Data Protection Policy

Dublin Bus

Contents

Data Protection Policy

1 Introduction

1.1 Purpose of the personal data management system

In line with data protection requirements and good practice, a **Personal Data Management System (PDMS)**, enables Dublin Bus to put in place, and be able to demonstrate appropriate and effective management of Personal Data.

Data protection laws in the EEA are governed primarily by the **General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)**, which is effective from the 25 May 2018. The GDPR is supplemented by national legislation and guidance published by competent supervisory authorities. In accordance with Section 1.3, this policy is to be kept under review and updated in light of such legislation and guidance as and when published.

Fundamental to the GDPR is the principle of accountability. Specifically, controllers and processors are responsible for, accountable, and must be able to demonstrate how they are compliant with data protection requirements. The PDMS provides a framework for maintaining and improving compliance with data protection requirements and good practice.

1.2 Purpose of this document

Dublin Bus collects, processes and stores significant volumes of Personal Data and limited quantities of special categories of personal data on an ongoing basis. Special categories of personal data are defined in Section 1.6 and are also a form of personal data. Dublin Bus is committed to complying with data protection legislation and good practice. The aim of this policy is to ensure that everyone handling personal data under Dublin Bus's control is fully aware of the requirements and acts in accordance with data protection procedures.

The purpose of this document is to provide a statement of overall intentions and directions of Dublin Bus as formally approved by senior management for managing compliance with data protection requirements and good practice. This document should be read in conjunction with any other related policies or procedures (including those referenced in this document) that Dublin Bus maintains regarding compliance with applicable data protection legislation.

The objectives of the data protection policy are to:

1. Enable Dublin Bus to meet its own requirements for the management of personal data.
2. Ensure Dublin Bus meets applicable statutory, regulatory, contractual and/or professional duties.
3. Protect the interests of individuals and other key stakeholders.
4. Support organisational objectives and obligations.
5. Impose controls in line with the company's acceptable level of risk.

This document also highlights key data protection procedures within Dublin Bus.

1.3 Policy review, approval and continuous improvement

In line with best practice, this policy has been approved by senior management, along with a commitment to continually improve the PDMS. This document will be reviewed at least annually by senior management and the Dublin Bus Data Protection Officer to ensure alignment to appropriate risk management requirements and its continued relevance to current and planned operations, legal developments, legislative obligations, guidance from the Data Protection Commission and the European Data Protection Board.

1.4 Scope and constraints

This policy applies to all personal data processed by the Dublin Bus, regardless of the media on which the Personal Data is stored (paper-based, electronic, CCTV or otherwise). This policy applies to Dublin Bus. This policy applies to Dublin Bus's directors and officers (or other persons occupying a similar status or performing a similar function), its employees and any other persons performing a function for Dublin Bus or who has access to personal data and is subject to Dublin Bus's supervision and control (which may include contractors, sub-contractors, advisors, temporary employees, other officers of other entities within the Dublin Bus group of companies or other persons that are designated accordingly).

Lastly, it should be noted that if personal data is flowing within the CIÉ Group of companies, each company, whether it is a parent company or a subsidiary, is a distinct legal entity with its own set of legal and data protection responsibilities. Each company within the Group may, therefore, be a controller in respect of the personal data which it has obtained and for which it is legally responsible, and it is necessary for each controller to assess whether disclosures of personal data to other CIÉ Group companies are permissible and where it is to implement appropriate safeguards. Effectively, companies within the CIÉ Group must be treated as separate legal entities and separate companies, to which standard data protection requirements and good practice apply in respect of the sharing of information. Further information is provided in Section 9.1.

It is the responsibility of all employees and any other person to whom this policy applies to comply with this policy. Failure of any employee to comply with this policy may lead to disciplinary action being taken against the defaulting employee in accordance with Dublin Bus's disciplinary procedures, up to and including summary dismissal. Failure of a third party contractor, subcontractor or any other person or entity to comply with this policy may lead to termination of the contract and/or legal action.

1.5 References

1. General Data Protection Regulation

Data Protection Act 2018 http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

2. Data Protection Act 2018

(ref: https://www.oireachtas.ie/viewdoc.asp?DocID=37646)

This document forms part of the Dublin Bus Personal Data Management System, and should be read in conjunction with the other documents within the management system:

- Dublin Bus - Records of processing activities
- **Dublin Bus Data protection policy – this document**
- Dublin Bus Data retention policy
- Dublin Bus Privacy Notice(s)
- Dublin Bus Subject access request policy
- Dublin Bus Data breach policy

1.6 Definitions

The following key terms (including certain terms defined in the GDPR) are provided here for ease of use. For a complete list of definitions refer directly to the GDPR (ref: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1465452422595&uri=CELEX:32016R0679).

1. **Anonymisation:** The process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

   Recital 26 also clarifies anonymous information "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is

not or no longer identifiable. This regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes".

2. **Personal data:** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3. **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, criminal conviction. Although Dublin Bus does not specifically target children's data. In some instances, images of children may be used for promotional, marketing and other activities. In such instances, consent from the child's legal guardian is sought. In such cases , as consent was used as the ground to gather data, the data is deemed to be a special category of personal data.

Dublin Bus will seek to avoid processing special categories of personal data where possible. It is understood that certain business activities within Dublin Bus may require the processing of special categories of personal data (e.g. processing of data concerning health or trade union membership salary deductions). The general processing of special categories of personal data is prohibited in Dublin Bus, and in the rare instance it is required, Head of Departments must ensure that all processing is defined in the Records of processing activities, along with an appropriate legal basis (reference 1, Art 9 and reference 2, Chapter 2) for processing of such special categories of personal data recorded within the Data Inventory.

4. **Controller:** The natural or legal person, public authority, agency or another body which, **alone or jointly with others**, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

   In certain instances, Dublin Bus alone determines the purpose and means of processing and in other instances jointly with the other CIÉ companies. In both circumstances, Dublin Bus would be considered a controller of this information. Note also that each company, whether it is a parent company or a subsidiary, is a distinct legal entity with its own set of legal and data protection responsibilities. Each company within a group of companies may, therefore, be a controller in respect of the personal data which it has obtained and for which it is legally responsible. Further information is provided in Section 9.1.

5. **Data subject:** Any living individual who is the subject of personal data held by an organisation. Data subjects within Dublin Bus may include members of the public, clients and customers, claimants, current, past and prospective employees, suppliers (such as sole traders), and other individuals with whom Dublin Bus communicates.

6. **Child:** A person aged under 16.

7. **Processing:** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by

automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

8. **Processor:** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

   Within the CIÉ Group, it is perfectly feasible for Dublin Bus to be a processor on behalf of one of the operating companies for certain personal data categories and/or vice-versa for other categories of personal data.

9. **Profiling:** any form of automated processing of personal data consisting of the of the use of personal data to evaluate certain personal aspects relating to a living person, in particular to analyse or predict aspects concerning the person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

10. **Automated data:** Information that is processed by electronic or digital means. Examples of this include: emails, electronic records or CCTV footage.

11. **Manual data:** Information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. An example of this would be a paper file.

12. **Pseudonymisation:** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person.

    Examples of pseudonymisation within Dublin Bus may include the use of accident reference numbers, or claim reference numbers whereby the individual cannot be identified unless additional information is obtained (e.g. access to a particular application). Where anonymisation cannot be used, the next best of pseudonymisation should be used.

13. **Recipient:** A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with current union or member state law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

2 Roles and responsibilities

2.1 To whom this policy applies

Please see Section 1.4 for information regarding the parties to whom this policy applies.

2.2 Roles and responsibilities

Everyone to whom this policy applies is responsible to ensure compliance with Dublin Bus's data protection requirements and obligations. It is the responsibility of all employees in particular to:

1. Familiarise themselves with this policy and handle personal data in accordance with this policy, the data protection principles, and data handling rules (see Section 10.2).

2. Complete the mandatory data protection training provided. A record of attendance will be maintained for audit purposes.

