions of this Agreement shall prevail; and

1.6.2 any of the provisions of this Agreement and the applicable SCCs, the provisions of the applicable SCCs will prevail.

2. PERSONAL DATA AND PROCESSING PURPOSES

2.1 Each Party shall comply with its respective obligations under the Data Protection Legislation in relation to all Customer Personal Data.

2.2 The Parties agree and acknowledge that the processing operations relating to Customer Personal Data to be carried out in the performance of this Agreement conform to the description set out in SCHEDULE 1 to this Agreement.

2.3 With respect to the Parties' respective rights and obligations under this Agreement, if at any time Checkmarx processes Customer Personal Data then the Parties agree that Customer is the controller and that Checkmarx is the processor.

2.4 The Customer retains control of the Customer Personal Data and remains responsible for its compliance obligations under applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Checkmarx. The Customer's instructions shall comply with the Data Protection Legislation.

2.5 The Customer shall have sole responsibility for the accuracy, quality and legality of Customer Personal Data provided to Checkmarx.

2.6 Checkmarx shall only process Customer Personal Data:

2.6.1 as needed to provide the Services;

2.6.2 in accordance with the documented instructions that it has received from Customer by way of this Agreement or otherwise, including with regard to any transfers of personal data to third countries or international organisations; and

2.6.3 as needed to comply with applicable law (in which case, Checkmarx shall provide prior notice to the Customer of such legal requirement, unless that law prohibits such disclosure on important grounds of public interest).

3. SECURITY AND PERSONNEL

3.1 Checkmarx shall ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2 Checkmarx shall ensure the security of the Customer Personal Data that it processes in accordance with the requirements of Data Protection Legislation, in particular:

3.2.1 taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Checkmarx shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(i) the pseudonymisation and encryption of Customer Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing;

(iii) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident;

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; and

3.2.2 in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed.

4. CHECKMARX ASSISTANCE RELATING TO ANY CUSTOMER PERSONAL DATA

4.1 Checkmarx shall provide reasonable assistance to the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights in respect of Customer Personal Data.

4.2 Checkmarx shall notify the Customer within four (4) Business Days if it receives a request from a data subject to exercise any of their rights in respect of their Customer Personal Data under Data Protection Legislation.

4.3 Checkmarx shall provide reasonable assistance to the Customer, taking into account the nature of processing and the information available to Checkmarx, to ensure the Customer's compliance with its obligations in respect of the security of processing of Customer Personal Data, conducting data protection impact assessments and prior consultations with supervisory authorities.

4.4 Checkmarx shall immediately inform the Customer if, in its opinion, an instruction infringes the Data Protection Legislation.

5. PERSONAL DATA BREACHES

5.1 Checkmarx shall without undue delay notify the Customer if it becomes aware of a personal data breach relating to any Customer Personal Data and shall provide reasonable assistance to the Customer in responding thereto and any notification requirements which arise as a result thereof.

5.2 Checkmarx will cover all reasonable expenses associated with the performance of its obligations set out in Clause 5.1 unless the personal data breach arose from the Customer's specific instructions, negligence, wilful default or breach of this Agreement or Data Protection Legislation in which case (without prejudice to Checkmarx's other rights and remedies hereunder) the Customer will cover all expenses associated therewith.

6. SUB-PROCESSORS

6.1 Customer hereby grants to Checkmarx a general written authorisation for Checkmarx to use sub-processors for the provision of the Services, provided that Checkmarx shall ensure that:

6.1.1 it engages such sub-processors by written agreement and the terms of each written agreement must be consistent with the material terms of this Agreement, as if the sub-processor were Checkmarx. However, Checkmarx may accept non-negotiable terms where having used its best endeavours it failed to impose the material terms of this Agreement;

6.1.2 where the sub-processor fails to fulfil its data protection obligations under such written agreement, Checkmarx remains fully liable to the Customer for the sub-processor's performance of such obligations;

6.1.3 it has carried out reasonable due diligence to satisfy itself of the sub-processor's suitability and sufficient organisational and technical measures in place to guarantee the protection of Customer Personal Data against unauthorised or unlawful processing; and

6.1.4 it will notify the Customer of any intended changes concerning the addition or replacement of a sub-processor thereby giving the Customer the opportunity to object to the addition or replacement within fourteen (14) days of the notification.

