Data Processing Policy

1. Introduction and scope

Where Unit4 provides Services to its Customers, Unit4 will be acting as Processor and Customer will be acting as (or with full authority on behalf of) the Controller. This Data Processing Policy together with any applicable local addendum on the Unit4 Website ("**Policy**") sets out Unit4's commitments regarding Unit4's Processing of Personal Data of the Customer Data Subjects, as part of the provision by Unit4 of Services to its Customers.

This Policy applies to all Services provided by Unit4 to its Customers under Agreements executed on or after the effective date of this Policy. For the avoidance of doubt this Policy forms part of the Agreement between Unit4 and the Customer.

Unit4 Processes Personal Data on behalf of Customer in accordance with Data Protection Laws. Insofar as necessary, the Agreement will be supplemented with an addendum to the Agreement to set out any additional matters that are specific to Customer and cannot be regulated in this Policy, such Addendum to take precedence over this Policy in the event of any conflict.

This Policy does not apply to the collection of Personal Data through our website or through cookies with respect to which Personal Data Unit4 can be considered a Controller; we refer to our separate Privacy Statement and Cookies Statement for more information.

This Policy is available through the Unit4 Website. Unit4 reserves the right to update this Policy from time to time to reflect changes in practices and/or changes to applicable laws and regulations. Notwithstanding the foregoing, the version of the Policy that applies and will continue to apply to a particular Agreement will be the version of the Policy that is published on the Effective Date of the Agreement (subject to updates to the Subprocessors under section 5), unless amendments are required to comply with Data Protection Laws in which case Unit4 will notify the Customer of such changes and the most recent version of the Policy published on the website shall apply.

2. Definitions

The following terms shall apply in this Policy. Capitalised terms used in this Policy but not defined shall have the meaning given to such terms in Unit4's General Terms of Business.

Agreement	means any written contract, any written statement of work, or any other written binding agreement, including any annexes thereto, for the provision of Services by Unit4 to Customer;
CPA	means the Colorado Privacy Act 2021;
CPRA	means the California Consumer Privacy Act 2020 as updated by the California Privacy Rights Act 2023;
Controller	shall have the definition given to data controller by the GDPR;
Customer	means the counterparty to the Agreement with Unit4;
Customer Data Subjects	shall mean the former and current directors, officers and employees and customers of Customer or its Affiliates;
Data Protection Audit	means audits, including data protection compliance questionnaires, carried out by Customer or a third-party on behalf of Customer, with the objective to verify Unit4 compliance with the data protection obligations stated in the Agreement and this Policy;
Data Protection Laws	means, in relation to any Personal Data which is Processed in the performance of the Agreement and in each case only to the extent applicable, the GDPR together with all implementing laws and any other data protection, privacy laws or privacy regulations such as CPA, CPRA, FADP, FIPPA, PPDA, PIPA, PIPEDA, or VCDPA;
FADP	means the Swiss Federal Act on Data Protection revised and updated in 2023;
FIPPA	means, in each case to the extent applicable to the Processing, the Freedom of Information and Protection of Privacy Act, RSBC 1996;
GDPR	means, in each case to the extent applicable to the Processing: (i) Regulation (EU) 2016/679 ("**EU GDPR**"); (ii) as implemented in the United Kingdom by the EU (withdrawal) Act 2018 and as amended by the Data Protection Act 2018;
PDPA	means the Singaporean Personal Data Protection Act as amended by the Personal Data Protection (Amendment) Act 2020;
Personal Data	means any information relating to an identified or identifiable natural person which natural persons for the purposes of this Policy will be Customer Data Subjects;
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data;
PIPA	means, in each case to the extent applicable to the Processing, the Personal Information Protection Act, SBC 2003 enacted in British Columbia;
PIPEDA	means, in each case to the extent applicable to the Processing, the Canadian Personal Information Protection and Electronic Documents Act 2000;
Process, Processing	means any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation

and Processed	or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Processor	shall have the definition given to data processor by the GDPR;
Services	means services Unit4 provides to Customer under an Agreement;
Subprocessor	means any data processor appointed by Unit4 to process Personal Data on behalf of the Customer;
Unit4	means the Unit4 Affiliate that is the contracting entity to the Agreement; and
Unit4 Website	means www.unit4.com/terms being the website where Unit4 publishes its most up to date terms and conditions;
VCDPA	means, in each case to the extent applicable to the Processing, the Virginia Consumer Privacy Act.

