PRIVACY POLICY

Version: 1.0

Version date: 11 October 2022

Table of contents

1 Legal and strategic framework

1.1 Legal

On 25 May 2018 the GDPR (General Data Protection Regulation) became binding law in all EU Member States. The purpose of the GDPR is to protect and regulate the privacy of all those located in the EU.

This policy sets out, inter alia, the way in which the obligations arising under the GDPR will be applied, and proper compliance with these obligations supervised, within the ECT organisation.

1.2 Strategic

ECT is committed to the careful processing of Personal Data. This means that ECT takes seriously the job of protecting the privacy of its employees, customers, and other business relations. ECT expects its employees and external partners to be aware of the confidential nature of Personal Data and to handle it with care.

When it handles Personal Data, ECT is guided by its privacy principles, which are:

1. The safe storage of data;
2. The conscious sharing of information;
3. The respecting of each person's privacy;
4. The immediate reporting of any (potential) data leak;
5. Ensuring that Data Subjects are able to exercise their rights.

1.3 Revision

This policy document will be assessed every three years by the privacy coordinator and, where necessary, updated. Irrespective of whether the document is updated, it will be submitted to the board every three years for its approval, whereby the policy for the next three years will be adopted.

It is possible for there to be an intermediate revision of the document on the instructions of the director responsible for data protection, or because a revision becomes necessary. In such cases too, the revised Privacy Policy will be submitted to the board for its approval.

2 Definitions, roles and responsibilities

2.1 Definitions

- **Dutch DPA:** Dutch Data Protection Agency.

- **Data Subject:** any party to whom Personal Data relates.

- **Special categories of Personal Data:** Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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, data pertaining to criminal-law, and related security measures.

Security incident: a breach of security that threatens or could threaten the availability, integrity or confidentiality of data or data-processing systems.

- **Data breach:** a security incident whereby Personal Data is mistakenly or unlawfully destroyed, lost, or amended, or where the unlawful disclosure of, access to, or processing of such Personal Data cannot reasonably be excluded.

- **ECT:** ECT Delta Terminal B.V. and Euromax Terminal Rotterdam B.V.

- **Personal Data:** any information pertaining to an identified or identifiable natural person.
  ECT regards all data that is directly or indirectly traceable to a natural person as Personal Data. The term 'natural person' also includes partnerships, but not legal entities [1]. However, if the UBO (Ultimate Beneficial Owner [2]), or representative of the legal entity is a natural person, then such person does qualify as a natural person. The term only covers living persons.
  The privacy coordinator (see section 2.2.2) ensures that there is sufficient understanding of the term 'Personal Data' within ECT.

- **Sub-processor:** the party designated by the Processor who is instructed by the Processor to process Personal Data.

- **Processing of Personal Data:** any operation or set of operations relating to Personal Data, including collection, recording, structuring, storage, adaptation or alteration, consultation, use, disclosure and destruction.
  Within ECT, personal data is processed in paper form and digitally in various ways. The processing register and accompanying matrix set out all processes as well as the applications used in the storage and processing of Personal Data.

- **Processor:** the party that processes Personal Data for the Controller, without being under the control of the Controller. The Controller is the party that decides on the methods of processing.

- **The Controller:** ECT.

2.2 Roles and responsibilities

The roles and responsibilities pertaining to data protection within ECT are set out under a matrix of six functions and organs that together ensure the correct level of technical and organisational security measures for the protection of Personal Data.

2.2.1 Director responsible for data protection

ECT expressly focuses attention on data protection, which is embedded in its organisational structure. The responsibility for protecting Personal Data ultimately lies with the Director HR & Services or (in their absence) with a deputy appointed by such director (the 'responsible director').

[1] A legal entity is expected to stipulate the need for confidentiality either in a non-disclosure agreement or as a term of a contract.

[2] A UBO is in respect of a private or public limited company, a natural person who directly or indirectly is entitled to at least 25% of the economic ownership of a company, or who exercises control over such company. This 25% rule does not include quoted companies.

