Unit4 Data Protection Policy

Information Security and Privacy Office

Contents

Document properties

Author	:	Information Security and Privacy Office
Approved by	:	René Bentvelzen - DPO
Version	:	1.2
Data	:	March 2021Classification : Proprietary

Introduction

This policy describes Unit4's approach within the Unit4 group to identify and control information security and privacy risks regarding the collection, storage, processing and removal of all data relating to Unit4 customers ("**Customer Data**"), whether or not those customers are past, current or prospective and whether individuals, sole traders, partnership or companies ("**Customers**"). This document is part of the *Unit4 Global Information Security Framework* and provides more detailed requirements to contribute in meeting the information security objectives of the *Global Information Security Policy*.

This policy is designed:

1. to reduce the risk to Unit4 in handling and processing Customer Data (i.e. reducing the risk that data is lost, including as a result of theft);

2. to establish auditable and demonstrable controls over handling and processing Customer Data;

3. to ensure compliance with statutory principles, including that Customer Data:

    a. is not retained for longer than is considered necessary to fulfil the purpose for which it was collected; and

    b. is not processed for any purpose(s) other than those for which it was collected; and

    c. to establish a common approach across the Unit4 group of companies.

Who does this policy apply to?

This policy applies to all Unit4 employees and contractors worldwide who are involved in collecting, processing and using Customer Data. It is important that all individuals comply with this policy in order to provide assurances to Customers that Unit4 takes appropriate steps when handling and processing Customer Data.

If you have any concerns or questions relating to this policy, you should speak to the Global Unit4 Data Protection Officer (DPO) who is located in Sliedrecht, The Netherlands:

Name: René Bentvelzen

Telephone number: +31882471777

Email address: dpo@unit4.com

Version control

Version	Date	Author	Summary of Changes
1.2	28-03-2019 02-03-2021	Kenney den Hollander	New house style, minor edits, made into a policy document

Policy

1. When should Customer Data be collected?

1.1 When migrated, stored or processed within a Software as a Service ('Saas') or Cloud environment managed by Unit4. Data ownership of this Customer Data will **NOT** transfer to Unit4. The Customer will remain the 'data controller' while Unit4 functions as the 'data processor'. Additional processor agreements will define the detailed role of Unit4 in processing and protecting this Customer Data.

1.2 It is Unit4's policy that collecting Customer Data, especially 'live data', should be a **'last resort'.** Unit4 should aim to only collect and process Customer data when it is vital to resolving a support or technical issue, executing an agreement with the Customer, or is required for product development, verification and/or validation.

1.3 It is Unit4's policy that the collection of 'sensitive personal data' (data that relates to an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health condition, sexual life, the commission or alleged commission of any offence or proceedings for any actual or alleged offence, the disposal of such proceedings, or the sentence of any court in such proceedings) **should be avoided.** If the collection of this kind of personal data is unavoidable, the data should be clearly marked as 'Sensitive' and subjected to additional safeguards.

2. How should Customer Data be collected?

2.1 If it is necessary to collect Customer Data based on one or more of the reasons mentioned in paragraph **1.2,** the Customer Data must be directly collected from the Customer and not from a third party (unless you have the consent of the Customer). To comply with this requirement, the following points should be considered:

1. Where possible you should request that the Customer submits 'test data' (i.e. not 'live data'). The type of data that is supplied should always be clearly indicated as 'Test Data' or 'Live Data'. You **must** gain email or an alternative form of **written confirmation** from the Customer that the Customer Data is 'test data'. If you are unable to obtain written confirmation, you **must** assume that Customer Data is 'live data'. You should -where practically possible- never accept data with live personal bank accounts or credit card details, and you should - where practically possible- request the Customers to scramble or remove such data before providing it to us.