3. Deal with queries in relation to personal data promptly and courteously. When an employee receives an enquiry about the handling of personal data, they will know what to do, and/or where to refer it.

To ensure all users are aware of their responsibilities as users of Dublin Bus systems, this policy has been defined and the following includes additional requirements based on key data protection roles within Dublin Bus:

2.2.1 Additional responsibilities of Data Protection Officer

As Dublin Bus is a public body, it is mandatory that a suitably trained, independent, senior person is appointed to the role of Data Protection Officer. This may be performed as a team function provided a single individual is the lead person "in-charge' and roles within the Data Protection Officer team are clearly defined. The term 'Data Protection Officer' used in this policy refers to the Data Protection Officer function, whether performed by an individual or as a team.

Within Dublin Bus, the Dublin Bus Data Protection Officer and the team may be contacted using the information below. Please note that while Dublin Bus will disclose the contact details for the Dublin Bus Data Protection Officer, it is not necessary to disclose the personal name of the Dublin Bus Data Protection Officer to data subjects.

Data Protection Officer Contact Details	
Name:	**Data Protection Officer**
Address:	**Dublin Bus** **59 Upper O'Connell Street,** **Dublin 1**
Email:	**dataprotection@dublinbus.ie**
Telephone:	**01 7033003**

The responsibility of the Data Protection Officer function within Dublin Bus is to:

1. Respond to individuals (data subjects) whose personal data is processed on all issues relating to the processing of their Personal Data and the exercise of their data protection rights.
2. Cooperate with the supervisory authority, and act as the organisation's contact point for the supervisory authority on all issues relating to the processing of personal data in Dublin Bus.
3. Inform and advise Dublin Bus and the employees of their obligations pursuant to data protection legislation.

4. Monitor compliance with data protection obligations, in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of employee
5. and other persons (e.g. contractors) involved in processing operations, and the related audits.
6. To provide advice and assistance in relation to the requirement to perform data protection impact assessments and monitor their performance.
7. Arrange at least annual data protection training sessions for Dublin Bus employees.
8. Maintain a data breach policy and also a log of all data breaches and communication of breaches to all relevant parties when required to do so (supervisory authority, controllers and data subjects). Please refer to Section 6 for more details.

To allow for the effective performance of the Data Protection Officer tasks, Dublin Bus will ensure:

1. The Data Protection Officer will be suitably trained and have expert knowledge of data protection laws.
2. Dublin Bus will support the Data Protection Officer in performing the tasks above by providing resources necessary to carry out those tasks. The key to this is to provide sufficient time, finance and employees where appropriate to fulfil the Data Protection Officer duties.
3. No tasks and duties should result in a conflict of interest for the Data Protection Officer.
4. Dublin Bus senior management will ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data, and will be in a position to perform their duties and tasks in an independent manner.

This includes:

a. The Data Protection Officer will have direct independent access to the CEO of Dublin Bus as required in relation to data protection.
b. The Data Protection Officer will have direct independent access to the Audit, Finance and Risk Committee (AFRC) as required in relation to data protection.
c. The Data Protection Officer's involvement will be sought where decisions with data protection implications are taken. All relevant information must be passed on to the Data Protection Officer in a timely manner in order to allow it to provide adequate advice.
d. The Data Protection Officer will be invited to participate regularly in meetings with senior and middle management.
e. The opinion of the Data Protection Officer will always be given due weight.
f. The Data Protection Officer will be promptly consulted if a data breach or other data protection incident has occurred and in accordance with Section 6.

2.2.2 Additional responsibilities of Human Resources

Dublin Bus Human Resources personnel have a key role in the implementation of the Personal Data Management System which includes responsibility for:

1. Ensuring all new employees are made aware of this policy document at induction stage and it is referenced in employee Terms and conditions and role profiles .
2. Ensuring new starters, temporary employees and contractors who require training complete the first available data protection training course after their start date.
3. Handling all personal data in accordance with this policy, the data protection principles, Data handling rules and applicable data protection legislation.

2.2.3 Additional responsibilities of Heads of Departments and Line Managers

Line Managers and Heads of Departments have a key role in the implementation of the Personal Data Management System which includes responsibility for:

1. Ensuring all processing within their department is in compliance with the Dublin Bus Data protection policy and privacy best practice. Specifically, maintaining the Data Inventory of all information processed by their department, and for ensuring that employees in their area are aware of this policy, general obligations and requirements of data protection legislation and guidance.
2. Ensuring reporting employees complete the mandatory data protection training.
3. Ensuring sufficient resources are available to support the effective implementation of this policy.
4. Ensuring appropriate technical and organisational security measures are in place in areas for which they are responsible. Specifically and in accordance with Section 5.2, security risk assessment will be undertaken to check that the Personal Data is sufficiently protected and are in line with security policy and this policy. To deal with appropriate technical and organisational security measures, the line manager or Head of Department may delegate the security tasks, in full or partially, to another Dublin Bus representative. This delegation does not exempt the line manager or Head of Department from their responsibility and they must make sure that the delegated jobs have been carried out correctly.
5. Ensuring data privacy risks are appropriately managed within their function. Specifically, to ensure the handling of Personal Data is regularly assessed and evaluated.

Under the GDPR there are a number of changes which will affect both in-house changes and contracts for new projects. It is therefore important that if any new projects are being considered then data protection needs to be built in at the beginning (privacy by design and by default). Contracts will need to reflect the changes.

6. Ensuring that where processing "is likely to result in a high risk to the rights and freedoms of natural persons", which may include:

a. processing on a large scale of special categories of data or data relating to criminal convictions and offences;
b. a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect individuals; and/or
c. systematic monitoring of a publicly accessible area on a large scale, a data protection impact assessment is formally carried out in relation to each new project or proposal where such is required (see Section 5.3 for more details on Data Protection Impact Assessments). The Dublin Bus Data Protection Officer must be informed and involved at an early stage.

2.2.4 Additional responsibilities of Technical Solutions Architects / Technical Design Leads / Project Managers

Ensure all aspects of the Personal Data Management System are followed for all changes and Managed Projects within Dublin Bus. This includes implementation of the data protection by design and data protection by default principles and retaining evidence for audit purpose as part of the Project Management Lifecycle (see Section 5 for more details).

2.3 Security awareness/data protection training details

Data protection training is mandatory for all relevant Dublin Bus employees. Annually, all relevant Dublin Bus employees will have to complete this training and a record will be maintained for audit purposes.

3 How Dublin Bus complies with the data protection principles

Dublin Bus is committed to ensuring all Personal Data is processed in line with the General Data Protection Regulation's principles and good practices. This includes:

3.1 Lawfulness, fairness and transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

Dublin Bus is committed to ensuring the lawful, fair and transparent collection of personal data. Our records of processing activities record all information processed, including the lawful basis of such processing. In addition, our privacy notice provides details to the data subject in a concise, transparent, intelligible and easily accessible form including the purposes of processing, the period of processing, their rights, the lawful basis for the processing, the recipients of the personal data, and where personal data may be transferred to a non-EEA country, the safeguards which have been adopted in relation to such transfer and any other information required to be provided by applicable data protection legislation. These privacy notices must be provided to data subjects prior to collecting personal data regardless of the collection method (phone, CCTV, forms, interview, website etc.).

Lawful basis

For personal data to be processed fairly, Dublin Bus must be able to rely on one of a range of 'lawful bases' that are set out under the GDPR. In relation to employees, Dublin Bus generally relies upon the 'processing being necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller' basis which is applicable to Dublin Bus, 'the processing is necessary for the performance of a contract' and 'the compliance with a legal obligation' basis. Full details of the lawful basis for processing are set out in Dublin Bus's data inventory.

For special categories of personal data to be processed fairly, Dublin Bus must be able to rely on one of a range of 'lawful bases' that are set out under the GDPR and in national legislation. In the context of HR data, Dublin Bus generally relies upon the 'processing is required or authorised under applicable employment law' basis, 'the processing is necessary for the purposes of occupational medicine or to assess an employee's ability to work' and 'the processing is necessary for the purpose of obtaining legal advice, establishing, exercising or defending legal claims and rights or any legal proceedings or claims (including prospective legal proceedings and claims)'.

