



**CENTUM INVESTMENT COMPANY PLC**

**DATA PROTECTION AND PRIVACY FRAMEWORK**

**May 2025**

This Document is version controlled, all amendments to be tracked in the table below:

Version Number	Policy Date	Change Description	By:	Date of Approval	Effective Date
1.0	May 02, 2023				
2.0	May 2025	Initial updated & Combined Version	Parker Russell Eastern Africa LLP	11 July 2025	11 July 2025

## Content

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	Policy Overview .....	1
1.2	Purpose.....	1
1.3	Scope .....	1
1.4	Data Protection Privacy and Principles .....	2
<b>2</b>	<b>DATA PROTECTION, PRIVACY GOVERNANCE AND ACCOUNTABILITY POLICY.....</b>	<b>4</b>
2.1	Data Governance .....	4
2.2	Governance Structure.....	4
2.3	Roles and Responsibilities .....	5
2.3.1	Board Risk Committee .....	5
2.3.2	Business Teams.....	5
2.3.3	Enterprise Risk Function .....	5
2.3.4	Data Privacy Officers.....	6
2.3.5	Data Privacy Champions .....	7
2.3.6	Human Resource Officer .....	7
2.3.7	IT Team .....	7
2.3.8	Legal Function .....	8
2.3.9	Internal Audit .....	8
2.3.10	All Centum Staff .....	9
2.4	Personal Data Classification.....	9
2.5	Monitoring and Assurance .....	9
2.6	Data Privacy Risk Management .....	10
2.6.1	Data protection Impact Assessment (DPIA) .....	11
2.6.2	Data Minimization .....	13
2.7	Data Security - Technical and Organizational Measures .....	14
2.8	Data Subject Rights .....	15
2.8.1	Data Subjects Right (DSR) Business Specifications.....	15
2.8.2	Roles and Responsibilities .....	17
2.9	Third Party Risk Management.....	18
2.9.1	Outsourcing/Third Party Risk Assessment .....	18
2.9.2	Data Transfer/ Data Sharing .....	19
2.9.3	Third Party Monitoring .....	19
2.10	Incident and Breach Management.....	20
2.11	Data Breach Management .....	20
2.12	Data Lifecycle Management .....	23
2.13	Privacy by Design and Privacy by Default .....	24
2.14	Training and Awareness.....	26
<b>3</b>	<b>DATA PRIVACY STRATEGY .....</b>	<b>27</b>
3.1	Rationale.....	27
3.2	Pillars of Data Privacy Strategy.....	27
<b>4</b>	<b>REVIEW AND APPROVAL .....</b>	<b>29</b>
4.1	Review of the Policy .....	29
4.2	Approval .....	29

## 1 INTRODUCTION

### 1.1 Policy Overview

As the world around us grows more interconnected and technology-driven, the proliferation of data - including the personal data of each data subject is increasingly an issue of concern. Organizations need to protect data subjects' personal data, and to use and share such information in ways that are fair and ethical. Our clients deserve no less from us. In addition to this responsibility to our clients, we also have regulatory obligations to uphold, through which our compliance safeguards Centum's reputation.

Working at the Centum Investment Company PLC ("Centum") and its subsidiary entities may bring you in contact with the personal data of our employees, third-parties and/or clients. To safeguard the trust that has been placed in us as well as secure ongoing compliance, it is imperative that you follow our data protection and privacy framework including the supporting policies, standards, and procedures during all phases of personal data handling. Careful consideration of the information provided in this document and subordinate standards and procedures will help you fulfill your responsibilities of protecting our employees and client's personal data.

### 1.2 Purpose

The purpose of this policy is to establish client's and other stakeholders trust by ensuring ethical, secure, and compliant use of personal data in support and service to our stakeholders.

### 1.3 Scope

This policy focuses on 4 pillars of Privacy & Ethics, Quality, Security, and People as follows:

<b>Privacy and Ethics</b>	<p>Implementation of the Kenya Data Protection Act (DPA) and the data protection regulation is a key focus of Centum and its subsidiaries.</p> <p>At Centum our focus for privacy and ethics is:</p> <ul style="list-style-type: none"> <li>• Data protection by design.</li> <li>• Adequate risk management.</li> <li>• Empowering business to capitalize on data opportunities in a risk informed way.</li> <li>• Enhancement of Individual's rights.</li> <li>• Adequacy of data Sharing.</li> <li>• Fair and Lawful processing.</li> <li>• Incident Management.</li> </ul>
<b>Quality</b>	<p>Data quality defines how we manage our compliance to the provisions of data protection. As an institution we believe it is essential to maintain good data quality to identify and communicate with our stakeholders. To facilitate this, we focus on:</p> <ul style="list-style-type: none"> <li>• Adequacy of data capturing mechanisms.</li> <li>• Data validation through continuous audits of our systems holding personal data.</li> <li>• Necessity of data.</li> <li>• Continuous update of clients, employee and other stakeholders' personal data.</li> </ul>
<b>Security</b>	<p>Data protection is a key focus of Centum, and we strive to ensure effective security controls and mechanisms are implemented to meet the expected</p>

	<p>industry standards and the provisions of the data protection Act. As a business we focus on:</p> <ul style="list-style-type: none"> <li>• Monitoring and improving our security controls environment.</li> <li>• Investing in technology solutions that assure the security of the data we hold and process.</li> <li>• Addressing clients and other stakeholders' expectations around privacy and responsible data use.</li> </ul>
<b>People and Culture</b>	<p>Our staff play a great role in how as an organization we collect, process, and use personal data and we recognize that data governance maturity can only be truly realised where the processes and tools are fully embedded in the behaviours of our staff, in a sustainable manner.</p> <p>At Centum we focus on:</p> <ul style="list-style-type: none"> <li>• Enhancing the capacity of our people to build and promote the business culture to embrace security and privacy in all our operations.</li> <li>• Defining clear roles and responsibility in data privacy and building synergies in our operations.</li> <li>• Building trusted partnerships.</li> </ul>

#### 1.4 Data Protection Privacy and Principles

Centum and its subsidiaries shall ensure that personal data is processed in accordance with the following data protection and privacy principles:

1. **Adherence to the Right to Privacy** - Centum and its subsidiaries shall establish adequate controls to ensure the right to not have information relating to personal data unnecessarily revealed or infringed. Centum shall implement appropriate processes to ensure timely response to data subjects rights as applicable.
2. **Lawfulness, Fairness and Transparency**- Centum and its subsidiaries shall ensure personal data is processed lawfully, fairly, and transparently. A data subjects' personal data should not be processed unless there are lawful grounds for doing so and the data subject informed as to how and why their personal data is being processed either upon or before collecting it.
3. **Purpose Limitation** - any processing of personal data by Centum and its subsidiaries must be done for a specific, explicit purpose and only for additional purposes that are compatible with the original purpose. Any further processing should trigger additional customer consent process unless there is a legal basis such as fulfilling regulatory requests.
4. **Data Minimization** - Data collected should be limited to minimum data necessary for the purpose of collection only the categories of personal data chosen for processing by Centum and its subsidiaries must be necessary to achieve the declared overall aim of the processing operations.
5. **Data Accuracy** - Centum and its subsidiaries should ensure personal data is accurate and where appropriate, kept up to date. Incorrect data should be rectified as soon as possible. Centum shall develop a process for ongoing data update such as face to face on online portals for clients, staff, and other stakeholders to update their data.
6. **Storage Limitation** - Centum and the subsidiaries shall ensure that personal data is not kept for longer than is necessary.
7. **Data Integrity and Confidentiality** - Centum shall ensure appropriate technical or organizational measures are implemented when processing personal data to protect personal data against accidental, unauthorized, or unlawful access, use, modification, disclosure, loss, destruction, or damage.

8. **International Data Transfer** - When transferring personal data to a territory outside Kenya, Centum and its subsidiaries shall ensure effective due diligence and controls/safeguards are in place to ensure an adequate level of protection.

