Telefónica UK Policy
Data Retention Policy

POLICY CONTROL PAGE

Policy Details:	
Policy Name:	Data Retention
Policy Category	**Information Policies**
Policy Number:	CDC/2016/01
Policy Contact:	Simon Carey
Policy Author Name:	*Tony Sparrow*
Role:	*Information Governance Manager*
Policy Owner Name:	*Eddie Short (on behalf of the Enterprise Data Committee)*
Role:	Chief Information Officer
Policy Approved by:	UK ExComm
Policy Approval date:	20 June 2016
Policy Effective date:	25 May 2018

Policy Overview:

Failure to apply this policy may lead to action under the employee Conduct, Attendance and Performance policy.

The Data Retention Policy defines which corporate records must be retained for legal, operational, scientific, or historical purposes and the retention period for each type of document or class of data. It should be read in conjunction with the Data Retention Schedule which specifies the retention periods.

It covers all forms in which data is held: Structured (e.g. database) and unstructured (e.g. documents, email or photographs) information as well as information stored both electronically (e.g. computer) or non-electronically (e.g. paper documents).

It applies to everybody at Telefónica UK – our people, contractors and third parties.

There is a confidential helpline if employees have any concerns about the misuse of information or data.

Telefónica UK will implement this policy through appropriate management and controls, and will periodically monitor compliance.

Preamble Statements applicable to all policies:

- To the extent that this policy may in any way conflict with the requirements of a Group policy, unless specifically stated, the Group Policy requirements will take precedence.
- We comply with all applicable laws and regulations while also adhering to our own internal policies.

Policy review requirements:	
Review period:	2 Years
Retention period:	Life of the Company (archive when superseded)
Next review date:	May 2020
Location where Policy located:	Information Policies
Policy Keyword Search	Information Retention Policy Data
Related Policies/Procedures	See Information Policy Framework

Change History			
Version	**Date**	**Changed by**	**Changes**
V 1	20/7/16	Tony Sparrow	First issue of new Policy replacing GC/2015/08 & 09
V1.1	14/03/2018	Tony Sparrow	Draft changes for GDPR
V1.2	16/03/2018	Tony Sparrow	Final changes for approval
V2.0	24/5/2018	Tony Sparrow	Published version following CDC Approval
V2.1	02/03/2020	Simon Carey	Addition of exception to policy statement

Introduction

Telefónica UK attaches particular importance to the retention of its data and that of its employees and customers. It is therefore vital that in accordance with this Policy, our people and existing and potential new suppliers have appropriate retention procedures in place.

Having a Data Retention Policy enhances the legal position of Telefónica UK Limited by defining the deletion and destruction schedule associated with specific documents and data.

Compliance with this Policy and the Data Retention Schedule will assist us to meet our statutory and regulatory obligations in relation to the management of information.

It is part of a wider framework of Information Governance policies designed to establish and enforce formal management controls over all Telefónica UK Information and Information Assets.

To the extent that this policy may in any way conflict with the requirements of a Group policy, unless specifically stated, the Group Policy requirements will take precedence.

We comply with all applicable laws and regulations while also adhering to our own internal policies.

Any exceptions or variations to compliance with this Policy must be recorded by the Information Governance Manager and approved by the Enterprise Data Committee.

Objective

The objectives of the Data Retention Policy are:

- To comply with applicable law
- To maintain confidentiality by storing fewer corporate records, and only keeping them ffor as long as necessary
- To prevent premature destruction of records that need to be retained for a specified period to satisfy legal and other requirements
- To reduce maintenance and record storage costs

Policy Statements

1) Any exceptions or variations to compliance with this Policy must be recorded by the Information Governance Manager and approved by the Customer Data Committee.

2) When preparing tender documents and/or negotiating contracts with third parties for services that involve retaining and managing Records, reference to this Policy will help ensure that consistent data retention obligations are met.

3) Records must be maintained according to the Data Retention Schedule. The intention is that only one copy of a record is retained, but ensure that before you destroy any records in circumstances where you believe multiple copies of a record exist that at least one copy (or the original) is retained.

4) Records should be kept only for the Retention Period unless they are subject to an approved Variation or exception, or the Suspension Procedure (see below); Records must be disposed of or destroyed once this period expires in line with the IT Security Policy.

5) Each department is responsible for maintaining its own Records and should liaise with Telefónica UK Legal and the Information Governance Manager before taking any step in relation to the management of its Records that differs from the regime defined by this Policy.