Where the lawful basis is "consent"

Where the lawful basis of processing is based on consent, Dublin Bus shall incorporate procedures for the obtaining and withdrawal of consent. Consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes and the controller must be able to demonstrate that the data subject provided their consent to the processing. Where consent is withdrawn, processing based on consent must cease, except where such processing is otherwise permitted by applicable law.

Where processing is based on the lawful basis of consent and the data processing relates to a child (currently under 16 years), the department must ensure they have obtained and recorded consent provided by the holder of parental responsibility for the child, unless it is in connection with a contract for necessities.

Refer to the Dublin Bus Data Protection Officer, for further guidance, clarification and consultation in relation to the lawfulness of processing and conditions for consent.

3.2 Purpose limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Dublin Bus is committed to only collecting and processing personal data for a specified, explicit and legitimate purpose. All personal data processed, along with the business purpose is detailed and clearly stated within the records of processing activities, will be reviewed, updated at least annually or when any significant changes occur in the personal data processed, where it is processed or with whom it is shared.

Personal data will only be processed for the defined purpose, subject to limited exceptions. Where you are planning any new activity or implementing any new initiative that will involve changing the original purpose, please contact the Dublin Bus Data Protection Officer in advance.

3.3 Data minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Dublin Bus is committed to only collecting and processing appropriate personal data to the extent needed to fulfill the purpose for which it was obtained and to comply with all applicable statutory, regulatory, contractual and/or professional duties. Personal data will be minimised and enforced through our data protection impact assessment and our data protection by design and default procedures within our change management/project management office.

3.4 Accuracy

Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Dublin Bus is committed to ensuring that the data it holds is at all times accurate, complete and up-to-date. Dublin Bus requests employees and others to notify it of changes to their Personal Data (for example, upon change of address). Dublin Bus takes reasonable efforts to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified.

3.5 Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Dublin Bus have documented the required data retention periods along with justification and action to be taken when the retention period expires. This document outlines the retention period for all personal data across Dublin Bus, and what will occur when the retention period expires. It applies to all Personal Data regardless of the media on which it is stored (paper-based, electronic, CCTV or otherwise). This policy helps ensure that Dublin Bus is maintaining the necessary personal data for an appropriate length of time, based on legal and business requirements and in line with the data protection 'storage limitation' principle. Everyone is responsible for ensuring that this policy is adhered to.

3.6 Security, integrity and confidentiality

Personal data shall be processed 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.

Dublin Bus ensures that Personal Data is processed 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. Brief details regarding Dublin Bus's Data security and cyber security practices are described in Section 5 and also in its Data handling rules described in Section 10.2. Dublin Bus is committed to protecting and not disclosing personal data, either within or outside of Dublin Bus to any unauthorised recipient. Everyone is responsible to protect against the accidental loss, destruction or damage to personal data regardless of the media on which it is stored (paper-based, electronic, CCTV or otherwise) and to follow the Data Handling Rules described in this policy.

To the extent that any third party processes personal data on behalf of Dublin Bus, Dublin Bus ensures that there is a written agreement in place with that third party which includes, among other things, appropriate security obligations regarding such personal data. In addition, Dublin Bus will undertake due diligence on a third party processor prior to engaging it and will only engage those third party processors where it is satisfied that the third party processor provides sufficient guarantees as regard the security measures to be applied to the processing of personal data. See Section 9 for further details.

In addition to this policy, all employees and any other person who has access to Dublin Bus's IT systems are subject to security and acceptable use policies, which outline their responsibilities when using Dublin Bus's IT systems. Further details regarding the technical and security measures implemented by Dublin Bus are set out in Dublin Bus Security and risk policies and Acceptable usage policies (including those below), Data Security and Cyber Security in Section 5 and also the Data Handling Rules in Section 9.2.

- CIÉ Board Information Risk Policy | CIÉ Group Information Security Policy | Acceptable Use Policy for Information Systems | Acceptable Use Policy for Enterprise Owned Mobile Devices

4 Individual Rights

Under data protection legislation, data subjects (for example, employees) have certain rights in relation to the Personal Data which Dublin Bus process on their behalf, subject to certain limited exemptions.

4.1 Common procedures to exercise individual rights

Any queries regarding data protection or any requests to exercise data subject rights whether from the person themselves or from a third party (for example, their solicitor) must be referred to the Data Protection Officer as soon as the request is received as the statutory time limits for responding to such a request are sensitive (for example, 1 month to respond to an access request). Any person wishing to exercise data subject rights can apply in writing or email to the Data Protection Officer.

The following procedure and principles are applicable to Dublin Bus's response to all requests from data subjects to exercise their data subject requests under applicable data protection legislation:

1. Dublin Bus is obliged to comply with any request by a data subject to exercise their rights within strict timelines imposed under data protection legislation, except to the extent that any exemption provided for under data protection legislation applies. These timelines are generally one month, but this period can be extended by another two months where requests are complex or numerous. To extend the timeline, the Data Protection Officer will inform the requestor of the extension within one month of receiving the request and shall explain why the request is necessary.

2. Employees and other persons (such as contractors or temporary employees) who receive a request from a data subject should notify the Data Protection Officer as soon as they receive the request. It is important to be aware that a request does not need to be in writing and does not need to specifically reference the GDPR or any national implementing legislation. That said, on receipt of a request by telephone, please ask the caller to put their request in writing (or email) and to address such to the Dublin Bus Data Protection Officer. Never give out personal information over the phone.

3. Notify the Data Protection Officer as soon as you receive a request and also note the date on which the request was received. This is particularly important so as to avoid an expiration of the time limit in which to comply with the request.

4. The Data Protection Officer will verify the requestor's identity, which may be undertaken in the following ways:

   a. If the request is from a current employee or contractor, the Data Protection Officer will use an alternate means of communication to confirm the request was made by the employee or contractor. For example, if the request was sent via email, contact the employee or contractor by phone to confirm the request.

   b. If the request is made by someone other than a current employee or contractor, proof of identity should be requested. This may take the form of a copy of passport, drivers licence or other photo identification together with a copy of a utility bill dated within the past six months.

5. If the Data Protection Officer determines that the request is manifestly unfounded or excessive, it may refuse to deal with the request. As the burden for demonstrating the manifestly unfounded or excessive character of the request falls on a controller, the Data Protection Officer will document its rationale for determining that the request is manifestly unfounded or excessive.

6. Dublin Bus will respond to requests in relation to the exercise of data subject rights in a concise and transparent manner.

4.2 Right Of Access

Data subjects (including employees and the general public) have the right to access Personal Data held about them and to receive certain details in relation to the processing of that Personal Data, subject to any applicable exemptions provided for under applicable data protection legislation.

1. The Data Protection Officer will identify the scope of the request, and where the request is overly broad it will ask follow-up questions to the requestor to narrow the scope of the request. This may include asking the requestor to:

   a. Specify the information requested;
   b. Identify a date range.
   c. Identify where the Personal Data is located, e.g. to name specific teams within Dublin Bus.

2. Once the parameters of the request are known, the Data Protection Officer will contact the relevant departments (e.g. Customer Service, HR and IT) and request them to conduct a search of all personal data within the parameters of the request that may be held by them. The relevant department should conduct searches of the relevant sources to locate the personal data and should keep a record of all such searches. Departments should be advised that while searches should be kept broad to ensure that all relevant data is captured, it should use search parameters that reflect the personal data the data subject is likely to be interested in:

   a. Include 'easy' information e.g. personnel files.
   b. Apply date ranges.
   c. Use pre-defined keyword searches to search emails and other electronic information and exclude archived data.
   d. Exclude back-up and deleted data, even if it might be possible technically to recover it.