Responsibilities

I. The responsible director ensures that the company applies adequate data protection. His tasks include supervising the management, periodic testing, and accountability in the field of data protection. He ensures that privacy is embedded as much as possible in a management system file, that is also used for quality and certification purposes.

II. He[3] requests the board to give attention to the adequate functioning of ECT's privacy management system ('management review').

III. He will decide whether any (potential) Data Breach should be reported to the Dutch DPA.

IV. The responsible director shall be notified whenever a Data Subject wishes to exercise their rights.

2.2.2 Central privacy coordinator

ECT has appointed a central policy coordinator ('policy coordinator') for the entire company and Data Subjects outside the organisation. This role has been assigned to both the Legal Counsel HR and the Enterprise (Security) Architect, who jointly act as privacy coordinator and are engaged in the daily (operational/tactical) aspects of privacy management within ECT. The privacy coordinator reports to the responsible director and functions as the contact person for the Dutch DPA.

Responsibilities

I. The privacy coordinator is the contact person for any Data Subject seeking to exercise their privacy rights. He ensures an adequate compliance with these rights within the stipulated 'reasonable' term of one month following receipt of the request (extendable by a maximum additional period of two months). The privacy coordinator will take such steps once the responsible director has been informed of the situation.

II. The privacy coordinator will also ensure that the agreed procedure for data breaches is followed in respect of any potential Data Breach. The privacy coordinator will investigate a Data Breach together with, and as part of, the privacy team to discover what exactly has occurred and to be able to fully inform the responsible director.

III. The privacy coordinator ensures that reports are made to the Dutch DPA, but only after conducting an investigation into the facts and with the consent of the responsible director.

IV. The privacy coordinator and the privacy team are together responsible for the operational management of ECT's privacy management system. This involves keeping in good order the administrative organisation that covers, inter alia, the privacy statements, the processing contracts, the procedure for notification of data breaches, the processing activities, and the processing register, in accordance with the management agreements. The privacy coordinator conducts (or arranges for the conducting of) the operational checks and draws up the reports by which the company can demonstrate that it is in control of data protection.

V. The privacy coordinator periodically tests whether ECT processes data in accordance with the principles and issues a periodic report to the responsible director. The privacy coordinator also draws the attention of the director for data protection and employees (where relevant) to the correct application of the said principles.

[3] Reference to the masculine pronoun in this text includes reference to the feminine pronoun.

2.2.3 Privacy team

The team supporting the privacy coordinator and the board for the management and continued development of the privacy management system. The team comprises all members of the Governance, Risk & Compliance Team and has the expertise to support ECT's privacy management.

Responsibilities

I. The privacy team and the privacy coordinator are together responsible for the operational management of ECT's privacy management system.

II. The team is involved in advising about, and controlling, the privacy management system and in taking the necessary measures.

III. In the event of a potential security incident and/or Data Breach, the team follows the agreed privacy procedures. Where necessary, the team assists with an investigation into the facts carried out by the privacy coordinator, and thereby attempts to discover whether the incident constitutes a Data Breach and the relevant circumstances.

IV. Members of the privacy team are responsible for conducting an annual update of the processing activities, for which purpose each member completes the processing activity form for the department-specific processes for which they are responsible.

2.2.4 Process owners

Each process owner is responsible for guaranteeing the privacy measures within their own process. They are supported in this by the privacy coordinator, who supplies them with the correct mechanisms to be able to carry out the relevant tasks.

Responsibilities

I. The process owner ensures within their own process for Privacy by design (see § 5.4) and Privacy by default (see § 5.5).

II. The process owner is responsible for reporting security incidents and data breaches within their own process.

III. The process owner is responsible for deciding on the processing activities for their own process. The privacy coordinator supports this decision making.

2.2.5 Employees

All employees of ECT are obliged to deal with Personal Data in accordance with the obligations under the GDPR.