## 2 DATA PROTECTION, PRIVACY GOVERNANCE AND ACCOUNTABILITY POLICY

### 2.1 Data Governance

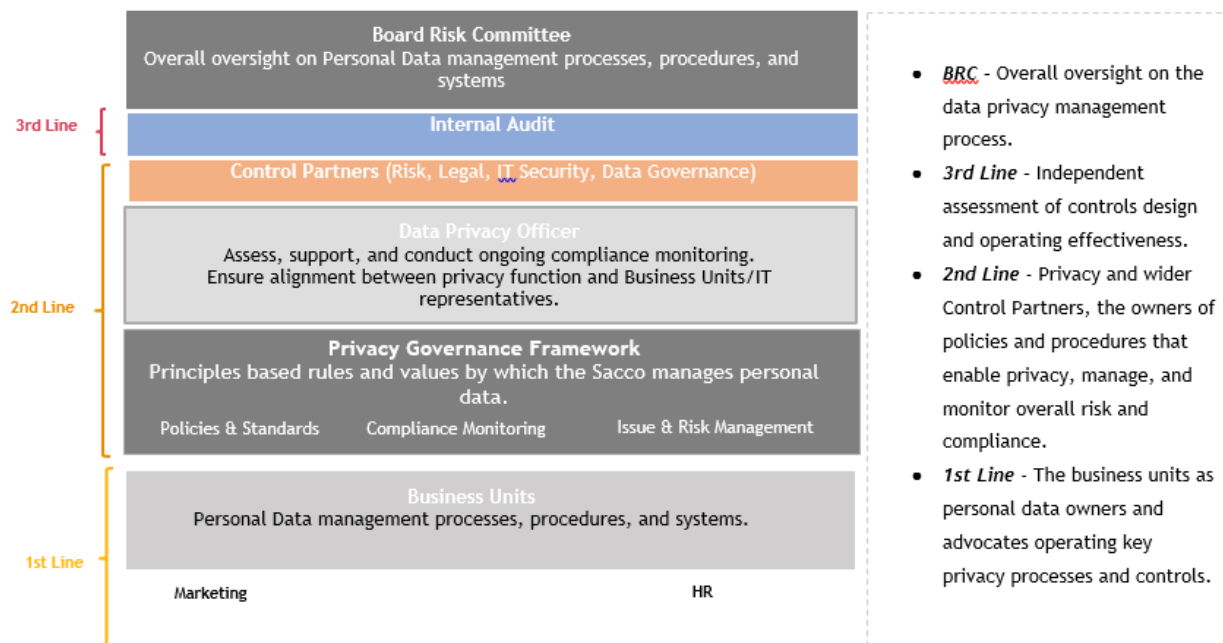
The Centum Investment Company PLC data governance defines Centum's data privacy vision including how the business manages the risks and opportunities arising from collecting, processing, and using personal data. At Centum data governance means:

1. Data can be onboarded securely at ease based on the right processing basis.
2. Policies are fit for purpose and regularly refreshed to reflect regulatory and best practices.
3. Data is owned, with accountability and responsibility assigned across the business.
4. Non-compliant data is proactively identified and remediated.
5. Technical and organizational controls are in place to protect personal data.
6. Data journeys/flows are understood, documented, and managed.
7. Data is only used for its designated purpose.
8. Only the right people have the right access to the data.

### 2.2 Governance Structure

Data protection and privacy is the responsibility of all staff, directors, and contractors and third parties of Centum. All parties must ensure the privacy of the personal data held by the business is maintained for its entire lifecycle.

The roles and responsibilities anticipated in this framework shall leverage on the 3 lines of defense governance structure and should be read in conjunction with the supporting policies which include IT policy, data privacy policy, data retention policy, risk management framework and other business specific policies affecting the collection, processing, storage, and destruction of personal data.



## 2.3 Roles and Responsibilities

### 2.3.1 Board Risk Committee

The Board Risk Committee shall:

1. Provide oversight and monitor governance on all matters relating to data protection and privacy.
2. Review and approve data protection and privacy standards ensuring the business practices remain aligned to the data protection regulations and best practices.

### 2.3.2 Business Teams

The various business functions shall:

1. Align on the strategic vision for personal data use and Centum strategy.
2. Provide line-of-sight into industry trends, planned projects, and areas of exploration involving personal data.
3. Provide support in aligning the business privacy strategy with the broader strategic direction and develop privacy as a brand differentiator for Centum.
4. Take overall accountability for awareness on the data privacy framework.
5. Institute and maintain procedures to ensure adherence to the data privacy standards and regulations.
6. Report conflicts or irregularities on data privacy management practices to the Data Privacy Officer to ensure alignment.

### 2.3.3 Enterprise Risk Function

1. Support the Data Privacy Officer (DPO) with implementation of Centum's Privacy Policy and related Governance.
2. Provide Privacy-related guidance to the business.
3. Train and provide guidance to the Privacy Champions on privacy processes and development /implementation of appropriate controls, e.g., guidance on data privacy impact assessments (DPIA's) and related recommendations. The aim is to support numerous Privacy Champions. There will be one Privacy Champion per major initiative involving personal data.
4. Lead the development of tailored privacy policies and role-based processes (and training, such as a clean desk policy) to both maintain alignment with Centum's overall data protection policy and considered businesses' unique needs.
5. Ensure appropriate responses to individual-rights-related requests (including redactions).
6. Support Internal Audit with privacy-specific compliance audits.
7. Support development of privacy materials and processes.
8. Develop privacy processes that are aligned with and leverage Data Governance processes, policies, and standards (e.g., data inventory and responsibilities of data stewards).
9. Lead training by delivering privacy training across the business.
  - a) Develop specialized role-specific training for business leaders and data stewards.
  - b) Provide training at the senior leadership level (privacy advisory and requirements for strategic initiatives).
  - c) Develop a short document with a summary of privacy guidelines on key topics (e.g., clear sets of privacy and data use. parameters for business to operate within, and defined methods of escalation should business operate outside of these parameters).

10. Provide Privacy by Design advisory through guidance/direction to the business at the early stages of an initiative.
11. Provide guidance on privacy-related processes, controls, and related communications.
12. Drive, own, and approve programs such as the Privacy Checklist and DPIA processes as part of project management, the Privacy Breach Management (including notices and communications) and consent language and processes.
13. Update and maintain privacy policies, frameworks, standards, procedures, and guidelines.
14. Support the DPO to conduct impact assessment to determine operational changes that may need to take place because of upcoming regulatory requirements. Facilitate workshops across relevant business unit leaders to determine impact.

#### 2.3.4 Data Privacy Officers

The data privacy officer shall:

1. Coordinate Privacy reporting to the Head of Risk and other relevant executives within the business.
2. Coordinate the liaison activities with the Office of the Data Protection Commissioner (ODPC).
3. Champion the Privacy program and oversee the development and maintenance of privacy enablers to ensure sustainment of the privacy program. Oversee the periodic development/updates of privacy enablers such as policies and standards.
4. Identify all regulatory obligations relating to data privacy, maintain a register of the regulatory universe and recommend to business units which controls they should build to integrate the data privacy obligations into existing practices and procedures.
5. Engage with internal and external stakeholders on data privacy matters.
6. Assess and report any material data privacy risks and data privacy breaches through the reporting governance structures.
7. Ensure that any data privacy breaches, or suspected breaches are reported to the Regulator within 72 hours as per the Data Protection Act guidelines.
8. Monitor and report on Centum's adherence to the data privacy standards.
9. Lead training by owning Privacy training across the Entity.
10. Provide Privacy by Design advisory through guidance/direction to the business.
11. Support the 1st line with standard processes by providing:
  - a) Direction regarding notice and consent processes and related communications.
  - b) Feedback as the ultimate decision maker for individual rights requests responses.
  - c) Direction on and owning the privacy component of Breach Management.
  - d) Oversight on and owning the Privacy Checklist and Data Privacy Impact Assessment (DPIA) processes.
12. Oversee the development of standard privacy and data protection contractual terms for vendors, and approval of any deviations from these privacy and data protection terms.
13. Monitor changes with a potential privacy impact, such as upcoming regulatory changes and requirements, new projects, or new or updated personal data handling practices. Identifies where a full DPIA may be required, directs the business in completing the DPIA, and then works with business units and their control partners to identify the impact and potential remediation required.



