1. General

1.1. Introduction

This policy is mandatory for all employees of Scania South Africa (Pty) Ltd and its subsidiaries without exception

The functional scope of this policy covers all processes where the Personal Data of natural and juristic persons is in whole or in part automatically collected, stored, organised, linked, transferred, used, modified, selected, destroyed or processed otherwise. This applies to the Personal Data of customers, employees, and suppliers and other business partners, etc. This policy also applies to the non-automated processing of Personal Data when and as covered by the scope of applicable privacy and data protection legislation.

1.2. Issuance and approval

The Document Issuer shall update this policy as and when the need arises

Document Versions .

Revision	Date	Version	Comment
1	30/04/2021	1.0	First Issue
2	18/06/2021	1.1	Inclusion of POPIA
3			
4			

1.3. Objectives

To ensure compliance with SGP10 Handling of Personal Data Policy and local data protection regulation, Protection of Personal Information Act (POPIA) 4 of 2013
Regulatory requirements enjoy preference over Group policies and should there be any discrepancy between the two the strictest provision applies.

1.4. Summary of Changes

Revision	Date	Version	Changes
2	18/06/2021	1.1	Inclusion of detailed POPIA requirements
3			
4			

1.5. Terms and Definitions

Anonymization: of Personal Data means that all identifying information (e.g. name, email address, user ID) is deleted or modified so that the identity of the Data Subject cannot be determined or can only be determined with a disproportionate effort.

Consent is any freely given, informed act related to a specific case where permission to process the data is unambiguously confirmed by the data subject.

Data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Responsible Party is also referred to as the Controller on Group level, is any natural person or legal entity, public authority, agency or other body who, alone or jointly with others, determines the purposes and means of Personal Data processing.

Operator also referred to data processor on Group level, is any natural person or legal entity, public authority, agency or other body that processes Personal Data on behalf of a Responsible party in terms of a contract or mandate, without coming under the direct authority of that party

Information Officer is also referred to as Data Protection Coordinator on Group level, is an official role formally described in the Act with the tasks of informing and advising the business on data protection matters and of monitoring compliance with conditions for lawful processing of personal information

Data Recipient is the natural person or legal entity, public authority, agency or any other body to which the Personal Data is disclosed, whether a third party or not.

Data Subject is the identified or identifiable natural or juristic person to whom the Personal Data refers, e.g. drivers, contacts at a customer or employees of a Group company.

Personal Data/ Information is information about an identified or identifiable natural or juristic person. An identifiable natural or juristic person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as and not limited to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural or juristic person.

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymisation is the processing of Personal Data in a way that it can no longer be attributed to an identifiable natural person without the use of additional, separately stored information.

Special categories of Personal Data is Personal Data from which the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership can be deduced. This also includes the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as Personal Data connected with administrative offences, crimes, or criminal convictions.

Third Party means a natural or legal person, public authority, agency or body other than the data subject, responsible party, operator and persons who, under the direct authority of the responsible party or operator, are authorised to process Personal Data;

Transfer is any disclosure of Personal Data to a natural person or legal entity, public authority, agency or body. A transfer also takes place if another body has the opportunity to access Personal Data.

2. Purpose

The purpose of this policy is to:

- Set the requirements for processing as well as guaranteeing a high level of protection for natural and juristic persons when their Personal Data is processed by Scania South Africa
- Set down the fundamental rules for handling Personal Data and defines a systematic way of working regarding data protection within Scania Group
- Define an overall approach to information security including:
  - Detection and pre-emption of information security breaches such as misuse of network, data, applications and computer systems
  - Uphold ethical and legal responsibilities in terms of information protections
  - Respect data subjects' rights

For us at Scania, protection of Personal Data comes naturally from our core values. When we respect the individual and uphold high integrity – e.g. in our interactions with our customers as well as our co-workers – compliance with data protection legislation is a natural outcome.

3. Protection of Personal Information Act 4 of 2013 Guidance Policy

3.1. Introduction

Scania Southern Africa (Scania SA) is a Southern Africa subsidiary of Scania Group. Scania SA assembles trucks and busses as well as the sale of parts, vehicle consumables and services.

Leading the way in this new millennium, Scania South Africa develops leading technology to keep us at the top of our industry, providing our customers with innovative, quality products. As a leading enterprise in our industry, Scania South Africa is obliged to comply with the Protection of Personal Information Act 4 of 2013 ("POPI").