3. When the data has been collated, the Data Protection Office will review and ensure that (i) any third party Personal Data, (ii) exempt Personal Data, such as data that are subject to legal professional privilege and (iii) information which is not Personal Data, is redacted. It is important to keep a record of the rationale underlying each redaction.

4. Once this review and redaction are completed, the Data Protection Officer will draft a response letter to be sent to the requestor, along with the Personal Data, explaining any exemptions that have led to partial disclosure. The following information must also be included in this letter:

   a. The purposes of the processing.
   b. The categories of personal data processed.
   c. The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.
   d. Where possible, the envisaged period for which personal data will be stored, or if not possible, the criteria used to determine that period.
   e. The right to lodge a complaint with the Data Protection Commission.
   f. The existence of the right to request rectification or erasure of personal data or to request to have personal data restricted or to object to such processing.
   g. The existence of any automated decision making.
   h. The safeguards put in place in respect of any international data transfers. In addition, where data have not been obtained directly from the data subject, Dublin Bus must provide any available information as to their source.

4.2.1 CCTV Footage

CCTV footage is Personal Data within the meaning of the GDPR as images and recordings of individuals may capture their Personal Data and can identify them.

(a) Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own Personal Data from the footage, which is known as the right to access personal data (See above for more details).

(b) When Dublin Bus receives an access request for CCTV footage, it should ask the requestor to provide it with a reasonable indication of the timeframe of the recording being sought - i.e. the requestor should be asked to provide details of the approximate time, the specific date(s) and location in which their image was recorded.

(c) Obviously, if the recording no longer exists on the date on which Dublin Bus receives the access request, it will not be possible to provide access to a copy. CCTV footage is usually deleted within one month of being recorded.

(d) For Dublin Bus's part, the obligation in responding to the access request is to provide a copy of the requester's personal data. This normally involves providing a copy of the footage in video format. In circumstances where the footage is technically incapable of being copied to another device, or where the supply of a copy in video format is impracticable, it is acceptable to provide stills as an alternative. Where stills are supplied, it would be necessary to supply a still for every second of the recording in which the requester's image appears in order to comply with the obligation to supply a copy of all personal data held.

(e) Where images of individuals other than the requesting data subject appear on the CCTV footage, the onus lies on Dublin Bus, where it is the controller, to pixelate the images of those other individuals before supplying a copy of the footage or stills from the footage to the requester. Alternatively, Dublin Bus may seek the consent of those other individuals whose images appear in the footage to release an unedited copy containing their images to the requester.

All data subject requests regarding CCTV must be referred to the Data Protection Officer.

4.3 Right to rectification

Data subjects (including employees and members of the general public that may have availed of Dublin Bus's services, or received communications or information from Dublin Bus) have the right to the rectification of inaccurate personal data concerning him or her that is held by Dublin Bus. Where Dublin Bus receives a request to rectify personal data, it will take reasonable steps to rectify that Personal Data without undue delay, and at least within one month of the request. Where the request is complex, or where Dublin Bus has received a number of requests, it will notify the data subject that this period will be extended by another two months. Dublin Bus will consider which third parties it has disclosed the personal data to, and if such third parties are acting as processors on behalf of Dublin Bus, ask them to rectify the copies of the personal data held by them.

As Dublin Bus does not anticipate that it will receive a significant number of rectification requests, such requests will be processed on a case by case basis by the Data Protection Officer.

4.4 Right to erasure (The right to be forgotten)

Data subjects (including employees and the general public) have the right to obtain from the controller the erasure of personal data concerning him or her in one of the following circumstances:

(a) Such personal data is no longer necessary in relation to the purpose(s) for which it was collected or otherwise processed.
(b) The data subject withdraws their consent on which the processing was based, and there is no other lawful basis for the processing.
(c) The data subject objects to the processing, as provided in Section 4.7 below.
(d) Where the data subject's personal data has been unlawfully processed.
(e) The data subject's Personal Data has to be erased for compliance with a legal obligation in EU or Member State laws.

Dublin Bus can refuse the erasure of such personal data if the processing of such personal data is necessary for:

(a) Exercising the right of freedom of expression and information;
(b) complying with legal obligations which require the processing by EU or Member State Law to which Dublin Bus (as controller) is subject.
(c) Performance of a task carried out in the public interest or in the exercise of official authority vested in Dublin Bus.
(d) Reasons of public interest in the area of public health, scientific or historical research purposes or statistical purposes.
(e) The establishment or defence of legal claims.

Where a right to erasure request is received from an individual, Dublin Bus's policy is to permit the request and delete the relevant personal data unless there are reasonable grounds for refusing the request. If Dublin Bus is engaged in a legal dispute with the requestor, or has reason to believe that a legal claim may be made by the requestor, the views of legal counsel should be sought before deciding whether to comply. Dublin Bus will consider which third parties it has disclosed the personal data to, and if such third parties are acting as processors on behalf of Dublin Bus, ask them to delete any copies of the personal data held by them.

As Dublin Bus does not anticipate that it will receive a significant number of erasure requests, such requests will be processed on a case by case basis by the Data Protection Officer.

4.5 Right to data portability

Where Personal Data is processed based on the lawful basis of 'consent' or 'necessary for the performance of a contract' and the processing is carried out by automated means, data subjects have a right to receive that Personal Data in a structured, commonly used and machine readable format and to have it transmitted to a third party controller.

The right to data portability only applies to personal data that has been provided to a controller (e.g. Dublin Bus) by the data subject. Although this would seem to restrict the right to only Personal Data that has been directly or actively provided by the data subject, the Article 29 Working Party (soon to be known as the European Data Protection Board) has issued Guidance that insists that this right also applies to "observed data". If these Guidelines are accepted as the correct interpretation of the right, which is not beyond doubt, Dublin Bus should take the data portability right to extend to raw data that is observed in relation to data subjects.

Where a data portability request is received, Dublin Bus's policy is to permit the request and provide the individual's Personal Data unless there are reasonable grounds for refusing the request (e.g. Dublin Bus is not satisfied as to the identity of the requester or believes

the request to be manifestly unfounded). If Dublin Bus is engaged in a legal dispute with the requester, or has reason to believe that a legal claim may be made by the requester, the views of external counsel should be sought before deciding whether to comply with a data portability request.

As Dublin Bus does not anticipate that it will receive a significant number of erasure requests, such requests will be processed on a case by case basis by the Data Protection Officer.

4.6 Rights in relation to automated decision making

Data subjects have the right not to be subjected to processing which is wholly automated and which produces legal effects or otherwise which significantly affects an individual, and which is intended to evaluate certain personal matters, such as performance at work, unless one of a limited number of exemptions applies.

These exemptions are that the automated decision making is necessary for entering into, or performance of, a contract between the data subject and Dublin Bus; the automated decision making is authorised by EU or Member State law which also lays down suitable measures to safeguard the data subject's right and freedoms and legitimate interests, or the decision making is based on the data subject's explicit consent. Dublin Bus's policy is not to engage in automated decision making that produces legal effects, or similarly significantly affects data subjects.

4.7 Right to object

Data subjects have the right to object to the processing of their personal data where it is being processed based on the performance of a task in the public interest or legitimate interests grounds, or where it is being used for direct marketing purposes on any grounds.

Dublin Bus's policy is to consider whether the terms of the request fall with the scope of the right and then Dublin Bus will effect, on a case by case basis, a hold or freeze on any processing (other than mere storage of that data subject's personal data) while Dublin Bus's considers whether its legitimate grounds for processing override those of the data subject concerned. Third party processors should be informed of the cessation of processing.

Following receipt and consideration of a right to object request from a data subject, Dublin Bus must stop all processing of the Personal Data:

(a) where Dublin Bus, after due consideration, cannot demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

(b) unless the processing is for the establishment, exercise or defence of legal claims.

As Dublin Bus does not anticipate that it will receive a significant number of right to object requests, such requests will be processed on a case by case basis by the Data Protection Officer.

