



EUROFREIGHT LOGISTICS LTD

## **Data Privacy Policy**

---

## Contents

1.	Introduction .....	4
2.	Purpose .....	4
3.	Scope .....	4
4.	Objective .....	4
5.	Accountability and Management.....	5
6.	Privacy Notice and Transparency.....	5
7.	Choice and Consent.....	6
8.	Collection of Personal Information .....	7
9.	Data Minimization.....	8
10.	Limiting Use, Disclosure and Retention .....	8
11.	Data Subject Rights and Requests.....	8
12.	Transfer Limitation.....	9
13.	Disclosure to Third Parties .....	9
14.	Security Practices for Privacy .....	10
15.	Quality of Personal Information.....	11
16.	Privacy Monitoring and Enforcement .....	11
17.	Personally Identifiable Information (PII) of Eurofreight employee .....	11
18.	Staff data processing activities.....	11
19.	Record Keeping (Privacy Register).....	13
20.	Retention of records .....	13
21.	Data Privacy Impact Assessments (DPIA) .....	13
22.	Data Flow Management.....	14
23.	Monitoring .....	14
24.	CCTV .....	15
25.	Reporting Data Privacy Breach: .....	15
26.	Exceptions and exclusions:.....	15
27.	Glossary .....	15
28.	Appendix A: Privacy Principles .....	17
29.	Appendix B: Privacy Organization structure .....	18
30.	Appendix C: Privacy Impact Assessment guidelines .....	21
31.	Appendix D: Data breach response guidelines.....	23
32.	Appendix E: Data privacy controls .....	24

<b>Document Control</b>			
Document Title	Data Privacy Policy	Revision	0.1
Document Owner	EUROFREIGHT LOGISTICS LTD	Placement	
Location	Cyprus	Effective Date	February 2019
Department	Data Protection Office	Review Frequency	Annual

<b>Authorization</b>		
Prepared By	Reviewed By	Approved By
EY		
Signature / Date	Signature / Date	Signature / Date
EY / February 2019		

<b>Revision History</b>				
Revision No.	Effective Date	Prepared By	Approved By	Description
0.1	February 2019	EY		

---

## 1. Introduction

EUROFREIGHT LOGISTICS LTD and affiliated entities (here after “company acronym”, “we”, “our”, “us”, “the Company”) endeavours to meet leading standards for data protection and privacy. This Privacy policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

While our reasons are founded in ethical and corporate responsibility, our privacy practices as outlined in this policy facilitate the establishment of the following:

- ▶ **Competitive Advantage:** Our emphasis on protecting the privacy of customers, vendors, and employees distinguishes us from our competitors.
- ▶ **Good Corporate Citizenship:** A sound privacy policy is emblematic of reliable corporate citizens that respect data subjects’ privacy.
- ▶ **Business Enablement:** Since Eurofreight uses significant volumes of personal information, privacy notices become a prerequisite to building enduring business relationships.
- ▶ **Legal Protection:** Appropriate privacy notices offer an opportunity to eliminate allegations of unlawful usage of personal information.
- ▶ **Comply with the General Data Protection Regulation (GDPR):** failure to comply with the provisions of the GDPR may expose Eurofreight to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher.

This document (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

## 2. Purpose

This Policy defines requirements to help ensure compliance with laws and regulations applicable to Eurofreight collection, storage, use, transmission, disclosure to third parties and retention of Personal and special categories of personal data (also referred to as personal and sensitive personal information respectively in this policy).

## 3. Scope

This policy is applicable to all Eurofreight employees, contractors, vendors, interns, customers, and business partners who may receive personal information from Eurofreight, have access to personal information collected or processed by or on behalf of Eurofreight, or who provide information to Eurofreight.

This policy covers the treatment of personal information gathered and used by Eurofreight for lawful business purposes. This policy also covers the personal information we share with authorized Third Parties or that Third Parties share with us.

## 4. Objective

The main objectives of the Data Privacy Policy are:

- ▶ To ensure that all the personal information in Eurofreight custody is adequately protected against threats to maintain its security.
- ▶ To ensure that Eurofreight employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches.
- ▶ To limit the use of personal information to identified business purposes for which it is collected.
- ▶ To create an awareness of privacy requirements to be an integral part of the day to day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy.
- ▶ To make all the employees aware about, the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal information.
- ▶ To ensure that all third parties collecting, storing and processing personal information on behalf of Eurofreight provide adequate data protection.
- ▶ To ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal information are adhered to.

## 5. Accountability and Management

- 5.1. A Data Privacy Policy shall be developed and maintained to document the privacy principles and practices followed by Eurofreight. (Refer: Appendix A – Privacy principles)
- 5.2. A privacy organization shall be defined for governance of data privacy initiatives. (Refer: Appendix B – Privacy organization structure)
- 5.3. A Data Privacy Officer (DPO) shall be appointed (or DPO function) to process complaints and requests for information related to Eurofreight privacy practices.
- 5.4. Implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- 5.5. Establish procedures for the identification and classification of personal information.
- 5.6. Eurofreight Privacy Policy statement shall be made available on Eurofreight internal portal.
- 5.7. The Data Privacy Policy shall be communicated to Eurofreight internal personnel.
- 5.8. Procedures shall be established for disciplinary and remedial action for violations of the Data Privacy Policy.
- 5.9. Changes or updates to the Data Privacy Policy shall be communicated to Eurofreight internal personnel when the changes become effective.
- 5.10. Establish procedures for performing mandatory registration with regulatory bodies.
- 5.11. Risk Assessment is to be carried out on a periodic basis to ensure risks to personal information are identified and mitigated.
- 5.12. The potential impact on data privacy is assessed when new processes involving personal information are implemented, or when significant changes are made to such processes. (Refer: Appendix C – Privacy Impact Assessment guidelines)

## 6. Privacy Notice and Transparency

- 6.1. Appropriate notice shall be provided to data subjects at the time personal information is collected.
- 6.2. When Eurofreight is the Data Controller for PII data it must provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent,

- intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.
- 6.3. The privacy notice or policies and other statements to which they are linked shall provide as full information as is reasonable in the circumstances to inform an individual how their personal information will be used so that Eurofreight use is fair and lawful. The following information should be considered for inclusion in a notice (as is appropriate in individual circumstances):
- 6.3.1. Purposes for which personal information is collected, used and disclosed;
  - 6.3.2. Choices available to the individual regarding collection, use and disclosure of personal information, wherever applicable;
  - 6.3.3. Period for which personal information shall be retained as per identified business purpose or as mandated by regulations, whichever is later;
  - 6.3.4. That personal information shall only be collected for the identified purposes;
  - 6.3.5. Methods employed for collection of personal information, including 'cookies' and other tracking techniques, and third party agencies;
  - 6.3.6. That an individual's personal information shall be disclosed to Third Parties only for identified lawful business purposes and with the consent of the individual, wherever possible;
  - 6.3.7. That an individual's personal information may be transferred within Eurofreight entities, globally as per requirement, for business purposes with adequate security measures required by law or as per guidance of provided by industry leading practices;
  - 6.3.8. Consequences of withholding or withdrawing consent to the collection, use and disclosure of personal information for identified purposes;
  - 6.3.9. Data subjects are responsible for providing Eurofreight with accurate and complete personal information, and for contacting the entity if correction of such information is required;
  - 6.3.10. Process for an individual to view and update their personal information records;
  - 6.3.11. Process for an individual to register a complaint or grievance with regard to privacy practices at Eurofreight;
  - 6.3.12. Contact information of person in charge of privacy practises and responsible for privacy concerns with address at Eurofreight;
  - 6.3.13. Process for an individual to withdraw consent for the collection, use and disclosure of their personal information for identified purposes; and
  - 6.3.14. That explicit consent is required to collect, use and disclose personal information, unless a law or regulation specifically requires or allows otherwise.
- 6.4. Data subjects shall be provided a Privacy Notice in case any new purpose is identified for using or disclosing personal information before such information is used for purposes not previously identified.
- 6.5. When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