3. Personal Data Processed by Unit4

The subject matter of the Processing is the performance of the Services. Further details of the Personal Data that will be Processed by Unit4 on behalf of Customer, including the duration, purpose and types and categories of Personal Data are set out in the Processing Information on the Unit4 Website.

4. Use of personal data

Unit4 shall not Process the Personal Data other than:

- as necessary to provide the Services and as described and authorised in the Agreement and/or in accordance with the documented instructions of Customer; and
- as required to comply with Data Protection Laws or other laws to which Unit4 is subject, in which case Unit4 shall (to the extent permitted by law) inform Customer of that legal requirement before Processing the Personal Data.

The Customer shall not instruct Unit4 to Process Personal Data in violation of Data Protection Laws. Unit4 will inform Customer if, in Unit4's opinion, an instruction from Customer infringes Data Protection Laws.

5. Subprocessing

Unit4 may appoint certain third parties, including Unit4 Affiliates, to provide (or assist in the provision of) part of the Services to Customer. By signing the Agreement, the Customer agrees that Unit4 may subcontract the Processing of Personal Data to those Subprocessors listed on the Unit4 Website, and agrees to the processing by the Subprocessors in the locations specified on the Unit4 Website. All Subprocessors are subject to appropriate data protection terms between Unit4 and the Subprocessor, which terms are to all material extents no less protective than those set out in this Policy. Unit4 will inform Customer in advance of any intended changes concerning the addition or replacement of Subprocessors and thereby give Customer the opportunity to object to such changes. If Customer does not object in writing within fifteen (15) days of receipt of the notice, Customer is deemed to have accepted the new Subprocessor. If Customer does object in writing within fifteen (15) days of receipt of the notice, Unit4 and Customer will discuss possible resolutions within a reasonable timeframe and without detriment to the Parties and to their compliance with each of their respective obligations set forth in the Agreement. If the Parties are unable to come to an agreement on possible resolutions within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Services which cannot be provided by Unit4 without the use of the objected-to new Subprocessor.

For the avoidance of doubt, where a Subprocessor fails to fulfil its obligations under the data protection terms, Unit4 shall remain liable to the Customer for the fulfilment of Unit4's obligations under this Policy.

6. Confidentiality and security

Unit4 shall keep the Personal Data confidential and will ensure its staff and Subprocessors are bound by the same confidentiality obligation. Unit4 shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk required pursuant to applicable Data Protection Laws and, where applicable to Unit4, shall take all measures required pursuant to Article 32 GDPR. In assessing the appropriate level of security, Unit4 shall take account of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. The applicable security measures are further described in documentation published on the Unit4 Website. Any subsequent versions of the documents shall be applicable to the Agreement and its content will be no less stringent than its previous version.

7. Co-operating with requests of Customer

Unit4 shall, upon request and to the extent required under Data Protection Laws, co-operate with requests of Customer that relate to the Processing of Personal Data. In particular Unit4 shall co-operate with requests that relate to Personal Data Breaches, Customer Data Subject rights, Data Protection Impact Assessments and audit rights as described below.

Customer Data Subject rights: Unit4 shall co-operate as requested by Customer to enable Customer to comply with its obligations with any exercise of rights by a Customer Data Subject in respect of Personal Data under Data Protection Laws, provided in each case that Customer shall reimburse Unit4 in full for all costs (including for internal resources and any third party costs) reasonably incurred by Unit4 performing its obligation to assist Customer in its compliance under this section.

Data Protection Impact Assessment: Unit4 shall provide reasonable assistance to Customer with any data protection impact assessments which are required under Data Protection Laws, including Article 35 GDPR, and with any prior consultations to any

supervisory or regulatory body of Customer which are required under Data Protection Laws, including Article 36 GDPR, in each case in relation to Processing of Personal Data by Unit4 on behalf of Customer and taking into account the nature of the processing and information available to Unit4.