4.8 Restrictions

There are restrictions on the exercise of this right in certain circumstances which will mean that Dublin Bus will not be required to adhere to certain individual rights. The Data Protection Officer will consider each request on a case by case basis and it is likely that such restrictions would not apply to the complete data set and more likely to a restricted and very specific set of Personal Data.

For example, Dublin Bus may not be permitted to apply a blanket exemption to the right of access to an entire claim file as some elements may be considered privileged, while others not.

If Dublin Bus wishes to withhold certain subject rights, this must be referred to the Data Protection Officer who may refer to the Dublin Bus Group Solicitor. Restrictions on exercise of data subject rights are laid out in the Data Protection Bill (reference 2), and shall be considered carefully when performing data subject requests.

It should be noted that the existence of proceedings between a data subject and the controller does not, of itself, preclude the data subject from making an access request nor justifies the controller in refusing the request. For example, if a data subject access request is refused, a response clarification as to which exemption is been applied including the specific restriction must be cited.

5 Data security and cyber security

The GDPR requires Dublin Bus to take into account the **state of the art**, the costs of implementation and the **nature, scope, context and purposes of processing** as well as the **risk of varying likelihood and severity** for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) The **pseudonymisation** and **encryption** of personal data.
b) The ability to ensure the **ongoing confidentiality, integrity, availability** and **resilience** of processing systems and services.
c) The ability to **restore the availability and access** to personal data in a **timely manner** in the event of a **physical or technical incident**.
d) A process for **regularly testing**, **assessing and evaluating the effectiveness of technical and organisational measures** for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular **from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed**.

Dublin Bus fulfils these obligations by a number of means, specifically:

1. Deployment of data protection by design and by default within our Project Management Lifecycle for all new systems/changes to processing (reference Section 5.1 for further details)

2. Regular risk assessments/testing to assess and evaluate the effectiveness of technical and organisational measures on existing processing (reference Section 5.2 for further details)

3. Formalised data protection impact assessments where processing **"is likely to result in a high risk to the rights and freedoms of natural persons"**. (reference Section 5.3 for further details)

4. All persons who have access to Dublin Bus's IT systems and devices are subject to security and acceptable use policies which outline their responsibilities in using such systems and devices.

5. All persons to whom these policies apply to must comply with the Data Handling Rules in Section 10.2

Records of all of the above activities will be forwarded to the Dublin Bus Data Protection Officer and retained for audit purposes.

5.1 Data protection by design and default

Two key principles under the GDPR require that data protection compliance be implemented by data protection by design and by default:

1. **Data protection by design** - Data protection by design is the notion that the means and purposes of the processing of personal data are designed at the outset, with data protection in mind. This requires Dublin Bus to implement technical and organisational measures that will guarantee and protect the privacy of data subjects, such as pseudonymisation and data minimisation.

2. **Data protection by default** - Data protection by default means that the controller shall implement appropriate technical and organisational measures **for ensuring that, by default**, only personal data which are necessary for each specific purpose of the processing is processed. That obligation applies to the **amount** of personal data collected, the **extent of their processing**, the period of their **storage and their accessibility**. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention **to an indefinite number of natural persons**.

As part of the implementation of data protection by design and by default principles, a data protection and security design review will be performed during the development stage/part of project management of all new projects. The following provides a minimum checklist of areas that will be examined and documented as part of this review. Records will be maintained for audit purposes with the output from each area examined:

1. Has the data inventory been updated with any new forms of processing including data categories processed, where it is processed, and to whom it is shared?

2. Has a valid lawful basis for this processing been defined within the data inventory?

3. Does the new form of processing include a relevant data privacy notice including all required information as defined in the Dublin Bus Data Privacy Notice(s) policy.

4. Is the information collected for a specifically defined purpose?

5. Is only the required information collected or is information collected which may be deemed excessive (for example, is the personal data that is collected minimised)?

6. How personal data is kept reasonably accurate and up to date?

7. How long Personal Data is retained for, and does the retention period and destruction method comply with the Dublin Bus Data retention policy?

8. Is it necessary for Dublin Bus to be able to identify the individuals for this processing or could anonymisation be used?

9. Could pseudonymisation be enforced to protect the personal data, for example, restrict reports to a reference (for example, Claimant reference) and leaving out the direct individual identification (for example,. claimant name). Specifically, in this example, all reports will be pseudonymised to prevent the direct identification of individuals?

10. Is the personal data encrypted at rest and/or in transit or can this be performed?

11. How is the information protected against unlawful or accidental loss, destruction or damage?

12. How does the new form of processing allow for the implementation of Individual Rights including the Right to Access, Right to Rectification and Erasure?

13. Is all processing within the EEA?

14. Has a technical penetration test or risk assessment been performed and remediation actions taken?

15. Are appropriate user access management procedures applied, specifically:

    a. Is physical or remote access needed to the office in order to access the personal data?
    b. Is user access restricted on a need-to-know basis?
    c. Is all user access audited and does Dublin Bus have an audit trail of all user access?
    d. Is there a formal process for joiner/leavers/movers to facilitate user access management?
    e. Are user access reviews performed which are signed-off by relevant business owners and recorded for audit purposes?

16. Are other relevant and appropriate technical and organisational security measures applied, including (for example):

    a. Is a formalised patching policy applied and maintained?
    b. Are reliable and recent backups in place, and are these tested regularly?
    c. Are all backups encrypted?
    d. Are appropriate perimeter security controls applied?
    e. Are appropriate anti-malware defences deployed?

17. Can personal data which is shared externally for reporting purposes, or retained for analytics/statistics, be anonymised?

5.2 Regular risk assessment

The GDPR Requires a process for **regularly testing, assessing and evaluating the effectiveness of technical and organisational measures** for ensuring the security of the processing.

It is the responsibility of the Head of the Department to ensure appropriate technical and organizational security measures are in place in areas for which they are responsible. Specifically, regular security risk assessments must be commissioned to check that the personal data is sufficiently protected and are in line with security policy based on the level of risk. Security risk assessments will be commissioned regularly and a record maintained for audit purposes with the output from each area examined. At a minimum, this must evaluate and record the technical and organisational measures identified in the previous section (Section 5.1).

Dublin Bus will ensure that any risks to the privacy of data are assessed, and that measures that are implemented are appropriate to the risks of the processing on the systems used. To facilitate this, each data category name, data store, and recipient/s are assigned a risk level based on a defined criteria within each department's data inventory.

5.3 Data protection impact assessment (dpia)

The GDPR requires that a formalised DPIA is performed where processing **"is likely to result in a high risk to the rights and freedoms of natural persons"**.

Examples of such 'high risk' processing that are given in the GDPR are:

(a) Systematic monitoring of a publicly accessible area on a large scale.
(b) Processing on a large scale of special categories of data or of data relating to criminal convictions and offences.
(c) Systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, on which decisions are based that produce legal effects concerning natural persons.

The above examples are not exhaustive. Further details of processing considered to be 'high risk' are published and maintained by data protection authorities.

At a minimum, the DPIA will contain the following details:

(a) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller (e.g. Dublin Bus) .
(b) An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
(c) An assessment of the risks to the rights and freedoms of data subjects (e.g. privacy rights).
(d) The measures envisaged to address the risks that have been identified and to demonstrate compliance with this GDPR. Note: that the list provided regarding data protection by design and default in Section 5.1 will also be completed for the DPIA.
(e) Where the outcome of a DPIA is that the processing would result in a high risk to data subjects, Dublin Bus will consult with the Irish Data Protection Commission.

Dublin Bus also considers whether a Privacy Impact Assessment **(PIA)** is necessary when it engages in material changes to its processing of personal data that do not require a DPIA.

Both DPIAs and PIAs are carried out before the processing activity in question is commenced.

Each DPIA and PIA that is carried out by Dublin Bus shall be regularly reviewed on an ongoing basis.

