Data Governance Manual

PHX127

Contents

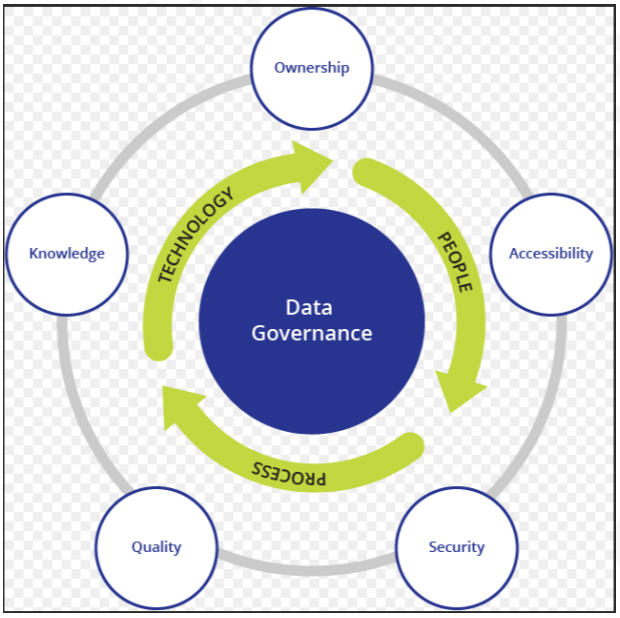
Purpose of the Data Governance Manual

Phoenix Software recognises the need for high quality data to drive innovation, sustain its growth plans and meet its customer needs. To achieve this Phoenix must ensure its business data and information is managed and used correctly throughout its lifecycle, in compliance with law, regulation and corporate policy. This includes from how data is created or collected, accessed, and handled, its quality, security, confidentiality, and retention to how it is archived, removed, or destroyed.

This manual aims to provide a comprehensive guide to establishing and maintaining an effective data governance program within Phoenix. It covers the key concepts, best practices, and actionable steps to ensure the correct management and use of data assets.

Through the orchestration of people, process and technology Phoenix sets out to manage its data assets by using roles, responsibilities, policies, and procedures to align with its business objectives so that it can be leveraged towards strategic goals. To accomplish this, Phoenix has developed a Data Governance Framework that sets out how its employees are required to manage data within the Phoenix enterprise.

Illustration 1.0 Data Governance Framework



Scope

This manual covers a comprehensive range of topics related to data governance throughout the Phoenix enterprise and applies to all employees of Phoenix. Topics including data policies and procedures, data protection, security, management and data governance metrics and monitoring.

Definitions

For this Manual, the following definitions apply. A further Business Glossary of terms has been defined and is available in Phoenix PowerBI

- **'Business Unit'** is a distinct segment of the Phoenix organisation, responsible for a specific set of products, services, or functions.
- **'Data'** is defined as 'words, numbers or images that need to be organised or analysed to solve a business problem.'
- **'Data asset'** represents the source data along with any associated metadata.
- **'Corporate data'** means all data collected, generated, or received by Phoenix for the purposes of operational or management information reporting.
- **'Data accessibility'** refers to the retrieval of data in an authenticated manner approved by Phoenix. This may be for the purposes of reading, modifying, copying, or moving data from a system*.
- **'Data domain'** is a set of data related to a particular business area such as HR, IT Services, Finance, Development.
- **'Data governance'** includes the people, processes and technologies used by Phoenix to manage and protect its corporate data assets including definitions for how Phoenix assigns accountability and control over the assets and their use.
- **'Data lifecycle management' (DLM)** is a phased approach to data and storage management that recognises that the value of information changes over time and that it must be managed accordingly.
- **'Data literacy'** is the 'ability to read, write and communicate data in context, including an understanding of data sources and constructs, analytical methods and techniques applied, as well as the ability to describe the use case, application and resulting value.
- **'Data quality'** refers both to the characteristics associated with high quality data and to the processes used to measure or improve the quality of data.
- **'Data security'** includes data confidentiality, data integrity, and data accessibility (See Data Security and Privacy below).
- **'Enterprise'** is used to qualify aspects of the Phoenix-wide network infrastructure, including its cloud-based solutions, and although not exclusively so, centrally managed by the Infrastructure Services team.
- **'Overlay'** is reference to subject matter experts that oversee the sales operations providing expert advice in multiple business.
- **'Personal data'** refers to the data covered by the UK General Data Protection Regulation when read with the Data Protection Act 2018. The Data Protection Laws outline principles for the collection and management of personal data. Application of the data protection principles, and other recognised standards and practices for data management provide a framework for assuring the accuracy, integrity, quality, and sustainability of institutional data assets.
- **'UK GDPR'** means the General Data Protection Regulation (GDPR) brought into UK law under the Data Protection Act 2018

Risks and Threats

Phoenix recognises the risks and threats associated with its use of data and has plans in place to mitigate against its key risks:

Data breaches

The risk of a data breach is a major concern for Phoenix, particularly in the handling and management of sensitive data such as personal information or financial data. Breaches can result in loss of reputation, legal liability, and financial costs.

Non-compliance

Failure to comply with relevant regulations and standards, such as GDPR can result in significant fines and legal consequences.

Data loss or corruption

Data loss or corruption can result in significant disruptions to business operations, as well as financial losses, reputation damage and regulatory fines.

Inaccurate or incomplete data

If data is inaccurate or incomplete, it can lead to incorrect business decisions being made, which can have significant consequences for the organization and its customers.

Unauthorized access

Unauthorized access to data can result in data breaches, identity theft, and other security risks.

Lack of transparency

Lack of transparency in data governance processes can result in mistrust from stakeholders, which can damage the reputation of Phoenix.

Insider threats

Insider threats, such as employees intentionally or unintentionally sharing or mishandling data, can pose a significant security and operational risk to Phoenix.

Cyber-attacks

Cyber-attacks, such as phishing or ransomware attacks, can compromise the security of data and result in significant financial losses and legal liability.

Third-party risks

The use of third-party vendors or contractors introduce additional risks around data governance, particularly if they have access to sensitive data.

Effective data governance

Involves identifying these risks and threats and implementing appropriate controls to mitigate them. This can include measures such as access controls, encryption, regular backups and archives,

and regular training and awareness programs for employees. Data risks are logged on the Phoenix Risk Register and reviewed at regular intervals.

Principles

Principles are a key element in the structured processes that collectively define and guide Phoenix, from values through to actions and solutions.

The principles denoted in Annex B shall be applied to the management of all corporate data within the Phoenix enterprise through each phase of the DLM and should also be applied to associated operational processes, goals, and staff training.

Exceptions to these principles must be documented, approved and visible, including allowing for exception handling (e.g. Data should be collected and recorded only once wherever possible without the need for multiple systems).

Roles and Responsibilities for Data Governance

All members of staff who interact with data at Phoenix have a role to play in the improvement of data completeness and accuracy in compliance with this manual. Certain groups and members of staff have roles defined with the governance framework, essentially forming Phoenix's data stewardship.

All defined roles in the stewardship shall have easily understood and unambiguous responsibilities and where applicable, these shall be incorporated into job descriptions to ensure they form part of the post rather than parallel activities.

An information life cycle recognises different relationships to data. Producers of data (whether people or systems) control the data they create. Data can be created for one purpose but used for other purposes by data consumers. Because data producers have knowledge of the purposes and functions of associated processes they own, they can modify processes to ensure they meet the needs of their data consumers.

Any person (or system) with access to data is by default a data consumer therefore data consumers comprise all Phoenix staff, whether they contribute directly to data collection or to editing data. Data consumers have a responsibility to follow established guidelines for accessing, sharing, and updating data as well as to participate in activities that define data for use.

Table 1.0 Roles and Responsibilities Matrix

Phoenix Data Stewardship - Roles and Responsibilities Matrix		
Role	**Responsible for**	**Who?**
Data Governance Committee (DGC)	Oversight and enforcement Conflict resolution Authoritative decision making	Managing Director Chief Data Officer (CDO) Operations Director Governance Manager
Data Protection Lead (DPL)	Supporting and reviewing of Data Governance policy and procedures Governance for the management of personal data and its lawful use, including sharing of personal data with external parties	Governance Manager
Data Owners	Managing, securing, and classifying data within their data domain Regulatory and policy compliance Approving data access	HR, Payroll and Facilities Manager Finance Director Head of Service Delivery Contracts Manager Marketing Manager Governance Manager Infrastructure Manager Business Unit Managers SAM and ITAM Manager
Data Stewards	Monitoring data quality and usage within their data domain Maintaining data standards Data auditing Managing data enquiries and resolving data issues	Sales Team Training Team Operations Team Marketing Team BI Team Finance Team Governance Team HR Team Service Desk Team SAM Data Manager
Data Custodian	Protecting the data from unauthorised access, alteration, destruction, or usage	Infrastructure Manager Chief Data Officer
Data Consumers	Creation and use of data in conjunction with this Manual Participating in resolution of data issues Consuming data only from authorised sources and identifying data that isn't authorised Identifying and reporting data issues to Data Owners	All members of staff

Accountability and responsibility for delivering activities defined in this policy lies within a core network of staff in data ownership and stewardship roles. **Annex C** provides a detailed list of responsibilities for the roles identified in this manual.

