Records Retention Code of Practice

Date: 10/05/18
Owner: Data Protection Officer
Version: 1.0
Status: Final

Table of Contents

Document Control

Change History

Status	Version	Author(s)	Date of Distribution	Reason for Change
Draft	v 0.1	Meera Karan		First Draft
Draft	v 0.2	Ross Garvey	12/01/18	Updated with Document Control
Draft	v 0.3	Ross Garvey	19/01/18	Updated with DPO revisions
Draft	v 0.4	Craig Gill	13/04/18	Updated with BU feedback
Draft	v 0.5	Craig Gill	16/04/18	Updated with DPO revisions
Draft	v 0.6	Craig Gill	30/04/18	Updated with BU feedback
Draft	v 0.7	Craig Gill	10/05/18	Updated with BU feedback
Final	v 1.0	Craig Gill	14/05/18	Final version signed of by DPO

Reviewers

Name	Role	Version
Tony Bentall	Workstream Lead - Generation	1.0
Arun Duggal	Workstream Lead – NNB	1.0
Dawn Fortune	Workstream Lead - Customers	1.0
Helen Whiteman	HR Work Stream Lead	1.0

Approvals

Name	Title/Role	Confirmed	Date	Version
Lisa Deverick	Data Protection Officer & Head of UK Group Compliance	Y	14/05/2018	1.0

Distribution List

EDF Energy			
Name	**Role**	**Business Area**	**Info Only /Review**
Sarah Farrant	Customers GDPR Project Manager	Customers	Info Only
Sapna Barodi	Governance Workstream Lead	CSF	Info Only
Gary Austin	Third Party Workstream Lead	CSF	Info Only
Jayanta Ray	IT Workstream Lead	CSF	Info Only
Kelly Gilmartin	Engagement & Communications Workstream Lead	CSF	Info Only
Glen Thorney	Programme Manager Generation	Generation	Info Only
Jeremy Bailey	Renewables Solicitor	Generation	Info Only

Overview

EDF Energy is committed to privacy and respecting the rights of those whose personal data we collect and use. Supporting good governance, confidentiality and privacy requires all of us to have an awareness of the rules over how long we must retain data, how long we are entitled to retain it and how it is maintained and managed.

Personal data (new and existing) should be managed from creation or receipt, through maintenance and use to eventual disposal. The period for retaining personal data is determined by its type, the reason we have collected it and legal basis we intend to process it.

This Code of Practice applies to all personal data processed by EDF Energy whether in physical form, on our IT systems or on approved third-party software.

Management of personal data in accordance with this Code of Practice will also ensure that we are better able to:

1. Carry out our business
2. Make informed decisions
3. Protect the information rights of our colleagues and other stakeholders
4. Provide an audit trail and continuity in our management and administration
5. Create an accessible and consistent source of information about our business & achievements

The retention periods for personal data that is common to all Business Units are set out in **Appendix 1** of this document.

Personal data means any information relating to a living individual who can be identified, directly or indirectly form such data. For example: names, email addresses, IP addreses and mobile phone numbers. Descriptions of individuals with sufficient specificity or opinions expressed in relation to them will also be considered personal data.

Records Retention Principles

This Code of Practice is governed by the following principles:

1. **Legal Retention** – we will comply with applicable law and company policies when storing records. For example, the Mandatory Privacy Principles.
2. **Managed Retention** – we will only store personal data for as long as we need to.
3. **Safe Retention** – we will store records in accordance with our company policies and Codes of Practice (for example, our Information Security Policy). Records must be stored appropriately for their classification and in a way that they can be easily identified.
4. **Destruction** – we will delete, destroy or put records beyond use at the end of their stated retention period.

Accountability

Each Business Unit (BU)/ Corporate Steering Function (CSF) is responsible for creating, maintaining and updating Retention Schedules for any records which hold personal data and which do not come within the categories set out in Appendix 1. Each BU/CSF is responsible for ensuring their employees manage records in accordance with this Code and the Retention Schedules including by providing appropriate training and guidance. Each BU/CSF is responsible for reporting to DPO on compliance with the Retention Schedules at stipulated periods. The Data Protection Officer (DPO) and its delegated BU points of contact shall undertake reviews of this Code of Practice to ensure it is up-to-date and continues to assist EDF Energy to achieve its ambitions.