## 7. Choice and Consent

- 7.1. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

- 7.2. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.
- 7.3. If Consent is given in a document which deals with other matters, then the Consent must be explicit from those other matters.
- 7.4. A Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.
- 7.5. Consent may need to be refreshed if there is intention to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.
- 7.6. Explicit consent shall be obtained from data subjects at the time of collection of personal information or as soon as practical thereafter.
- 7.7. Explicit consent shall be obtained from data subjects for the collection, use and disclosure of their personal information, unless a law or regulation specifically requires or allows otherwise. A record is maintained of explicit consent obtained from data subjects.
- 7.8. Consent shall be obtained from data subjects before their personal information is used for purposes not previously identified.
- 7.9. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.
- 7.10. Eurofreight must maintain evidence on types of Consent and keep records of all Consents captured so that the Company can demonstrate compliance with Consent requirements.
- 7.11. Requests for consent should be designed to be appropriate to the age and capacity of the data subject to consent for themselves and to the particular circumstances (e.g. children who are not older than 16th, vulnerable data subjects unable to understand and consent for themselves).
- 7.12. Organisation should establish communication guidelines to notify other data controllers (with whom PII was shared) for rectification/deletion/restricting of personal data of data subject.
- 7.13. Organisation should document guidelines for managing directories of subscribers to electronic services which include the following:
  - Guidelines for obtaining consent from the end users.
  - What information is to be provided to the data subject at the time of data collection (purpose, search functions, right to object and information how personal data can be rectified or deleted).

## 8. Collection of Personal Information

- 8.1. The collection of personal information shall be limited to the minimum requirement for lawful business purposes.
- 8.2. The GDPR allows Processing for specific purposes, some of which are set out below:
  - a. The Data Subject has given his or her Consent;
  - b. The Processing is necessary for the performance of a contract with the Data Subject;
  - c. To meet our legal compliance obligations;
  - d. To protect the Data Subject's vital interests;
  - e. To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need

- 
- to be set out in applicable Privacy Notices or Fair Processing Notices; or
- f. [OTHER GDPR PROCESSING GROUNDS]: identify and document the legal ground being relied on for each Processing activity [in accordance with the Company's guidelines on Lawful Basis for Processing Personal Data].
- 8.3. Methods of collecting personal information shall be reviewed by management to ensure that personal information is obtained:
    - 8.3.1. Fairly, without intimidation or deception, and
    - 8.3.2. Lawfully, adhering to laws and regulations relating to the collection of personal information.
  - 8.4. Management shall confirm that Third Parties from whom personal information is collected:
    - 8.4.1. Use fair and lawful information collection methods, and
    - 8.4.2. Comply with the Eurofreight Data Privacy Policy and their contractual obligations with respect to the collection, use and transfer of personal information on behalf of Eurofreight
  - 8.5. Data subjects shall be notified if additional information is developed or acquired about them.
9. Data Minimization
- 9.1. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
10. Limiting Use, Disclosure and Retention
- 10.1. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
  - 10.2. Personal information retention shall be only for the duration necessary to fulfil the identified lawful business purposes or as prescribed by law.
  - 10.3. Guidelines and procedures shall be developed for the retention and disposal of personal information. These shall address minimum and maximum retention periods, and modes of storage.
  - 10.4. Upon the expiration of identified lawful business purposes or withdrawal of consent, Eurofreight shall either securely erase or anonymize the data subjects' personal information. Data is anonymized to prevent unique identification of an individual.
11. Data Subject Rights and Requests
- 11.1. The organisation should ensure that it has established the following:
  - 11.2. The organization has established mechanism for data subjects to raise requests related to their rights (access/rectification) electronically (especially where personal data are processed by electronic means).
  - 11.3. Organization has established following related to right of access and rectification:
    - 11.3.1. Documented process and mechanism for provisioning access to personal data and rectification.
    - 11.3.2. Identified mandatory information to be provided to data subject
    - 11.3.3. Guidelines for administrative fees can only be charged to data subject for subsequent PI access
    - 11.3.4. Personal Data to be provided in electronic form unless requested otherwise



- 
- 11.3.5. Track the received requests from data subjects and respond within 1 month with appropriate response
  - 11.4. Assessments are performed regularly – and at least annually – of whether the rectification of personal data has been performed correctly and without undue delay.
  - 11.5. Organization has established following related to right of deletion:
    - 11.5.1. Policies and procedures to process/respond to PI deletion requests from data subjects within 1 month
    - 11.5.2. Documented the Personal data deletion guidelines considering the grounds for deletion and the applicable exceptions
  - 11.6. Organization has established guidelines for restrictions of data processing which address:
    - 11.6.1. Documented grounds which are compared with criteria for restricting mentioned in the data subject request and a formal sign-off process to ensure that appropriate decisions are taken and implemented for a defined period of time
    - 11.6.2. Process to inform data subject prior to lifting the restriction of processing of personal data
  - 11.7. Organization has implemented mechanism to inform data subjects if it alters, restricts the processing of or removes personal data.
  - 11.8. Organization has established guidelines to process data portability requests from data subjects. The guidelines are compliant with data portability considerations.
  - 11.9. Organization has established means for data subject to object online.

## 12. Transfer Limitation

- 12.1. Eurofreight shall limit data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined
- 12.2. Eurofreight may only transfer Personal Data outside the EEA if one of the following conditions applies:
  - (a) The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
  - (b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
  - (c) The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
  - (d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

## 13. Disclosure to Third Parties

- 13.1. Where reasonably possible, management shall ensure that third parties collecting, storing or processing personal information on behalf of Eurofreight have:

- 
- 13.1.1. Signed agreements to protect personal information consistent with Eurofreight Data Privacy Policy and information security practices or implemented measures as prescribed by GDPR;
  - 13.1.2. Signed non-disclosure agreements or confidentiality agreements which includes privacy clauses in the contract; and
  - 13.1.3. Established procedures to meet the terms of their agreement with Eurofreight to protect personal information.
- 13.2. Personal information may be transferred outside European Union (EU) jurisdiction from where Eurofreight operates for storage or processing where any of the following apply:
- 13.2.1. The individual has given consent to the transfer of information
  - 13.2.2. The transfer is necessary for the performance of a contract between the individual and Eurofreight, or the implementation of pre-contractual measures taken in response to the individual's request.
  - 13.2.3. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between Eurofreight and a third party.
  - 13.2.4. The transfer is necessary or legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
  - 13.2.5. The transfer is required by law
  - 13.2.6. The transfer is necessary in order to protect the vital interests of the individual.
  - 13.2.7. The transfer is made under a data transfer agreement.
  - 13.2.8. The transfer is otherwise legitimised by applicable law.
- 13.3. Remedial action shall be taken in response to misuse or unauthorized disclosure of personal information by a third party collecting, storing or processing personal information on behalf of Eurofreight