Data Security and Privacy

Security

For Phoenix to achieve its business objectives, data must be secured, yet readily available to those who need it. It is the responsibility of data owners to ensure that data accessibility is controlled, and that data has a classification in accordance with Phoenix information security policies. Technical security measures should match the requirements in accordance with the information classification.

In accordance with UK GDPR 2018, Phoenix has implemented security controls to meet regulatory compliance. Below is a matrix of GDPR requirements and the security controls Phoenix has in place to meet them:

Table 2.0 GDPR control requirements matrix

GDPR requirement	Article Ref	Description
Technical Measures	Art 28 (1)	Phoenix's accreditation to ISO 27001 and Cyber Essentials Plus comprises technical cybersecurity controls such as encryption, vulnerability management, logical and physical access management, secure disposal and MFA
Organisational Measures	Art 28 (1)	Organisational controls include Information security and other policies and procedures, business continuity plans, risk assessments, staff awareness training, reviews, audits and due diligence
Lawfulness of Processing	Art 6	Data Protection Impact Assessment (DPIA) are in place for processing activities where Phoenix act as the Controller. Records of Processing Activities (ROPA) are in place for processing activities where Phoenix act as a Processor The grounds for processing are included within the appropriate DPIA or ROPA
Legal data Transfer	Art 44	Legal data transfer details are documented within the Master Services Agreement between Phoenix and the customer.
Contract Compliance	Art 28 (3)	Data protection clauses are within contracts with customers.
Processing Records	Art 30 (2)	Record of Processing Activities (ROPA) is maintained.
Data Protection Officer	Art 37	Phoenix does not require a Data Protection Officer by law. A Data Protection Lead is appointed.
Sub Processing	Art 28 (2)	Sub-processors are subject to contractual controls with regards to data security – namely the clauses captured within the Master Services Agreement.
Breach Notification	Art 33 (2)	Notification requirements and processes are in place.
Subject Right Assistance	Art 28 (3e)	Subject access requirements and response processes are in place.
Data Sharing	Art 4 (7)	Data Sharing Agreements exist between Phoenix and other corporations where it is necessary to share data

Phoenix Software has been registered with the Information Commissioners Office (ICO) under registration no. Z4809807 since 4 July 2000.

Privacy

Phoenix employs a privacy by design, risk-based approach when initiating campaigns, projects or introducing new technology systems or developing existing ones within its enterprise. This ensures considerations are made for security and privacy compliance, data sovereignty, availability, and that contractual requirements are in place prior to implementation of any systems.

All new projects undergo a Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis, where risks shall be identified, and mitigating actions determined. Where necessary, a DPIA shall be performed and if required, a ROPA shall be registered and maintained.

Existing systems that require development work will be subject to the creation and approval of a functional specification record, signed off by the authorised, interested parties. These records include the identification of security risks and privacy impacts.

Phoenix Infrastructure Services is responsible for the adequacy and security of the Phoenix enterprise. The following network controls are in place:

- network devices default passwords changed
- access to the management consoles for network devices is restricted
- Wi-Fi connections in the office are securely protected from unauthorised access
- appropriate logging and monitoring is applied to enable recording and detection of actions that may affect, or are relevant to, information security

Privacy by design is also relevant to consultancy engagements with our customers in the design of solutions. As customers rely on Phoenix expertise to deliver production systems and environments, it is paramount these solutions are appropriate and secure. To ensure consultancy design work is of quality, assurance peer reviews take place on all design documents issued by Phoenix. Those authorised to provide peer-signature have all completed data protection training tailored to technical environment designs, the use of third-party toolsets, systems and organisation for service provisioning and off-boarding requirements to ensure secure data throughout any handover requirements.

Data Integration

Data integration involves the integration of data from various sources. Data stewards should determine the methods used for the formatting of data, including naming conventions, and transformation rules to facilitate the mapping and extraction of data from source to target systems within the enterprise.

Data validation rules and procedures should be created to ensure expected outcomes are achieved and exception and error handling is managed. recognises a six-phase lifecycle for data and has determined the activities and management controls associated with, and necessary for each phase.

Data Lifecycle Management (DLM)

Phoenix recognises a six-phase lifecycle for data and has determined the following activities and management controls associated with, and necessary for each phase:

Data Creation

Where data is created or generated within the enterprise. This encompasses activities by all Data Consumers such as data capture, data entry, data acquisition, or data ingestion from multiple sources:

- Data Capture: Surveys, Email and Phone Communications, Questionnaires, Interviews, Discussions, Observations, Research
- Data Entry: Inputting data into a system or database (manually or automated)
- Sensor data: Data generated real-time by monitoring systems
- Social media interaction: Posts, Likes, Shares
- Website interaction: Clicks, Searches, Form Submissions
- Machine learning training: Feeding data to machine learning algorithms to train them to make predictions or classifications (e.g. PowerBI)
- Customer transactions: Sales, Purchases, Refunds and Exchanges
- Financial transactions: Bank transactions, Investments and Payments

Data Storage

Storage encompasses the needs for security and data accessibility. This phase considers data classification and scalability:

- Data accessibility: Data owners must ensure data across the enterprise is accessible to users who need it when they need it. A storage solution must provide easy access to data that supports quick retrieval times
- Scalability: Storage can grow rapidly. The enterprise must scale to meet the needs of the business
- Security: Data security is a critical consideration, particularly when dealing with sensitive or confidential data. Data owners shall ensure the Data Custodian applies strong security measures, including encryption, access controls and classification in conjunction with Information Security Policy and GDPR

Data Transformation

Transformation encompasses the cleansing, visualisation, normalisation, and enrichment of data.

- Data cleansing: Data stewards at Phoenix should identify and correct errors in data, remove duplication and redundant data. Data formats should be standardised and structured and any data anomalies handled accordingly, including the correction of any missing data
- Visualisation: Includes the creation of graphs, charts, and other visual representations of the data, including the appropriate visualisations for the type of data and question being answered. This should also comprise of customisation and labelling to highlight important trends or insights and improve readability and understanding
- Normalisation: Data stewards should identify and remove any data redundancies and ensure data consistency across different sources. Data should be converted into a standard and recognised format and rescaled where necessary to a common range
- Enrichment: Includes the addition of new data to existing data sources such as demographic information or historical data. Data Consumers may combine data from multiple sources to create a more complete dataset and extract additional insights from the data. Using machine learning algorithms to generate predictions or recommendations based on the data constitutes data enrichment

Data Usage

Usage encompasses the day-to-day consumption of data by Phoenix Data Consumers, including data analysis and reporting.

- Data analysis: Data Consumers shall examine and interpret data to extract meaningful insights, identify patterns and make informed decisions. Statistical analysis may involve data mining, machine learning and visualisation. Data analysis shall be performed on all types of data and shall be used for different purposes including descriptive, predictive, and prescriptive analytics
- Reporting: Comprises the creation and presentation by Data Consumers of reports that summarise the findings of data analysis. Reporting shall take different forms, including dashboards, charts, graphs, tables, and written reports. The purpose of data reporting is to communicate the insights and conclusions of data analysis to stakeholders in a clear and concise manner, to enable informed decisions based on the data

Data Archive

Archive encompasses the data backup activities and the retention of data in conjunction with the Phoenix enterprise strategy and respective data domains.

- Data backup: Backup of the enterprise has been designed in conjunction with Phoenix's business impact analysis and assessment of critical business systems. Further detail on the enterprise backup strategy is found in Confluence
- Retention: The retention periods of data stored within the enterprise is determined by regulatory considerations, business need and risk and is held in accordance with the Phoenix Data Retention Policy

Data Destruction

Destruction of data occurs when data becomes obsolete and encompasses the secure removal of data and the methods used to accomplish it. The media types and means of destruction include:

- Digital and paper media: In conjunction with Phoenix information security policy, physical data shall always be destroyed by shredding, pulverising, or degaussing, ensuring the destruction renders the data permanently unreadable.
- Electronic media: Virtual data shall be deleted from electronic devices ensuring it cannot be recovered using standard recovery tools. Specialised software tools shall be used to securely erase data from removable storage media.
- A chain of custody shall be followed to create an audit trail including the date of destruction, the methods used and evidence of the destruction process

Data Compliance

Compliance enables Phoenix to leverage data in a responsible and secure manner while ensuring transparency and accountability in its data practices. Phoenix acknowledges the need to conduct its business ethically, to protect individuals' rights, maintain trust with its stakeholders, and mitigate legal and reputational risks associated with data handling. Further information can be found in the Phoenix Data Protection Policy, and in this Manual in **Annex F**

Data Audit

Regular audits of data help maintain its integrity, improve data-related processes, and ensure compliance, ultimately supporting effective data governance. As part of the Phoenix data governance strategy, data owners shall ensure their data is audited through assessments and examinations of six focus areas and making any recommendations to ensure data quality, accuracy, compliance, and security is maintained.