Classifying Records

What is a record?

This Code of Practice applies to personal data records, which means recorded personal data in any form that is created, received or maintained for EDF Energy .

EDF Energy Document Marking

All records created or maintained by EDF Energy should be classified in accordance with the Security Code of Practice and Information Classification, Marking and Handling Process which can be found here.

Retention & Destruction Practices

Destruction Practices

Each BU/CSF will only maintain records for as long as it needs to. Once the applicable retention period expires the record will be marked for destruction in accordance with existing site procedures.

EDF Energy shall apply the following approach to these records:

1. **Physical records** shall be destroyed by placing in Confidential Bins or shredding, as per existing site procedures
2. **Electronic records** shall be destroyed by permanent deletion of data in electronic form or by putting the data beyond use such that it is no longer processed.

Destruction of any record which is subject to or likely to be relevant to a **legal claim** shall be approved by Legal prior to destruction.

Archives & Back-up Systems

Copies of records hosted either in archives or back-up systems that are readily accessible are also subject to appropriate destruction in accordance with the Code of Practice.EDF Energy shall apply the following approach to these records

1. **IT back-ups** – should follow the same procedure for Electronic records above, [consider which systems and media these back-ups are stored on]
2. **Historic databases** – should follow the same procedure for Electronic records above, considering the extent to which information, especially personal data, is stored in these databases and how secure they are or can be made. Consideration should be given to whether deletion is operationally possible

3. **Off-site archiving** – hard copy archives should follow the same procedure for Physical records above, consider the extent to which documents are archived and how their classification and relevant retention period can be identified.

Appendix 1: Record Retention Schedule for Records Common to All BUs/CSF

Record Type	Classification	Retention Period
Employee files (inc Payroll, benefits, health records, criminal check outcomes*)	Protect Private	Date of birth + 100 years
Employee Travel & Expense	Protect Private	7 years from entry Profiles purged 1 year from employment end data
External Job Applicants	Protect Private	1 year from final correspondence
Wifi Registration Details	Protect Private	1 year from creation
Third Party Curriculum Vitaes	Protect Private	1 year from receipt
CCTV	Protect Private	28 days from recording
Site Access – Access Gate Control Data	Protect Private	1 year from site entry
Site Access – Permanent Access	Protect Private	1 year from receipt of application
Site Access – Escorted Access	Protect Private	1 year after site entry
Physical Site Visitor Logs	Protect Private	2 years after site entry
Electronic Site Visitor Logs	Protect Private	1 year from site entry
Contract Management – General	Protect Commercial & Contracts	7 years from end of contract
Contract Management – Deeds	Protect Commercial & Contracts	12 years from end of contract
IT Performance Management - End User Computing Experience	Protect Private	1 year from capture
IT Operational Security Monitoring	Protect Private	3 years from capture

*please note that we only record whether the result of a criminal records check was satisfactory or unsatisfactory on an employee's file

Glossary of Terms

Word	Meaning
Sensitive Personal Data	Means special categories of personal data, the special categories include: ▪ Genetic data, Biometric data, Racial or Ethnic origins, Political Opinions, Religious Beliefs, Sexual Orientation
Data Controller	The Data Controller is an entity who (either alone or jointly or in common with other entities) determines the purpose for which and the manner in which any personal data are, or to be, processed
Processing	Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: ▪ Organisation, adaptation or alteration of the information or data ▪ retrieval, consultation or use of the information or data ▪ disclosure of the information or data by transmission, dissemination or otherwise making available ▪ alignment, combination, blocking, erasure or destruction of the information or data
DPO	Data Protection Officer
Put Beyond Use	Data has been 'put beyond use', if not actually deleted, provided that the data controller holding it: ▪ is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way ▪ does not give any other organisation access to the personal data ▪ surrounds the personal data with appropriate technical and organisational security ▪ commits to permanent deletion of the information if, or when, this becomes possible