The Policy sets out the way Scania SA deals with their all information collected, received, stored, processed, retrieved and disposed as well as and stipulates the purpose for which said information is used. The Policy is made available on the Scania SA website https://www.scania.com/za/en/home/misc/privacy-statement.html

We recognize the following notes, records and documents as information, regardless of primary source:

- Written
- Typed
- Voice
- Graphics

3.2. Data Subject Personal Information Definition

Data Subject is defied under POPI Act as means the person to whom personal information relates. Information can be one or a combination of the following:

- Race
- Gender
- Sex
- Pregnancy
- Marital status
- National / ethnic / social origin
- Colour
- Sexual orientation
- Age
- Physical or mental health
- Disability
- Religion / beliefs / culture
- Language

- Educational
- Medical
- Financial
- Criminal
- Employment history
- ID number
- Email address
- Physical address
- Telephone number
- Location
- Biometric information
- Personal opinions, views or preferences

3.3. Conditions for Lawful Processing of Information

The conditions for the lawful processing of personal information by or for a responsible party are the following:

- Accountability, as referred to in section 8 of the POPI Act;
- Processing limitation, as referred to in sections 9 to 12;
- Purpose specification, as referred to in sections 13 and 14 of the POPI Act;
- Further processing limitation, as referred to in section 15 of the POPI Act;
- Information quality, as referred to in section 16 of the POPI Act;
- Openness, as referred to in sections 17 and 18 of the POPI Act;
- Security safeguards, as referred to in sections 19 to 22 of the POPI Act;
- Data subject participation, as referred to in sections 23 to 25. of the POPI Act;

The conditions, as referred to in subsection (1) of the POPI Act are not applicable to the processing of personal information to the extent that such processing is:

- excluded, in terms of section 6 or 7, from the operation of this Act or Protection Of Personal Information Act, 2013 Act No. 4 of 2013 24

- exempted in terms of section 37 or 38, from one or more of the conditions concerned in relation to such processing.

The processing of the special personal information of a data subject is prohibited in terms of section 26, unless the:

- provisions of sections 27 to 33 of the POPI Act are applicable; or
- Regulator has granted an authorisation in terms of section 27(2), in which case, subject to section 37 or 38, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

The processing of the personal information of a child is prohibited in terms of section 34, unless the:

- provisions of section 35(1) are applicable;
- -or Regulator has granted an authorisation in terms of section 35(2), in which case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

The processing of the special personal information of a child is prohibited in terms of sections 26 and 34 unless the provisions of sections 27 and 35 are applicable in which case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

The conditions for the lawful processing of personal information by or for a responsible party for the purpose of direct marketing by any means are reflected in Chapter 3, read with section 69 insofar as that section relates to direct marketing by means of unsolicited electronic communications.

Sections 60 to 68 provide for the development, in appropriate circumstances, of codes of conduct for purposes of clarifying how the conditions referred to in subsection (1), subject

to any exemptions which may have been granted in terms of section 37, are to be applied, or are to be complied with within a particular sector.

3.4. Rights of the Data Subject

A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3 of the POPI Act, including the right

- to be notified that:

  (i) personal information about him, her or it is being collected as provided for in terms of section 18; or

  (ii) (ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;

- to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;

- to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;

- to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)(a); (e) to object to the processing of his, her or its personal information:

  (i) at any time for purposes of direct marketing in terms of section 11(3)(b); or

  (ii) in terms of section 69(3)(c);

- not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1);

- not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;

- to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any Protection Of Personal Information Act, 2013 Act No. 4 of 2013 26 data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and

- to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99.

In Scania SA, we recognize the following type of persons as data subjects

- Employees and potential employees

- Vendors and potential vendors, including but not limited to:

    - Trading secrets including intellectual property, quotes and pricing schedules

    - Financial instruments and bank generated documents

    - Their employees personal details including academic qualifications

- Customers and potential customers

- Scania Group business processes, policies, procedures and intellectual property

3.5. Limited Purpose Information Collection

Section 9 of POPI states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

Scania SA regards information as:

- Written notes in paper, whiteboards and post it notes
- Electronic documents regardless of format (i.e., PDF, word, excel, PowerPoint etc.)
- Voice recordings
- Video recordings
- Scanned documents regardless of initial format
- Electronically transmitted and stored information including emails, hard disks and cloud servers
- Photos and drawings including maps
- Electronic signatures

Scania SA is guided its Information Classification and Data Handling Policy when requesting, processing, storing and deleting information

Scania will notify any part which it is collecting from the purpose of the information. The following purposes will apply for the relevant information requested

Information Owner	Information Type	Requester	Purpose	Request Platform	Storage and Processing
Customer/ Franchisor	Client company information and credit information	Supply Chain/Functional Head	KYC and credit line approval	Email	email
Customer	Contact details	Marketing	Consented marketing	Manual forms, website, Social media	CRM
Employee	Employee academic, residential, employment history and/or medical records	Human Resource/Functional Head	Configuring employee on Sage VIP, email, Ascala and fulfilling department of labour and B-BBEE requirements	Manual forms and email Email	File share servers and
Contractor	Client company information	Supply Chain/Functional Head	KYC	Manual Forms,Email	File share servers and email
Dealerships	Financial and market performance	Scania South Africa	Dealership contract adherence	Email	Automaster

		Commercial/ Retail			

The requested information will be retained according to the **Data Retention Policy**

The key purpose for collecting client information is as follows:

- Scania SA collects and processes the client's personal information for marketing purposes to ensure that our products and services remain relevant to our clients and potential clients.