Data Quality

Assessing data completeness, accuracy, consistency, and timeliness. The audit may examine data profiling mechanisms, how data is cleansed, and validation processes that identify and rectify data quality issues.

Data Privacy and Compliance

Assessing whether an organization's data handling practices comply with UK GDPR 2018, including the review of Phoenix privacy policies, consent management procedures, data retention and deletion practices, and security measures. The audit aims to identify any gaps in compliance and ensure that appropriate safeguards are in place to protect personal data.

Data Security

Evaluates the security measures in place to protect data from unauthorized access, breaches, and vulnerabilities. Involving the review of access controls, encryption practices, network security, incident response plans, and employee training in conjunction with Phoenix policies. The audit aims to identify security weaknesses, ensure compliance with security standards, and recommend improvements to mitigate risks.

Data Governance Framework Audit

Assessing the effectiveness and adherence to Phoenix's data governance framework, including reviewing data related policies, procedures, and controls to ensure they are comprehensive, well-defined, and properly implemented. Auditing shall include roles and responsibilities, data stewardship practices, and the overall governance structure. Recommendations may be made to improve data governance practices and alignment with organizational goals.

Data Usage and Access

Reviewing data access controls and usage to ensure compliance with Phoenix information security policies and UK GDPR 2018. An audit may examine user permissions, access logs, data usage patterns, and data sharing agreements and aims to identify any unauthorized or inappropriate data access, ensure data usage aligns with business needs, and recommend improvements if required to enhance data access controls.

Data Retention and Archiving

Evaluating Phoenix's data retention and archiving practices, including reviewing data retention policies, archiving procedures, and compliance with legal and regulatory requirements. The audit may assess the effectiveness of data disposal processes, backup strategies, and data recovery plans. Recommendations may be provided to ensure proper data retention, minimize storage costs, and comply with UK GDPR 2018.

Data Governance Metrics and Monitoring

Regular audits of data help maintain its integrity, improve data-related processes, and ensure compliance, ultimately supporting effective data governance. As part of the Phoenix data governance strategy, data owners shall ensure their data is audited through assessments and examinations to ensure quality, accuracy, compliance, and security is maintained.

Key Performance Indicators (KPI's)

Phoenix recognises the need to measure and assess the effectiveness of its data governance activities and has identified the following KPI's based on its business objectives and organisational priorities. KPI data shall be collected, analysed, and reported using PowerBI

- **Data Security and Compliance**
  Measures the number of data breaches or data related security incidents
  To be defined

- **Data Availability**
  Measures the availability of data to authorised data consumers within Phoenix
  To be defined

- **Data Quality**
  Measures the number of data enquiries raised and issues consequently resolved
  To be defined

Continual Improvement

Continual improvement is recognised by Phoenix as a fundamental principle of effective data governance. By implementing a culture of continual improvement, Phoenix can enhance its data quality, strengthen data security, and maximize the value of its data assets.

To drive continual improvement in data governance, Phoenix shall encourage a feedback loop enabling stakeholders to provide input and suggestions for enhancement. Data owners shall seek feedback from data consumers, data stewards, and IT teams to identify pain points, challenges, and opportunities for improvement. Feedback enables Data owners to make informed decisions about prioritizing improvement initiatives and Phoenix to continually refine and optimize its data governance practices.

Audits shall evaluate data quality, data security, compliance adherence, and data usage patterns, providing valuable insights into the strengths and weaknesses of the data governance program, and enabling Phoenix to focus its improvement efforts.

Annex A – Characteristics of Data Quality

1. **Accuracy**
   - Data should provide a clear representation of the activity/interaction
   - Data should be in sufficient detail
   - Data should be captured once only as close to the point of activity as possible

2. **Validity**
   - Data should be recorded and used in accordance with agreed requirements, rules, and definitions to ensure integrity and consistency

3. **Reliability**
   - Data collection processes must be clearly defined and stable to ensure consistency over time, so that data accurately and reliably reflect any changes in performance

4. **Timeliness**
   - Data should be collected and recorded as quickly as possible after the event or activity
   - Data should remain available for the intended use within a reasonable or agreed time period

5. **Relevance**
   - Data should be relevant for the purposes for which it is used
   - Data requirements should be clearly specified and regularly reviewed to reflect any change in needs
   - The amount of data collected should be proportionate to the value gained

6. **Completeness**
   - Data should be complete
   - Data should not contain redundant records

Annex B – Data Principles

Table 3.0 Data Principles

Principle #	Name	Description
Enterprise Data Principles		
1	Data is an asset	Data has value and is managed according
2	Data is shared	Users require access to the data necessary to perform their roles and responsibilities, data is therefore shared across business functions and departments
3	Data is accessible	Data is accessible for users to perform their roles
4	Data is quality assured	Data elements have a recognised role for data quality
5	Data is protected	Data is secured from accidental or malicious access or alteration by unauthorised users through its lifecycle, at rest, in transit or in storage
6	Data is reused	Data is more valuable if it can be used or reused for more than one purpose. NOTE: Reuse of personal data as defined by the DP Act 2018, for a secondary purpose which is incompatible with the purpose for which the data was originally collected, is unlawful
7	Data is defined using common vocabulary	Data is defined consistently throughout Phoenix. Definitions are understandable and appropriately published
8	All data elements have ownership	Data elements, at business domain level, have a named data owner and ownership persists regardless of the use of that data through its lifecycle
9	All data elements have a master – a single source of truth	Every data element has a single known source of truth, a master data source
Data governance and management principles		
10	Data governance is everyone's responsibility	All data stakeholders contribute to data governance policies, their implementation and adoption
11	Data is understood	Data experts shall understand complex data
12	Data integrity is maintained	Use of data shall always be lawful across all decisions taken about the data
13	Data use is transparent	All parties using data or whose data is being used shall know how it is being used wherever possible. NOTE: There is an exemption in data protection terms for management forecasting and planning which allows for any data subject access requests or privacy notices surrounding that activity to be suspended
14	Data is audited	Data is available to audits and all decisions, controls and processes about data can be subject to audit
15	Data is managed by competent staff	Staff with responsibility for and access to data are appropriately trained and understand where their responsibility for data lies, including how to process or format data, and what to do in the event of a breach
16	Data is standardised	Rules and guidelines (such as data classification, privacy and availability arrangements) shall be followed to ensure data is standardised

17	Data use is maximised	Data is useable by anyone who needs it within approved and lawful limits to optimise impact
18	Data is controlled	Control procedures are in place to ensure data security. Procedures shall be followed for the creation, storage, validation, handling, sharing, updating, archiving and destruction of data in compliance with policy, relevant laws and regulations
19	Data is assigned a lifecycle status	All data elements have a lifecycle status assigned to determine if they are active, inactive or obsolete within lawful limits
20	Obsolete data is destroyed	Obsolete data is destroyed in accordance with regulation and policy
21	Data transfers are controlled	Data transfers between applications shall be undertaken using an approved, secure managed file transfer method
22	Data is distributed/published only using managed applications	Interfaces included Power BI and Reporting Services are used to distribute or publish data. Direct access to data tables is restricted. Ex
23	Sensitive data is identified, classified, and protected	Data that is sensitive, such as personal data is classified and protected in accordance with the Phoenix Information Security Manual
24	Data lineage is recorded and available	Data lineage provides important metadata for data consumers and should be recorded and available where needed

Annex C – Roles and Responsibilities in the Data Stewardship

The data stewardship comprises all staff who interact with data as part of their role at Phoenix Software. Every member of staff has a role to play in the improvement of data quality; however, certain members of the Phoenix team have ownership or stewardship responsibilities for the active governance and management of data.

Data governance committee
The DGC is responsible for the oversight and enforcement of the data governance practices with Phoenix consistent with organizational goals and objectives

Accountability: The DGC is accountable in ensuring the ethical use of and compliance with applicable laws and legislation.