### 2.3.5 Data Privacy Champions

1. Champion privacy considerations and engender privacy awareness across their respective line of business or subsidiary.
2. Support their respective Business Unit and or subsidiary and the Privacy Officer with rollout and uptake of any new privacy-related policies, directives, standards and/or processes.
3. Provide guidance for their line of business on:
  - a) Centum's Privacy Policy considerations.
  - b) The DPIA process and executing efforts against related recommendations.
  - c) Personal data inventory maintenance.
  - d) Privacy control design.
  - e) Appropriate escalations to the Privacy Officer and/or beyond.
4. Provide strategic updates on data privacy on the scope of strategic initiatives early in the design phase for a clear intake process.
5. Engage Data Privacy Officer in the design of high-risk initiatives that use personal data. Invite the Data Privacy Officer to early design meetings and provide consultations on privacy risks during design.

### 2.3.6 Human Resource Officer

1. Track internal breach processes by identifying and escalating improper data sharing among Centum employees that results in privacy breaches.
2. Request advisory from DPO on inquiries for handling employee personal data if required.
3. Receive training from the Privacy Officer and attend the regular Privacy Forum meetings.
4. Champion privacy considerations and engender privacy awareness across HR.
5. Support Business Leads with rollout and uptake of any new privacy-related policies, directives, standards and/or processes.
6. Provide guidance for their line of business on:
  - a) Centum's Privacy Policy considerations.
  - b) the DPIA process and executing efforts against related recommendations.
  - c) Personal Data inventory maintenance.
  - d) Privacy control design.
  - e) appropriate escalations to the Privacy Office and/or beyond.

### 2.3.7 IT Team

The IT team shall:

1. Document and implement the necessary governance strategies to effectively embed data privacy principles on Centum's IT infrastructure.
2. Implement and manage technical security controls to ensure personal data held by the Centum is well protected.
3. Implement adequate infrastructure for internal and external facing operations to enable and give effect to effective data protection within the business.
4. Flag security gaps that may have privacy implications and support the DPO with decision-making related to implementation of data protection effort.
5. Work alongside the data privacy team to develop joint risk assessment and data gathering processes for new initiatives.
6. Ensure the information security governance framework is sufficiently robust to protect data given its criticality and sensitivity.

7. Develop and deploy role-appropriate enterprise and operational security education and training.
8. Evaluate security-related service providers and vendor products for compliance with the Entity data governance principles.
9. Ensure appropriate security safeguards are put in place to protect personal data (e.g., encryption).
10. Work to detect data security gaps that may impact Centum.
11. Support senior management with decision-making related to implementation of data protection efforts.
12. Monitor and report on efforts to address security issues and gaps through to their remediation.
13. Support stakeholders with the implementation of information security practices, the identification of specific needs, undertake related revisions and update of information security processes and implementation of supporting tools/automation where applicable.

#### 2.3.8 Legal Function

1. Provide legal interpretation and legal guidance to the Entity and the DPO.
2. Provide privileged support on privacy matters that have a litigation related risk.
3. Identify personal data and related processing activities that must be retained under “legal hold” and outside of any other retention/destruction policy.
4. Advise on complex third-party access requests (e.g., from authorities etc.).
5. Advise on documentation of third-party agreements where processing of or access to personal information may be involved.
6. Direct and manage compliance with court orders and other legal processes requiring disclosure of personal data.
7. Support the DPO in engagement related to the Office of the Data Protection Commissioner.
8. Advise on breach reporting requirements and responses to clients and other stakeholders.
9. Advise on privacy requirements for third-party contracts (e.g., reporting requirements of third-party providers).

#### 2.3.9 Internal Audit

1. Provide independent review and assurance of the effectiveness of governance, risk management and internal controls.
2. Review the data privacy framework and standards to confirm that the approach taken towards data privacy risk does not expose the Entity to compliance risk.
3. Review the data privacy framework and standards for consistency with the applicable laws and regulations relating to the processing of personal data.
4. Review, document, and report on the effectiveness of risk management in the 1st and 2nd lines of defense.
5. Recommend improvements in the day-to-day data controls framework.
6. Periodically report on the soundness of processes and controls.

### 2.3.10 All Centum Staff

All Centum staff/employees play a role in Privacy Governance, they shall:

1. Attend privacy-related training and understand the risks and penalties related to a real or potential breach of privacy obligations.
2. Understand the rights of individuals regarding their personal information and know how to respond to related complaints or requests.
3. Identify opportunities to leverage privacy to improve brand and clients' trust.
4. Know how to report any suspected privacy breaches (including any loss of their laptop, device or other confidential material that could expose personal data).
5. Understand and follow key Centum directives and policies implemented to protect personal including, but not limited to:
  - a) Maintaining a clean desk.
  - b) Not discussing personal data in unsecure locations.
  - c) Not duplicating data in emails, on spreadsheets, in documents, for ease of reference rather than use provided systems of record.
  - d) Obtaining Data Steward and Privacy Advisor approval to share personal data across businesses.
  - e) Transferring personal information using only Security-approved processes.

## 2.4 Personal Data Classification

Personal data shall be classified into 2 classifications as anticipated in the Data Protection Act. The 2 shall be embedded and linked back to the broader data classification embraced by Centum and its subsidiaries. The 2 classes are General Personal data and Sensitive Personal data.

SN	Classification	Data Included
1	General Personal data	Name, date of birth, country of birth, national ID no, service ID no, email address, residential address, telephone number.
2	Sensitive Personal data	Data revealing the natural person's race, health status, ethnic and social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the data subjects' children, parents, spouse or spouses, sex, or sexual orientation.

Employees who process either general personal data or sensitive personal data must ensure that it is appropriately labelled to show its classification level. General personal data or sensitive personal data must be handled in accordance with its classification throughout its lifecycle.

## 2.5 Monitoring and Assurance

Adherence to the privacy framework and policies must be independently monitored. Monitoring must include assurance on the implementation and compliance with the Entity's privacy policy and standards.

Monitoring and assurance must cover, among others:

1. Adequacy and effectiveness of controls which may relate to People, Process and Technology supporting personal data.
2. IT systems, databases, applications, cross border transfers, third parties processing personal data.

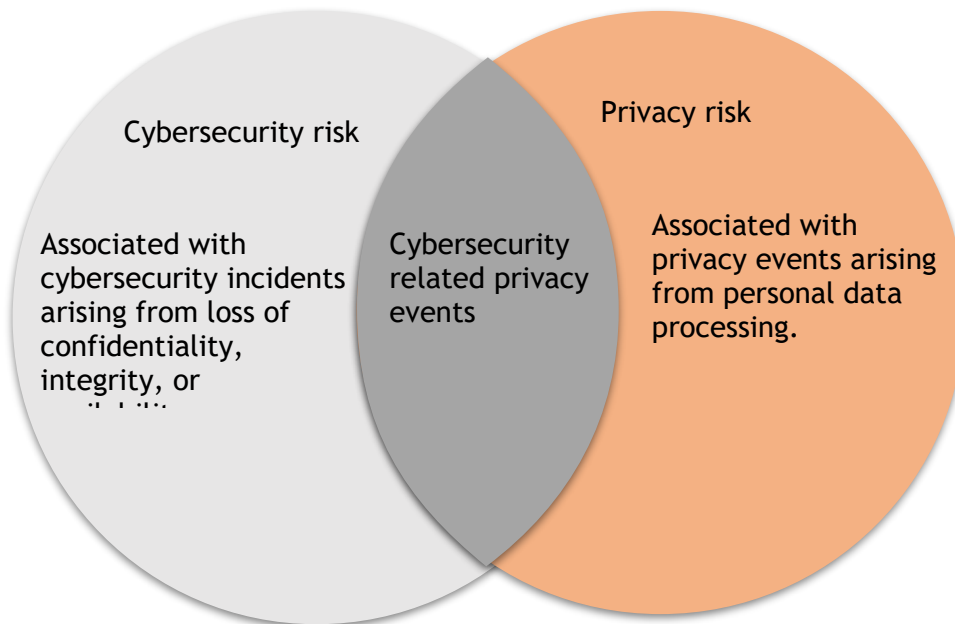
3. The effectiveness and appropriateness of corrective actions taken in relation to non-adherence to privacy policies and data protection regulations.

Data Privacy risk may have an independent assessment performed annually and depending on the merits of each privacy incident may also have an independent assessment performed in response to such privacy incident. The monitoring and Assurance reports must be submitted to the management team before submission to the Board Risk Committee with the eventual tabling to the main Board.