- Scania aims to have agreements in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding with regard to the protection of the client's personal information. Scania SA suppliers will be subject to the same regulations as applicable to Scania SA.

- With the client's consent, Scania may also supplement the information provided with information Scania SA receives from other providers in order to offer a more consistent and personalized experience in the client's interaction with Scania SA.

- To provide clients with an accurate analysis of their product and services needs.
    - For purposes of this Policy, clients include potential and existing clients.
    - Providing products or services to clients and to carry out the transactions requested;
    - For underwriting purposes;
    - Assessing and processing claims;
    - Conducting credit reference searches or verification;
    - Confirming, verifying and updating client details;
    - For purposes of claims history;
    - For the detection and prevention of fraud, crime, money laundering or other malpractices;
    - Conducting market or customer satisfaction research;
    - In connection with legal proceedings;

- Providing Scania SA services to clients, to render the services requested and to maintain and constantly improve the relationship;
- Providing communication in respect of Scania SA and regulatory matters that may affect clients; and
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

3.6. Limited Purpose Information Processing

Information collected from clients/customers, contractors, services providers, employees and franchisee as per **Limited Purpose Information Collection and Processing Policy** will be processed according to section 10 of POPIA.

Processing of information types includes, but not limited to:

- Collation
- Linking information
- Recording
- Distribution
- Merging
- Consultation
- Retrieval
- Distribution
- Erasure
- Restriction
- Destruction
- Organization
- Modification
- Use

- Alteration
- Updating
- Collection
- Receipt
- Storage
- Dissemination
- Degradation

According to section 10 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for Scania SA processing of Personal Information:

- The client's consents to the processing: - consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship;
- The necessity of processing: to conduct an accurate analysis of the client's needs for purposes of amongst other credit limits, insurance requirements, etcetera.
- Processing complies with an obligation imposed by law on the Scania SA;
- Processing is necessary for pursuing the legitimate interests of the Scania SA or of a third party to whom information is supplied — in order to provide Scania SA clients with products and or services both Scania and any of our product suppliers require certain personal information from the clients in order to make an expert decision on the unique and specific product and or service required.
- For audit and record keeping purposes;

Whenever information changes its sensitivity, information will be re-classified according to the **Information Classification and Data Handling Policy.**

The current Scania SA data processers and operators are:

Entity	Information Received	Processing Rights and limitation
{External Auditors}	Scania financial, vendors and human resources information	To ensure that Scania SA conforms and adheres to its
Iron Mountain	Scania SA, vendor, employee and partner records	Indexing and archiving
Pandae Green solution	Scania SA, vendor, employee and partner records	Shredding and disposal
eWaste	Scania SA computer equipment including removable media drives	Destruction and disposal
Sage Payroll VIP	Employees' salaries and wages information	Processing of salary information
Vodacom	Scania SA, vendor, employee and partner records	Hosting and provision of back-up services

3.7. Disclosure of Personal Information

Scania SA may disclose identifiable personal information to Scania SA commercial sites, Scania South Africa head office and joint venture partners.

Scania SA has consent acknowledgements which serves as agreements in place to ensure that compliance with confidentiality and privacy conditions.

3.8. Scania Southern Africa Commitment to POPI Act

3.8.1. Scania Southern Africa's Principles Relating to Processing Personal Data

Scania SA commits to the following personal information processing principles: Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

- Collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes, further processing for archiving purposes shall, in accordance with Condition 3,4 and 5 of POPIA not considered to be incompatible with the initial purpose ('purpose limitation').

- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed ('data minimization').

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

- Kept in a form which permits identification of data subjects for no longer than its necessary for the purpose for which the personal data are processed, personal data stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose in accordance with Condition 4 of POPIA, subject to implementation of the appropriate technical and organizational measures required by this regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

- The Operator shall be responsible for and be able to demonstrate compliance with Condition 1: Accountability of POPIA relating to POPIA.

Scania South Africa must ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC27001 international standard is a key part of the commitment.

3.8.2. Rights of the Individual

Scania SA shall at all times communicate the rights of the individual/data subject during information request and capturing. The rights of the data subject are under POPIA and GDPR are:

- The right to be informed.
- The right of access.
- The right of rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Scania South Africa that allows the required action to be taken within the timescales stated in the GDPR.

Data subject request	Time scale
The right to be informed	When data is collected (is supplied by data subject) or within one month (if not data subject)
The right of access	One month
The right of rectification	One month
The right to erasure	With undue delay
The right to restrict processing	With undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Not specified

table 1 timescales for data request

3.8.3. Consent

Unless it is necessary for a reason allowed under POPIA, explicit consent must be obtained from a data subject to collect and process their data. In the case of children below the age of 18 (this may be lower in individual EU member states) parental consent must be obtained.