In line with Phoenix requirements the DGC shall:

- Establish the data governance policies and standards, setting the expectations for data management, including data quality, privacy, security, retention, and use
- Develop the data governance framework for implementing data governance practices, including processes for data collection, storage, analysis, and dissemination
- Monitoring practices, including compliance with policies and standards, assessing risks, and identifying potential issues
- Resolve conflicts related to data management, including ownership, access, and quality
- Communicating with all stakeholders
- Reviewing and approving data-related initiatives such as projects or process improvements
- Assign classifications to data items depending on their sensitivity in accordance with
- Phoenix's Classification denoted in the Information Security Manual
- Authorise user access requests to master source data where there is legitimate need
- Monitor data quality in line with approved and published dimensions
- Support data stewards to analyse data quality issues and identify and fix root causes
- of poor data quality
- Provide training and guidance to employees and other stakeholders

Data owners
Data owners have responsibility for ensuring data is maintained to agreed quality standards.

Accountability: In line with principles and guidelines, data owners are accountable for the data management and governance activities in their data domains.

In line with Phoenix requirements the data owner shall:

- Champion compliance with the data governance policy
- Promote good data governance and data literacy in their business area
- Ensure consistency of approach in data collection, definition and sharing processes

- Maintain the principle of using 'master source' data wherever reasonably possible
- Support data profiling activities in support of business strategies and initiatives
- Maintain relevant entries in data dictionaries and local business glossaries
- Assign classifications to data items depending on their sensitivity in accordance with Phoenix's Classification denoted in the Information Security Manual
- Authorise user access requests to master source data where there is legitimate need
- Monitor data quality in line with approved and published dimensions
- Support data stewards to analyse data quality issues and identify and fix root causes of poor data quality
- Propose and manage data quality improvement activities
- Define and monitor data quality metrics
- Mandate changes to business processes and applications to improve data quality
- Propose new standards to improve data quality
- Escalate to the DGC if data quality issues cannot be resolved within a single domain
- Ensure the DGC has an accurate record of data stewardship assignments

Data stewards
Data stewards are caretakers of systems data and are responsible for various day-to-day processes to ensure data fulfils business requirements including the understanding of current and downstream use of data.

Accountability: In line with Phoenix principles and guidelines data stewards are accountable for local data usage in their data domains.

In line with Phoenix requirements the data steward shall:

- Serve as a first point of contact for colleagues with data domain queries
- Understand the purpose of all data within their data domain
- Train and coach system(s) users to understand and use data effectively
- Analyse data quality issues and propose improvements and/or solutions to data owners to eliminate root causes of poor data quality
- Follow agreed data management processes to manage data quality
- Support data owners to define and measure data quality metrics
- Manage approval processes for the use of domain data
- Adhere to the Phoenix Information Classification policy when using or providing data
- Propose new or amended data structures based on requirements for developments and initiatives
- Support the creation of conceptual data models and mappings
- Propose new standards to improve data quality
- Escalate to data owners if data quality issues cannot be locally resolved
- Support collaborative data governance and data literacy initiatives

Data consumers
Data consumers have responsibilities to participate in activities that define data for use.

Accountability: Data consumers are accountable for the proper usage of data as defined in this Manual and in Data Sharing Agreements.

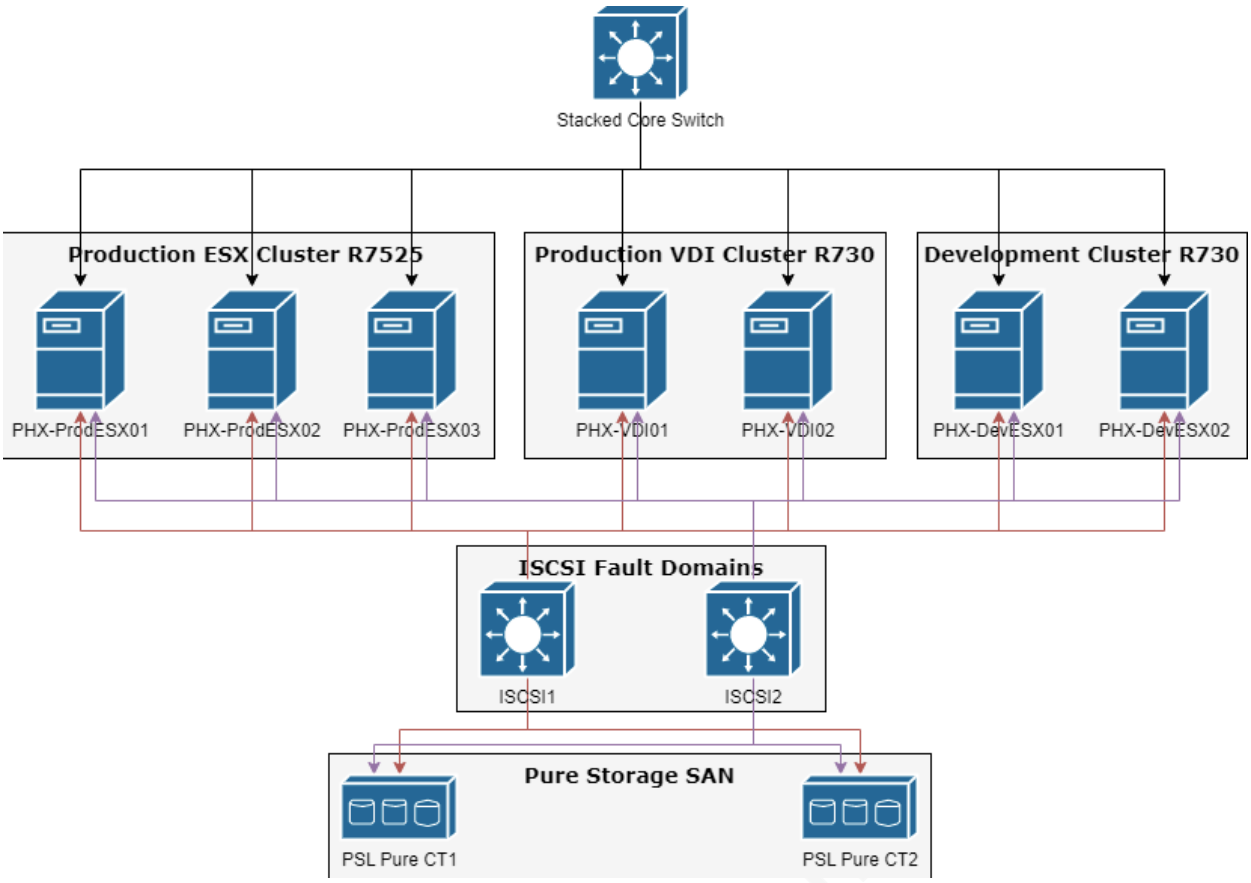
In line with Phoenix requirements data consumers shall:

- Participate in defining business terms and definitions to ensure usability within their business processes
- Participate in the identification of business rules, data quality rules, and data quality thresholds
- Participate in defining Data Sharing Agreements so they understand the authoritative source of data and any data constraints, such as security and privacy, for data usage
- Participate in the resolution of data issues as requested by data owners or their delegates
- Consume data only from authoritative sources identified by the DGC
- Identify data needs that are not supported by authoritative sources
- Identify data issues and bring them to the attention of data owners as soon as they are recognised
- Identify data control requirements that should be implemented by data owners to ensure quality and integrity in the data supply chain based upon the compliance requirements of the business processes

Annex D -Data Architecture

A good data architecture is essential for managing and controlling data assets in a consistent and organized manner. Phoenix has structured its enterprise and created standards for data management within its data domains, ensuring data is accurate, reliable, secure, and compliant with regulatory requirements

Illustration 2.0 Network Architecture



The Phoenix enterprise comprises the following primary data systems:

SharePoint Online (SPOL):
SPOL is used to manage data accessibility, in liaison with the Data Custodian, Data Owners shall allocate Consumers access to SPOL on a need only basis.

SAN storage (P: Drive):
All Data Consumers are granted access to P: drive by default

Oasis:
Oasis is a SQL Server to hold customer business and contact data and supporting sales and purchasing documentation.

HubSpot:
Application to support the generation of marketing leads and activities. in liaison with the Data Custodian, Data Owners shall allocate Consumers access to HubSpot on a need only basis

Sage Payroll:
Human Resources application to create payroll for all employees. High level access controls in place.

Access HR:
Human Resources application to store employee data. Accessed by HR and also by Consumers on different security access levels

In conjunction with Phoenix information security policy, all staff are prohibited from storing company data on personal devices or local drives.

Annex E – Phoenix Data Organisation

Guidelines and Procedures
Data Consumers should save customer and supplier data assets to SharePoint OnLine (SPOL). Data assets can include documents such as templates, contracts, agreements, tenders, quotes, statements, reports, general correspondence, procedures, and guidelines.

Within SPOL there is a structured system of Customer and Supplier data (thus avoiding duplication or isolation on P Drive, H Drive, OneDrive). Account Managers shall only have access to their designated Business Units, with Overlays having access to all based on their needs.

The Customer area is structured by Sector, Sub-Sector and then Customer. Under each Customer there are three separate folders, Bids & Tenders, Contracts & Agreements and General.