Responsibilities

I. Employees are responsible for compliance with the GDPR within their own range of tasks.

II. Employees should recognise and report potential incidents that could result in a Data Breach.

III. A deliberate failure to report an incident is a reason to potentially impose sanctions.

2.2.6 The Works Council

The Works Council shall be notified about the state of data protection within ECT.

In regard to the adoption, amendment of, or withdrawal of the Privacy Policy, the Procedure for mandatory notification of data breaches, the Privacy Regulation and the Employees Privacy Statement, and any other regulation or part thereof, concerning the processing and/or protection of Personal Data of employees of ECT the consent of the Works Council is required.

2.2.7 The external supervisor, the Dutch DPA

ECT and the Processors it engages must always cooperate with the Dutch DPA and comply with requests for information within reasonable and stipulated timeframes.

3 Processing of Personal Data

3.1 The principles of processing Personal Data

Within ECT Personal Data is processed in accordance with the principles set out in the GDPR. The GDPR sets out the following principles[4]:

I. Personal Data is processed by ECT that with regard to the Data Subject is lawful, fair and transparent (**lawfulness, fairness, and transparency**);

II. Personal Data is collected by ECT for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes (**purpose limitation**);

III. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**);

IV. Personal Data must be accurate and, where necessary, updated by ECT; every reasonable measure must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**);

V. Personal Data is kept in a form by ECT which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (**storage limitation**);

VI. Personal Data is processed by ECT in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

ECT will ensure, and is responsible for, compliance with these principles. As part of its obligation of responsibility, ECT must also be able to demonstrate its compliance with these principles.[5]

[4] Article 5 GDPR.

[5] The guiding principle throughout this policy is accountability (Article 5 section 2 GDPR). See also Q&A on the website of the Dutch DPA.

3.2 Lawfulness of the processing

Within ECT it is not permitted to process Personal Data if there is no basis for such processing. Within ECT the following bases for processing Personal Data may be applied:

I. Performance of a contract: the processing of such Personal Data as is necessary for the performance of a contract to which the Data Subject is a party, or the taking of measures at the request of the Data Subject before entering into the contract (pre-contract phase);

II. Compliance with statutory obligations: the processing of such Personal Data as is necessary to be able to comply with a statutory obligation upon ECT;

III. Legitimate interest: the processing of such Personal Data as is necessary to meet a compelling, legitimate interest of ECT, if this interest outweighs the interests of the Data Subject;

IV. Consent: The Data Subject gives their consent for the processing of Personal Data for one or more specific purposes;

V. Vital interest: The 'vital interest' basis is usually only applied in exceptional circumstances, especially, but not exclusively, where the health of an employee is at stake. For example, a situation may arise where the Personal Data must be processed to be able to provide someone with medical care. This basis may only be applied if no other basis is possible and there is nevertheless a need to process the data to protect a vital interest.

3.2.1 Legitimate interest:

Processing on this basis is not permitted if the interests, basic rights, or fundamental freedoms of the Data Subject outweigh the interests of ECT. If the Data Subject is still a minor, ECT shall not reply on this basis.

A legitimate interest may arise in the case of processing to comply with a duty of care of ECT in the context of prevention of fraud, money laundering, or tax evasion.

3.2.2 Consent:

There is no processing of the personal data of employees on this basis. Processing on this basis requires the consent of the Data Subject. The following requirements must be satisfied:

I. ECT shall inform the Data Subject regarding the identity of ECT, the purpose and legal basis for the processing for which consent is sought, what Personal Data is collected and used, and the rights of the Data Subject with regard to the Processing;

II. it can be established that the Data Subject has given their consent for the processing of their Personal Data on this basis;

III. if consent is sought in writing in a statement that also covers other matters, then it is stated in simple language what the consent relates to;

IV. any consent may subsequently be revoked. A Data Subject will be advised of this before giving their consent. Furthermore, the revocation of the consent must be as

simple a process as the giving of the consent. The revocation of any consent does not work with retroactive effect;

V. a Data Subject under the age of 16 years is deemed unable to give their consent. Consent should be given by persons with parental responsibilities. In such a case, ECT will check whether the person exercising parental responsibility has also given the consent.