#### 14. Security Practices for Privacy

- 14.1. Eurofreight information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by Eurofreight.
- 14.2. Eurofreight shall comply with all applicable aspects of Eurofreight Information Security Program or comply with the administrative, physical and technical safeguards implemented and maintained in accordance with the GDPR and relevant standards to protect Personal Data.
- 14.3. Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.
- 14.4. Management shall establish procedures that maintain the logical and physical security of personal information.
- 14.5. Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
- 14.6. Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices. (Refer: Appendix D – Data breach response guidelines)
- 14.7. Eurofreight must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows: (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.  
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.  
(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

---

## 15. Quality of Personal Information

- 15.1. Eurofreight may perform additional validation procedures to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
- 15.2. Eurofreight shall ensure that personal information collected is relevant to the business purposes for which it is to be used.

## 16. Privacy Monitoring and Enforcement

- 16.1. Procedures shall be established for recording and responding to complaints/ grievances registered by data subjects.
- 16.2. Each complaint regarding privacy practices registered by data subjects shall be validated, responses documented and communicated to the individual.
- 16.3. Annual privacy compliance review shall be performed for identified business processes and their supporting applications.
- 16.4. A record shall be maintained of non-compliances identified in the annual privacy reviews. Corrective and disciplinary measures shall be initiated and tracked to closure, guided by Eurofreight management.
- 16.5. Procedures shall be established to monitor the effectiveness of controls for personal information and for ensuring corrective actions, as required.
- 16.6. Any conflicts or disagreements relating to the requirements under this policy or associated privacy practices shall be referred to the Data Privacy Officer for resolution.

## 17. Personal Identifiable Information (PII) of Eurofreight employee

Data protection laws govern the use of personally identifiable information. This term means any data relating to a living individual who can be identified using that data. Eurofreight may hold the following types of sensitive and non-sensitive PII:

- names, addresses, telephone numbers and other personal contact details;
- gender, date of birth, physical or mental health or condition;
- marital status, next of kin, racial or ethnic origin, sexual orientation, religious, philosophical, political or similar beliefs;
- national insurance or social insurance number, immigration status, trade union membership;
- personnel records including training, appraisal, performance and disciplinary information, and succession planning;
- bank details, salary, bonus, benefits and pension details and other financial information; and
- criminal offences committed (or allegedly committed) including any proceedings and sentencing in relation to any such criminal offence.

## 18. Staff data processing activities

Personal information about individuals may only be processed for a legitimate purpose. Eurofreight may undertake a number of activities with an individual employee's personal information including, but not limited to:

- salary, benefits and pensions administration;
  - health and safety records and management;
  - security vetting, criminal records checks and credit checks and clearances (where applicable and allowed by law);
  - confirming information on résumés, CVs and covering letters, providing reference letters and performing reference checks;
  - training and appraisal, including performance evaluation and disciplinary records;
  - staff management and promotions;
  - succession planning;
  - equal opportunities monitoring;
  - any potential change of control of a group company, or any potential transfer of employment relating to a business transfer or change of service provider;
  - other disclosures required in the context of staff employment;
  - promoting or marketing of Eurofreight, its products or services;
  - provision of staff or business contact information to customers and agencies in the course of the provision of Eurofreight's services;
  - CCTV monitoring for security reasons;
  - compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches;
  - establishing, exercising or defending Eurofreight's legal rights;
  - disclosures to other companies in the Eurofreight group of companies, including companies in other countries to the extent permitted by law, including for the following purposes: as required in connection with the duties of the employee; legal compliance; audit; group level management; in connection with the fulfilment of customer and partner contracts;
  - any other reasonable purposes in connection with an individual's employment or engagement by Eurofreight;
  - providing and managing use of services provided by third parties, such as company provided mobile phones, company credit cards and company cars and billing for such services.
- 18.1. Eurofreight may also collect and process personal information about your next of kin, so they can be contacted in an emergency or in connection with use of a company car provided by Eurofreight. Their personal information will also be processed in accordance with the data protection laws and as described in the policy.
- 18.2. In order to fulfil the purposes set out above, Eurofreight may disclose personal information to contractors and suppliers that provide services to Eurofreight and who may assist in the processing activities set out above and also to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law or for administration/taxation purposes, to the extent local law allows and requires.
- 18.3. Eurofreight may disclose your personal information to third parties for the purposes of establishing and managing your employment relationship. For example, Eurofreight may disclose some of your personal information to:
- benefits providers (for example, pension and insurance providers);
  - payroll and data processing suppliers and other service providers who assist us in establishing or managing your employment relationship with us;
  - insurance claims and medical related service providers; and
  - parties requesting an employment reference.

- 
- 18.4. Eurofreight shall take appropriate measures to ensure that its contractors and suppliers also process personal information in a compliant way and such measures may include a data processing agreement.
- 18.5. Eurofreight may transfer personal information to other group companies, partners, suppliers, law enforcement agencies and to other organisations in all cases that are located outside of the country where you are based for the purposes of:
- HR administration (for example, staff recruitment);
  - payroll processing for employees working outside the country where they are based;
  - employee relocation;
  - security clearances;
  - visa applications;
  - taxation and registrations for employees working outside the country where they are based;
  - fulfilling Eurofreight's legal requirements;
  - fulfilling customer contracts for the provision of Eurofreight's services;
  - overseas legal proceedings;
  - Outsourcing Eurofreight functions.
- 18.6. The laws of some jurisdictions may not be as protective as the laws in the country in which you are based. Eurofreight may transfer your personal information across provincial or national borders to fulfil any of the above purposes, including to service providers located in countries who may be subject to applicable disclosure laws in those jurisdictions, which may result in that information becoming accessible to law enforcement and national security authorities of those jurisdictions.
19. Record Keeping (Privacy Register)
- 19.1. Eurofreight shall keep full and accurate records of all data Processing activities.
- 19.2. Eurofreight must keep and maintain accurate corporate records reflecting Processing including records of Data Subjects' Consents and procedures for obtaining Consents.
- 19.3. These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.
20. Retention of records
- 20.1. Eurofreight has a statutory duty to keep certain records for a minimum period of time. In other cases Eurofreight shall not keep personal information for longer than is necessary or as may be required by applicable law.
21. Data Privacy Impact Assessments (DPIA)
- 21.1. The organisation should conduct Data Privacy Impact Assessment (DPIA) for its business activities for which the processing of personal data is "likely to result in a high risk to the rights and freedoms of natural persons". A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights

---

and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

- 21.2. The firm should assess all its business processes and define which of them are high-risk. For the purpose of the assessment it should use appropriate risk criteria to help on the factual identification of high-risk business processes. (ie. criteria as set in the Article 29 of GDPR PIA evaluation).
- 21.3. The organisation should choose a methodology for the implementation of its DPIAs. The DPIA should be compliant with the minimum features described in Annex 2 in Article 29 of GDPR on performing DPIA.
- 21.4. The company should continuously review and re-assess its business activities as certain changes could increase or decrease their risk.