The Supplier area is structured by Building Services, Professional Services, and IT Suppliers. Under each Supplier there are three separate folders, General, Legal & Contracts, Price Lists.

If Data Consumers are unable to find a customer folder, first check for the correct vertical; use the "Search this library" function within the SharePoint site, and if necessary, create a new folder under the correct area by selecting 'New'. Once the customer or suppliers name is added, the folder structure shall automatically be created using Power Automate so Data Consumers don't have to manually create these.

Data Consumers should apply diligence to ensure a single source of truth on Phoenix customers. When creating new customer folders, avoid duplication by ensuring they do not already exist somewhere else, listed against their acronyms, or have been renamed because of acquisition or rebrand. Ensure top level folders do not exist against the same customer.

Benefits:
- Single centralised document management system giving a clear understanding of what work has been agreed and completed for a customer
- Improved sharing, collaboration, and document handling between departments and across the company, avoiding searching around for documents
- Improved information and document search capabilities
- Management and change control of documentation

The type of documents that should be saved is inclusive of but not limited to:

Table 4.0 Document Types

Bids & Tenders	- Final Tender Document (to be added after award decision is made to ensure the final version is saved - Proposals - Tender Questionnaires e.g. Brexit/COVID 19 - Cost Models

Contracts & Agreements	- Non-Disclosure Agreements (NDA) - Master Services Agreement (MSA) - Volume Services Agreement (VSA) - ELA Contracts - Signed Statement of Works
General	- Customer Org Chart - Customer Complaints/Satisfaction Letters - Managed Services Reports - Responses to Customer DataAccess Requests
General	- Supplier Policy Documents
Legal & Contracts	- Supplier Application Form - Goods And Services Agreement - Supplier Assurance Assessment - Non-Disclosure Agreements (NDA) - Commercial Agreements
Price Lists	- Price Lists

Best practice training videos are also available on LMS –

https://phoenixsoftware.sharepoint.com/sites/LMS365/SharePoint%20Online%20Demos?referrer=Course%20Catalog%20WebPart

Annex F – Phoenix and Data Protection

Definitions in accordance with the UKGDPR 2018

Table 5.0 UK GDPR 2018 DCDP Definition

Data Controller	Is a legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it. Data controllers are key decision-makers. They have the overall say and control over the reason and purposes behind data collection and the means and method of any data processing.
Data Processor	Is a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of a data controller.

GDPR statement

Here at Phoenix we take data protection and privacy very seriously and are committed to complying with the UK General Data Protection Regulation (GDPR). This statement outlines our commitment to protecting personal data and how we collect, process, and store it.

Data Collection:
We only collect personal data that is necessary for the purpose it is collected for. This may include names, email addresses, phone numbers, and other relevant information. We shall only collect personal data with the explicit consent of the individual, and we shall never sell or share it with third parties without explicit consent.

Data Processing:
We process personal data in accordance with GDPR regulations. This includes ensuring that the data is accurate, up-to-date, and processed lawfully and transparently. We use appropriate measures to protect personal data from unauthorized access, loss, destruction, or alteration.

Data Storage:
We store personal data for as long as it is necessary for the purpose it was collected for. We securely store data in compliance with GDPR regulations, and we have appropriate measures in place to protect personal data from unauthorized access, loss, destruction, or alteration.

Data Subject Rights:
Individuals have the right to access, rectify, or erase their personal data. They also have the right to restrict or object to processing, and the right to data portability. We shall respond to these requests in a timely and compliant manner.

Data Breaches:
In the event of a data breach, we shall notify the relevant authorities and affected individuals within the required timeframes. We shall also take appropriate measures to mitigate the impact of the breach and prevent future occurrences.

Further information:
Available on our website are our Data Protection notices. If you have any questions or concerns about our GDPR compliance, please contact us at gdpr@phoenixs.co.uk

Legal basis for processing data

A lawful basis shall always be determined by Phoenix Software prior to any personal data being processed. Personal data is processed under one, or more, of the following lawful bases:

- Consent – the individual has given their consent to the processing of their personal data
- Contractual – processing of personal data is necessary for the performance of a contract to which the individual is a party or for Phoenix Software to take pre-contractual steps at the request of the individual
- Legal Obligation – processing of personal data is necessary for compliance with a legal obligation to which Phoenix Software is subject
- Legitimate Interests – processing of personal data is necessary under the Legitimate Interests of Phoenix Software or a Third Party, unless these interests are overridden by the individual's interest or fundamental rights

The core business activities of Phoenix do not include the processing of personal data, the UK GDPR 2018, therefore has limited application, however the following areas have been identified and controls implemented to ensure appropriate management of this data -

Employee and Contractor information

As Data Controller and Data Processor, Phoenix collects, stores and processes personal data of its employees as denoted in the following table and in accordance with its Data Protection Policy.

Table 6.0 Personal Data Types

Personal Data	Data Type	Risk Category
Name	Personal Data	Medium
Date of Birth	Personal Data	Medium
Physical Address and Postcode	Personal Data	Medium
Job Role	Personal Data	Low
Drivers Licence Number	Personal Data	Low
Vehicle Registration Number - Optional	Personal Data	Low
Passport Number and Details	Personal Data	Medium
National Insurance Number	Personal Data	Medium
Visa Permit Number	Personal Data	Medium
Mobile Telephone Number	Personal Data	Medium
Email Address	Personal Data	Low
Next of Kin Details	Personal Data	Medium
Work Place	Personal Data	Low
Places of education	Personal Data	Low
Absence Record	Personal Data	Low
Accident Record	Personal Data	Low
Performance Reviews	Personal Data	Low
Payroll, Salary and Benefits	Personal Data	Low

Bank Details	Personal Data	High
Employment Records	Personal Data	Low
Security Question	Personal Data	Low
Complaints	Personal Data	Low
CCTV / Video images	Personal Data	Low
Hotel and Travel arrangements	Personal Data	Low
Loan arrangements	Personal Data	Low
External business interests	Personal Data	Low
Pension records	Personal Data	Low
Personal Assurance records	Personal Data	Low
Gender	Special Category Data	High
Ethnicity	Special Category Data	High
Religion	Special Category Data	High
Disability Information	Special Category Data	High
Sexual Orientation	Special Category Data	High
Philosophical Beliefs	Special Category Data	High
Dietary Requirements	Special Category Data	High
Health Adjustments	Special Category Data	High
Private Healthcare	Special Category Data	High

Processing of special categories of personal data is prohibited (GDPR Article 9 (1)), unless the data subject has given explicit consent. The special data category information held by Phoenix is optional information for the employee (data subject) to provide with the data subject being at no detriment should they chose not to provide the information.

Special category personal information is held for the purposes of reporting and statistical analysis of company ethics and diversity, or to ensure appropriate modifications have been made to assist individuals should they require it.

Phoenix = Controller
Phoenix = Processor
Legal grounds of processing: Contractual and legitimate interests

Business to Business customer contact information

Data includes name, business contact information, business address, employer.

This data is used to contact customers for sales and marketing purposes, and to fulfil contractual obligations with the customer. If applicable, this information is shared with third parties in the interest of contractual obligation, in which case the customer is aware. For example, for the purchasing of vendor software, customer contact information needs to be provided to the appropriate vendor for procurement and application.

Phoenix = Controller
Phoenix = Processor
Legal grounds of processing: Marketing – legitimate interest; Sales and Services – Contractual Obligation

Services data

Data includes name, business contact information, business address, employer, IP address

This data is used to perform the services procured by the customer organisation. This is customer-owned data. A Data Impact Assessment should be completed by the Controller (customer organisation) with the support of Phoenix as Processor.

Controller: Customer
Processor: Phoenix
Legal grounds of processing: Contractual obligation

In transacting with suppliers and customers as part of its daily operations, Phoenix is always processing personal data and is required to manage such data in compliance with the UK GDPR 2018, as Data Controller, Data Processor, or both.

The following are examples of common scenarios where Phoenix has regulatory and contractual obligations under the UK GDPR 2018 as a Data Controller or Data Processor:

- Phoenix provides a Managed Service to a customer directly. For example, Phoenix carries out a mailbox migration on behalf of Customer X

  Customer X = Controller
  Phoenix = Processor

- Phoenix engages a subcontractor to deliver a Managed Service to the customer **directly**. For example, a subcontractor providing a Managed Service to a customer directly, monitoring availability of physical assets of the customer. Phoenix are billing and liaison only. Contract between subcontractor and customer.

  Customer = Controller
  Subcontractor = Processor
  Phoenix = Processor

- Phoenix utilises an approved supplier to provide a toolset to support with the delivery of a Phoenix Managed Service to a customer. For example, Phoenix Managed Service involving data analytics provided by Supplier X.