Transparent information about usage of their personal data must be provided to the data subject at the time that the consent is obtained and their rights regarding their data explained, such as the right to withdraw consent this information must be provided in an accessible form, written in clear language and free of charge.

If the personal data is not obtained directly from the subject, then this information must be provided within reasonable period.

3.8.4. Privacy by design

Scania South Africa has adopted a principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be the subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purpose.
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
- Assessment of the risk to individuals in processing the personal data.
- What controls are necessary to address the identified risk and demonstrate compliance with legislation.

Use of techniques such as data minimization and pseudonymization will be considered where applicable and appropriate.

3.8.5. Transfer of Personal Data

Transfer of personal data outside the South Africa and European Union must be carefully reviewed prior to the transfer taking place to ensure that fall within the limits imposed by POPIA and GDPR. This depends partly on the South African Information Regulator's and/or European Commission's judgement as to adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfer must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

3.8.6. Data protection officer

A defined role Data Protection Officer (DPO) is required under the POPIA, if the organization performs large scale monitoring or if it processes particularly sensitive types of data on a larger scale, The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria Scania South Africa requires a Data protection officer to be appointed due to the volume of client, employee, vendor and corporate data transactions within Scania SA.

3.8.7. Breach Notification

Scania SA's must be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal date. In line with POPIA, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed with in 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

The Information Regulator will be notified on the following address:

The Information Regulator of South Africa 33 Hoofd Street Forum III, 3rd Floor Braampark Johannesburg	Mr Marks Mathibela Chief Executive Officer Cell No.: +27827464173 Email: inforeg@justice.gov.za

3.8.8. Addressing compliance to POPIA

The following actions are undertaken to ensure that Scania SA always complies with the accountability principal of POPIA.

- The legal basis for processing personal data is clear and unambiguous.
- A Data Protection Officer is appointed with specific responsibility for data protection in the organization.
- All staff involved in handling personal data understand their responsibilities for following good data protection practice.
- Training in data protection has been provided to all staff.
- Rules regarding consent are followed.
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively.
- Regular reviews of procedures involving personal data are carried out.
- Privacy by design is adopted for all new or changed systems and processes.
- The following documentation of processing activities is recorded.
- Scania SA and relevant details.
- Purposes of personal data processing.
- Categories of individuals and personal data processed.
- Categories of personal data recipients.
- Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place.
- Personal data retention.
- Relevant technical and organization controls in place.

These actions will be reviewed on a regular basis as part of the management review process of the information security management system

4. Important data protection concepts

Data protection principles, terms and definitions, and whether mandatory or not, may vary from one country to another but adherence to the following concepts applies unless in collision with local regulation.

4.1. Record of processing activities

The responsible party shall maintain a record of processing activities covering all assets and processes that include/process Personal Data. The record, also referred to as a register or directory, shall contain information such as; purpose of processing, name of the responsible party and of operator, categories of Data Subjects, categories of Personal Data, categories of Data Recipients, international transfer of Personal Data, documented contractual safeguards and retention period.

Also the operator shall maintain a record of processing activities carried out on behalf of the responsible party. It shall include information such as contact details of the responsible party, categories of processing carried out, international transfers of Personal Data and description of technical and organisational measures.

4.2. Data Protection Impact Assessment (DPIA) Annexure B

A Data Protection Impact Assessment (DPIA) must be performed where processing is likely to result in a high risk to the rights and freedoms of the persons concerned. A DPIA evaluates the risk, likelihood and impact, of a compromise to the confidentiality, integrity and/or availability of Personal Data.
For every contract entered into, with the supplier, by the Business unit, the Information Officer (IO) should be informed to evaluate whether or not the DPIA should be performed before information is shared between the parties

4.3. Contractual Safeguards

The transfer of Personal Data requires that adequate contractual safeguards are in place, regardless of whether the transfer is between Scania and its suppliers/ partners or within the Volkswagen Group. Data Processing Agreement (DPA) and data transfer mechanisms are examples of safeguards.
For every contract entered into with the supplier by the Business unit, the Information Officer (IO) should be informed to evaluate whether or not the DPA should be in place before information is shared between the parties