## 2.6 Data Privacy Risk Management

The Privacy Framework approach to privacy risk is to consider privacy events as potential problems the business, clients and staff could experience arising from system, product, or service operations with personal data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal.

The business recognizes that cybersecurity risk framework contributes to managing privacy risk however it's not sufficient as privacy risks can also arise by means unrelated to cybersecurity incidents hence the business approaches privacy risk management as a blend of cybersecurity and privacy risk management practices as illustrated below.



Data privacy risks may arise as an adverse effect of data processing conducted by the business or the third parties as it seeks to meet its mission or business objectives leading to adverse effects to the rights of data subjects.

The business also recognizes that risks to data subject rights can arise simply from clients and staff interactions with systems, products, and services, hence privacy risk management is a key factor in data handling and processing practices.

The privacy risk management process shall seek to identify the likelihood and impact of any actions arising from the processing of personal data that could cause an adverse effect on either the business or the data subjects.

The business shall manage privacy risk at the Enterprise Risk Management level by integrating the privacy risk management practices with the ERM framework steps for:

1. Risk assessment - identification, analysis, and evaluation
2. Risk treatment practice
3. Recording and reporting
4. Monitoring and evaluation
5. Communication and consultation

The approach will ensure Centum brings the privacy risk into parity with other risks being managed in the broader risk portfolio.

This will help:

1. Drive risk linkage from problem arising from data processing to individuals (direct impacts such as financial loss, discrimination) to the business (resulting impacts e.g., clients abandoning products, reputation damage, noncompliance costs).
2. Drive more informed decision making on resource allocation to strengthen the privacy program.
3. Drive privacy risk management as a cross-functional set of processes that helps the business understand how its systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks.
4. Create information that can help the Entity weigh the benefits of the data processing against the risks and to determine the appropriate response.

### 2.6.1 Data protection Impact Assessment (DPIA)

Section 31 of the Data Protection Act requires a DPIA to be undertaken when a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context, and purposes.

A DPIA shall be done prior to the processing and includes:

1. Description of the envisaged processing operations and the purposes of the processing, including (where applicable) the legitimate interest pursued by the data controller or processor.
2. Assessment on the necessity and proportionality of the processing operations in relation to the purpose.
3. Assessment of the risks to the rights and freedoms of data subjects.
4. Description of the measures to be put in place to address the risks.

The DPIA process is not designed to be an onerous task, it seeks to offer a variety of benefits to the business, such as:

1. Identify privacy risks at an early stage helping to embed safeguards following the privacy by design model.
2. Providing insight into areas where data collection can be minimized, and processes can be simplified.
3. Enhancing informed decision making.
4. Increasing trust amongst consumers, employees, contractors, and the public by increasing transparency and demonstrating that the business takes privacy seriously.

A DPIA shall be conducted under the following instances or projects:

1. Using personal data and sensitive data such as race, ethnicity, personal preferences, or interests, to create profiles, evaluate, score, make decisions or predict certain outcomes.

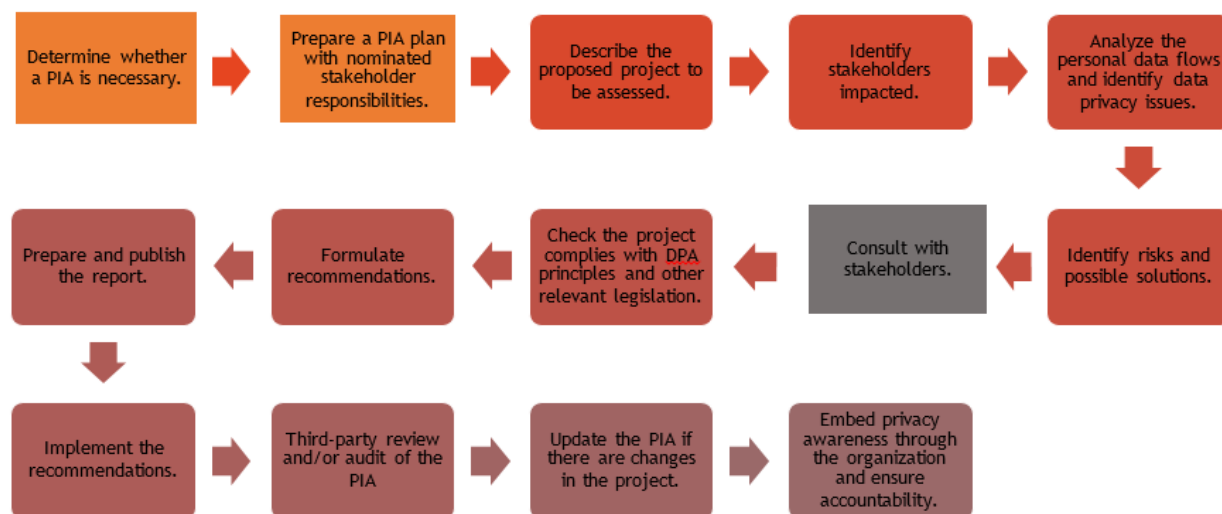
2. Automated decision making / processing that results in taking decisions on individuals that results in legal or equally significant effects, for example decisions that result in exclusion or discrimination.
3. Systematic monitoring to observe, control or monitor data subjects.
4. Collecting sensitive data including special categories such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union clientship, genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation.
5. Data processing on a large scale. There hasn't been a definition of what constitutes large scale, however, some key factors to consider determining if data is being processed on a large scale is the number of data subjects, the volume of data being collected, the duration of the processing activity and the geographical extent of the processing.
6. Using datasets that have been matched or combined, for example that have been collected by different purposes or/and by different controllers, in a way that would exceed the reasonable expectations of the individual.
7. Data concerning vulnerable individuals where there is a power imbalance between the individual and the data controller and the individual such that the individual may be unable to consent to or oppose the processing of their data. Such groups can include children, the mentally ill, elderly etc.
8. Innovative use or applying technological or organizational solutions such as combining use of fingerprint and face recognition for improved physical access control, etc.
9. Data transfer across borders outside Kenya.
10. When the processing prevents data subjects from exercising a right or using a service or a contract. For example, processing performed in a public place where people passing cannot avoid or processing that aims at allowing, modifying or denying a service or entry into a contract.

Before starting a DPIA the project owner shall complete an assessment to determine if DPIA is required for the business change or proposed project, either product or system development.

Once the need for a DPIA has been identified, the following process should be followed to ensure that the DPIA covers the relevant scope, includes the relevant stakeholders, and has the necessary project management to be completed appropriately.

Multiple iterations of this process may be followed over the course of a project to monitor if the risks have been addressed by the relevant solutions/mitigating controls or if the scope of the project changes.

At the end of the process, a DPIA report should be produced, using the 'Privacy Impact Assessment template'



### 2.6.2 Data Minimization

Data minimization requires personal data collected to be adequate, relevant, and not excessive in relation to what is needed for the purpose of processing.

The business shall build on effective data management and data governance to pave way for incorporating data minimization in practice within the business in both its capacity as controller and processor to demonstrate good data handling practices in line with regulatory and clients' expectations.

The risk management function shall engage with different process owners on a continuous basis to understand the points at which data is handled within the Entity processes in order to build effective data minimization practices at different points in the data lifecycle.

The key points within the data lifecycle where the data minimization principle should be observed are as follows:

1. Data collection
2. Use
3. Transfer
4. End of life

The following key considerations shall be made to ensure the business entrenches data minimization principles in its operations.