  Customer = Controller
  Phoenix = Processor
  Supplier X = Sub-processor

- Phoenix engages a subcontractor to deliver a service to the customer **indirectly**. For example, a subcontractor providing a Managed Service for a customer **and Phoenix are contractually the main supplier** (Phoenix with no access to the customer environment data).

  Customer = Controller
  Subcontractor = Sub-processor
  Phoenix = Processor (regardless of access for processing, contract is with Phoenix under this arrangement)

- Phoenix engages a **subcontractor** to co-deliver a service to the customer **directly**. For example, Phoenix and a subcontractor are jointly responsible for deliverables within a service (Both have access to the customer environment data).

  Customer = Controller
  Subcontractor = Processor (if both parties are listed on the contract with the Customer for delivery of service and they aren't really a 'subcontractor' in the usual sense)
  Phoenix = Processor

- Phoenix engages with a **supplier to provide Phoenix** with a new service or application, For example, implementation of a new HR System

  Phoenix = Controller
  Supplier = Processor

Data Protection Impact Assessment (DPIA)

A DPIA is an essential tool for any organization to identify, assess and mitigate privacy risks associated with their processing activities, comply with data protection regulations, and build trust with their customers and stakeholders. Phoenix recognises that failure to conduct a DPIA where required can result in regulatory fines and reputational damage.

Phoenix has developed a supporting guidance document for its suite of Managed Services to assist both Phoenix and its customers in being able to conduct data protection impact assessments, either as Data Controllers or Processors.

Records of Processing Activity (ROPA)

Where Phoenix provides services to others it is acting as the Data Processor of any personal data it uses for those services. Under Article 30 of the GDPR Phoenix is required to keep some basic records of how that personal data is managed and protected and has therefore developed an asset register to record details of processing activity, found here: Phoenix Data Processing & Asset Register.xlsx (sharepoint.com).

Data Subject Access Requests (DSAR)

Individuals whose personal data is being processed, otherwise known as Data Subjects, might request a Data Subject Access Request (DSAR) for various reasons, such as:

- To verify the accuracy of their personal data: Data subjects have the right to request access to their personal data held by an organization. This enables them to check the accuracy of their data and ensure that it is up-to-date.

- To identify the purposes for which their data is being processed: Data subjects have the right to know why their data is being processed. By making a DSAR, they can obtain information about the purposes for which their data is being used.

- To obtain a copy of their personal data: Data subjects have the right to obtain a copy of their personal data held by an organization. This allows them to see what data is being held about them and how it is being used.

- To request rectification or erasure of their personal data: If data subjects find that their personal data is inaccurate or incomplete, they can request that the data be rectified or erased. This enables them to ensure that their data is accurate and up-to-date.

- To object to the processing of their personal data: Data subjects have the right to object to the processing of their personal data in certain circumstances. By making a DSAR, they can request that their data not be processed in a particular way

If any member of staff at Phoenix receives a DSAR request, the Phoenix DPL must be notified without undue delay and the following procedure executed:

1. **Acknowledge receipt of the DSAR:** When a Data Subject Access Request (DSAR) is received, acknowledge receipt of the request within one month as required by the UK GDPR 2018. This initial response should include confirmation of the request, any necessary identification verification, and information about how Phoenix plans to handle the request.

2. **Determine the scope of the request:** Review the request to determine the scope of the information requested. This may include reviewing your data inventories and records of processing activities to identify all relevant personal data.

3. **Identify potential exemptions:** Determine whether any exemptions apply to the request, such as if the disclosure of the information would impact national security or the rights and freedoms of others. Consult with legal counsel if necessary.

4. **Obtain consent and/or additional information:** If necessary, seek additional information or consent from the data subject to fulfil the request.

5. **Search for and collect the data:** Conduct a thorough search for the requested information, including any backup or archived data.

6. **Review and redact the data:** Review the data to ensure it does not include any third-party information or confidential business information that should not be disclosed. Redact any sensitive information as required by law.

7. **Prepare the response:** Prepare a response to the data subject that includes all the information requested, or an explanation for any information that cannot be disclosed. Provide the response in a format that is easy to understand, and in a way that does not infringe upon the rights of other individuals.

8. **Send the response:** Send the response within the time frame required by the UK GDPR 2018, which is generally within one month of receipt of the DSAR. If the request is complex or you need to request an extension, let the data subject know as soon as possible.

9. **Review and improve the process:** After responding to the DSAR, review the process and identify any areas for improvement. Use this opportunity to refine your procedures and ensure compliance with the UK GDPR 2018.

Annex G – Data Processing/Data Sharing Agreements

Data processing agreements set out an operating framework to enable lawful disclosure of information to, and data processing by the Data Processor working on behalf of the Data Controller, taking account of the UK GDPR 2018, the common law duty of confidence and other applicable legislation.

Phoenix has in place a standard Data Processing Agreement, to be enforced prior to any data sharing or processing with any other third party Data Processor.

Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all parties involved in sharing to be clear about their roles and responsibilities. Vendors should always be challenged on the benefits from sharing data, and the sharing of data should always be of value to Phoenix.

All business entities exchanging data with Phoenix shall be governed by contracts signed and agreed by the parties involved. This includes but is not limited to Phoenix & Customer; Phoenix & Supplier; Phoenix & Sub-contractor; Phoenix & Bytes.

Table 7.0 Types of Customer Agreement

Goods and Service Agreement	Governs data transfer between Phoenix and Suppliers
Master Services Agreement	Governs data protection between Phoenix and the customer for Professional and Managed services-only.

Personal data (PII) must not be shared without authorisation from the Data Protection Lead and guidance on contractual requirements should always be sought from the Contracts Manager.

For account mapping purposes, Phoenix **can** share:
- Organisation Names
- Company Domains

Phoenix **cannot** share:
- Personal identifiable information (email addresses, addresses, phone numbers names)
- Postcodes
- Spend revenue
- Spend margin
- Customer rankings
- Large volumes of data that could insinuate market share

Annex H – Personal Data Breach Notifications

Phoenix has developed a breach notification procedure to be followed by all Phoenix staff in the event of a data breach affecting personal data under the UK GDPR 2018. This procedure, supported by the Data Breach Flowchart, is intended to help ensure that all potential data breaches are identified, assessed, and reported in a timely and appropriate manner.

1. **Identification of a data breach**: All Phoenix employees and third-party contractors who have access to personal data must report any suspected or actual data breach to the Phoenix appointed Data Protection Lead (DPL) as soon as possible. A data breach can be any incident where personal data is accidentally or unlawfully destroyed, lost, altered, disclosed, or accessed.

2. **Assessment of the data breach:** Once a potential data breach is reported, the DPL shall head an initial assessment with the skeleton team (gdpr@phoenixs.co.uk) to determine if the breach is real and whether it is necessary to notify the Information Commissioner's Office (ICO) and affected individuals. The team shall consider the following factors when assessing a potential data breach:

    - The nature and sensitivity of the personal data involved
    - The potential risk of harm to individuals affected by the breach
    - The number of individuals affected
    - The likelihood of the data being misused

3. **Notification of the data breach:** If the team concludes that the data breach poses a risk to the rights and freedoms of individuals, the DPL shall notify the ICO within 72 hours of becoming aware of the breach. The team shall work with the relevant department heads to notify affected individuals as soon as possible. The notification to the individuals shall include:

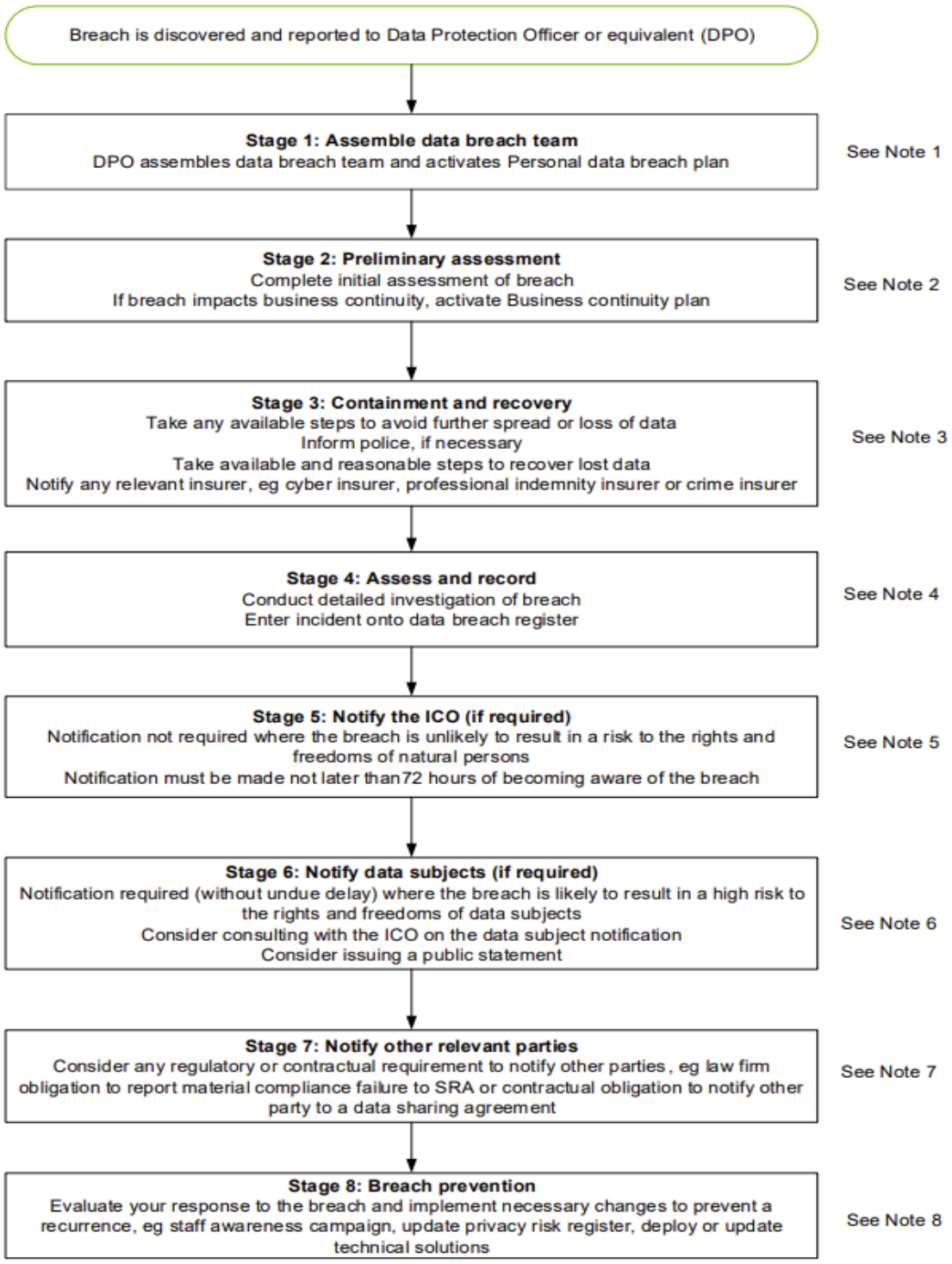
    - A description of the nature of the breach
    - The categories and approximate number of individuals affected
    - The likely consequences of the breach
    - The measures taken or proposed to be taken by the controller to address the breach and prevent future occurrences

4. **Record-keeping and reporting:** All data breaches shall be recorded in the organization's non-conformity log, regardless of whether they are notified to the ICO, or individuals affected. The Governance Team shall maintain a record of all data breaches, including the nature of the breach, the categories and approximate number of individuals affected, and the measures taken to address the breach.

5. **Training and awareness:** All employees and third-party contractors who have access to personal data shall receive regular training on their obligations under the GDPR. This training shall be provided during the onboarding process and regularly thereafter to ensure that all employees understand their responsibilities.

Data breach flowchart

Illustration 3.0 Data breach flow



Data breach – Stage Notes

Stage 1 - assemble data breach team
The first step is to assemble a data breach team. Consider who within the organisation would be best placed to react swiftly to news of the breach and who should be involved with the subsequent investigation. This shall often involve input from specialists across the business such as IT, HR and compliance/legal—and, in some cases, contact with external stakeholders and suppliers.

Precedent: A data breach plan encourages you to assemble a skeleton data breach team in advance of a data breach occurring, so you do not lose precious time working out what disciplines you shall need on your team.

Members of the Phoenix skeleton data breach team can be identified by expanding email distribution group gdpr@phoenixs.co.uk

Stage 2 - preliminary assessment
Conduct a very high level, preliminary assessment of the personal data breach so you can take steps to contain the breach and, if possible, recover lost data.

Stage 3 - containment and recovery
Take any available and reasonable steps to avoid further spread or loss of data. Inform the police, if the nature of the breach is criminal and inform company insurers without delay. Take available and reasonable steps to recover lost data.

Stage 4 - assess and record
Having dealt with containment and recovery, assess the risks associated with the breach, including:

- what type of data is involved?
- how sensitive is the data?
- who is affected by the breach?
- the likely consequence of the breach on affected data subjects?
- where data has been lost or stolen, are there any protections in place such as encryption?
- what could the data tell a third party about the data subject?
- what are the likely consequences of the personal data breach for your organisation?
- are there wider consequences to consider, e.g. loss of public confidence in an important service you provide or loss of legal professional privilege?

Document the personal data breach, including the relevant facts relating to it, its effects and the remedial action taken.

Stage 5 - notify the ICO (if required)
Notify the ICO of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. The only exception is where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This shall require some

sort of assessment of the severity of the data breach in advance of deciding about whether to notify (ref: Stage 4).

Notifications are made via the ICO's Report a breach page. This includes information about reporting the breach by telephone and/or using an online personal data breach reporting form.

Your report must include:

- a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
- the name and contact details of the data protection officer or other contact point where more information can be obtained
- the likely consequences of the personal data breach
- the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effect
- when and how you found out about the breach, and
- who else you have told

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The ICO expects organisations to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify the ICO of the breach when you become aware of it and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to the ICO, stating when you expect to submit more information.

Stage 6 - notify data subjects (if required)
Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, you must communicate the breach to those data subjects without undue delay. This is not subject to a long-stop of 72 hours as in the obligation to notify the ICO. In fact, the GDPR recitals state that data subject notification should be made as soon as reasonably feasible and in close co-operation with the supervisory authority (ICO), respecting guidance provided by it or other relevant authorities, such as law enforcement agencies. This suggests you should notify the ICO first before communicating with data subjects.

Note:
A 'high risk' means the threshold for informing individuals of the data breach is higher than for notifying the ICO. You shall need to assess:

- the severity of the potential or actual impact on individuals because of a breach, and
- the likelihood of this occurring

A risk shall be higher if the impact of the particular breach is more severe, or the likelihood of the consequence is higher.

In such cases, you shall need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

There are 3 situations under UK GDPR 2018 in which it is not necessary to notify the data subject:

- you have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption (assuming the encryption key is secure)
- you have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise
- it would involve disproportionate effort to notify the data subject(s)—you must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner

Where it is necessary to notify data subjects, the notification should include:

- the name and contact details of the data protection officer or other contact point where more information can be obtained
- the likely consequences of the personal data breach
- the measures you have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects

If you decide not to notify individuals, you shall still need to notify the ICO unless you can demonstrate the breach is unlikely to result in a risk to rights and freedoms.

Stage 7 - notify other relevant parties
You should also consider whether there are any other parties that should be informed, e.g.:

- are you under any other legal or contractual obligations to notify anyone else?
- if it was not necessary to contact the police at an earlier stage, has this changed?
- what about the media - are there any reputational issues and do you need to make a public statement?

Stage 8 - prevent future breaches
Once you have dealt with the data breach, you should take steps to review your data security arrangements and, so far as possible, prevent a recurrence. The data breach team should:

- establish what security measures were in place when the breach occurred
- assess whether technical or organisational measures could be implemented to prevent the breach happening again
- consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- consider whether it is necessary to prepare or update the organisation's Privacy risk register
- debrief data breach team members following the investigation

Annex I – Data Protection – Sales/Customer FAQs

Question:
Why doesn't Phoenix Software have or require a Data Protection Officer (DPO)?

According to the Information Commissioner's Office (ICO), the 3 criteria areas to determine whether an organisation is required to assign a DPO:

1: Is Phoenix Software Ltd a "public authority" (Freedom of Information Act 2000)/a "Scottish public authority" (Freedom of Information (Scotland) Act 2002)?
No, Phoenix Software Ltd is registered as a Private Limited Company at Companies House and therefore not a 'public authority' as defined above.
2: Does Phoenix Software Ltd carry out large-scale monitoring of individuals?
No, currently the products and services offered by Phoenix do not constitute a large-scale monitoring of individuals.
3: Does Phoenix Software Ltd carry out large-scale processing of special categories of personal data or personal data relating to criminal records as a core activity?
No, currently Phoenix does not, as part of its core activities, process special category personal data or personal data relating to criminal records.

Answer:
Phoenix does not have a DPO, it has an allocated Data Protection Lead (DPL).

Question:
What do I do if a customer contact asks me to unsubscribe their entire organisation?