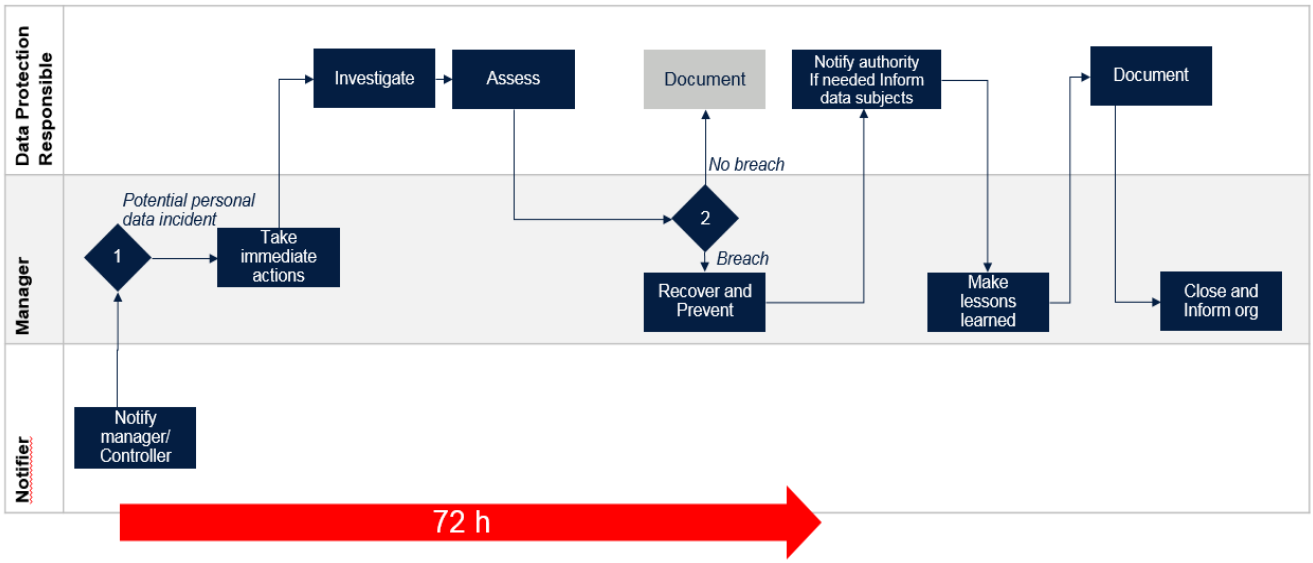
4.4. Incident and Breach management

A Personal Data breach is an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. A breach can have significant implications for affected Data Subjects, as well as for Scania, and shall be identified and stopped as soon as possible.
Example of data breaches are mail or email with personal data which has been sent to the wrong receiver, incorrect access to an IT-system, personal data that has wrongly been available in a public area, an unencrypted mobile or computer that has been forgotten in a public area, burglary and hacking.

Where there are reasonable grounds to believe that the personal information has been accessed by an unauthorized person, the Information Officer shall as soon as reasonably possible notify the Regulator and the Data Subject

The Information Officer has to first determine whether the suspected data breach really is a data breach, and if it must be reported to the supervisory authority. This investigation, including the reporting, must be done within 72 hours

4.5. Incident Reporting Procedure



Notifier must notify line manager by filling in a form

(Annexure B – Personal Data Incident Report)

Investigations and considerations taken, including whether to inform Data Subjects concerned and whether to report to the Regulator, shall be documented.

4.6. Data Subject Access Requests (DSAR)

The Information Officer must facilitate the exercise of Data Subject rights, and shall not refuse to act on the request of the Data Subject unless the Responsible Party is unable to identify the Data Subject

A record of all Data Subject requests is kept on group level and all requests shall be facilitated by the IO

4.7. Data Protection by Design and by Default

Data Protection by design and by default is an approach to processes, methods and systems development, which takes data protection into account throughout the Personal Data life cycle. The concept is an example of value sensitive design, i.e., to take human values into account in a well-defined manner throughout the whole process. There are Scania Guidelines which support the application and realisation of the “Privacy by Design Principles” when specifying and designing all kinds of IT solutions.

5. Roles and responsibilities

5.1. Management Team

The Management Team of the respective company is legally responsible for compliance with the statutory and company-specific provisions relevant for data protection. The Management Team shall appoint a member, or another person with great mandate, to take on the role as **Privacy Manager**

Furthermore, the Management Teams shall appoint a **Data Protection Coordinator**, who can act independently and participate in the global privacy and data protection network, and shall also support the line managers and the members of the data protection organisation in the fulfilment of their duties particularly by providing sufficient staff and material resources. The Data Protection Coordinator role is described in in this document

The **Privacy Manager** and the **Data Protection Coordinator** are notified to the Scania Group Data Protection Office.

5.2. Line managers (All levels)

It is the obligation of the line managers of all levels within the business to ensure compliance with the statutory and company-specific provisions on data protection in their area of responsibility. It is important that they allocate time for data protection, informing their employees and taking the measures required to comply with relevant legislation and internal policies

The departments shall also be able to demonstrate compliance by correct handling and appropriate documentation, including the record of processing activities. This is a responsibility of the business and not of the privacy and data protection organisation.

5.3. Employees

Every employee has an individual duty to perform her/his professional activities in compliance with the internal rules and local data protection legislation

5.4. Internal Audit Function

Internal audit supports the company's data protection activities as part of its general duties by taking account of suitable audit proposals for data protection when planning its audit program.

5.5. Privacy and data protection organisation (BU)

For Group Privacy and data protection organization, refer to SGP10

The aim of the privacy and data protection organisation is to design data protection processes, methods and tools as efficiently and effectively as possible in a way close to practice, and to support the business in being compliant.