The Data Protection Officer shall be consulted at each stage of a DPIA, and shall provide advice and guidance on the following:

- Whether or not a DPIA is required to be undertaken;
- What methodology to follow when carrying out a DPIA;
- Whether to carry out the DPIA in-house or whether to outsource it;
- Whether or not the DPIA has been correctly carried out and to consider whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) trigger certain legal obligations, for example consulting with the Data Protection Commission.

It is vital that the Data Protection Officer is involved in each DPIA, and evidence of all consultation with him/her is retained for audit purposes. Where adherence is not paid to the Data Protection Officer's advice, the reasons for not adhering to the advice of the Data Protection Officer should be formally recorded in the DPIA.

Further external Guidance on the performance of a DPIA is provided by the Article 29 Working Party (soon to be known as the European Data Protection Board) in Guidance entitled **'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing is likely to result in a high risk for the purposes of Regulation 2016/679 (WP 248 rev 01)'**, which was adopted on the 4 April 2017 and last revised and adopted on the 4 October 2017.

6 Personal data breach handling

6.1 What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

According to the Article 29 Working Party (soon to be known as the European Data Protection Board), a controller should be regarded as having become aware of a personal data breach when it has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. During the period in which an initial investigation of a personal data breach is undertaken, Dublin Bus may not be regarded as being 'aware' of a breach, but this will be specific to each situation.

Examples of typical data breaches are:

1) Loss or theft of data or equipment on which data is stored.
2) Loss or theft of documents/folders.
3) Unforeseen circumstances such as a flood or fire which destroys information.
4) Inappropriate access controls allowing unauthorised use.
5) A hacking/cyber attack.
6) Obtaining information from the organisation by deception/misaddressing of e-mails/human error.

It is important to note that breaches also include the accidental loss of personal data (e.g. fire causing the loss of paper files). In addition, statistics indicate that most breaches are internal in nature and due to non-malicious user behaviour (e.g. loss of unencrypted laptop or USB, files etc.).

Please note that data security incidents may occur, which do not necessarily result in an unauthorised disclosure, loss, destruction or alteration of personal data.

6.2 How do employees report a data protection breach?

In order for the Dublin Bus to be able to comply with the GDPR (reference 1), it is essential that all incidents (including suspected incidents) which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data are reported without delay to the Data Protection Officer.

In the event of a suspected personal data breach happening, the Data Protection Officer must also be notified immediately. It must not be assumed that someone else has already notified the breach.

6.3 How personal data breaches will be handled in dublin bus

The GDPR requires that Dublin Bus

1. Document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance

A summary of all personal data breaches which may occur, containing the facts relating to the personal data breach, its effects and the remedial action taken, will be recorded in the Dublin Bus log of data breaches that is maintained by the Data Protection Officer.

Within Dublin Bus, the Data Protection Officer will assess the breach, and make a decision on the next steps to be taken.

6.4 Notification of data breach requirements to controllers, supervisory authorities and data subjects

6.4.1 Notification to Supervisory Authority

After review of the breach by the Data Protection Officer, where a personal data breach occurs, the Data Protection Officer will inform the Data Protection Commission within **72 hours of Dublin Bus becoming aware** of the breach, unless it is unlikely to result in a risk to the rights and freedoms of a data subject. The details of the notification will include:

(a) Description of the nature of the personal data breach including where possible, the categories and an approximate number of data subjects concerned and the categories and an approximate number of Personal Data records concerned.
(b) Name and contact details of the Data Protection Officer or other contact point where more information can be obtained.
(c) Description of the likely consequences of the personal data breach.
(d) Description of the measures taken or proposed to be taken by Dublin Bus to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If necessary, Dublin Bus may provide the Data Protection Commission or the relevant Supervisory Authority with information on a phased basis, where it is not possible to provide the information at the same time.

6.4.2 Notification to Data Subjects

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The notification shall describe in clear and plain language the nature of the personal data breach and contain at least:

(a) Name and contact details of the Dublin Bus Data Protection Officer.
(b) Description of the likely consequences of the personal data breach.
(c) Description of the measures taken or proposed to be taken by Dublin Bus to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

There are, however, certain circumstances where a notification is not required even where the threshold for notification is initially satisfied. Dublin Bus will have regard to the following principles, which are relevant when assessing whether a personal data breach requires notification to affected data subjects:

(a) High risk to the rights and freedoms of affected data subjects – The requirement for a notification to data subjects requires a likelihood of a 'high' risk to the rights and freedoms of affected data subjects, in contrast to the standard of requirement for a notification to the supervisory authority which only requires a risk. When assessing whether there is a **high risk** to data subjects Dublin Bus will bear in mind that one of the core purposes for notifying data subjects is to help data subjects take steps to protect themselves from any negative consequences of the breach.

(b) Conditions where notification is not required – A notification to affected data subjects is not required in the event of a breach when:

i. Dublin Bus has applied appropriate technical and organisational measures to protect Personal Data prior to the breach (e.g. robust encryption).
ii. Dublin Bus has taken subsequent measures to ensure that a high risk to data subjects does not materialise (e.g. it recovers personal data that was lost).
iii. It would involve a disproportionate effort to notify data subjects directly, in which case a public announcement or similar measure should be adopted.

6.4.3 Notification to Controllers

Where Dublin Bus performs the role of processor the Data Protection Officer will notify the relevant controller without undue delay after becoming aware of a personal data breach and shall provide the following details:

(a) Description of the nature of the personal data breach including where possible, the categories and an approximate number of data subjects concerned and the categories and an approximate number of Personal Data records concerned.

(b) Description of the likely consequences of the personal data breach.

(c) Description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7 Third country transfers

Under data protection legislation, Dublin Bus may not (save where one of a limited number of exemptions applies) transfer Personal Data outside of the European Economic Area (EEA) to any third country or international organisation, unless that third country or international organisation ensures an adequate level of protection for the Personal Data in question. This prohibition on the transfer of Personal Data can be overcome where Dublin Bus uses one or more of the following legitimising transfer mechanisms:

a. **Explicit consent** - the data subject has explicitly consented to the data transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

b. **Adequacy Decision** - The EU Commission has approved a list of third countries which are considered to provide an adequate level of data protection. The effect of an adequacy decision is that Personal Data can flow to that third country in the same manner that a transfer within the EEA is permitted. So far Switzerland, Guernsey, Argentina, Isle of Man, Faeroe Islands, Jersey, Andorra, New Zealand, Uruguay and Israel have been approved in full and Canada for certain types of personal data.

c. **Standard Contractual Clauses** - A data transfer agreement, in the form approved by the European Commission or a data protection supervisory authority, has been executed by the exporter of data and the importer based outside of the EEA.

d. **Code of Conduct** - The transfer is made pursuant to a Code of Conduct that has been approved under applicable data protection legislation, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

e. **Certification** - The transfer is made pursuant to a certification mechanism that has been approved under applicable data protection legislation, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

f. **Privacy Shield** - The data importer is subject to a framework approved by the European Commission to facilitate transfers (e.g. the EU – U.S. Privacy Shield).

g. **Binding Corporate Rules** - the development of a set of "Binding Corporate Rules" governing the transfer of data to third countries and where such rules have been approved by the relevant data protection supervisory authorities.

The general policy is that personal data which Dublin Bus holds and processes, in its capacity as a controller, must remain within the EEA. If it is necessary for Dublin Bus to transfer personal data to a third country or an international organisation outside of the EEA, Dublin Bus shall ensure that it relies upon one of the above legitimising transfer mechanisms and documents this. Details of Dublin Bus's transfers of personal data outside the EEA shall be recorded in the Records of Processing Activities, together with the details of the basis on which those transfers are made.

A transfer of personal data outside the EEA may arise where transferring personal data to an external service provider based outside the EEA (or where the external service provider has remote access from a location outside the EEA to personal data held in the EEA). Particular attention is required to the selection of processors and when using online services for the processing of personal data

and to ensure all processing remains within the EEA (e.g. online marketing surveys, hosting of data etc.) or that a legitimising transfer mechanism is used. Where you require the transfer of Personal Data outside of the EEA, you must contact the Dublin Bus Data Protection Officer for consultation and guidance.