## 22. Data Flow Management

- 22.1. For all high-risk business procedures as defined in the Privacy Impact Assessment.
- 22.2. Organisation should define guidelines for data mapping. Data mapping addresses below mentioned:
  - Documenting the data processing activities.
  - Type of personal data used for each processing activity along with personal data storage location.
  - The organisation should identify and document data flows specific to how personal information is moving through the underlying systems and software within the organization (including third party operations).

## 23. Monitoring

- 23.1. Eurofreight's IT and communications systems are intended to promote effective communication and working practices within our organisation.
- 23.2. For business reasons, and in order to carry out legal obligations in our role as an employer, use of Eurofreight's systems on whatever platform including the telephone (mobile and fixed) and computer systems (including email and internet access), and any personal use of them, is monitored. If you access services by the use of passwords and login names on Eurofreight's IT and communication systems, this might mean that your personal access details are seen by Eurofreight.
- 23.3. Monitoring is only carried out if and to the extent permitted or as required by law and as necessary and justifiable for business purposes. The resulting log files may be used so that instances of attempted misuse and other security events can be detected, and that information is available to support any subsequent investigation. To the extent permitted by law and, where breaches of this and other Eurofreight policies or applicable law are found, action may be taken under the disciplinary procedure.
- 23.4. The employees are informed that the telephone system used by the Company allows identification of all dialled numbers and received calls.
- 23.5. Eurofreight reserves the right to retrieve the contents of messages, check searches which have been made on the internet, require the immediate return of devices supplied by Eurofreight and access data stored on such devices for the following purposes (this list is not exhaustive):
  - to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy (and employees acknowledge that the Company can use software to monitor the identity of senders and receivers of emails);
  - to find lost messages or to retrieve messages lost due to computer failure;
  - to assist in the investigation of wrongful acts; or

- to comply with any legal obligation.

23.6. If evidence of misuse of Eurofreight's IT systems is found, Eurofreight may undertake a more detailed investigation in accordance with Eurofreight's disciplinary procedures, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary, such information may be handed to the police in connection with a criminal investigation. Investigations and disclosure of information to the relevant authorities shall be carried out only to the extent permitted by law.

## 24. CCTV

- 24.1. Some of Eurofreight's buildings and sites use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded. Use of CCTV and recording of CCTV data is only carried in accordance with Eurofreight approved guidelines.
- 24.2. Eurofreight shall take reasonable efforts to alert the individual that the area is under electronic surveillance.

## 25. Reporting Data Privacy Breach:

- 25.1. The GDPR requires Data Controllers to notify any Personal Data Breach to the Cyprus Data Protection regulatory authority and, in certain instances, the Data Subject.
- 25.2. Eurofreight shall put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where is legally required to do so.
- 25.3. Where there is a suspicion of a Personal Data Breach occurrence, the DPO, the information technology or security department should be notified immediately and should follow the Eurofreight SECURITY INCIDENT RESPONSE PLAN. All evidence relating to the potential Personal Data Breach should be preserved.

## 26. Exceptions and exclusions:

- 26.1. Controls related to monitoring of Eurofreight's IT system and Infrastructure will not be applicable to Eurofreight's operations in <this scenario or in this location>.

## 27. Glossary

Term	Definition
Anonymize	To process a collection of personal data or information such that a natural person cannot be identified on the basis of the output collection of data or information
Data subject	A living individual about whom personal information is processed by or on behalf of Eurofreight
Vulnerable data subject	A Data subject that may be over the age of 16 however do not have the competence to understand and consent for themselves
"Eurofreight", "we", "our", "us", "the Company"	EUROFREIGHT SYSTEMS LIMITED / its Subsidiaries / its Group Companies / its affiliates, its directors, employees (excluding the User/affirming employee in this context), assigns and successors.

Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Personal Data or personal information	Any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person
Sensitive personal data or sensitive personal information	<p>Definition of sensitive personal information as per various laws are stated below:</p> <p><u>The Data Protection Act, United Kingdom</u>          Sensitive personal data means personal data consisting of information as to:</p> <ol style="list-style-type: none"> <li>1) the racial or ethnic origin of the data subject,</li> <li>2) his political opinions,</li> <li>3) his religious beliefs or other beliefs of a similar nature,</li> <li>4) whether he is a member of a trade union,</li> <li>5) his physical or mental health or condition,</li> <li>6) his sexual life,</li> <li>7) the commission or alleged commission by him of any offence, or</li> <li>8) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.</li> </ol> <p><u>The Federal Data Protection Act, Germany</u>          ‘Special categories of personal data’ (Sensitive personal data) shall mean information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.</p> <p><u>The Federal Data Protection Act, Switzerland</u>          Sensitive personal data: data on:</p> <ol style="list-style-type: none"> <li>1) religious, ideological, political or trade union-related views or activities,</li> <li>2) health, the intimate sphere or the racial origin,</li> <li>3) social security measures,</li> <li>4) administrative or criminal proceedings and sanctions;</li> </ol> <p>- Data file: any set of personal data that is structured in such a way that the data is accessible by data subject;          - Personality profile: a collection of data that permits an assessment of essential characteristics of the personality of a natural person;</p>
Third party	All external parties – including without limitation contractors, interns, summer trainees, vendors, service providers and partners – who have access to Eurofreight information assets, information systems or who are pass personal information from them.



---

## 28. Appendix A: Privacy Principles

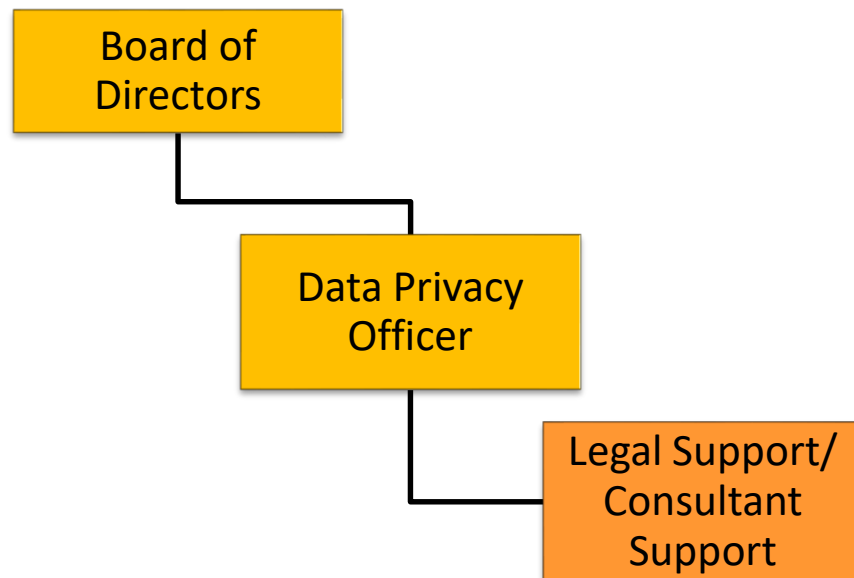
Eurofreight Data Privacy Policy aligns with Generally Accepted Privacy Principles. In view of the changing legislative and technological environment for data privacy, the Data Privacy Policy will undergo revisions. The guiding privacy principles articulated in this policy document are as follows:

