Data Retention Policy

PHX031

Contents

Purpose Of This Policy

Phoenix recognizes the importance of maintaining accurate and relevant data while balancing the need for data privacy and security. This policy outlines the retention periods for different types of data and the procedures for their disposal when they are no longer required for business or legal purposes.

Scope

This policy applies to all employees, contractors, and third-party service providers who handle or have access to data owned or controlled by Phoenix. It covers all forms of data, including electronic, paper-based, and other media types.

Retention Principles

All data collected or generated by Phoenix shall be retained for the minimum period necessary to fulfil legal, regulatory, or business requirements.
Data retention periods may vary depending on the type and nature of the data, applicable laws and regulations, industry standards, and business needs.
Data shall be retained in a manner that ensures its confidentiality, integrity, and availability throughout the retention period.
Records shall be protected from loss, destruction, falsification, unauthorised access, and unauthorised release, in line with legal, regulatory, contractual, and business requirements

Data Categories

The following categories and table illustration outline the types of data and their corresponding retention periods. Note that these are general guidelines, and specific legal or regulatory requirements may supersede these periods.

Personal Data
Personal data, including but not limited to customer information, employee records, and financial data, shall be retained for a period as required by applicable laws, regulations, and contractual obligations.

Financial Data
Financial records, including invoices, receipts, and financial statements, shall be retained for a minimum period of six years from the end of the fiscal year in which they were created.

Operational Data

Operational data may include system logs, access logs, and security event logs to facilitate system administration, security investigations, and compliance monitoring, retained for a minimum period of three years. Internal meeting minutes, Customer agreements and correspondence shall have minimum retention periods.

Legal and Regulatory Data

Data that is subject to specific legal or regulatory requirements shall be retained for the period specified by the relevant laws or regulations.

Backup and Disaster Recovery Data

Backup and disaster recovery data shall be retained for a period necessary to meet business continuity and disaster recovery requirements, ensuring the ability to restore critical systems and data.

Data Disposal

Data that has reached the end of its retention period and is no longer required shall be securely disposed of using methods that render it unreadable and unrecoverable.
The disposal methods shall comply with applicable laws and regulations and take into account the sensitivity and confidentiality of the data being disposed of.
Secure disposal methods may include physical destruction, cryptographic erasure, or the use of professional data destruction services.

Phoenix shall maintain records of disposal activities as required by applicable laws, regulations, or internal policies.

Record	Provision	Category	Retention and Disposition
Details of Shareholder's meetings - minutes, decisions, resolutions, members, contracts, share allocations, etc.	Companies Act 2006	Operational	7 Years then destroy
Legal contracts, agreements, confidentiality or provision of services and NDAs	Limitation Act 1980	Operational	7 Years upon expiry then destroy
Credit Card Details	PCI DSS – Level 4	Operational	24 Hours from Successful Payment then removed from Live. Daily snapshot 32 days then destroy. Monthly snapshot 1 year then destroy. Yearly snapshot 2 years then destroy.
Complaints (internal and customer)	GDPR 2018, Quality Policy	Operational	3 Years then destroy.

Phoenix SOC Event Logs (Microsoft Sentinel)	Security Policy	Operational	Microsoft Azure – Log Analytics Workspace 90 days then destroy
M365	Security Policy	Operational	Daily snapshot 32 days then destroy. Monthly snapshot 1 year then destroy. Yearly snapshot 2 years then destroy.
SecurityHQ Event Logs (IBM QRadar)	Security Policy	Operational	90 days then archive Archive 275 days then destroy
Files (On-premise systems and files)	Security Policy	Backup	Daily snapshot 30 days Monthly snapshot 1 year then destroy
Backups and disaster recovery files (Data stored at disaster recover site)	Security Policy	Backup	2 days then destroy
Digital data files (Drive data)	Security Policy	Backup	Minimum 30 days then destroy
Tax and accounting records	Taxes Management Act 1970	Financial	7 Years then destroy
All information relevant for VAT purposes	VAT Act 1994 & HMRC Notice 700/21	Financial	7 Years then destroy
Purchase Orders, Sales orders & Invoices	Limitation Act 1980, Finance Act 1998, VAT Act 1994	Financial	7 Years then destroy
Income Tax and National Insurance records	The Income Tax (PAYE) Regulations 2003	Personal	7 Years then destroy
Payroll and wage records	Taxes Management Act 1970 and Finance Act 1998	Personal	7 Years then destroy
Maternity pay, and sickness records	Statutory Maternity Pay Regulations 1986 and Statutory Sick Pay Regulations 1982	Personal	3 Years then destroy
Employment contracts, training records, promotions, performance reviews for both permanent and temporary employees	Limitation Act 1980 and GDPR 2018	Personal	3 Years upon expiry then destroy
Information relating to pension payments	Retirement Benefits Schemes (Information Powers) Regulations 1995	Personal	7 Years then destroy

Job applicant letters, CVs, references	The Information Commissioner Employment Practices Code (Recruitment & Selection)	Personal	1 Year then destroy
Records relating to hours worked and payments made to workers	National Minimum Wage Act 1998 and National Minimum Wage Regulations 1999	Personal	3 Years then destroy
Accident Reports	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995/3163	Legal and Regulatory (H&S)	3 Years then review, if no longer needed destroy
Maintenance records, asset records, H&S inspections, property, and equipment management	Limitation Act 1980, Health And Safety At Work Act 1974, Energy Performance of Building Regs 2012	Legal and Regulatory (H&S, Environmental)	7 Years upon expiry then destroy
COSHH & Asbestos records	Health And Safety At Work Act 1974	Legal and Regulatory (Environmental)	50 Years then destroy
Waste Transfer Notes	Environment Protection Act 1990 and Waste Regulations 2011	Legal and Regulatory (Environmental)	2 Years then destroy

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original
ISC	2.0	25/09/2018	Revisions following review
ISC	3.0	10/10/2019	Revisions following review
ISC	4.0	11/11/2020	Addition Data Deletion Statement
ISC	4.0	09/09/2021	Reviewed / No changes
ISC	5.0	28/02/2023	Added details of maintenance and COSHH record retention
ISC	6.0	29/06/2023	Rewrite policy to align with Data Governance Manual and merged content of Digital Data Retention Policy PHX048 and Document Control Process PHX005

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	2.0	25/09/2018	Managing Director
Sam Mudd	3.0	10/10/2019	Managing Director
Sam Mudd	4.0	11/11/2020	Managing Director
Sam Mudd	4.0	09/09/2021	Managing Director
Clare Metcalfe	5.0	28/02/2023	Operations Director
Clare Metcalfe	6.0	14/07/2023	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 14/07/2023