Audit rights: On reasonable request and notice, Unit4 will co-operate in the conduct of any Data Protection Audit or inspection reasonably necessary to demonstrate Unit4's compliance with the processor obligations laid down in Data Protection Laws and this Policy related to the Agreement, provided always that this requirement will not oblige Unit4 to provide or permit access to information concerning: (i) Unit4 internal pricing information; (ii) information relating to Unit4's other Customers; (iii) any of Unit4 non-public external reports, (iv) any internal reports prepared by Unit4's internal audit function, or (v) any trade secrets and/or proprietary or otherwise confidential information. The Customer shall avoid causing any damage, injury or disruption to Unit4's equipment, personnel and business in the course of such Data Protection Audit or inspection. A maximum of one Data Protection Audit may be carried out under this section in any twelve (12) month period, unless the audit is following upon a Personal Data Breach caused by Unit4 in the same period. Data Protection Audits shall conducted be at Customer's cost and expense save to the extent that the Data Protection Audit identifies a material non-compliance by Unit4 with the requirements of this Policy.

The Customer's requests provided in this section 7 will be fulfilled in co-operation with and under supervision of Unit4's Chief Information Security Officer, Unit4's Data Protection Officer, and/or similar Unit4 local officials.

8. Deletion or return of Customer Personal Data

Unit4 will, at the choice of Customer, return the Personal Data at the end of the provision of the Services relating to Processing and then delete the Personal Data from its systems, or otherwise simply delete the Personal Data without returning a copy to Customer. Unit4's obligation to delete the Personal Data under this paragraph 8 will not apply to the extent that (i) any law including any Data Protection Law, statute, order, regulation, rule, requirement, practice and guidelines of any government, regulatory authority or self-regulating organisation that applies to the Services in the country where those Services are being provided, or (ii) a competent court, supervisory or regulatory body, require the retention of such Personal Data by Unit4. If no choice has been made by Customer within 30 days of the end of the provision of the Services, Unit4 will automatically delete the Personal Data.

9. Incident management

Unit4 shall notify Customer without undue delay after becoming aware of a Personal Data Breach, providing Customer with sufficient information to enable Customer to meet any obligations to report a Personal Data Breach under Data Protection Laws. Upon request by Customer, Unit4 shall fully co-operate with Customer and take such reasonable steps as are directed by Customer to assist in the investigation, mitigation and remediation of each Personal Data Breach, in order to enable Customer to comply with its obligations under Data Protection Laws such as Article 33(3) GDPR ("**Remediation Measures**"). If Unit4 or a Unit4 Affiliate has caused the Personal Data Breach, Unit4 shall bear its own costs of the Remediation Measures. If Customer has caused the Personal Data Breach, Customer shall compensate Unit4 for the reasonable costs incurred by Unit4 in relation to any Remediation Measures. The Remediation Measures shall: (i) be completed within a reasonable period after Unit4 has become aware of a Personal Data Breach, and (ii) be carried out within the regular business hours of the local office where the Remediation Measures are required to be taken.

10. International transfers of Customer Personal Data

Customer authorises Processor and its Subprocessor(s) to make international transfers of Personal Data in accordance with this Policy so long as Processor and/or Subprocessor(s) as applicable take(s) steps to ensure that such transfers are made in compliance with applicable Data Protection Laws (including making transfers on the basis of appropriate safeguards such as approved standard contractual clause agreements). At Customer's request, Unit4 shall inform Customer of the applicable basis for the cross-border transfer of the Personal Data.

11. Liability

The Customer warrants that all Personal Data made available to Unit4 for the purposes of provision of the Service has been and shall be Processed by Customer in accordance with Data Protection Laws.

Save for this section 11, the indemnities, liabilities and exclusions or limitations thereof set out in the Agreement, shall also apply to the obligations of the parties pursuant to this Policy and the Agreement, and in case of any conflict will prevail.

12. Contact us

If you have any queries about this Policy or about the privacy practices of Unit4 Group, please send an email privacy@unit4.com and be sure to indicate the nature of your query.