- ▶ **Management:**  
Define, document, communicate, and assign accountability for Eurofreight Data Privacy policy and procedures
- ▶ **Notice:**  
Provide notice about Eurofreight Data Privacy policy and procedures and identify the purposes for which personal information is collected, used, retained, and disclosed
- ▶ **Choice and Consent:**  
Describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information
- ▶ **Collection of personal information:**  
Collect personal information only for the purposes identified in the notice
- ▶ **Limiting Use, Disclosure and Retention:**  
Limit the use, storage and retention of personal information is limited to the purposes identified in the data privacy notice and for which the individual has provided implicit or explicit consent. Retain personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately dispose of such information.
- ▶ **Access for review and update:**  
Provide data subjects with access to their personal information for review and update
- ▶ **Disclosure to third parties:**  
Disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual
- ▶ **Security practices for privacy:**  
Protect personal information against unauthorized access (both physical and logical)
- ▶ **Quality of personal information:**  
Maintain accurate, complete, and relevant personal information for the purposes identified in the notice
- ▶ **Monitoring and enforcement:**  
Monitor compliance with Eurofreight Data Privacy policy and procedures, and have procedures to address privacy related complaints and disputes

## 29. Appendix B: Privacy Organization structure

The privacy organization has been designed keeping in mind the various business units across locations where Eurofreight operates. Stakeholders and oversight from key business functions and senior leadership provides sustainable and practical guidance for the privacy framework.

### 29.1. Privacy organization structure



### 29.2. Board of Directors

The role of the Board of Directors is to channel resources and address organizational issues related to privacy.

Responsibilities of Board of Directors:

- ▶ Review and approve the Data Privacy Policy at least on a three-year cycle.
- ▶ Establish a process for the enforcement of Data Privacy Policy.
- ▶ Ensure the implementation of a data privacy program that enables compliance with the Data Privacy Policy and applicable regulations with respect to data protection.
- ▶ Define processes to address grievances and handling complaints from data subjects with respect to their personal information held by Eurofreight.
- ▶ Determine the action to be taken against grievances and information request cases presented by the Data Privacy officer.
- ▶ Review the findings from periodic privacy compliance reviews and sanction the implementation of corrective actions if applicable.
- ▶ Monitor the data privacy program effectiveness.
- ▶ Identify and appoint a Data Privacy officer.

### 29.3. Legal Support

The role of the Legal Support is to guide and monitor the data privacy program and present timely reports to the Board

#### Responsibilities of Legal Support:

- ▶ Provide legal assistance to the Data Privacy Officer for identifying applicable regulations relations related to data privacy.

#### 29.4. Data Privacy Officer

The role of Data Privacy Officer (DPO) is to act as a central resource for the implementation of Eurofreight privacy program. The DPO is required to advocate for the privacy program, articulate and communicate the organization's privacy goals, and promote enforcement of the Data Privacy Policy. The DPO will act as a single point of contact for internal personnel as well as external data subjects seeking redress regarding their personal information held by Eurofreight or information about Eurofreight privacy practices.

#### Responsibilities of Data Privacy Officer (DPO):

- ▶ Conduct review of the Data Privacy Policy over a three-year cycle and recommend changes or policy updates to the Board.
- ▶ Monitor compliance with the Data Privacy Policy.
- ▶ Provide counsel relating to privacy aspects of business contracts and partnerships.
- ▶ Participate in audits
- ▶ Coordinate with the offices of governmental agencies and supervisory authorities during the investigation of a privacy complaint against the organization.
- ▶ Handle requests for information made by individuals and third-party agencies (including law enforcement agencies).
- ▶ Ensure that the Data Privacy Policy is aligned with applicable laws or regulations and updated when there are changes to legislation.
- ▶ Facilitate privacy awareness training for all employees of Eurofreight. The privacy awareness training should be designed with the following considerations:
  - ▶ Providing briefings, information and resources for employees to keep them apprised of current and emerging privacy requirements;
  - ▶ Providing employees with adequate guidance on identifying and appropriately handling data protection issues that may affect the performance of their job; and
  - ▶ Sensitizing employees to the importance of data privacy to data subjects and the organization.
- ▶ Maintain an organization-wide view of business processes impacting privacy, and the nature, size and sensitivity of personal information held by Eurofreight.
- ▶ Respond to data breach notifications as per the defined data breach response plan.
- ▶ Implement processes to address grievances and handling complaints from data subjects with respect to their personal information held by Eurofreight.
- ▶ Respond to requests for access to and correction of personal information and general issues concerning personal information held by Eurofreight.
- ▶ Maintain a record of all grievances and inquires registered by data subjects.
- ▶ Collate all grievances and information requests along with relevant and share relevant details to the Board for exceptions to established response processes.
- ▶ Facilitate the periodic (three-year cycle) independent privacy compliance reviews, either through the Internal Audit function or an independent Third-Party auditor. Through the compliance review process the following are to be considered:
  - ▶ Present the findings from the periodic privacy compliance reviews and privacy impact assessment to the Board.
  - ▶ Perform annual personal information inventory review and ensure reconciliation with the information asset inventory.

- 
- ▶ Formulate mitigation strategies for identified risks to privacy arising from Eurofreight business operations, data collection practices, supporting technology, facilities and services exchanged with external parties.
  - ▶ Provide counsel relating to privacy aspects of business contracts and partnerships.
  - ▶ Ensure that the Data Privacy Policy is aligned with applicable laws or regulations and updated when there are changes to legislation.
  - ▶ Act as a liaison person for data privacy legal issues between the business functions and external Legal support if required.

### 30. Appendix C: Privacy Impact Assessment guidelines

A Privacy Impact Assessment (PIA) can be used to demonstrate that the system owners and functional management have applied data privacy controls throughout the system development lifecycle. In addition, performing a PIA for proposed changes identifies any conflicts between the post-implementation state and the privacy framework. For example, the PIA prior to introducing a new business application will identify if the way personal information is shared by the new application is in violation of the Data Privacy Policy.

A PIA should be triggered by events that significantly change the privacy environment of the company or if an existing process which significantly affects the privacy rights of data subjects is identified. For example, the introduction of new technology may change the manner in which personal information is stored and processed. In some cases, the technology may only collect personally identifiable information for a moment. For example, a security camera stream may capture the movements of an individual. While a record may not be maintained for later use, the initial capture and viewing may raise privacy concerns and a PIA could be required. Other instances of technology with privacy implications include: systems utilizing radio frequency identification devices (RFID), biometric scans, data mining, or location tracking.

In other cases, the technology may not be changing, but a program or system opts to use data from a new source such as a commercial aggregator of information. A PIA is required when such new sources of information are used.

The introduction of a new business process and notable changes to existing business processes may trigger a PIA for various reasons. New business processes may introduce new uses of personal information, new information systems and infrastructure supporting the changed processes, and new methods of collection, processing and disclosure. Some new business processes may require updates to agreements and contracts, potentially impacting the management of personal information.