The members of the privacy and data protection organisation are responsible for coordinating the company's data protection activities, for supporting the company's Management and employees in the performance of their duties, including fulfilment of data protection requirements, and for monitoring and reporting compliance.

5.6. Data Protection Coordinators (DPC)

The management of each company in the Scania Group shall appoint a person affiliated with the company as the Data Protection Coordinator.
Management has appointed the **Compliance Officer** as a DP, who shall also resume the role of an Information Officer in accordance to local data protection regulation, POPIA.

The DPC shall endeavour to advice and support their company on statutory and company provisions on data protection. He/she shall together with the Privacy Manager establish a suitable data protection organisation.

The DPC is the first contact for all questions relevant for data protection in their company, and in their capacity as DPC, they report directly to the Management Team of their company.

The tasks of the Data Protection Coordinators include in particular:

5.6.a. Providing guidelines and instructions on data protection

5.6.b. Informing and advising management and employees regarding data protection questions

5.6.c. Processing inquiries on data protection law, above all from employees, customers, suppliers, and public authorities

5.6.d. Maintaining a local register of processing activities

5.6.e. Monitoring compliance with the statutory and internal company data

5.6.f. Facilitate Data Protection Impact Assessments (DPIA)

5.6.g. Update central register with Personal Data processing on behalf of the business

5.6.h. Follow up status & risk reporting

5.6.i. Providing support for the fulfilment of possible reporting duties in accordance with local data protection law

5.6.j. Ensuring his/her own ongoing professional development in data protection for specific areas

5.6.k. Reporting the data protection activities of the company to local Management, to the departments of the area concerned and to the Group DPO

5.6.l. Notification and reporting

It is the responsibility of the Information Officer to report personal Data breaches and if relevant notify the concerned Data Subjects.

It is therefore of outmost importance that all employees are aware of the data breach process applied in each company.

The Group DPO must always be informed without undue delay if:

- Personal Data has been disclosed to unauthorised persons or otherwise unlawfully processed or processed in a manner not in accordance with this policy or if tangible facts justify a corresponding suspicion and as a result of this, harms to the rights or protected interests of a significant amount of Data Subjects is anticipated;
- there is a statutory reporting duty to a public authority on account of the breach of provisions for protecting Personal Data
- penalties are imposed or have already been imposed on the company by courts or public authorities due to breaches of data protection legislation;
- a national data protection authority has initiated an investigation involving the Business Unit.

5.6.m. Reporting Personal Data breaches where the company is a Responsible Party to the Information Regulator and to the Scania Group DPO

5.6.n. Notifying the Group DPO if the National Data Protection Authority has initiated an investigation involving the local company.

A DPC is obligated to preserve the confidentiality of all matters that become known to them in their capacity as DPC.

5.7. Privacy Manager

The management of each company in the Scania Group shall appoint a person affiliated with the company as the Privacy Manager who is responsible for the following:

5.7.a. ensuring compliance with the statutory and company specific provisions governing the protection of Personal Data

5.7.b. bound by the Group and Business Unit's processes, methods and instructions, and is ultimately responsible for data protection

5.7.c. Consequently ensure the priority given to this matter with respect to resources and knowledge supply.

5.7.d. shall empower the line managers to apply privacy mindset and embed data protection in their daily work.