6.2 Those sub-processors approved as at the commencement of this Agreement are as set out in SCHEDULE 3.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 By entering into this Agreement, Customer as 'data exporter' and Checkmarx as 'data importer' accept and agree to be bound by the SCCs in respect of any data transfer of Customer Personal Data to the extent this is necessary in order to comply with Data Protection Legislation.

7.2 Subject to Checkmarx's compliance with clause 6, the Customer hereby consents to the data transfers of Customer Personal Data to each sub-processor of Checkmarx provided that:

7.2.1 the sub-processor is located in a country which benefits from a finding of adequacy recognised under Data Protection Legislation; or

7.2.2 where 7.2.1 does not apply, Checkmarx either complies with its obligations under the SCCs in relation to appointing a further processor, or, as the case may be, implements with the sub-processor a data transfer mechanism recognised under Data Protection Legislation. Customer authorises Checkmarx to enter into SCCs on its behalf wherein the Customer shall be regarded as the “data exporter” and the sub-processor as the “data importer”. Subject to confidentiality, Checkmarx will make the executed transfer mechanism available to the Customer on request. Checkmarx will provide reasonable assistance to Customer in carrying out a transfer impact assessment.

7.3 Checkmarx shall review the legality of any request for disclosure of Customer Personal Data by a public authority and use reasonable endeavours to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Unless otherwise required by law, Checkmarx shall suspend any disclosure of Customer Personal Data to the public authority pending a decision on the merits of the challenge by a competent judicial authority.

7.4 Checkmarx will keep informed about developments in its country of residence and notify the Customer without delay upon becoming aware of any new laws, changes to law or practice, and significant changes in leadership in government bodies that will likely give rise to a risk of surveillance that is not legitimate, strictly necessary and proportionate.

7.5 Checkmarx may at any time replace the SCCs by notice to Customer with immediate effect with such SCCs that are required under Data Protection Legislation.

8. RECORDS AND AUDITS

8.1 Checkmarx shall maintain all records required by Article 30(2) of the UK GDPR, and (to the extent they are applicable to Checkmarx's activities for Customer) Checkmarx shall make them available to Customer upon written request. The records relating to any Customer Personal Data shall contain the following information:

8.1.1 the name and contact details of the Customer and, where applicable, the joint controller, the Customer's representative and the data protection officer;

8.1.2 the categories of processing carried out on behalf of the Customer;

8.1.3 where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation, including where applicable, the documentation of any suitable safeguards required by the GDPR Article 49(1)(second sub-paragraph);

8.1.4 where possible, a general description of the technical and organisational security measures.

8.2 In relation to its processing of Customer Personal Data Checkmarx shall during the Term provide the Customer with information reasonably necessary to demonstrate compliance with Data Protection Legislation, and shall allow for and contribute to audits, including inspections, concerning Customer Personal Data conducted by the Customer or another auditor mandated by the Customer as agreed by the Parties from time to time provided that:

8.2.1 The Customer gives at least thirty (30) days' prior written notice to conduct such audit or inspection;

8.2.2 the auditor is subject to binding obligations of confidentiality; and

8.2.3 the audit or inspection is undertaken so as to cause minimal disruption to Checkmarx's business and other customers.

8.3 Upon the Customer’s written request, Checkmarx shall delete or return all Customer Personal Data to the Customer following the end of the Term, and shall delete all existing copies unless applicable law requires storage of Customer Personal Data, subject to clause 2.6.3.

9. CUSTOMER WARRANTY

9.1 The Customer warrants that it:

9.1.1 shall comply with all requirements and obligations of a controller under Data Protection Legislation;

9.1.2 shall have sole responsibility for the accuracy, quality and legality of Customer Personal Data; and

9.1.3 is entitled to disclose the Customer Personal Data to Checkmarx so that Checkmarx may process the Customer Personal Data in accordance with the Agreement on Customer's behalf.

9.2 The Customer shall at all times both during and after the Term fully indemnify and hold Checkmarx harmless from any claim, loss or damage awarded against, or incurred or paid by, Checkmarx as a result of or in connection with any actual or alleged breach by or on behalf of the Customer of any of the warranties set out in Clause 9.1.

10. TERM AND TERMINATION

10.1 This Agreement shall commence on the Effective Date.

10.2 This Agreement will remain in full force and effect until the earlier of the following dates (subject to Clause 10.3):

10.2.1 the termination of the Services Agreement; or

10.2.2 Checkmarx ceases to retain any Customer Personal Data related to the Services Agreement in its possession or control.