8 Children's data

Dublin Bus is a processer for the NTA Leap Card. As such, it can be deemed to a processor of children's Leap Card data. Apart from this, with the exception of certain activities such as its Corporate and Social Responsibility Initiatives, Dublin Bus does not knowingly collect information from children under the age of 16. In compliance with its Protection of children and vulnerable adults policy, in the event that images of children are being used for promotional, marketing or other reasons, Dublin Bus will ensure that:

- Parents/Legal Guardians and children consent to the use of an image and that this is recorded
- Photographs/images likely to be published in press on the internet are not used in conjunction with the children's first names (first name and surname) and detailed addresses.
- Parents/Legal guardians are always aware of the way the image will be used.
- Images of the children will not be used for any other reason with the consent of the Legal Guardian.

9 Data sharing – controller, processors and third parties

9.1 What is our role within dublin bus group – controller or processor

The CIÉ Group of companies consists of CIÉ (holding/parent), and three wholly owned subsidiary/operating companies set up under the Companies Acts as provided for in the Transport (Re-organisation of Córas Iompair Éireann) Act, 1986. Specifically, the CIÉ Group of companies includes CIÉ (the Holding Company including CIÉ Tours) and its operating companies Bus Éireann, Dublin Bus and Iarnród Éireann (subsidiaries). This policy applies to **Dublin Bus only**.

It should be noted that if personal data is flowing within the Group of companies, each company, whether it is a parent company or a subsidiary, is a distinct legal entity with its own set of legal and data protection responsibilities. Each company within a group of companies may, therefore, be a controller in respect of the personal data which it has obtained and for which it is legally responsible, and it is necessary for each controller to assess whether disclosures of personal data to other companies within the group of companies are permissible. In this instance, the other company is most likely a processor. The sharing of personal data between members of a group of companies does not necessarily create a relationship of joint data control, and in fact, this is likely to arise in relatively few cases (e.g. processing of incidents/accidents). It is more likely that where data is shared for a valid purpose, each company will be acting as a controller in its own right in respect of the personal data (because they are using the data separately for their own purposes) or other company of the group may be acting in the role of processor if it is using the data to provide a service to the company. However, Dublin Bus notes that the determination of whether each of the companies are a controller, processor or a joint controller is a factual analysis of a number of factors including considering, who has primary responsibility for the personal data and who determines the purposes for the processing.

The Article 29 Data Protection Working Party (soon to be known as the European Data Protection Board) previously published an Opinion on the concepts of controller and processor entitled **'Opinion 1/2010 on the concepts of "controller" and "processor"'** which was adopted on 16 February 2010, which goes into some detail into the assessment required to determine whether joint control exists. For example, **"persons working for another organisation, even if it belongs to the same group or holding company, will generally be third parties"**. As a result, sharing between the Holding company and operating companies is considered the same as sharing with any other external recipient (whether processor or joint controller) and the usual obligations [this requires][then arise] as defined in this policy.

'controller' means

1. the natural or legal person, public authority, agency or other body which,
2. alone or jointly with others,
3. determines the purposes and means of the processing of Personal Data;

The following provides 3 example scenarios within the Dublin Bus Group:

Scenario	Dublin Bus	CIE Holding Company or other Operating Company (Subsidiary)
Processing of Incident/Accident Data	Controller	Controller
Processing of Claims Data	Controller	Controller
Providing Dublin Bus IT Managed Services to operating companies	Processor	Controller

Each specific data classification has been examined on a case-by-case basis and our role included within the Data Inventory. Where a request is made for sharing of Personal Data within the CIÉ Group of companies which would not be considered appropriate this should be escalated to the Dublin Bus Data Protection Officer for clarification.

9.2 What are our requirements in the use of processors and how dublin bus complies with them?

Common examples of processors, include companies that provide outsourced services such as payroll, service providers, operators of CCTV systems, IT support service providers, cloud hosted software provided etc. In addition, some CIÉ entities may process personal data on behalf of Dublin Bus e.g. as part of intra-group services arrangements. If a third party has access to personal data that Dublin Bus, holds in its capacity as a controller, that third party is likely to be acting as a processor of such personal data. In such circumstances, Dublin Bus complies with its obligations in connection with engaging processors.

Whenever Dublin Bus share personal data with a recipient outside of CIÉ holding company, the following must be adhered to:

a. Dublin Bus undertakes due diligence to ensure that it is appropriate to engage the processor.
b. Dublin Bus ensures that the sharing of the personal data must be governed by a written contract that complies with the requirements under applicable data protection legislation and includes the clauses set out in Section 9.5 or substantially similar provisions in agreements with processors.

9.3 Evaluation of processors and pre-processing agreements

Dublin Bus must use only processors providing sufficient guarantees to implement, and be able to demonstrate, appropriate technical and organisational measures taking into account the nature, scope, context

and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

The following provides a list of standard questions which must be asked when engaging a processor and prior to engagement of processor (used to help evaluate of a processor pre-contract).

Ref	Requirement
1	Dublin Bus requires the solution to adhere to good industry security practice and must be in compliance with Dublin Bus legislative and regulatory requirements: • Dublin Bus Policies. • Legislative Requirements (e.g. EU GDPR, Data Protection Acts) Dublin Bus Policies will be made available to the successful tenderer. If partially compliant, please specify explicitly the areas of non-compliance.
2	Please confirm you will make available to Dublin Bus all information necessary to demonstrate compliance with data protection good practice and GDPR.
3	The supplier must allow for, and contribute to audits and vulnerability testing, conducted by Dublin Bus or another auditor mandated by Dublin Bus The supplier agrees to facilitate such a technical verification test and agree to repair defects found which are as a result of not conforming to a requirement detailed in this document.
4	Please describe all external/public interfaces to the proposed solution, in particular, those which may be accessed directly by the public.
5	Please describe all internal and administrative interfaces to the proposed solution along with the user profiles/type of user expected to use each interface.
6	It must be possible to trace all activity on the system through the use of an audit trail (e.g. login events/failed logins etc.). Audit trail should be time stamped and retained for a sufficient period of time to allow for the offline retention and/or enable investigation of incidents.
7	Please describe security controls implemented on the external/public interfaces, specifying how controls are implemented to prevent (for example): a. Input validation issues such as SQL injection, Command injection, Cross-Site scripting etc. b. Authentication issues (e.g. bypassing authentication). c. Authorization issues (e.g. ability to view or manipulate other users' data). d. Access control issues (e.g. masquerading as a different user). e. Password strength and brute-force issues (e.g. password lockout/reset issues). f. Session management Issues (e.g. session predictability, hi-jacking or lack of session management). g. Parameter tampering (e.g. ability to manipulate values on the server for gain, or to gain access to unauthorised data). h. Administrative processes and issues (e.g. ability to escalate privileged commands or connect to the administrative interface). i. Other flaws which may result in breaches of confidentiality, integrity or availability. It is expected that best practice web application security will be applied in the solution to prevent the above issues.
8	The solution design needs to be compliant with the data protection requirements and good practice, including: a. Secure by design b. Secure by default c. Pseudonymisation (where possible) d. Data retention period enforcement e. Encryption of data at rest and in transit f. Implementation of "minimum rights" for users g. Auditing of user access Please describe how your solution demonstrates compliance with above (a) – (g), in particular for high risk and special categories of personal data (e.g. medical records).

Ref	Requirement
9	The information needs to be processed in compliance with the EU GDPR principles. Including: a. Data minimisation: only process the information required. b. Accuracy: Information processed needs to be reasonably kept up to date. c. Stored for only the period required: For example, should a member cease membership and are no longer required how the information is removed from the solution. d. Data protection by design and by default. Please describe how your solution **demonstrates** compliance with above (a) – (d), in particular for high risk and special categories of personal data (e.g. medical records).
10	Processing of special categories of personal data (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), is prohibited under the EU GDPR unless explicit consent is provided. Please describe: a. All special categories of personal data proposed to be processed. b. Where the information will be stored c. Necessity and proportionality of the information processing / why it is required. d. How the solution proposes to collect explicit consent for the processing of special categories of personal data. e. How the solution proposes to maintain records of explicit consent for special categories of personal data.
11	The subjects have a right to access, rectification, and erasure of the information. Please describe: a) How the solution supports extracting all information relating to a specific individual (in order to fulfil data subject access requests). b) How the solution supports erasure of all information related to a particular individual (to support the data subject's rights to erasure).