Data Minimization Consideration	
Data Collection Point	<ul style="list-style-type: none"> <li>To ensure alignment with leading practice and provision of the DPA the following considerations shall be made at the point of data collection:               <ul style="list-style-type: none"> <li>What data is collected.</li> <li>What are the channels used to collect data?</li> <li>Why is data collected/Data collection purpose?</li> <li>Appropriateness of collection time i.e., based on the processing needs.</li> <li>Collection monitoring i.e., review of the data collected.</li> <li>Data storage i.e., maintenance of an inventory of applications handling the data.</li> </ul> </li> <li>The data collecting team/department shall consider the legal basis during collection ensuring the Entity remains compliant with the data minimization principles.</li> </ul>

Data Minimization Consideration	
	<ul style="list-style-type: none"> <li>The business shall review its intake tools such as onboarding forms, online collection portals, telephone calls, CCTV camera's etc. to ensure that only minimum amount of relevant, adequate, and sufficient data is collected.</li> </ul>
Data Use	<ul style="list-style-type: none"> <li>The business uses the data it collects in various ways as it seeks to offers services to its clients. To entrench the data minimization principles around the use of data the Risk Management team shall ensure all functions within the business understand what personal data is collected by the different business units and the storage mechanisms to avoid replication of data. The following considerations shall be made in data use to enhance data minimization: <ul style="list-style-type: none"> <li>The necessity of the collected data fields for processing i.e., are all the collected field necessary for processing.</li> <li>Completion of adequate assessment to determine the minimal data that needs to be stored.</li> <li>Replication of data across various systems.</li> <li>Data storage with third parties.</li> <li>Inclusion of the right personal data classification tags (general personal data or sensitive personal data).</li> <li>Deidentification of personal data where data use does not need to include identity of data subjects.</li> <li>The adequacy of access controls.</li> <li>Adequacy of access reviews procedures.</li> </ul> </li> </ul>
Transfer	<ul style="list-style-type: none"> <li>The business may transfer personal data it collects from its clients and staff in its normal operations. To entrench data minimization principles in the data transfer process the following considerations shall be made: <ul style="list-style-type: none"> <li>Review of data before transfer.</li> <li>Presence of default settings set to maximum privacy for automated transfer of data to different portals or medias.</li> <li>Adequacy of the third-party policies to address collection, storage, retention, and destruction of data.</li> <li>Ability to identify data sources both structured and unstructured.</li> </ul> </li> </ul>
End of Life	<ul style="list-style-type: none"> <li>Data should be retained only if required for the purpose for which the data was collected, or when there are specific legal or regulatory requirements. To achieve this, the business shall ensure it data retention periods are aligned with the various regulatory guidelines. At the end of retention period the business shall ensure both structured and unstructured data records are reviewed and deleted unless there is a particular legal or contractual reason for retaining the data. The business shall ensure its systems have inbuilt capabilities to set retention period and flag data when the holding period lapses.</li> <li>The following considerations shall be made in data retention and destruction: <ul style="list-style-type: none"> <li>The period needs for data retention to fulfill the collection purpose.</li> <li>Adequacy of retention schedules and policies for both electronic and physical records.</li> <li>Ability to delete backups and replicated information on deletion of original records.</li> <li>Clean desk policies.</li> </ul> </li> </ul>

## 2.7 Data Security - Technical and Organizational Measures

The integrity, confidentiality, and availability of personal data that Centum possesses, or controls must be secured.

Appropriate, reasonable technical and organizational measures must be implemented to prevent:

1. loss of, damage to or unauthorized destruction of personal data.



2. alteration of personal data.
3. disclosure of personal data.
4. unlawful access to personal data.
5. unlawful processing of personal data.

Appropriate controls must be implemented in accordance with the Privacy by Design principle and Centum Information Technology, cybersecurity, and data retention policies. The controls shall be maintained against the risks identified to ensure that safeguards against privacy risks are designed and implemented properly.

The effectiveness of implemented controls must be verified and updated continually to cover new risks or deficiencies in existing safeguards.

## 2.8 Data Subject Rights

Data subjects enjoy certain rights under the DPA and the General Regulations. These rights include:

1. Being informed of the use of their personal data.
2. Accessing their personal data that is in custody of the data controller or data processor in this case Centum.
3. Objecting to the processing of all or part of their personal data.
4. Correction of false or misleading personal data that is held by the data controller or data processor.
5. Deletion of false or misleading personal data about them that is held by the data controller or data processor.

In addition, data subjects are required to be informed of:

1. The fact that personal data is being collected and the purpose for which it is being collected.
2. The third parties with whom personal data have been or will be transferred to, including details of safeguards adopted.
3. The contacts of the data controller or data processor and on whether any other entity may receive the collected personal data.
4. A description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data.
5. Whether the personal data being collected pursuant to any law and whether such collection is voluntary or mandatory.
6. The applicable consequences (if any) where the data subject fails to provide all or any part of the requested data.

The Entity is committed to satisfying the rights of Data Subjects with respect to their Personal Data. The business shall define a Data Subjects Right System (“DSR System”) that will be supporting the process by which it will receive, review, and respond to requests to exercise individual DSRs, as well as the process for handling Data Subject privacy complaints.

### 2.8.1 Data Subjects Right (DSR) Business Specifications

DSR requests, shall be received directly from the data subjects. Instructions detailing how to submit a DSR request should be included on Centum and its subsidiaries external website. Data subjects may submit a DSR request via phone or email.

Once a DSR request is submitted via phone or email, customer care will create a case within their DSR Management tool/ ticketing system and authenticate the request before queuing the request for action based on the nature of request and the roles and responsibilities matrix.

Correspondence with the data subject should occur via the DSR Management tool/ticketing system for compliance purposes.

Where a data subject's request is manifestly unreasonable or excessive particularly where a request is repetitive the business may:

1. Charge a fee commensurate with the administrative costs of responding to the request, or
2. Deny the request.

The DPO, in consultation with Head of Risk, will determine whether a DSR request is unreasonable or excessive. If a DSR request is determined to be unreasonable or excessive, DPO will document the rationale within DSR Management tool and maintain the request for as long as the retention policy and schedule require.

Data subjects must receive a response to their requests within the stipulated timeline under Part II - Enabling the rights of data subjects of the General Data Protection Regulations. See a summary of the rights and response time in the table below:

Nature of Request	Response time
Restriction to processing	Within 14 days of the request or within 14 days of refusal where the request is manifestly unfounded or excessive.
Objection to process all or part of a data subject personal data	<p>Within 14 days of request where the right to object processing is absolute i.e., where processing is for direct marketing including profiling related to such direct marketing.</p> <p>Where the right to object is not absolute and the request is denied inform the data subject of the reasons for declining the request and their right to lodge a complaint with the Data Commissioner where dissatisfied.</p>
Access to personal data	Within 7 days of the request.
Rectification of data	<p>Within 14 days of the request rectify the affected personal data in the database where satisfied that a rectification is necessary.</p> <p>Where rectification is declined notify the data subject of the refusal within 7 days providing reasons for refusal.</p>
Portability	<p>Within 30 days of the request upon payment of the prescribed fees port the personal data</p> <p>Where portability is declined notify the data subject within 7 days of the decline and the reasons for the decline in writing.</p>
Erasure/ destruction of personal data	Within 14 days of the request.

Whenever DSR request is address, the employees should document all relevant information within the DSR management tool. Any individual associated with the DSR request must document all pertinent details regarding the receipt of DSR requests, the resolution of the request, and dates in the DSR Management tool. If a request is denied, the DPO should document the rationale.

The DSR correspondences shall be sent to the data subjects on email using the either:

1. DSR Identity Verification Template
2. DSR Authentication Failure Template
3. DSR Erasure Denial Template
4. DSR General Denial Template

5. DSR Resolution Template
6. Third Party Consent for Disclosure Template
7. Third Party Correction Request Notification Template
8. DSR Access Requests Approval

### 2.8.2 Roles and Responsibilities

The table below outlines the key roles and responsibilities of individuals involved in the DSR request fulfilling process.

Role	Responsibility
Data Subjects	<ul style="list-style-type: none"> <li>Initiate Data Subject Requests under the DSR request fulfillment process.</li> </ul>
Customer Care	<ul style="list-style-type: none"> <li>Authenticate the DSR requests against the data subject's rights matrix.</li> <li>Identify the Systems of Record holding Data Subjects' Personal Data.</li> <li>Contact IT, Business Unit Teams/Data Owners and/or Third Parties if necessary to fulfill DSR requests.</li> </ul>
Data Owners	<ul style="list-style-type: none"> <li>Authorize or deny access to certain data.</li> <li>Maintain the accuracy and integrity of their data.</li> <li>Respond to requests in a timely manner.</li> <li>Maintain administrative control of the specific personal datasets.</li> </ul>
Data Privacy Officer ("DPO")	<ul style="list-style-type: none"> <li>Maintain involvement in all issues related to data protection, including DSR requests.</li> <li>Receive and review Data Subjects' privacy complaints.</li> <li>Report relevant privacy program metrics to the Data Protection Commissioner, as needed.</li> </ul>
Information Technology ("IT")	<ul style="list-style-type: none"> <li>Responds to requests from Business Representatives or the Privacy Office.</li> <li>Create workflows in the system for DSR.</li> </ul>
Privacy Office	<ul style="list-style-type: none"> <li>Oversee and execute the DSR request fulfillment process.</li> </ul>
Third Parties	<ul style="list-style-type: none"> <li>Provide Data Subjects' Personal Data to the Privacy Office, when required.</li> <li>Receive Data Subjects' Personal Data transferred from the Privacy Office, when required.</li> </ul>

## 2.9 Third Party Risk Management

Centum continues to grow, expand, and remodel its approach to service delivery driven by rapid technological advancements, changing regulatory environment and the changing needs of the clients. The growth in business, the penetration of I.T systems, the need to focus on core services and introduction of new services and products continue to influence the need of outsourcing. Apart from cost savings and accessing specialist expertise not available internally, for achieving strategic aims and efficient delivery mechanisms, outsourcing remains preferred destination for enabling perfection in selective business processes. While outsourcing can bring cost savings and other benefits, it may also increase the risk profile of Centum and its subsidiaries.