2. Customers must always be informed of:

(a) The **purpose(s)** for which Unit4 is collecting and processing their data;

(b) The **identity of Unit4** as the 'data processor' for statutory purposes and how they may contact Unit4;

(c) How their data will be **stored** by Unit4;

(d) Their rights regarding the collection and processing of their data, including but not limited to, the **right of access,** the **right to rectification,** the **right to erasure,** the **right to data portability,** and the **right to object.**

3. When Customer Data is provided electronically, the aim must be to ensure that appropriate security measures are in place to protect the Customer Data when it is being

transferred from the Customer to Unit4. Such security measures include, but are not limited to:

(a) **Secure ftp** (file transfer protocol) methods. Support desk and Technical Services have appropriate means of providing this when required;

(b) **Removable media (e.g. CD/DVD/hard drive/tape media)** sent by secure or registered post; and

(c) **Encrypted e-mail** when other methods are not available, or for urgency on behalf of the customer.

4. Prior to accepting 'live data', permission **must** be sought from either your local quality manager (where applicable), your company manager, or the Global DPO.

5. You should always consider whether Customer Data will need to be transferred to other companies within the Unit4 group or other third parties (e.g. to provide a service request). If Customer Data needs to be transferred to another party, the Customer should always be notified and their consent **must** be obtained before the transfer takes place. **Sensitive data** (as described in paragraph 1.3) **must never be transferred** outside of the European Economic Area (EEA). For every change in the data transfer process, consent must be obtained from the Customer.

2.2 It is important to keep in mind that once Customer Data has been collected, it should only be retained by Unit4 for as long as there is a **business need** to retain it or as required under any applicable data retention periods. For every data processing process a retention schedule must be in place to ensure data retention occurs in accordance with the GDPR and other applicable laws. If you have any question regarding these data retention periods, please contact your local quality manager (where applicable) or the Global Data Protection Officer in Utrecht, the Netherlands.

3. Restrictions on the use of Customer Data

3.1 The use of Customer Data is bound to restrictions. Customer Data must:

1. Only be accessed and used when there is a specific business purpose to do so;

2. Not be:

(a) Used for electronic direct marketing (for example, by e-mail, fax, telephone and/or SMS) without having previously gained the Customer's **consent** to such use (With the exception of a legitimate interest for Unit4. Does it concern advertising mail to our customers? Then it also takes into account that direct marketing must be in accordance with the customer's expectations and thus with what this customer can reasonably expect in terms of offers)

(b) Used for your own personal purposes; or

(c) Shared with third parties (unless approved by the Customer)

3.2 When you have a business need to access and use Customer Data, you must:

1. Only use Customer Data for the **purpose for which it was collected**; and

2. Obtain consent if you need to use the Customer Data for a new purpose.

4. Retention of Customer Data

4.1 All Customer Data is to be deleted or returned to the Customer immediately following completion of the purpose for which it was collected, unless Unit4 is:

1. Expressly asked to keep it by the Customer; or

2. Required to keep the Customer Data in accordance with any applicable data retention periods. If you have any questions relating to these data retention periods, please contact your local quality manager (where applicable) or the Global Data Protection Officer in Sliedrecht, The Netherlands

4.2 Any Customer Data retained by Unit4 must only be stored in locked machine rooms (preferably in safes) and **must not** -where practically possible- be stored on Unit4 laptops or other mobile storage media.

5. Requests from Customers regarding Customer Data

5.1 When a Customer exercises his/her rights regarding the collection and processing of their data (**paragraph 2.d**), you **must** escalate any such request immediately to your local quality manager (where applicable), or the Global Data Protection Officer in Sliedrecht, The Netherlands.

6. General remarks regarding Customer Data outside of the office

6.1 It is Unit4's policy that Customer Data (whether that be 'live data' or 'test data') **must not be taken out of the office/off-site** on laptops, memory sticks, USB sticks, CD or other storage media without the **prior written permission** of both the Customer **and** your manager.

6.2 Where you have gained consent, you **must** ensure that:

1. The Customer Data and storage media on which it is held **is not left** in an unlocked car or unattended in a place where it could be viewed or removed by others; and

2. Any and all **security systems** on the storage media on which the Customer Data is held (such as password protection and disk encryption) **are activated.**