10.3 Any provision of this Agreement that expressly or by implication comes into or continues in force on or after termination of the Services Agreement in order to protect Customer Personal Data will remain in full force and effect.

10.4 If a change in any Data Protection Legislation prevents either Party from fulfilling all or part of its Services Agreement obligations, the Parties will suspend the processing of Customer Personal Data until that processing complies with the new requirements. If the Parties are unable to bring the Customer Personal Data processing into compliance with the Data Protection Legislation within sixty (60) days, either Party may terminate the Services Agreement on written notice to the other Party. Notwithstanding anything to the contrary in the Services Agreement, if the Services Agreement is terminated pursuant to this clause, all amounts that would have otherwise become due and payable after the effective date of such termination shall become due and payable on the effective date of such termination of the Services Agreement. Furthermore, Customer shall not be entitled to a refund of any amounts already paid under the Services Agreement.

11. SEVERANCE

If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable it shall be deemed deleted but that shall not affect the validity and enforceability of the rest of this Agreement.

12. NOTICE

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

12.1.1 for the Customer:

Attention:
Address: As set forth at the head of the Agreement

12.1.2 for Checkmarx:

Attention: Chief Financial Officer
Address: As set forth at the head of the Agreement
With copy to cxlegal@checkmarx.com

12.2 Clause 12.1 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.

13. LIMITATION OF LIABILITY

Each Party’s and all of its affiliates’ liability, taken together in the aggregate, arising out of or related to this Agreement, whether in contract, tort or under any other theory of liability, is subject to the ‘Limitation of Liability’ section of the Services Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that party and all of its affiliates under the Services Agreement and this Agreement together.

14. GOVERNING LAW

This Agreement is governed by English law. Both parties submit to the exclusive jurisdiction of the English courts in relation to any dispute concerning this Agreement.

SCHEDULE 1
(DESCRIPTION OF PROCESSING)

A. LIST OF PARTIES

Data exporter(s): Customer entity as out in the Agreement.
Data importer(s): Checkmarx entity as set out in the Agreement.

B. DESCRIPTION OF PROCESSING AND DATA TRANSFER

Description of data subjects	Current, former and potential employees and subcontractors of the Customer and other authorised users of the Services.
Description of Customer Personal Data	Name, phone number, postal address, email address, position, transactions, usage details (incl. e.g. URLs visited, events triggered on defined actions such as page loads, clicks, logins and purchases), IP addresses, cookies, analytics data.
Sensitive data processed (if applicable) and applied restrictions or safeguards,[1] keeping a record of access to the data, restrictions for onward transfers or additional security measures.	N/A
Description of processing	Accessing Customer Personal Data when providing the Services.
Purpose(s) of processing	The nature and purpose of the processing of Customer Personal Data are: • for Checkmarx to perform its obligations pursuant to the Services Agreement; • for delivery and provision of the Services to the Customer; and • for customer support and technical troubleshooting.
Retention period or the criteria used to determine that period	For the purpose of providing the Services to Customer: during the term of the Services Agreement.
Details of each data transfer	Checkmarx may access a Customer device remotely or Customer may send data to Checkmarx.
The frequency of the data transfer	Each time Services are provided, e.g. daily.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the SCCs

Checkmarx agrees that the competent authority will be determined by Customer acting reasonably according to the country of the Customer and/or data subject and their applicable Data Protection Legislation and may include one or more EU member state, UK or other data protection supervisory authorities.

[1] Safeguards must 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).

SCHEDULE 2
(TECHNICAL AND ORGANISATIONAL MEASURES)

Checkmarx shall implement appropriate technical and organisational measures to safeguard Customer Personal Data as envisaged under the Agreement and the Services Agreement, including as set out in this schedule.

Checkmarx has implemented and adheres to the technical and organizational security measures set forth in the ISO:27001 standard. Supplier maintains the administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of the personal data as described in a SOC 2 Type II report which is produced by independent auditors and updated on an annual basis.

SCHEDULE 3
(LIST OF SUB-PROCESSORS)

Checkmarx and its affiliates uses certain sub-processors to assist it in providing to Customer the Services.