The failure of the business to provide a specified service, a breach in security, a breach in data privacy or noncompliance with legal and regulatory requirements by either the Entity or the outsourcing institution can lead to financial losses or reputational risk for the business.

These guidelines aim at safeguarding the interest of Centum, its shareholders and clients by adopting sound and responsive management practices through due diligence, management of data privacy risks arising from outsourcing activities, data transfer/sharing activities and regulatory changes.

The following key considerations shall be followed when engaging third parties that access and or process personal data on behalf of Centum and its subsidiaries:

1. All third-party engagements must be executed in line with the procurement policy. These guidelines supplement the procurement policy mainly for third parties accessing or processing personal data on behalf of Centum.
2. All departments must maintain a register of their third-party engagements detailing the extent to which the third-party handles personal data of either clients or staff of Centum.
3. Data privacy risk posed by the third parties must be assessed and documented including the mitigations/safeguards employed.
4. All contracts with third parties accessing or processing personal data on behalf of Centum and its subsidiaries must include a clause on data privacy safeguards.
5. All third parties processing personal data on behalf of Centum must be monitored on an ongoing basis to ensure compliance with the contractual obligations and adherence to data privacy practices.
6. Centum shall ensure privacy and security risks relating to the outsourcing arrangements are well managed by either performing regular audits or obtain assurance reports relating to the third parties control environment including data privacy technical controls and cyber postures.

### 2.9.1 Outsourcing/Third Party Risk Assessment

In considering whether to outsource Centum shall:

1. Perform a third-party risk assessment and document the risks and mitigations/safeguards employed to address the risks. The risk assessment shall consider the following risks:
  - a) Data Privacy Risk - Assessment of the risk that the service provider systems and procedures are in place to ensure personal data is processed as per Centum's guidelines and the data protection regulations preventing any form of data breach.

- b) Compliance Risk - Assessment of the risk that data protection laws and regulations are not adequately complied with by the service provider leading to fines and penalties by supervisory authorities.
  - c) Operational Risk - Assessment of the risk arising from technology or process failures impacting the capacity of the service provider to fulfill obligations and/or provide remedies.
  - d) Contractual Risk - Assessment of the risk that arises from inability or degree of ability of Centum to enforce the contract with the service provider.
2. A risk treatment plan shall be included for risks that pose high risk exposures to the rights of data subjects including approvals as per the Centum authority matrix.

### 2.9.2 Data Transfer/ Data Sharing

The DPA and the General Regulations provide for conditions that must be met for a transfer of personal data outside Kenya. A transfer of personal data outside Kenya should be based on the following:

1. appropriate data protection safeguards.
2. an adequacy decision made by the Data Commissioner.
3. transfer as a necessity.
4. consent of the data subject.

The processing of sensitive personal data out of Kenya must only be affected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards. Centum shall transfer personal data to another country, or a relevant international organisation based on the existence of appropriate safeguards where:

1. A legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the DPA and the General Regulations is available.
2. The entity having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organization, concludes that appropriate safeguards exist to protect the personal data.

Where a transfer of personal data takes place in reliance on the above grounds the transfer shall be documented including the date and time of the transfer, the name of the recipient, the justification for the transfer, a description of the personal data transferred. The documentation shall be maintained and be provided to the Data Commissioner on request.

Under the General Regulations, for the purpose of confirming the existence of appropriate data protection safeguards anticipated under the DPA and the General Regulations, any country or a territory is taken to have such safeguards if that country or territory has:

1. ratified the African Union Convention on Cyber Security and Personal Data Protection.
2. a reciprocal data protection agreement with Kenya.
3. a contractual binding corporate rules among a concerned group of undertakings or enterprises.

### 2.9.3 Third Party Monitoring

To mitigate the risk of data breach, Centum shall monitor the operations of third parties on a regular basis to ensure continued compliance with the data privacy standards and regulations. The monitoring activities shall be embedded on Centum's Annual Internal Audit Plan and Risk & Compliance Plans. Centum and its subsidiaries shall:

1. Review and monitor the security and data privacy practices and control processes of the service provider.
2. Implement procedures for regular updates by the service providers on the status of their control environment and require the service provider to disclose any security breaches.

3. Review the third parties' operations to ensure data processing is performed as per the issued instructions.

## 2.10 Incident and Breach Management

Section 43 of the DPA and Part VI of the General Data Protection Regulations provides for guidelines on the protection of the fundamental rights and freedoms of data subjects with regard to the personal data breaches, where a breach would result in a high risk to the rights and freedoms of data subjects.

Centum recognizes that while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

The regulations apply to controllers or processors that process personal data of subjects. In addition, the regulations must be applied in their entirety as no requirement is optional.

## 2.11 Data Breach Management

Initial detection and identification of a personal data breach can be initiated through a processor, external regulator, media outlet, or Centum/subsidiary own identification. Regardless, it is the responsibility of all parties to notify Centum and its subsidiaries "without undue delay" of any breaches so that the appropriate response procedures and communication can be followed.

Regardless of whether or not a breach needs to be notified to the data commissioner and data subjects, Centum shall always document suspected breaches including the relevant breach facts and remedial actions taken.

Breach notification to the data commissioner shall be done within 72 hours as stipulated in the Act. The notification shall include the nature of breach, the number of affected data subjects, and the mitigations the Entity has deployed to manage the impacts of the breach to the rights of data subjects.

The following guidelines shall be followed in data breach identification and management:

1. Identification - Centum may be informed of the personal data breach through processors (e.g., third parties), individuals (e.g., employees, clients, etc.) media organization, self-detection, or any other source.
2. Documentation - On receipt of information on possible breach the data privacy officer shall document the incident on the data privacy incident template.
3. Initial investigation - The initial investigation shall seek to establish the nature and extent of the breach by performing preliminary information gathering. To validate the occurrence of a personal data breach, Centum shall perform an initial triage to:
  - a) Verify the identity of the individual who reported the suspected incident.
  - b) Verify the information provided (critical information, facts vs. assumptions, knowns vs. unknowns).
4. Prioritize the personal data breach accordingly if the breach results in some level of risks (high, medium, or low) to the rights of data subjects the data protection officer shall categorize the breach as either:
  - a) Confidentiality Breach: Where there is an unauthorized or accidental disclosure of, or access to personal data.
  - b) Availability Breach: Where there is an accidental or unauthorized loss of access to, or destruction of, personal data (e.g., data has been deleted accidentally or by an unauthorized person, significant disruption of services which may render personal data unavailable temporarily or permanently).