6. Information security organisation

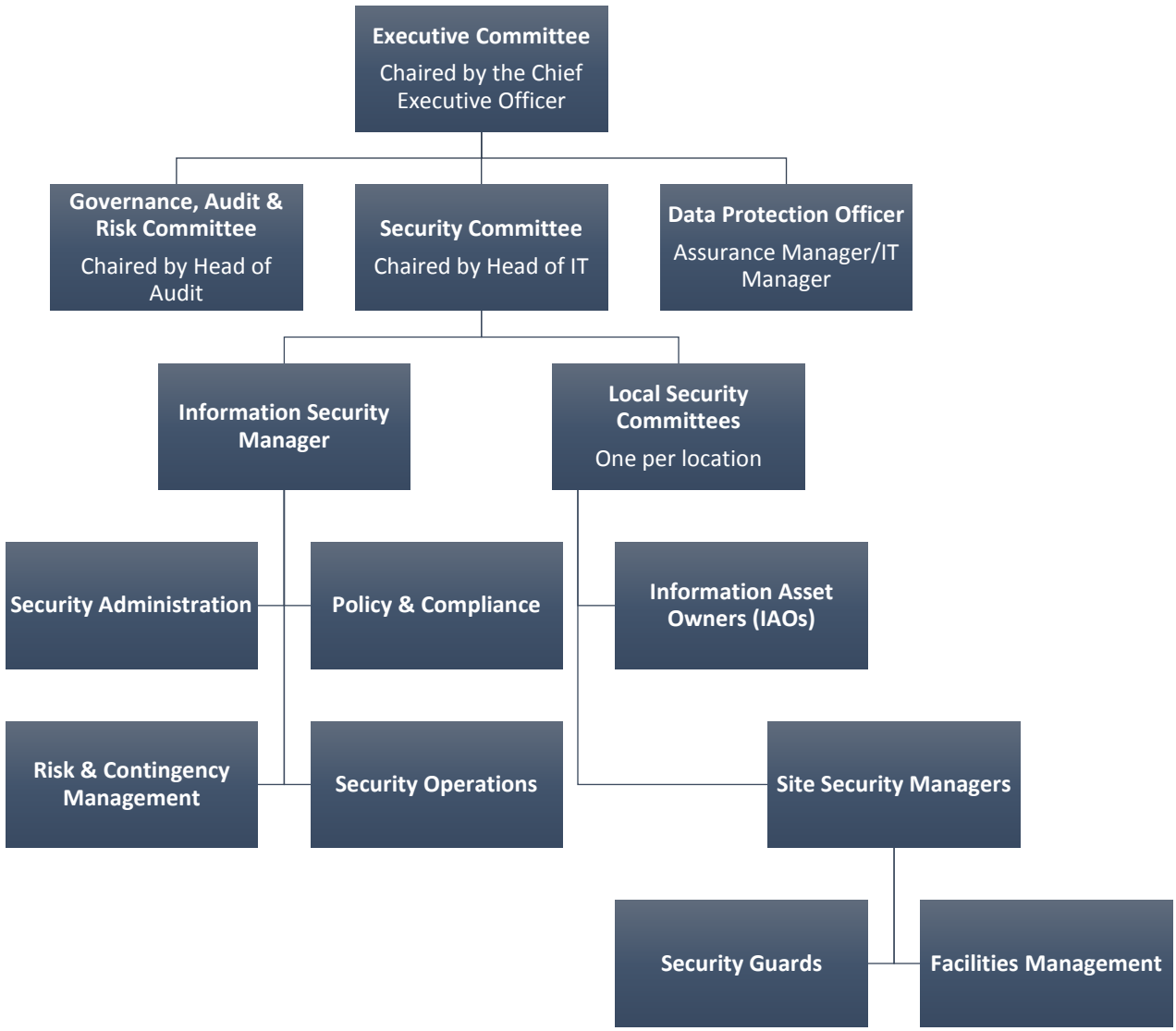
Data protection and information security tasks are tightly integrated within the context of technical and organisational protection of Personal Data. Information security supports the company's data protection activities in particular by defining and supplying the required technical and organisational security measures.

Furthermore, the data protection and information security organisations inform each other regularly about processes and methods that may be significant to the other respective area. See also the policy SGP32 Information Security.

Scania SA's seeks to manage information security as an organizational wide combined effort and as a result, Scania SA has configured a multi-disciplinary information security management organizational structure which will oversee information security matters as

per the Information Security Policy with the aim of fulfilling requirements of the Personal Protection of Information Act (POPIA) and EU General Data Protection Regulation (GDPR)

6.1. Information Security Structure



6.2. Management Commitment to Information Security

The Board of Directors ("the Board") is ultimately accountable for Scania SA's corporate governance as a whole as per the proposed King Code IV of Governance principle implementation.

Chief Executive Officer (CEO) of SCANIA SA has delegated information security as follows:

- Protection of information policies: IT and Group Assurance
- Protection of information processes and systems: IT Manager
- Resourcing of the protection of information strategy with competent people: Head of HR
- Data Protection Officer (DPO): {Confirm}

Executive and Non-Executive Directors give overall strategic direction by approving and mandating the information security principles and axioms but delegate operational responsibilities for physical and information security to the Security Committee (SC) chaired by the Head of IT

The board relies on the Information Security Organization Structure/Security Committee to:

- Coordination of information security throughout Scania SA which include updating of policies, procedures, records management and awareness
- Inform the audit and risk committee about new threats, risks and issues
- Resource Scania SA with right level of skills, systems and processes to mitigate risks as per the continuously revised risk register and treatment plan.
- Ensure that Scania SA's practices are aligned to signed off policies, processes and procedures.

The Executive Directors demonstrate their commitment to information security by:

- A statement of support from the CEO;

- Reviewing and re-approving the policies and procedures every year;
- Approving the IT budget including a specific element set aside for information security;
- Receiving and acting appropriately on management reports concerning information security performance metrics, security incidents, investment requests etc.

6.3. Information security co-ordination

The information Security Committee shall be responsible for information security coordination and ensure that Information security activities are procedurally coordinated throughout Scania SA to ensure consistent application of the security practices, processes and policy statements.