3.3 Special Personal Data

ECT does not process Special Personal Data, unless it is under a statutory obligation to do so.

New employees of ECT are screened for their reliability on entering employment. This complies with an obligation by virtue of the AEO status. The screening involves the performance of a background check and the request to supply a certificate of good conduct (VOG).

4 Rights of the Data Subjects

4.1 Rights

Every Data Subject has the right to:

1) information (Article 13 GDPR);
2) access (Article 15 GDPR);
3) rectification (Article16 GDPR);
4) erasure (right to be forgotten) (Article 17 GDPR);
5) restriction of processing (Article 18 GDPR);
6) data portability (Article 20 GDPR);
7) objection (Article 21 GDPR).

If the Data Subject indicates a wish to exercise any of the above rights, the privacy coordinator will comply in accordance with the conditions and time limits set out in the GDPR.

4.2 Informing Data Subjects about their rights

The aforesaid rights are notified to each Data Subject in writing by ECT via its Privacy Statement (on the website), its Employees Privacy Statement (on the Portal), or its Privacy Regulations (Regulations Manual). If ECT receives Personal Data from third parties it must satisfy additional information obligations.

4.3 Requests to exercise rights

All requests to exercise any of the aforesaid rights will be complied with by ECT, unless ECT is unable to satisfy any burden of proof in identifying the Data Subject. In the event of doubt as to the identity of the Data Subject, ECT shall request such additional information as is necessary to establish the identity of the Data Subject.

A request must be complied with by the privacy team within one month of receipt of the request. If having regard to the complexity or number of requests ECT is unable to meet the request within the time limit specified above, this time limit may be extended by a further period of two months by the board. The Data Subject will be notified of such decision within one month of receipt of their request.

A request for information received via electronic communications shall be answered by the same means, unless the Data Subject has requested a hard copy.

If the board of ECT, whether or not on the advice of the privacy coordinator, decides not to comply with a request from the Data Subject, reasons for this refusal must be sent to the Data Subject within four weeks of their request. The Data Subject must also be informed of the opportunity to file a complaint with the Dutch DPA or to bring a claim before the courts.

The Data Subject should be able to exercise their rights cost free, unless:

I. given the repetitive nature or excessiveness of the request reasonably-incurred costs may be passed on; or

II. the request of the Data Subject ought to be refused if it is unjustified.

4.3.1 Request for access

The Data Subject has the right to obtain confirmation as to whether their Personal Data has been processed and, if so, to obtain access to the processed Personal Data, together with:

I. the purposes of processing;

II. the categories of Personal Data involved;

III. the parties to which the Personal Data has been or will be sent;

IV. the storage period or, if it is not possible to indicate this, the criteria for determining the storage period;

V. the right of the Data Subject to request ECT to rectify, delete, restrict the processing, or object to the processing, of the Personal Data;

The Data Subject shall also be informed of their right to file a complaint with the Dutch DPA.

ECT shall give access to a copy of the Personal Data being processed.

4.3.2 Request for rectification

The Data Subject has the right to require ECT to immediately rectify Personal Data about that person that is not correct.

4.3.3 Request for deletion (right to be forgotten)

The Data Subject has the right to request ECT to delete Personal Data processed by ECT. If ECT agrees to the request, it will comply immediately.
Such a request will in any event be complied with if:

I. the Personal Data is no longer needed for the purposes for which it is collected or otherwise processed;

II. the Data Subject has withdrawn their consent and there is no other basis for the processing;

III. the Data Subject has objected to the processing and there are no other overriding interests for processing;

IV. the Personal Data has been unlawfully processed;

V. the Personal Data must be deleted on the basis of EU law or statutory rule.

If the Data Subject whose Personal Data is being stored requests its deletion, the board is entitled to refuse to delete it if the processing is necessary for the institution, exercise or substantiation of a legal claim.

If a request for deletion is complied with, this must be notified to the Data Subject.