- c) Integrity Breach: Where there is an unauthorized or accidental alteration of personal data.
  - d) If an incident affects the confidentiality, availability, or integrity of personal data, then it should be identified as a breach that could cause some level of risk to the individual affected. However, it is not yet necessary to determine a risk level as any level of risk to the individual must be reported to the Data Commissioner.
  - e) Refer to Centum's Incident Level matrix (Level 1 - Critical, Level 2 - Controlled (Medium) Level 3 - Low) which will assist in determining if a detected breach poses a risk to individuals' rights and freedoms as spelt under Section 37 (1) of the General Data Protection Regulations and notification to the Data Commissioner is required.
5. Once it's determined with a reasonable degree of certainty that a notifiable incident occurred, the 72-hour clock to report the incident to the Data Commissioner begins and the DPO must notify the data commissioner within 72 hours. Refer to the example scenarios below which describe when a controller becomes "aware" a personal data breach occurred:
- a) Third Party: A third party informs Centum that they have experienced a breach of personal data of one of Centum clients and provides evidence of the unauthorized disclosure. As the controller was presented with clear evidence of a confidentiality breach, then there can be no doubt that it has become "aware."
  - b) Network Intrusion: Centum detects a possible intrusion into its network through intrusion detection/prevention system or vulnerability scanning. Centum checks its systems to establish whether personal data held on that system is compromised and confirms this is the case. Centum has clear evidence of a breach and has now become "aware".
  - c) Ransomware: A cybercriminal contacts Centum after hacking its system and demands a ransom. After checking its system to confirm it was attacked Centum has clear evidence that a breach occurred, and it has become "aware."
  - d) Before notification to a data commissioner, it is important that a breach is reported to the appropriate levels of management following the incident escalation matrix triggering Centum incidence response plan.
6. Data Commissioner notification - Utilize the Data Commissioner notification template to notify the Commissioner of the breach. The notification should include:
- a) Description on the nature of the personal data breach (i.e., the root cause source) including the categories (e.g., children, employees, or clients, etc.) and approximate number of data subjects concerned and the categories (e.g., health data, financial details, account/clients numbers, ID numbers, etc.) and approximate number of personal data records concerned.
  - b) The name and contact details of the DPO or other contact point where more information can be obtained.
  - c) Description of the likely consequences of the personal data breach.
  - d) Description of the measures taken or proposed to be taken by the controller to address the personal data breach, where appropriate, measures to mitigate its possible adverse effects.
  - e) If the breach is complex or requires in-depth forensic investigation to fully establish the nature of the breach and the extent to which personal data have been compromised, inform the supervisory authority that not all required information is identified, and that Centum will provide more details in a phased approach. If further investigation reveals information indicating that a breach did

- not actually occur, then provide this information to the supervisory authority so as to amend the initial notification.
7. Seek guidance from the Data Commissioner regarding whether Centum should notify affected individuals based on the initial investigation results of the breach. Upon the supervisory authority's response, define the form of communication (e.g., email, other secure messaging, etc.) for phased updates about the breach investigation and the decision to notify affected individuals.
  8. Further Investigation - A more formal investigation to determine the cause, precise number of individuals affected, and more robust mitigation procedures can occur once a supervisory authority has been notified within the 72-hour timeframe. Seek additional incident response and investigation support accordingly.
  9. Based on further investigation findings, notify Data Commissioner of ongoing investigation timeline, results, and other identified consequences of the breach. Continue to seek guidance on decisions to notify affected individual based on new information.
  10. Eradication and Recovery - Concurrent with escalation and notification procedures, Centum must make every effort to eradicate and recover affected systems.
    - a) Eradication: Focus on removing the component causes of the exploited vulnerability. This will depend on the type of incident and the number of affected systems.
    - b) Recovery: Determine a timeframe for returning to normal operations based on predetermined Recovery Time Objects (RTO) and Recovery Point Objectives (RPO). Work closely with Infrastructure to rebuild and monitor systems and to improve defenses through control effectiveness testing (e.g., penetration testing).
  11. Accountability and Record Keeping - Centum shall establish an internal register of breaches governed and maintained by the DPO to maintain adequate records of the breach and the actions taken. The register should include:
    - a) Breach cause.
    - b) Timeline of events.
    - c) Investigation procedures and analysis.
    - d) Personal data impacted.
    - e) Effects and consequences.
    - f) Remedial actions taken.
    - g) Reasoning for decisions made during breach (e.g., reasons for delay are justified and not excessive).
  12. Managing Public and Investor Relations - Centum shall develop an external and internal communications plan and coordinate messaging to media including preparation and implementation of a holding statement, press release, website, and social media materials, as appropriate.
  13. Lessons Learned - In addition to quarterly tabletop exercises with the DPO, incident response stakeholders should hold a timely lesson learned session (led by the Incident Response Lead) to incorporate principles into this framework to establish progression.

To effectively manage incidents that may arise as a result of the engagement with third parties, Centum shall maintain a third-party incident escalation matrix that will require third parties to notify Centum of any suspected or actual breaches within 48 hours.



## 2.12 Data Lifecycle Management

Centum data lifecycle management process shall consists of a 5 stage (data collection, storage, usage, archival and destruction) process over the course of personal data life with the business. Each phase shall be governed by a set of guidelines that maximizes the data value during each stage of the lifecycle.

### 1. Data Collection and Creation

- a) Data shall be collected either directly or indirectly from the various data subjects. The process followed in the collection of the personal data must be aligned to the provisions of the DPA on data collection. The purpose of collection shall be disclosed to the data subject as per the Privacy Notice guidelines. The team collecting data shall ensure only required data is collected as per the data minimization standards.
- b) Data shall be properly valued and accurately reflected at the collection and creation stage.
- c) The business team shall ensure indirectly collected data either through publicly available sources or through third parties is error free and the data subject is notified within 14 days of the collection.
- d) Proper classification shall be done at the collection and creation stage to ensure the integrity of the data throughout the lifecycle.

### 2. Data Storage

Data shall be stored either electronically or in manual form. The electronic storage shall be done on the defined storage mechanisms as per the IT policies. Manual records shall be stored as per the records management principles.

### 3. Data Usage

Centum shall ensure data is used only for the purpose it was collected. The business shall also ensure adequate access restriction mechanisms are employed to ensure data is only accessed and used by the authorized personnel only.

Any change to the data use shall be informed by authorization obtained from the data subjects.

### 4. Data Archival

Data shall only be retained for the period necessary based on the data collection and processing purpose and the approved retention period. The business shall ensure both physical and electronic data is archived on the lapse of the retention period.

### 5. Data Destruction

Centum shall ensure that any data whose retention period has lapse is destroyed in line with the data destruction guidelines. The business can also anonymize the data to ensure that a data subject cannot be identified using the data in its custody upon lapse of the retention period.

To ensure effective monitoring of the personal data the business holds at any given point, the business shall maintain data inventory sheets and data flow maps showing the data flows with the organization.

## 2.13 Privacy by Design and Privacy by Default

Privacy and data protection must be embedded into the design of any technology, business process, product, or service. Privacy is an essential component of core functionality and, therefore, must be integral to all technologies, business processes, products, and services that involve personal data without diminishing functionality. By embedding PbD into the design prior to data collection, secure personal data lifecycle management is ensured from collection through disposal.

Strong technical and procedural safeguards must be in place to protect personal data from unauthorized collection, use, access, retention, and disposal. Architects and operators must ensure that safeguards are fit for purpose and provide maximum privacy and data protection. By enabling safeguards, PbD ensures that personal data is adequately secured and maintained.

Centum shall seek to create a culture that supports data protection by design and by default facilitated by governance oversight, a supportive workforce, and informed risk and compliance function. By creating a culture that supports PbD, the business seeks to accommodate all stated agreements and objectives, as well as applicable compliance requirements.

Personal data change management must be followed to evaluate the impacts of new or changing technologies, business processes, products, and services across the data lifecycle for personal data. These shall collectively be referred to as “projects and initiatives.” categorized into three types as noted below:

1. Technology Implementation Lifecycle
  - a) A new system or system upgrade occurring through the SDLC
  - b) Retiring or modifying an existing legacy system or application
  - c) A new way of collecting data
  - d) A new business process supported by IT tool(s)
  - e) A change in the way data is stored or secured
  - f) Engaging a third party to provide an IT service or application
2. Process Implementation Lifecycle
  - a) A new use case or disclosure of existing data on hand
  - b) A new or changing business process
  - c) Sharing data with a processor
  - d) Transferring data to a third party
  - e) Collection of new data
  - f) A decision to keep data for longer than designated in the retention schedule or as disclosed in a privacy notice
3. Product or Service Implementation Lifecycle
  - a) A new product or service offering
  - b) A new use of existing data to improve upon a product or service offering
  - c) Collection of new data to improve upon a product or service offering
  - d) Sharing data with a third party to support a product or service offering

To ensure PbD is incorporated into a project or initiative’s lifecycle, a privacy impact assessment shall be completed to determine whether personal data will be involved by completing a pre-assessment questionnaire and the privacy impact assessment template.