At minimum, the following triggers should be considered:

PIA Trigger	Description
Digitization of records	Converting paper-based records to electronic systems.
Anonymous to Non-Anonymous	Operations performed on existing personal information database changes anonymous information into Sensitive Personal Information (SPI) or personal information (PII).
Significant System Management Changes	New uses of existing IT systems, including application of new technologies, significantly changes how SPI or PII is managed in the system. For example, when the company employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.
Significant Merging	The company adopts or alters business processes so that databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously an issue.

PIA Trigger	Description
New User Access Mechanism	User-authentication technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by users (including Third Party users).
External Sources	The company systematically incorporates into existing information systems, databases of personally identifiable information purchased or obtained from third parties or public sources. An exception to this trigger would be merely querying such a source on an ad hoc basis using existing technology.
New Uses	Business partners work together on initiatives involving significant new uses or exchanges of information in identifiable form, such as marketing for products and solutions developed as joint ventures. In such cases, the Eurofreight Data Privacy Officer should be consulted and prepare the PIA.
Internal Flow or Collection	Alteration of a business process that results in significant new uses or disclosures of information, including incorporation into the system of additional PII.
Alteration in Character of Data	New PII is added to a database or information collection and thus, raises the risks to personal privacy. For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.
New Processes	Introduction of new business process that results in multiple triggers and changes to business agreements impacting management of personal information.

For a PIA performed on systems or projects prior to their implementation, responses to the PIA Questionnaire should be populated based on the planned system/ project specifications and processes.

---

## 31. Appendix D: Data breach response guidelines

The immediate response upon discovery of a data breach leading to compromise of personal information records should align with the information security incident response plan. This document provides guidelines on the procedural steps to be taken at minimum.

### 31.1. Incident reporting and tracking

- ▶ All privacy data breaches should be logged as incidents and [follow the incident reporting procedures] reported to the DPO with the information set out below to be provided. Please refer Incident Management Procedure for detailed actions.
- ▶ Ensure that the following information is captured:
  - ▶ Date of the incident
  - ▶ Time of the incident, if possible
  - ▶ Date and time when the incident was discovered
  - ▶ How the incident was discovered
  - ▶ Location of the incident
  - ▶ Suspected cause of the incident
  - ▶ The number of individuals whose data is affected

### 31.2. Breach containment and preliminary analysis

- ▶ Contain the breach and isolate the affected environment if possible.
- ▶ Notify the DPO and identify data subjects who will facilitate the investigation. The Data Privacy Officer (DPO) should lead the initial investigation or appoint an appropriate individual to act as a proxy.
- ▶ Identify the internal stakeholders who are affected by or involved in the data breach.
- ▶ Ensure that collection of incident information and evidences does not lead to accidental destruction of admissible evidence. Evaluate the risks associated with the data breach. [This should lead to identification of the following:
  - ▶ What personal information was involved
  - ▶ Extent of the data breach
  - ▶ How many data subjects were affected and who they are
  - ▶ What harm to the data subjects could result from the data breach
  - ▶ What harm to Eurofreight could result from the data breach]
- ▶ If the data breach involves theft, cybercrime or other criminal activity, notify the police and Computer Emergency Response Team (CERT).

### 31.3. The DPO, in consultation of the legal support, should:

- ▶ Determine whether the Cyprus DPA need to be notified.
- ▶ Determine what details should be included in the DPA notification.
- ▶ Determine whether affected data subjects need to be notified of the data breach.
- ▶ Define how and when affected data subjects should be notified.
- ▶ Determine what details should be included in the notification.
- ▶ Determine what other external stakeholders should be informed (Governmental Agencies, professional bodies, supervisory authorities, etc.)]

## 32. Appendix E: Data privacy controls

Data privacy controls have been developed based on the privacy principles. These controls serve as a means to measure the extent of implementation of the Data Privacy Policy.

Principles	Privacy security control	Owner	Review frequency
<b>Management</b>	Data Privacy Policy is documented	Data Privacy Officer	Annual
	Data Privacy Policy is published and communicated to all Eurofreight employees	Data Privacy Officer	Annual
	Consequences of non-compliance with Data Privacy Policy are periodically (at least annually) communicated to Eurofreight' employees responsible for collecting, using, retaining and disclosing personal information	Data Privacy Officer	Annual
	Changes in privacy policies are communicated to Eurofreight' employees shortly after the changes are approved	Data Privacy Officer	Annual
	Responsibility and accountability are assigned to an individual or group for developing, documenting, implementing, enforcing, monitoring and updating Eurofreight Data Privacy Policy	Data Privacy Officer	Annual
	The names of the individual or group and their responsibilities for developing, documenting, implementing, enforcing, monitoring and updating Data Privacy Policy are communicated to Eurofreight' employees	Data Privacy Officer	Annual
	Non-Disclosure Agreements (NDA) or Confidentiality Agreements are signed with Eurofreight' employees who access personal information records as part of their job role	Privacy Compliance Auditor and/or Data Privacy Officer	Annual
	Data Privacy Policy and changes to it, are reviewed and approved by management	Data Privacy Officer	Annual



Principles	Privacy security control	Owner	Review frequency
	Data Privacy Policy and associated procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made.	Privacy Compliance Auditor and/or Data Privacy Officer	Annual
	Data Privacy Policy and associated procedures are revised to conform to the requirements of applicable laws and regulations.	Privacy Compliance Auditor and/or Data Privacy Officer	Annual
	The Data Privacy Registry is developed and maintained. The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified in the Data Privacy Registry. Assets containing personal information records are classified as 'Confidential' and security controls are applied accordingly.	Data Privacy Officer	Annual
	Personal information is covered by the entity's privacy and related security policies and procedures.	Data Privacy Officer	Annual
	A risk assessment process is used to establish a risk baseline and, at least annually, to identify new or changed risks to personal information and to develop and update responses to such risks.	Board of Directors	Annual
	Identified privacy risks and privacy risk responses are aligned with the enterprise risk management framework (if available)	Board of Directors	Annual

Principles	Privacy security control	Owner	Review frequency
	Eurofreight internal personnel or advisors review contracts for consistency with Data Privacy Policy and associated procedures and address any inconsistencies.	Privacy Compliance Auditor and/or Data Privacy Officer	Annual
	Contracts are revised or amended to address identified inconsistencies with Data Privacy Policy and associated procedures	Privacy Compliance Auditor and/or Data Privacy Officer	Annual
	<p>The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following (but not limited to):</p> <ul style="list-style-type: none"> <li>▶ Infrastructure</li> <li>▶ Systems</li> <li>▶ Applications</li> <li>▶ Web sites</li> <li>▶ Procedures</li> <li>▶ Products and services</li> <li>▶ Data bases and information repositories</li> <li>▶ Mobile computing and other similar electronic devices</li> </ul>	Data Privacy Officer	Quarterly
	Privacy requirements are included in the functional and technical specification for all information system acquisition and development	Data Privacy Officer	Quarterly