The Executive Directors have empowered the Security Committee with the task of securing Scania SA's information assets. The Security Committee is responsible for:

- Management oversight and direction for both physical and logical aspects of information security including digital and physical security;
- Coordinating and directing Scania SA entire security framework, including the information security controls at all Scania SA's locations mediated through the Local Security Committees (see below);
- Commissioning or preparing information security policy statements, ensuring their compliance with the processes and procedures approved by the Executive Directors, and formally approving them for use throughout Scania SA;
- Annual reviewing of the security policy statements and procedures to ensure the efficiency and effectiveness of the information security controls infrastructure as a whole, recommending improvements wherever necessary;
- Identifying significant trends and changes to Scania SA's information security risks and, where appropriate, proposing changes to the controls framework and/or policies by sponsoring major strategic initiatives to enhance information security;
- Reviewing serious security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes through the corrective action request process;

- Periodically reporting on the status of the security controls infrastructure to the Executive Directors and liaising as necessary with the Risk Management and Audit Committees and other interested and affected partners using metrics and other information supplied by the IT Manager, Group Assurance, Local Security Committees, Internal Audit and others.

The SC can delegate some of its responsibilities but remains accountable to the Executive Directors for the overall effectiveness of information security throughout Scania SA.

Business units or locations within SCANIA SA have Local Security Committees (LSCs) which report to the SC. LSCs are responsible for:

- Providing the strategic direction, support and resources necessary to manage all types of local security issues and thus ensure that SCANIA SA's information assets are appropriately and consistently protected;
- Coordinating and sharing information with each other to ensure consistent execution of the information security policy manual across all SCANIA SA's locations;
- Identifying specific Significant Information Assets, classifying them and nominating suitable Information Asset Owners (IAOs) for them;
- Gathering metrics and other information on the overall effectiveness of information security controls in their remit, and reporting this to the SC.

6.4. Allocation of information security responsibilities

The Executive Directors have appointed a {Role to be confirmed}. The {Role to be confirmed} is responsible for:

- Chairing the Security Committee;
- Taking the lead on information governance, providing the overall strategic direction, support and review necessary to ensure that information assets are identified and suitably protected throughout Scania SA;
    - Appointing and managing the ISM and Information Security Management team.

The ISM and Information Security Management are responsible for:

- Defining technical and non-technical information security standards, procedures and guidelines;
- Supporting IAOs and managers in the definition and implementation of controls, processes and supporting tools to comply with the policy manual and manage information security risks;
- Reviewing and monitoring compliance with the policy statements and contributing to Internal Audit and Control Self Assessment (CSA) processes;
- Collecting, analyzing and commenting on information security metrics and incidents;
- Supporting IAO's in the investigation and remediation of information security incidents or other policy violations;
- Liaising as necessary with related internal functions such as IT Operations, Risk Management, Compliance and Internal Audit, as well as the LSCs, SC and external functions such as the Information Regulator and Police when appropriate;
- Organizing a security awareness campaign for personnel to enhance the security culture and develop a broad understanding of the requirements of the Protection of information Act, EU General Data Protection Regulation and ISO/IEC 27001:2013 Information Security Management System {confirm}

Managers throughout Scania SA are responsible for:

- Day-to-day implementation of the information security policy and associated policies, procedures and manuals;
- Ensuring that suitable technical, physical and procedural controls are in place in accordance with the manual and are properly applied and used by all workers. They must take measures to ensure that workers:

- Are informed of their obligations to fulfill relevant corporate policy statements by means of appropriate awareness, training and education activities;
- Comply with the policy statements and actively support the associated controls; and
- Are monitored to assess their compliance with the policy statements and the correct operation of the associated controls, and reminded of their obligations as appropriate;

- Providing the direction, resources, support, and review necessary to ensure that information assets are appropriately protected within their area of responsibility;
- Informing Information Security Management and/or IAOs of actual or suspected policy violations (information security incidents) affecting their assets; and
- Evaluating compliance with the policy axioms through the regular CSA process and occasional Internal Audits.

Information Asset Owners (IAOs) are managers held accountable for the protection of particular Significant Information Assets by their LSC or the SC. IAOs may delegate information security tasks to managers or other individuals but remain accountable for proper implementation of the tasks. IAOs are responsible for:

- Appropriate classification and protection of the information assets;
- Specifying and funding suitable protective controls;
- Authorizing access to information assets in accordance with the classification and business needs;
- [For new application system developments] Undertaking or commissioning information security risk assessments to ensure that the information security requirements are properly defined and documented during the early stages of development;
- Ensuring timely completion of regular system/data access reviews; and
- Monitoring compliance with protection requirements affecting their assets.

All Scania SA workers (i.e. employees on the payroll and others acting in a similar capacity, such as contractors, consultants, student placements etc.) are responsible for:

- Complying with the procedures and policies in the information security policy manual where relevant to their jobs.
- Maintaining the security of all information entrusted to them.
- Upon hire, as a condition of employment, each worker undertakes to comply with SCANIA SA's information security policies.

Any worker failing to comply with the security policies could be subject to disciplinary action, potentially including termination of employment or contract and/or prosecution.