The assessments shall be reviewed and approved by the head of risk.

For projects or initiatives where it’s determined that personal data will be used, the following steps shall be followed in the project or initiative lifecycle.

Stage	Requirement
Requirements Definition	<ul style="list-style-type: none"> <li>The project lead shall review privacy and security policies and standards to ensure the project or initiative complies with Centum requirements around the collection, use, access, retention, and disposal of personal data.</li> <li>Based on the PIA results and associated evidence, the project lead shall collaborate with the business, risk, and IT teams to identify specific privacy and security requirements to be incorporated into the overall project or initiative requirements.</li> </ul>
Design	<ul style="list-style-type: none"> <li>Once a project or initiative's privacy requirements have been reviewed and approved by the risk team, the project lead shall utilize those requirements to embed privacy and data protection into the overall design of the project or initiative by selecting appropriate privacy and security controls.</li> <li>As the project or initiative design is refined, the project lead continues to evaluate the existing privacy and security requirements and determine if additional controls need to be incorporated into the design.</li> <li>The project lead also identifies any changes to the original purpose for personal data processing approved in the initial PIA. In any of these cases, the project lead must modify the PIA and resubmit to the risk team for review.</li> </ul>
Development	<ul style="list-style-type: none"> <li>Projects and initiatives must include the development of procedures and guidelines to address risk and compliance requirements. Proper privacy and security controls must be put in place to protect and secure personal data in line with defined requirements.</li> </ul>
Test and Deploy	<ul style="list-style-type: none"> <li>During the testing phase, the project lead shall ensure that privacy and security controls are implemented as intended and in accordance with defined requirements.</li> <li>As testing ends and the project or initiative nears its deployment, the project lead shall determine if personal data used in the project or initiative has changed and whether an additional consultation must be completed with the risk and compliance team.</li> <li>The project lead shall train the respective business or IT representatives on relevant privacy and security controls in order to ensure proper transition as the project or initiative moves from development phase to the maintenance phase.</li> <li>Prior to deployment, the project lead shall validate that the project or initiative has addressed all the guidance and contingencies provided by risk and compliance team before deployment.</li> </ul>
Maintenance	<ul style="list-style-type: none"> <li>Once a project or initiative has been deployed, business and IT representatives shall periodically verify that appropriate privacy and security controls are executed throughout the lifecycle of the finalized technology, business process, product, or service with guidance from the risk and compliance team, when desired.</li> </ul>

## 2.14 Training and Awareness

Centum data privacy training and awareness program shall seek to build capacity within the business on data privacy practices.

The Board of Directors and all staff must complete continuous data privacy learning programs to ensure the privacy culture is properly embedded at Centum.

The learning program shall follow the Analyze, Design, Develop, Deliver and Evaluate model.

To effectively embed the privacy learning culture the business shall seek to develop internal learning materials and from time to time invite external data privacy specialists to training its staff on emerging matters in data privacy.

### 1. Analyze.

The DPO in collaboration with the HR team shall:

- a) Analyze employee's knowledge gap in matters data privacy on an annual basis and outline scope of training, audience and prioritization of content based defined criteria.
- b) Examine the available content development tools that will be used to create privacy learning materials.
- c) Lay out the overall approach/training strategy to deliver training to end users.

### 2. Design

The DPO in collaboration with the HR shall:

- a) Design training to bridge knowledge gaps.
- b) Develop a training plan detailing out each training course, length, and recommended audience.
- c) Develop a plan for the sequence of instruction for each training course and audiences.

### 3. Develop

The DPO in collaboration with the HR shall:

- a) Develop training materials according to the training design.
- b) Develop progress tracking matrix for staged reviews
- c) Develop Training Review & Approval Process, Quality Review Process & Sign-Off Criteria.

### 4. Deliver

The DPO in collaboration with the HR shall deliver the training based on the training strategy and plan. The Entity may from time to engage the services of a data privacy consultant to help in the delivery of data privacy training.

### 5. Evaluate

The DPO in collaboration with the HR shall on an ongoing basis monitor and report on the training completion progress.

### 3 DATA PRIVACY STRATEGY

#### 3.1 Rationale

1. Centum's data privacy strategy shall offer guidance in the management of the data privacy program. The strategy shall focus on:
2. The ecosystem forces that may pose challenges and threats to the confidentiality, integrity, and availability of personal data held by Centum.
3. Supporting Centum's business wide strategy by providing the data privacy guidelines necessary to adjust quickly to emerging threats, regulations, and market forces.
4. Overseeing the data privacy risk management activities by establishing processes that consider security and privacy throughout the data lifecycle.
5. The strategy is built on 6 strategic drivers that defines why it exists and what it aims to achieve hence helping Centum achieve it's mission, vision, and goals.

#### 3.2 Pillars of Data Privacy Strategy

#	Driver	Method of Addressing Ecosystem Forces	Ecosystem Forces Addressed			
			Regulatory Landscape	Business Challenge	External Threat	Internal Threat
1	Protect Centum's reputation through consistent security and privacy risk management	<ul style="list-style-type: none"> <li>• Through consistent security and privacy risk management, Centum will implement the necessary controls to reduce the vulnerabilities available for exploitation by external threat actors.</li> <li>• By minimizing and managing attacks, Centum's reputation as a good steward of data will be preserved.</li> <li>• Training employees on security and privacy risk and how their daily activities support their roles as the first line of defense against privacy and cyber risk and threats will decrease their likelihood of inadvertently supporting a breach.</li> <li>• Understanding and mitigating risks of intentional internal breaches will reduce their likelihood of occurring.</li> <li>• Having employees act as risk champions enhancing and protecting Centum's reputation as a trusted business</li> </ul>	□		□	□
2	Foster agility to flex with emerging threats, regulations, and market forces	<ul style="list-style-type: none"> <li>• Encouraging employees to consider flexibility when designing new products, services, systems, or controls, will allow Centum to adapt more quickly to changes in regulations, business challenges, and threats.</li> </ul>	ü	ü	ü	ü

#	Driver	Method of Addressing Ecosystem Forces	Ecosystem Forces Addressed			
			Regulatory Landscape	Business Challenge	External Threat	Internal Threat
3	Deliver well-defined and effective security and privacy services	<ul style="list-style-type: none"> <li>Well-defined security and privacy services will facilitate their consistent delivery.</li> <li>Consistency will precipitate comprehensive application of controls.</li> <li>Minimizing vulnerabilities and risk exposure will help to thwart both external and internal attacks.</li> </ul>			ü	ü
4	Promote Centum's culture to embrace a security and privacy mindset	<ul style="list-style-type: none"> <li>Training employees on security and privacy risk and how their daily activities support their roles as the first line of defense against privacy and cyber risk and threats will help security and privacy to become part of Centum's culture.</li> <li>Vigilant employees will facilitate the right actions to minimize the potential for attacks.</li> </ul>			ü	ü
5	Be a business enabler for innovation through proactive security and privacy engagement	<ul style="list-style-type: none"> <li>Consulting with the risk and compliance (data privacy) team during initial discussions to scope out new products, services, systems, or markets will allow the business to assess feasibility at the start of the development cycle.</li> <li>Security and privacy will provide new requirements for business consideration when exploring new products.</li> <li>Implementation of security and privacy controls may open new markets or products the business had not previously considered or been able to penetrate.</li> <li>Improving security and privacy controls to allow Centum better compete with their competitors, who are well-versed with data protection requirements.</li> </ul>	ü	ü		
6	Broaden trusted partnerships through security and privacy	<ul style="list-style-type: none"> <li>Demonstrating strong security and privacy controls will enhance trust with Centum's clients and their relationships with the business.</li> <li>The ability to demonstrate to clients and other stakeholders that Centum is forward-thinking in addressing regulatory changes and business challenges will strengthen existing partnerships and facilitate new relationships.</li> </ul>	ü	ü		

The strategy shall be anchored on the business wide strategy to ensure there is coherence in the operating activities.

## 4 REVIEW AND APPROVAL


### 4.1 Review of the Policy

The Risk Committee will discuss any revisions that may be required of this Policy and recommend any such revisions to the Board for consideration and approval.

### 4.2 Approval

#### Adopted by the Board

Date : 11 July 2025

Signature : 

Designation : Board Chairman