Answer:
For Prospecting
A contact is within their rights to opt out/unsubscribe all contacts within their organisation. If you are asked to do this, you must action it. You can either do this on behalf of the customer (see below **Illustration 1.0 Opt-out and Erasure flow**), or share the unsubscribe link with the contact:

www.phoenixs.co.uk/unsubscribe
www.licensedashboard.com/unsubscribe

For Account Management
A contact is within their rights to opt out/unsubscribe all contacts within their organisation. However, if:

- You have a close working relationship with the account
- They are a current customer
- The unsubscribe seems unprompted
- The request was instructed from a junior team member

then check with a senior manager that they are authorised to make this decision on behalf of the whole organisation. Until the above has been resolved, you must unsubscribe the individual(s). If the senior manager advises that the whole organisation does not need unsubscribing, confirm this in an email to the customer so that we have an audit trail. A copy of this email should then be saved onto SPOL in the relevant customer folder.

If the senior contact advises that the whole organisation needs unsubscribing, then please request this via email to: **gdpr@phoenixs.co.uk** and **marketing@phoenixs.co.uk**

Question:
If a single contact from an organisation unsubscribes, do I need to unsubscribe all other contacts within that same organisation?

Answer:
No. Unless the contact specifically asks for the whole organisation to be unsubscribed, you don't need to unsubscribe all contacts within that organisation.

Question:
If a contact says, 'do not contact me again', can I try contacting them again another time as I may have just caught them at a bad time?

Answer:
No. If a customer says, 'do not contact me again' or 'please can I opt out', you must unsubscribe them to ensure they do not receive any promotional marketing material.

Question:
If my contact has unsubscribed, can I still contact them (email, phone, Teams) about an existing agreement/ contract, renewal?

Answer:
Yes, providing you are making contact strictly for those purposes. You must only discuss the contract, agreement, or renewal in question. If the contact wishes to discuss wider topics that is permissible, providing the customer has initiated the conversation. For traceability of any request made by the customer to provide information via email or Teams, create a written response 'further to our conversation and as per your request…'

Question:
If my contact has unsubscribed, can I contact them (email, phone, Teams) about new services, products, vendors etc?

Answer:
For Prospecting
No. You must not contact a customer outside the parameters of their contract, agreement, or renewal.

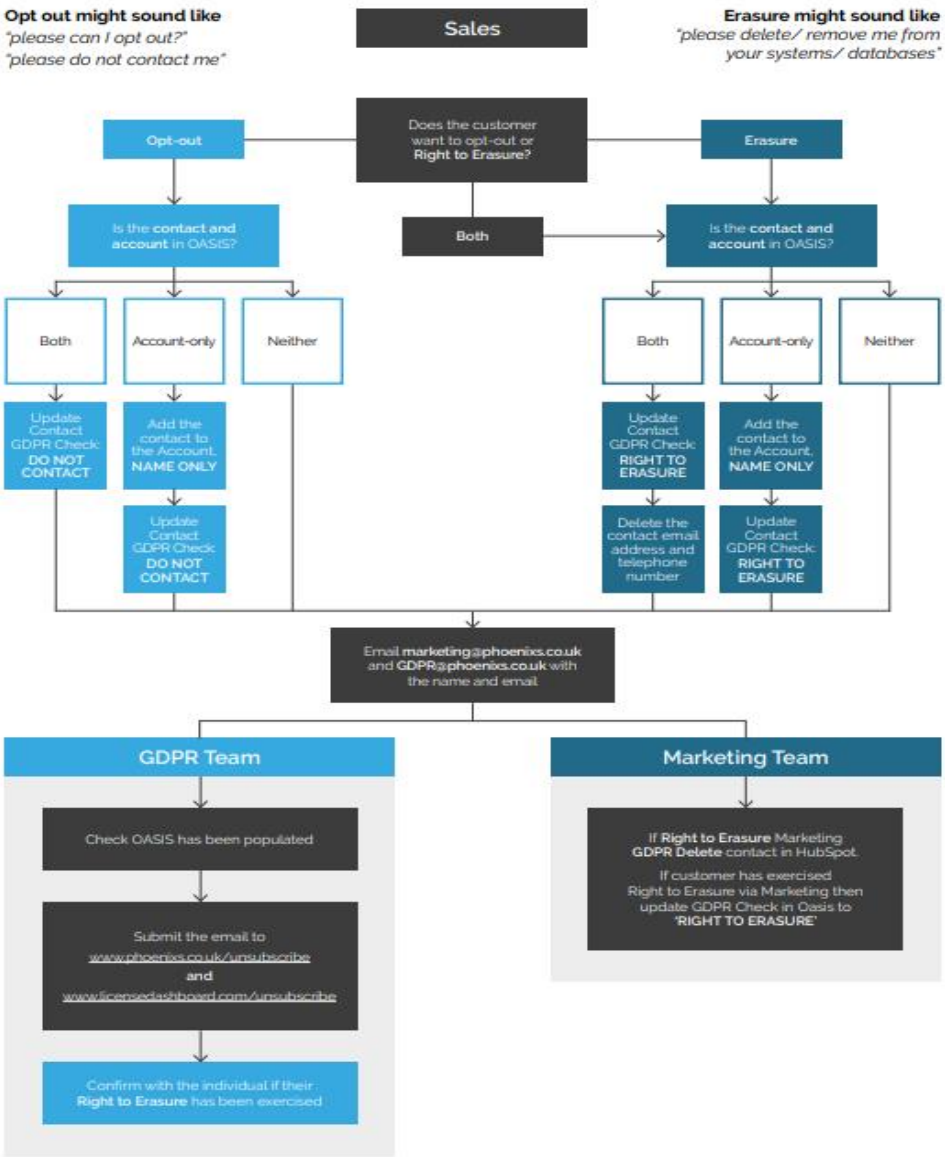
For Account management

Providing the contact is from an account that is a current customer and proactively buying, and you have a pre-existing and positively mutual relationship with the contact, then you can contact them regarding products or services that you think shall be complementary to their current infrastructure. If the contact is opted-out, but is receptive to your emails, you are able to ask them if they wish to opt back in to receive these communications from Phoenix by using the following copy:

Always stay up-to-date. Re-join our marketing communications - www.phoenixs.co.uk/subscribe

However, if the customer is not receptive to this kind of information, then you should stop contacting them regarding anything outside the parameters of their contract, agreement, or renewal.

Illustration 4.0 Opt-out and Erasure flow:



Annex J – Campaign Social Media Guidance

Phoenix recognises the risks associated with its use of social media platforms when sharing messages around events and campaigns and has produced guidance accordingly for personal data protection.

- If you are taking a photo in the offices, at an event, or a customer/ partner office, think Data Protection, please remember to:
  Ensure everyone is happy for you to share on social media if people are in the photo – this goes for using their image or sharing their names
- Do not include any confidential content on screens, notebooks, whiteboards etc. Please check and double check before posting. Confidential content includes names (customer or employees), any deals/ costs, email addresses, notes from meetings etc.
- If tagging a company or person in the post, please ensure it's the right account. If in doubt, check, ask, or don't include
- Use positive language and remember that while your account is personal to you, it's also connected to Phoenix Software
- Only use photos/ videos that you have permission to use – think about the rights of individuals under GDPR, copyright laws and don't just use images found on Google/ Bing. Make sure people are happy to appear in the photos – whether in the main area of the photo or the background
- When posting to social media and using a hashtag, please always title case each word. This aides with accessibility when it comes to readability:

    - #Whynotjointeamphoenix – this looks a mess and is hard to read
    - #WhyNotJoinTeamPhoenix – this is easier to read

- When posting something that you've done such as a volunteer day, taken your wellbeing hour, or taken part in a charity activity, please use our #TeamPhoenix hashtag. This is something we want to use for all posts connected to Phoenix and all of our employees, our values, our networks etc. so please include where you can. Please don't use for sales messages or webinar registrations etc. This will work across LinkedIn, Twitter and Instagram, and we also ask that you tag our Phoenix accounts by using the @ followed by our username (specific to the platform).

  When using a hashtag, try to only use them at the end of your message to make your post as accessible as possible

As a reminder, our accounts are as follows:

- LinkedIn - making customer and partner connections, sharing insights, webinars case studies etc.
    - https://www.linkedin.com/company/phoenix-software/
    - https://www.linkedin.com/company/license-dashboard/

- Twitter - brand awareness for webinars, resources, stats, quotes etc.

- https://twitter.com/PhoenixYork
- https://twitter.com/L_Dashboard

- Instagram - our values, charity work, our employees - NOT salesy etc.
  - https://www.instagram.com/phoenix_software/

- YouTube - hosting videos and clips we create to share with customers and partners
  - https://www.youtube.com/user/phoenixsoftwareyork
  - https://www.youtube.com/channel/UCD6V7le0h8nPszVGbB3tgLw

Version Control

Author	Version	Date	Description
Geoff McGann	1.0	13/04/2023	Original Document

Document Approval

Name	Version	Date	Position
Clare Metcalfe	1.0	30/05/2023	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 30/05/2023