4.3.4 Request for restriction on processing

The Data Subject has the right to a restriction on the processing if:

I. the accuracy of the Personal Data is disputed. In such a case, the restriction will be complied with for the duration of the investigation;

II. the processing is unlawful and the Data Subject does not request the deletion of the unlawful data;

III. the Data Subject believes that ECT no longer needs the data for processing, but the Data Subject needs the data to institute a legal claim;

IV. the Data Subject has objected to the processing and awaits a response from ECT as to whether the legitimate grounds override the objection.

4.3.5 Request for transfer of the Personal Data

If the Data Subject requests the transfer of the Personal Data, this request will be handled by the privacy team in accordance with the procedure description for the processing of Personal Data if the request:

I. relates to Personal Data (in)actively supplied by the Data Subject;

II. the processing is based on consent or on performance of the contract[6].

ECT will ensure that the data will be supplied in a structured, generally accepted and computer readable form.

4.3.6 Right to object

A Data Subject always has the right to object to the processing of their Personal Data in the case of Personal Data that has been processed on the basis of a legitimate interest. If ECT processes Personal Data on this basis, the board is authorised, following advice from the privacy coordinator, to find the objection to the processing to be unjustified if in the board's opinion there are compelling legitimate grounds within ECT for the processing that outweigh the interests of the Data Subject. In any event the board will comply with the request of a Data Subject to cease the processing of Personal Data in connection with direct marketing.

[6] ECT is thereby not obliged to transfer the Personal Data being processed on the basis of a statutory obligation.

5 Security

5.1 Introduction

ECT ensures, having regard to the state of the art, the costs of implementation, the risks involved in the implementation, and the nature of the Personal Data, that appropriate technical and organisational measures are taken to protect Personal Data against loss, destruction, damage, forgery, undesired access, distribution, or another other form of misuse.

5.2 System authorisations

The ICT systems within ECT are set up in such a way that information stored within the system is protected against potential misuse. As a preventive measure for the protection of Personal Data systems are equipped with the mechanisms to authenticate and authorise users. These mechanisms assign a role per user by which it can be ascertained whether or not information may be processed. The roles will be tested periodically by ETC (at least twice per year). If a role pursuant to a function ceases to be necessary, the role will be immediately revised.

5.3 System logging

To be able to control the processing of Personal Data, systems are equipped with the mechanisms to record activities, referred to as *logging*. This enables ECT, following a security incident or Data Breach, to investigate the circumstances and any peripheral damage. All logged activities are stored in encrypted form and can only be consulted by authorised employees.

5.4 Privacy by design

ECT ensures that, given the:

I. state of the art;

II. implementation costs;

III. the nature, scope, context, and purpose of the processing;

IV. as regards probability and the seriousness of the risks for the rights and freedoms of natural persons;

both in the choice of processing mechanisms and the processing itself appropriate technical and organisational measures have been drawn up for the purposes of implementing the data protection principles in an effective way and incorporating the necessary guarantees for compliance with the statutory regulations and to protect the rights of Data Subjects.

5.5 Privacy by default

The board of ECT in consultation with the privacy coordinator takes appropriate technical and organisational measures to prevent more Personal Data being processed than is necessary for a particular purpose, or being stored for a too long period, and that access thereto is restricted as far as possible.

6 Data Breaches

6.1 Handling data breaches

A Data Breach is handled and documented in accordance with the procedure descriptions.

In the event of a breach within ECT that involves Personal Data[i] ECT shall notify the Dutch DPA within 72 hours of ECT learning of the breach, unless there is no likelihood that the breach poses a risk to the rights and freedoms of any natural person.

Employees of ECT are expected to report a security incident and/or data breach as soon as possible after its discovery, and in any event within 24 hours of its discovery, via information.security@ect.nl.
If no report is made to the Dutch DPA within 72 hours, the reasons for this delay in reporting must be given.