Sub-processor	Location
Checkmarx, Ltd.	Israel
Checkmarx, Inc.	United States
Checkmarx UK Ltd.	United Kingdom
Checkmarx Portugal, Unipessoal Lda	EU
Checkmarx France S.A.S.	EU
Checkmarx Australia Pty Ltd.	Australia
Checkmarx India Technology Services Pvt. Ltd.	India
Checkmarx Singapore Pte. Ltd.	Singapore
Checkmarx Germany GmbH	Germany

Hosted Products / Services

Sub-processor	Location	Function
Amazon Web Services EMEA SARL	EU and UK; United States	Hosted Services Provider
LearnAmp (Rise to Limited)	UK and EEA	Training Platform

Support and Administrative

Sub-processor	Location	Function
Microsoft, Inc.	United States	Hosted Email Platform Hosted Services Provider
Ironscales Ltd.	EU	Anti-Phishing System
SFDC Ireland Limited	UK	CRM and Support Platform
Amazon Web Services EMEA SARL	EU and UK; United States	In-App Email provider
Sendgrid, Inc.	United States	Email provider
Mailchimp, Inc.	United States	Email provider
Momentive (Formerly known as SurveyMonkey)	EU	Surveys
HubSpot, Inc.	United States	Email and Customer Engagement
Ownbackup Ltd.	United States	Data Backups and Storage
CyberArk Software Ltd.	UK	Security tool for management of access to privileged accounts.
Gainsight Inc.	EU - Frankfurt, Germany	Customer Success and Product Experience Software

This list is subject to change from time to time and is current as of the date of this Agreement. The most recent list of sub-processors may be requested from Checkmarx by sending an email to support@checkmarx.com.

SCHEDULE 4
(STANDARD CONTRACTUAL CLAUSES)

MODULES 2 (C-P)

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation)[2] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in the Agreement (hereinafter each '**data exporter**'), and
(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in the Agreement (hereinafter each '**data importer**')

have agreed to these standard contractual clauses (hereinafter: '**Clauses**').

(c) These Clauses apply with respect to the transfer of personal data as specified in SCHEDULE 1 or as otherwise envisaged under the Agreement.

(d) The Schedules referred to in these Clauses form an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

[2] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 – Clause 8.1(c), 8.9(a), (c), (d) and (e);
(iii) Clause 9 – Clause 9(a), (e), (f) and (g);
(iv) Clause 12 – Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 – Clause 18(a) and (b).;

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, 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.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

(d) **UK interpretation rules:** Where these SCCs are relied on to satisfy the data transfer requirements under UK data protection laws, the following further rules of interpretation shall apply:

(i) "Regulation (EU) 2016/679" and "that Regulation" shall mean "UK data protection laws".
(ii) References to the “Union”, “EU” and “EU Member State” shall mean references the “UK”.

Clause 5 Hierarchy

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

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in SCHEDULE 1.

Clause 7 Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing SCHEDULE 1.

(b) Once it has completed the Appendix and signed SCHEDUE 1, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in SCHEDULE 1.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) Where applicable, the data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the data exporter and, where applicable, the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The data exporter and, where applicable, the controller, may give such instructions throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) Where applicable, the data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.[3]

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in SCHEDULE 1, unless on further instructions from the data exporter or, where applicable, the controller, as communicated to the data importer by the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including SCHEULE 1 as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in SCHEDULE 2 and personal data, the data exporter may redact part of the text of SCHEDULE 1 to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter as controller under Articles 13 and Clause 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in SCHEDULE 1. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and, where applicable, the

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in SCHEDULE 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority (and, where applicable, the controller so that the controller may in turn notify the competent supervisory authority) and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in SCHEDULE 1.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter and, where applicable, the controller, that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter and, where applicable, the controller.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request (including, where applicable, at the instruction of the controller), allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.

(d) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(e) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(f) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

at least 14 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in SCHEDULE 3. The Parties shall keep SCHEDULE 3 up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[5]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in SCHEDULE 2 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[6] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a) of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

[5] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[6] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b) the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in SCHEDULE 1, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[7];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request)

[7] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

indicating an application of such laws in practice that is not in line with the requirements in paragraph (a) The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and Clause 16(e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

Where applicable, the data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). Where applicable, the data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. Where applicable, the data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(f) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

These Clauses shall be governed by the law of, as applicable, the UK or one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the country where the relevant controller in relation to the personal data is established.

Clause 18 Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of England and Wales.

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the country of their habitual residence.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.