6) Suppliers and their subcontractors must have their own defined retention policy, which must be supported by documented retention requirements and procedures and which mirrors this Policy in all material respects.

7) Unless suppliers (where they act as Data Processors) have a legal obligation to do so, they should not retain Telefónica UK data after they have finished providing services to Telefónica UK.

8) All data sets should be logged in the Information Asset Register and assigned an owner, as covered in the Information Asset Ownership Policy.

9) Information Asset Owners should review data stored on their systems on at least an annual basis. If the data or system is classed as In Strictest Confidence or ALERT In Strictest Confidence, then it is recommended that reviews are conducted on a more frequent basis.

10) All data should be assigned an appropriate Privacy Marking to identify the associated level of risk– see the Telefonica UK Security Policy.

11) Encryption, Back-up and Disposal of information should be in accordance with the IT Security Policy.

12) Purge processes are mandatory for all applications and systems storing Personally Identifiable Information (PII) data.

Definitions and Interpretations

Telefónica UK stores, manages and processes different types of data. The following classifications have been used to structure this Policy:

Classification	Description	Examples	General Retention Period (see Schedule for variations)
Personal Data (sub-divided into)	Individuals can be identified from their data or via the data being linked with other information owned by a Data Controller.		
Customer Data	Personal data about an individual Customer used to enable and enhance their overall mobile experience.	- Customer Name - Mobile Number - Address - Date of Birth - SIM number - Email Address - Contact number - Security Q&A - Passwords - Customer web data - Driving Licence Number - Customer Invoices - Customer location data - Call Records	**Last Transaction + 12 Months**

Employee Data	Personal data about an individual employee recorded throughout their employment with Telefónica UK.	- Name - Address - Pay, benefits and tax - Pension - Driving Licence Number - Passport Information - National Insurance Number - Appraisals / Performance Review - Visa or Work Permit - Criminal Record Check - References - Training Record - Yammer conversations - Absence	**Employment Period + 6 years**
Non-Personal Data	Data that does not relate to an identifiable living individual. This includes aggregated data (combined statistical information about several individuals) and anonymous data (data that does not identify individuals on its own or in combination with other data).	- Machine to Machine Data - Qualitative data that has been anonymised - Anonymised samples of customers	**Up to 5 Years**
Financial Data	Records of Telefónica UK corporate, supplier, customer and employee financial transactions.	- Bank Statements - Corporate tax and VAT records - Annual audited financial statements - Payment and receipts - Supplier Accounts Payable Invoices - Customer Accounts Receivable Invoices - Employee Expense Records - Sales Ledger - Employee related/payroll tax records	**7 Years**
Corporate Data	Any information arising from Telefónica UK corporate operations excluding financial, personal and non-personal data. This includes data from procurement, legal, IT, property, sales and marketing, R&D, Environmental and Health and Safety.	- Management reports, designs and plans - Raw marketing information - Customer service statistics - Unpublished network topology - Unpublished network statistics - Policy and process documents - Contracts	**Life of the Company**

Refer to the Information Governance Policy for other definitions

Applicability

This is a Company Policy, in accordance with the classification established in the 'Rules for development and organisation of the governance framework', issued by Telefónica SA in January 2012.

This Data Retention Policy applies to:

- All Telefónica UK employees and its subsidiaries, contractors, 3rd party suppliers and their sub-contractors.
- All forms in which data is held: Structured (e.g. database) and unstructured (e.g. documents, email or photographs) information as well as information stored both electronically (e.g. computer) or non-electronically (e.g. paper documents).

Applications, systems or services that are not currently in compliance with the Telefónica UK Data Retention Schedule **need to be logged with the Information Governance Manager**. The information owner must apply reasonable effort in bringing the application in line with the Data Retention Schedule.

Failure to apply this policy may lead to action under the employee Conduct, Attendance and Performance policy.

Suspension Procedure

The following exception overrides the retention periods set out in this policy.
If you believe or are informed that Records are or may be in any way relevant to one or more of the following Suspension Events:

- contemplated or actual litigation or regulatory investigation;
- a data subject access request under data protection laws;
- a request for information in relation to the Freedom of Information Act;
- or an order for production from a regulatory or law enforcement body;

Then those Records must be preserved and not amended until the legal department determines they are no longer needed.

If you believe that a Suspension Event has arisen, you must contact Telefónica UK Legal and follow their Suspension Protocol.

Roles & Responsibilities

Telefónica UK has defined different roles and responsibilities when handling data. For more information, please see the Information Governance Policy.