6.2 Data breaches with Processor

If a Data Breach occurs with the Processor, it must immediately notify the ECT privacy coordinator, and provide the following information:

I. the nature of the breach of the Personal Data;

II. the name of the privacy coordinator or contact person with whom contact may be made;

III. the consequences of the breach;

IV. the measures proposed by the Processor.

6.3 Informing Data Subjects

ECT ensures that a Data Subject is immediately notified if the breach constitutes a high risk for the rights and freedoms of that Data Subject. No reporting is required if the breach comes within an exception to the need to report to Data Subjects as set out in the GDPR. The decision taken by the board will be in accordance with the procedure as set out in section 6.4.

6.4 Procedure for data breaches

The board will decide, on the advice of the privacy coordinator, in what cases a Data Breach is deemed to arise and when Data Subjects need to be informed. In any event, the occurrence will be registered and in the case of a Data Breach will be notified to the Dutch DPA.

7 Processors

7.1 Appointment of Processors

In its business operations, ECT engages a number of Processors which, in the case of an outsourcing relationship, are appointed on the basis of the principles for outsourcing within ECT. This policy formulates a number of processes and requirements that need to guarantee that ECT selects the right party. Under this policy, ECT is obliged to select only those

Processors that can offer adequate guarantees concerning the application of appropriate technical and organisational measures to ensure that the processing satisfies the requirements of the GDPR and guarantees the protection of the rights of the Data Subjects.

7.2 Contract with Processors

ECT uses a standard data processor contract as the basis. However, depending on the situation, either the ECT contract or the processor's own contract can be used. The board ensures, in consultation with the privacy team, that the instruction for the processing of certain Personal Data is set out in a (separate) contract which contains in any event the following matters:

I. the Processor is only entitled to process the Personal Data on the basis of the written instructions from ECT, in which ECT will in any event determine whether there is to be any transfer to third countries or to international organisations, unless the Processor is required to make such transfer under any statutory provisions. The Processor must report any such situation to ECT, unless it is forbidden to do so by any statutory obligation;

II. the Processor may only outsource Personal Data to Sub-processors if ECT has given its written consent. The Processor will impose on the Sub-processor through a sub-processor contract the same obligations as the Processor has towards ECT;

III. the Processor must guarantee that the persons authorised to process Personal Data and any Sub processors are under a duty of confidentiality and observe the same, or are otherwise bound by an appropriate statutory duty of confidentiality;

IV. the Processor will take appropriate measures to secure the Personal Data as specified in Article 32 of the GDPR. The Processor will ensure that any Sub-processors offer at least the same level of data protection as the Processor;

V. the Processor will take the measures set out in this policy in the event of the appointment of another Processor;

VI. the Processor will assist insofar as reasonably possible in a request by a Data Subject to exercise their rights as set out in Part 4 of this policy;

VII. the Processor will assist insofar as reasonably possible to comply with the obligations under the GDPR pertaining to the security of Personal Data, the obligation to notify the Dutch DPA/ Data Subject in the event of a Data Breach, and the carrying out of a DPIA. The Processor must always notify ECT **immediately – and in any event within 24 hours –** in the case of a Data Breach;

VIII. once the service has been supplied, the Processor must destroy the Personal Data and delete copies, unless the Processor is under any statutory obligation to store the same;

IX. the Processor shall assist in establishing accountability and in enabling audits or other inspections by ECT or a third party, and assisting in these. The Processor shall supply ECT with all relevant information to enable it to check compliance with its obligations as Processor;

X. the Processor shall work under the authority of ECT, whereby the Processor shall not process more personal data than is strictly necessary in the context of the engagement;

XI. the Processor shall cooperate with all reasonable requests by ECT or the Dutch DPA, including a request to submit the register of processing activities.

If ECT intends that Personal Data be processed by a Processor, the Purchasing department and the privacy coordinator shall together ensure that the privacy measures taken by the supplier are tested against the requirements set by ECT. The burden of the privacy measures stipulated by the supplier should be proportionate to the degree of privacy-sensitivity of the Personal Data to be processed, on the basis that the Personal Data must be adequately protected against unauthorised processing.