Principles	Privacy security control	Owner	Review frequency
	<p>The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected and authorized in accordance with Eurofreight' Data Privacy Policy</p>	Data Privacy Officer	Quarterly
	<p>A documented privacy incident and breach management program has been implemented. For this purpose standard contractual templates are used for contracts involving personal information. The contracts contain instruction for approved handling of personal data and breach management guidelines. This should include, but is not limited to, the following:</p> <ul style="list-style-type: none"> <li>▶ Procedures for the identification, management and resolution of privacy incidents and breaches</li> <li>▶ Defined responsibilities</li> <li>▶ A process to identify incident severity and determine required actions and escalation procedures</li> <li>▶ A process for complying with breach laws and regulations, including stakeholder breach notification, if required</li> <li>▶ An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties or discipline, as appropriate</li> <li>▶ A media representative to manage public perception/internal efforts during an active breach incident</li> <li>▶ A process for periodic review (at least annually) of actual incidents to identify necessary program updates based on the following:               <ul style="list-style-type: none"> <li>▶ Incident patterns and root cause</li> <li>▶ Changes in the internal control environment or external requirements (regulation or legislation)</li> </ul> </li> <li>▶ Periodic testing or walkthrough process (at least annually) and associated program remediation as needed</li> </ul>	Data Privacy Officer	Annual
	<p>Procedures are established for the communication of privacy breaches in Eurofreight to the affected data subjects, relevant authorities and internal stakeholders</p>	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	<p>Qualification criteria are established for Eurofreight' internal personnel responsible for protecting the privacy and security of personal information. Such responsibilities are assigned only to those personnel who meet these qualifications and have received the necessary training.</p>	Board of Directors	Annual
	<p>A privacy awareness program is established to include the following:</p> <ul style="list-style-type: none"> <li>▶ Information about the Data Privacy Policy and related matters provided to Eurofreight' internal personnel</li> <li>▶ Specific training for selected internal personnel depending on their privacy roles and responsibilities.</li> </ul>	Data Privacy Officer	Annual
	<p>For the jurisdiction in which Eurofreight operates, the effect on privacy requirements from changes in the following factors is identified and addressed:</p> <ul style="list-style-type: none"> <li>▶ Legal and regulatory</li> <li>▶ Contracts, including service-level agreements</li> <li>▶ Industry requirements</li> <li>▶ Business operations and processes</li> <li>▶ People, roles, and responsibilities</li> <li>▶ Technology</li> </ul> <p>Privacy policies and procedures are updated to reflect changes in requirements.</p>	Data Privacy Officer	Quarterly
	<p>The need to register/notify with data protection authorities in countries in which Eurofreight has operations is assessed and existing registrations/notifications are reviewed.</p>	Data Privacy Officer	Annual
<b>Notice</b>	<p>Notice is provided to the individual about Eurofreight Data Privacy Policy and associated procedures at collection or before the time personal information is collected, or as soon as practical thereafter</p>	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	Notice is provided to the individual about Eurofreight Data Privacy Policy and associated procedures at the time these are changed or as soon as practical thereafter	Data Privacy Officer	Annual
	Notice is provided to the individual about the Eurofreight' Data Privacy Policy and new purposes for personal information before their personal information is used for new purposes not previously identified.	Data Privacy Officer	Annual
	Data Privacy Policy is made available to data subjects (published on corporate website and at points of information collection)	Data Privacy Officer	Annual
	Data Privacy Policy is made available to data subjects (provided to external parties in hardcopy)	Data Privacy Officer	Annual
	Data Privacy Policy notifies data subjects of the personal information collected, purpose of collection, disclosure policy, and security practices.	Data Privacy Officer	Annual
	Data Privacy Policy describes the particular entities, business functions, locations and types of information to which the privacy policy applies	Data Privacy Officer	Annual
	Data Privacy Policy is in plain and simple language	Data Privacy Officer	Annual
	Data Privacy Policy is appropriately labelled and easy to locate (document should not be misleadingly or ambiguously labelled, link to privacy policy on the corporate website should be on the homepage or clearly designated location)	Data Privacy Officer	Annual
	Data Privacy Policy is linked to and displayed before all points of personal information collection	Data Privacy Officer	Annual
<b>Choice and Consent</b>	<p>The privacy notice describes following in a clear and concise manner:</p> <ul style="list-style-type: none"> <li>▶ Choices available to the individual regarding collection, use and disclosure of personal information.</li> </ul>	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	<ul style="list-style-type: none"> <li>▶ The ability of, and process for, an individual to change contact preferences.</li> </ul> <p>That explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.</p>		
	<ul style="list-style-type: none"> <li>▶ Data subjects are notified of the consequences of denying or withdrawing consent to the collection and use of their personal information (e.g. certain services cannot be provided to the customer or certain IT resources cannot be made available without the collection of personal information)</li> </ul>	Data Privacy Officer	Annual
	Explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented. A record is maintained of all explicit consent obtained from data subjects.	Data Privacy Officer	Annual
	If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified and explicit consent is obtained prior to such new use or purpose.	Data Privacy Officer	Annual
	Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.	Data Privacy Officer	Annual
	Consent is obtained before personal information is transferred to/from an individual's computer or similar device.	Data Privacy Officer	Annual
	Data Privacy Policy addresses the collection of personal information	Data Privacy Officer	Annual
	Data subjects are informed that personal information is collected only for the purposes identified in the notice.	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
<b>Collection</b>	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.	Data Privacy Officer	Annual
	Collection of personal information is limited to that necessary for the purposes identified in the privacy notice.	Data Privacy Officer	Annual
	Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained: (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	Data Privacy Officer	Annual
	Eurofreight' management authority confirms that external parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.	Data Privacy Officer	Annual
	External parties from whom personal information is collected (i.e. sources other than the individual) comply with the Eurofreight Data Privacy Policy and contractual obligations with respect to their collection and transfer of personal information records on behalf of Eurofreight	Data Privacy Officer	Annual
	Data subjects are informed if Eurofreight develops or acquires additional information about them for its use.	Data Privacy Officer	Annual
	Data Privacy Policy addresses the use, retention, and disposal of personal information.	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	Data subjects are informed that personal information is: (a) used only for the purposes identified in the notice and only if the individual has provided explicit consent, unless a law or regulation specifically requires otherwise; (b) retained for no longer than necessary to fulfil the stated purposes, or for a period specifically required by law or regulation, and (c) disposed of in a manner that prevents loss, theft, misuse or unauthorized access.	Data Privacy Officer	Annual
<b>Use, Retention, and Disposal</b>	Personal information is used only for the purposes identified in the notice and only if the individual has provided explicit consent, unless a law or regulation specifically requires otherwise.	Privacy Compliance Auditor and/or Data Privacy Officer	Annual
	Retention schedule is defined for personal information, based on the duration of lawful business purpose for which personal information was collected	Data Privacy Officer	Annual
	Retention period of personal information records is communicated to the custodians of these records	Data Privacy Officer	Annual
	Secure disposal of personal information records follows the same procedure as 'Confidential' information assets	Data Privacy Officer	Annual
	Personal information is disposed as per the defined personal information retention schedule	Data Privacy Officer	Annual
	Data Privacy Policy addresses providing data subjects with access to their personal information.	Data Privacy Officer	Annual
<b>Access</b>	Data subjects are provided the means to request access to their personal information record in Eurofreight' custody	Data Privacy Officer	Annual