7.3 Appointment of Sub-processor

If the Processor intends for all or any part of the work to be carried out by (another) Sub-processor it must first obtain the written consent of ECT. If at the time of entering into the contract the Processor has already made use of Sub-processors, then at the request of ECT the names of such parties must be disclosed to ECT. The Processor is responsible for ensuring that the terms set out in section 7.2 are included in the contract and that this contract also stipulates that the Processor remains liable despite the appointment of other Sub-processors.

8 Processes register

8.1 Requirements for the register

ECT shall ensure that all processing of Personal Data of ECT is registered in a processes register. The register shall as a minimum set out the following information:

I. the name and contact details of ECT, and the initials of the privacy coordinator or privacy team member;

II. the purposes of processing;

III. a description of the categories of Data Subjects, and the categories of Personal Data;

IV. the categories of recipients who have been or will be supplied with Personal Data;

V. third countries or international organisations with which Personal Data is shared;

VI. the periods for which the categories of Personal Data may be stored;

VII. a general description of the technical and organisational security measures as referred to in Article 32 section 1 of the GDPR.

9 Data Protection Impact Assessment

9.1 Data Protection Impact Assessment

On the advice of the privacy coordinator, the board may decide to conduct a data protection impact assessment (DPIA) of specific processes indicated by the board that, given their nature, scope, context and purposes, probably constitute a high risk for the Data Subjects.

Although no data is processed within ECT that requires a DPIA on the basis of the GDPR, ECT will nonetheless periodically carry out a DPIA. On the advice of the privacy coordinator the board will designate an employee to carry out the DPIA. In addition, the privacy coordinator will ensure that the DPIA is up to date and carried out at least once every three years.

9.2 Report of high-risk processing to the Dutch DPA

If a DPIA reveals that a processing involves a high risk if ECT fails to take measures to restrict the risk, the privacy coordinator must consult with the Dutch DPA on behalf of ECT. As part of such consultation, ECT should supply the Dutch DPA with at least the following information:

I. the responsibilities of ECT and the Processors involved in the processing;

II. the purposes of, and the mechanisms used for, the proposed processing;

III. the measures and guarantees to be taken to protect the rights of the Data Subjects;

IV. the contact details of the privacy coordinator;

V. the results of the DPIA;

VI. all information requested by the Dutch DPA.

10 Storage periods

10.1 Storage period

The policy of ECT requires that Personal Data is not stored for longer than is necessary having regard to its nature. The processing register specifies the storage periods per process.

Within ECT, Personal Data is stored in any event for at least the statutory storage period as from completion of the file. The Procedure for Personal Data Storage Periods on Leaving Employment applies.

10.2 Processing during the employment contract

At the start of employment Personal Data is processed in order to guarantee that such start of employment is properly handled.

During the terms of their employment contracts, the Personal Data of employees is processed by ECT in order to meet the obligations under their employment contracts. Such processes are performed within the scope of:

I. salary payments, payment requests;

II. notification of illness and recovery;

III. performance of pension obligations;

IV. education and training;

V. time recording;

VI. bailiffs, government bodies;

VII. sending out newsletters;

VIII. taking out insurance on behalf of employees.

In addition, Personal Data is processed in the context of the planning, training, and assessment of employees.

The principles underlying these processes can be:

I. performance of an employment contract;

II. compliance with a statutory obligation;

III. if ECT has a legitimate interest that outweighs the interests of the employee.

ECT shall communicate clearly and proactively to employees about the way in which Personal Data is processed.

10.3 Processing in the case of sick leave

If an employee reports sick, ECT is only permitted to process data insofar as necessary to establish whether there is an obligation to continue to pay salary and how to deal with the work performed by the employee.
In concrete terms, ECT may ask for and record the following data concerning a sick employee:

- telephone number and (convalescence) address;
- the anticipated duration of the sick leave;
- existing agreed terms and work tasks;
- whether the employee falls under any safety net provisions of the of the Dutch Illness Benefits Act (but not under which one);
- whether the illness relates to an industrial accident;
- whether it is the result of a road traffic accident in which a liable third party is involved.