Principles	Privacy security control	Owner	Review frequency
	The identity of data subjects is verified before providing access to their personal information records in Eurofreight' custody	Data Privacy Officer	Annual
	Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.	Data Privacy Officer	Annual
	Data subjects are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.	Data Privacy Officer	Annual
	Data subjects are provided the means to update their personal information in Eurofreight' custody. Procedures are established for data subjects to correct or update their personal information.	Data Privacy Officer	Annual
	Data Privacy Policy addresses the disclosure of personal information to external parties	Data Privacy Officer	Annual
	Data subjects are informed that personal information is disclosed to external parties only for the purposes identified in the notice and for which the individual has provided explicit consent unless a law or regulation specifically allows or requires otherwise.	Data Privacy Officer	Annual
<b>Disclosure to Third Parties</b>	Data Privacy Policy and other specific instructions or requirements for handling personal information are communicated to external parties to whom personal information is disclosed	Data Privacy Officer	Annual
	Personal information is disclosed to external parties only for the purposes described in the notice, and for which the individual has provided explicit consent, unless a law or regulation specifically requires or allows otherwise.	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	Personal information is disclosed only to external parties who have agreements with Eurofreight to protect personal information in a manner consistent with Eurofreight' Data Privacy Policy and security practices.	Data Privacy Officer	Annual
	Procedures are established to evaluate that the external parties have effective controls to meet the terms of the agreement, instructions, or requirements.	Data Privacy Officer	Annual
	Non-Disclosure Agreements (NDA) or Confidentiality Agreements are signed with external parties before giving them access to personal information records in Eurofreight' custody. The terms of agreement include clauses for remedial action in response to misuse or unauthorized disclosure of personal information by the external party, and Eurofreight' right to audit the personal information protection controls implemented by the external party.	Data Privacy Officer	Annual
	Personal information is disclosed to external parties for new purposes or uses only with the prior explicit consent of the individual.	Data Privacy Officer	Annual
	Eurofreight takes remedial action in response to misuse or unauthorized disclosure of personal information by an external party to whom personal information has been transferred.	Data Privacy Officer	Annual
	Data Privacy Policy (including any relevant security policies) addresses the security of personal information.	Data Privacy Officer	Annual
	Data subjects are informed that precautions are taken to protect personal information.	Data Privacy Officer	Annual
<b>Security</b>	A security program has been developed, documented, approved, and implemented that includes administrative, technical and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction. The security program should address, but	Data Privacy Officer, IT officer	Annual

Principles	Privacy security control	Owner	Review frequency
	<p>not be limited to, the following areas insofar as they relate to the security of personal information:</p> <ul style="list-style-type: none"> <li>a. Risk assessment and treatment</li> <li>b. Security policy</li> <li>c. Organization of information security</li> <li>d. Asset management</li> <li>e. Human resources security</li> <li>f. Physical and environmental security</li> <li>g. Communications and operations management</li> <li>h. Access control</li> <li>i. Information systems acquisition, development, and maintenance</li> <li>j. Information security incident management</li> <li>k. Business continuity management</li> <li>l. Compliance</li> </ul>		
	<p>Information asset labelling and handling guidelines include controls specific to the storage, retention and transfer of personal information</p>	<p>Data Privacy Officer, IT Officer</p>	<p>Annual</p>

Principles	Privacy security control	Owner	Review frequency
	<p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ul style="list-style-type: none"> <li>a. Authorizing and registering internal personnel and data subjects</li> <li>b. Identifying and authenticating internal personnel and data subjects</li> <li>c. Making changes and updating access profiles</li> <li>d. Granting privileges and permissions for access to IT infrastructure components and personal information</li> <li>e. Preventing data subjects from accessing anything other than their own personal or sensitive information</li> <li>f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities</li> <li>g. Distributing output only to authorized internal personnel</li> <li>h. Restricting logical access to offline storage, backup data, systems and media</li> <li>i. Restricting access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)</li> </ul>	Data Privacy Officer, IT Officer	Annual
	<p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ul style="list-style-type: none"> <li>j. Preventing the introduction of viruses, malicious code, and unauthorized software</li> </ul>	Data Privacy Officer, IT Officer	Annual
	<p>Physical access is restricted to personal information in any form (including the components of Eurofreight' information systems that contain or protect personal information).</p>	Data Privacy Officer, IT Officer	Annual
	<p>Hardcopy personal information record storage is located in access-controlled areas</p>	Data Privacy Officer, IT Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	Access logs are maintained for physical access to hardcopy personal information records storage and any components of Eurofreight' information systems that store personal information	Data Privacy Officer, IT Officer	Annual
	Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	Data Privacy Officer, IT Officer	Annual
	Personal information is protected when transmitted by mail or other physical means.	Data Privacy Officer, IT Officer	Annual
	Automated controls are established to validate the information provided from the data subject during data collection (e.g. through a web application form).	Data Privacy Officer, IT Officer	Annual
	Encryption is enabled for the collection and transmission of personal information over the Internet, over public and other non-secure networks or wireless networks	Data Privacy Officer, IT Officer	Annual
	Personal information stored on portable media or devices is protected from unauthorized access. Access to removable storage media (CDs, USB drives, external hard drives) and portable electronic devices (laptops, phones, tablets) that contain personal information is controlled or prohibited.	Data Privacy Officer, IT Officer	Annual
	Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.	Data Privacy Officer, IT Officer	Annual
	Privacy policies address the quality of personal information.	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	<p>Business continuity and IT Disaster Recovery plans to restore operations in case of disaster are defined, documented and implemented. In particular the organization should establish, but not be limited to, the following:</p> <ol style="list-style-type: none"> <li>a. Plans and recovery procedures detailing how organization will manage a disruptive event and will maintain its information security requirements to a predetermined level.</li> <li>b. Procedures to maintain existing information security controls during an adverse situation.</li> <li>c. Compensating controls for information security controls that cannot be maintained during adverse situation.</li> </ol>	Data Privacy Officer, IT Officer	Annual
	Data subjects are informed that they are responsible for providing Eurofreight with accurate and complete personal information and for contacting the entity if correction of such information is required.	Data Privacy Officer	Annual
<b>Quality</b>	Personal information is accurate and complete for the purposes for which it is to be used.	Data Privacy Officer	Annual
	Personal information is relevant to the purposes for which it is to be used.	Data Privacy Officer	Annual
	Privacy policies address the monitoring and enforcement of privacy policies and procedures.	Data Privacy Officer	Annual
	Data subjects are informed about how to contact the entity with inquiries, complaints and disputes.	Data Privacy Officer	Annual
<b>Monitoring and Enforcement</b>	A process is established to address inquiries, complaints and disputes.	Data Privacy Officer	Annual
	Each complaint is addressed, and the resolution is documented and communicated to the individual.	Data Privacy Officer	Annual

Principles	Privacy security control	Owner	Review frequency
	Compliance with Data Privacy Policy and associated procedures, privacy commitments and applicable laws, regulations, service-level agreements and other contracts is reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	Data Privacy Officer	Annual
	Annual privacy compliance reviews are conducted for business processes and supporting applications	Data Privacy Officer	Annual
	Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.	Data Privacy Officer	Annual
	On-going procedures are performed for monitoring the effectiveness of controls over personal information based on a risk assessment and for taking timely corrective actions where necessary.	Data Privacy Officer	Annual