Under no circumstances can the question be asked whether the illness is work related. Furthermore, ECT may not ask about the nature and cause of the illness. If the relevant employee talks of their own volition about their illness, such information may not be included in their personnel file or recorded in any other way. Information voluntarily supplied by the employee about their illness may only be recorded by ECT if the employee suffers an illness that may necessitate immediate colleagues knowing what to do in an emergency.

The following information will be forwarded to the health and safety service (Arbodienst):

- Personal Data that identifies the employee on sick leave.

The board shall ensure that only HR staff and immediate supervisors have access to the sick-leave system. This system shall record sick leave.

10.4 Storage period for personnel files

ECT keeps personnel files containing relevant data of its personnel. ECT shall store this data for as long as reasonably necessary, but no longer than the end of the limitation period following termination of the employment contract. The board is entitled to stipulate shorter

storage periods for all or certain data. In any event, data that is no longer necessary to store shall be deleted. The Procedure for Personal Data Storage Periods on Leaving Employment applies.

10.5 Rights of employees and other data subjects

ECT shall inform employees about the processing of Personal Data, including what data ECT collects, for what purposes, and on what legal ground.

The rights of Data Subjects set out in Part 4 of this policy apply to all employees, including the right of access, correction, deletion, and restriction of processing. Any request to exercise such rights should be made to the privacy coordinator who, where relevant shall consult with the board, and in principle grant the request, or give reasons for refusal[7].

Employees have the right to object to the processing of Personal Data on the basis of a legitimate interest.

10.6 Security of data of personnel

All Personal Data shall be stored in an adequate manner, having regard to Part 5 of this policy. Only members of the board and the HR department have access to this data, but as restricted as possible and only insofar as necessary. Managers may access at any time the data of employees under their authority insofar as this is strictly necessary for the exercise of their management function. The Privacy Regulation agreed with the Works Council is operative.

10.7 Transfer of Personal Data to third countries

There are various data flows within ECT whereby Personal Data may be forwarded to other countries as described in Article 44 of the GDPR. ECT shall take measures to ensure that the transfer of this data always complies with the statutory requirements.

Transfer within the group
Except in specific cases, such as secondment or talent development within the group, Personal Data and Special Personal Data shall only be shared within the group on the basis of a statutory obligation and in accordance with the terms agreed with the Works Council.
Transfer to entities of Hutchison Ports outside the European Union and/or European Economic Area must comply with the GDPR. ECT shall ensure that such transfer is never at the expense of the level of protection given to the Data Subject by the GDPR. The function of Legal Counsel in London shall decide under which conditions this is done. However, ECT remains liable for compliance with the privacy legislation concerning such transfer.

Transfer by virtue of engaging external parties
To be able to carry out its activities, ECT engages suppliers of services that may receive Personal Data. Some recipients with which ECT may share Personal Data and where relevant – but only where the law permits – Special Personal Data, may be located in countries outside the European Union and/or the European Economic Area. Personal Data and Special Personal Data will only be shared on the basis of a statutory obligation and in accordance with the terms agreed with the Works Council.

In the case of any transfer outside the European Economic Area ECT shall ensure that this transfer complies with the requirements of the GDPR. ECT shall ensure that such transfer is never at the expense of the level of protection given to the Data Subject by the GDPR. This means

[7] A request to delete cannot always be granted.

that if it is established that no adequacy decision has been taken with regard to the country in question, Personal Data will only be transferred if ECT can provide adequate guarantees and the Data Subjects have enforceable rights and effective legal remedies. The privacy coordinator will assess what measures are adequate having regard to the latest developments in this field.

The Purchases Manual sets out how in tendering procedures the Purchasing department can comply with the said measures. In any event, in the case of Personal Data, the privacy coordinator should be involved in good time, so that the right questions/components can be included in the request for proposal.

11 Adoption

11.1 Adoption and entry into effect

This policy was adopted at the Consultation Meeting held on 11 October 2022 and came into effect on the same date.