Processors must get permission to use further sub-processors – e.g. brokers. See Section 8.4 for further information.

9.4 Processing agreements

All processing engagement must be governed by a written contract that is binding on the processor which sets out the processor's data processing obligations. A template clause is set out below.

Definition: In this [Agreement] **"Data Protection Law"** means all applicable data protection law including, with effect from 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) and national implementing legislation; and the terms **'personal data'**, **'controller'**, **'processor'** and **'process'** shall have the meanings given to them under data protection law.

1.1 The processor acknowledges that in providing [Services] under this [Agreement] the processor will process personal data on behalf of Dublin Bus. In such circumstances, both parties acknowledge that Dublin Bus is the controller and the processor is the processor and the processor agrees that:

a. the processor processes [[insert detailed description of data – i.e. the type of personal data and categories of data subject] OR [insert appropriate cross reference, e.g. to an appendix setting out such details]], on behalf of Dublin Bus in the context of providing the [Services] under this [Agreement], for the duration of the [Term]. The obligations and rights of Dublin Bus shall be as set out in this [Agreement].

b. it processes the personal data only on documented instructions from the controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by European Union or member state law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

c. it shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d. it shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed; these measures shall include as appropriate: (i) the pseudonymisation and encryption of personal data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services, (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data.

e. it shall assist Dublin Bus by implementing appropriate technical and organisational measures, to allow Dublin Bus to comply with requests from data subjects to exercise their data subject rights under applicable Data Protection Law.

f. it shall inform Dublin Bus immediately in the event of receiving a request from a data subject to exercise their rights under Data Protection Law and provide such co-operation and assistance as may be required to enable Dublin Bus to deal with such request in accordance with the provisions of Data Protection Law.

g. it shall assist Dublin Bus in ensuring compliance with its obligations in respect of security of personal data, data protection impact assessments and prior consultation requirements under Data Protection Law. The processor shall immediately inform Dublin Bus if, in its opinion, an instruction infringes Data Protection Law.

h. it shall not engage any sub-processor without the prior written consent of Dublin Bus and where Dublin Bus has consented to the appointment of a sub-processor, the processor shall not replace or engage other sub-processors without the prior written consent of Dublin Bus.

i. that where any sub-contractor of processor will be processing such personal data on behalf of Dublin Bus, the processor shall ensure that a written contract exists between the processor and the sub-contractor containing the same data protection obligations as set out in this [Agreement], in particular providing sufficient guarantees to implement appropriate technical and organisational measures. In the event that any sub-processor fails to meet its data protection obligations, the processor shall remain fully liable to Dublin Bus for the performance of the sub-processor's obligations.

j. that when the processor ceases to provide [Services] relating to data processing, the processor shall (i) at the choice of Dublin Bus, delete or returns all personal data to Dublin Bus and (ii) delete all existing copies of such personal data unless Union or Member State law requires storage of the personal data.

k. it shall: (i) make available to Dublin Bus, all information necessary to demonstrate compliance with the obligations laid down in this clause [•]; and (ii) allow for and assist with audits, including inspections, conducted by Dublin Bus,or another auditor mandated by Dublin Bus, in order to ensure compliance with the obligations laid down in this clause [•], including its

data security obligations under Data Protection Law [provided however that Dublin Bus, shall be entitled, at its discretion, to accept adherence by the processor to an approved code of conduct or an approved certification mechanism to aid demonstration by the processor that it is compliant with the provisions of this clause [•]];

l. it shall notify Dublin Bus without undue delay, and in any event within twenty-four (24) hours, after becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and provide Dublin Bus with such co-operation and assistance as may be required to mitigate against the effects of, and comply with any reporting obligations which may apply in respect of, any such breach. Such notification by processor shall at least contain the following details: (i) a description of the nature of the breach including where possible the categories and approximate number of personal data records concerned; (ii) the name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) a description of the likely consequences of the breach; (iv) a description of the measures taken or proposed to be taken to address the breach including, where appropriate, measures to mitigate its possible adverse effects. The processor shall document the security breach, including the facts related to the breach, its effects and the remedial action taken and shall, upon request, immediately provide Dublin Bus with the relevant documentation in written or electronic form; and

m. no such personal data shall be transferred outside of the European Economic Area by the processor or any of its agents or sub-processors without the prior written consent of Dublin Bus which consent may be subject to terms and conditions (including, without limitation, that the data importer enters into model clauses in the form approved by the European Commission and, where relevant, complies with the provisions regarding sub-processors contained in such model contracts in respect of any sub-processors). The processor shall comply with the requirements of Data Protection Law in respect of transfers of such personal data outside of the European Economic Area, to the extent that CIÉ consents to any such transfer.

1.1 Controller to controller transfers

In certain circumstances Dublin Bus transfers personal data of which it is a controller of (e.g. data relating to employees) to third parties, or allows third parties to have access to such personal data, on a controller to controller basis. This means that the third party will process such personal data for their own purposes and not on behalf of Dublin Bus. By way of example, this may occur in the following circumstances:

a. **Pensions** - When employee data is provided to a pension service provider, the trustee(s) of the pension will be a controller in relation to such Personal Data. This Personal Data is then processed by the pension trustees (or the pension service provider) for the purposes of administering the pension.

b. **Health Insurance** - When employees are provided with health insurance, the health insurance provider (e.g. VHI) will be a controller in relation to the employee data that is used to administer the insurance.

c. **Legal advice** - When personal data is provided to solicitors in order to receive legal advice in respect of a claim or other matter, the solicitors firm is likely to be a controller of such personal data where they provide independent legal advice and make decisions regarding the legal strategy for the claim.

d. Audits - Where a third party is granted a right to audit Dublin Bus, and the audit is carried out on behalf of that third party (i.e. it is not an internal audit, or an audit by a third party that is requested by Dublin Bus), any personal data (e.g. relating to Dublin Bus employees) that is processed in the context of such audits is processed by the auditing party as a controller.

e. Claims - When personal data is provided to CIÉ Investigations Department, CIÉ is likely to be a controller of such personal data for the purpose of investigating the accident or claim.

Where there is a controller to controller transfer, the transferee is primarily responsible for complying with its own data protection obligations (i.e. Dublin Bus is not responsible for ensuring that a transferee of Personal Data complies with that transferee's own data protection obligations). Details of controller to controller transfers are set out in the data inventory.

10 Personal data handling rules

In order to apply appropriate technical and organisational measures, it is necessary to classify and define handling rules for the different classifications of Personal Data.

10.1 Personal Data Risk Levels

At the heart of the GDPR, is an analysis of the risks from the various types of processing taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. This is based on the impact or level of damage that may be suffered by the data subject (as opposed to Dublin Bus).

A risk rating has been assigned to each **Personal Data Category** based on the following criteria:

Category Risk Level	Description	Information Examples
Very High	The category contains personal data which includes special categories of personal data, or bank account, payment card number details or data relating to criminal convictions or offences.	• Anything revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning medical or health, data concerning a natural person's sex life or sexual orientation. • Bank Account or Payment Card Details. • Criminal background checks and declarations. • Other information highly sensitive in nature.
High	The category contains personal data which the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to the data may result in a high risk to the rights and freedoms of natural persons.	• Description of accidents/ claims, correspondence and evaluations (not medical) • Employee information including performance, reviews, employee contracts or other non-special categories of personal data.
Medium	The category contains personal data which the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorized access to the data is less likely to result in a high risk to the rights and freedoms of natural persons.	• Personal data including names and contact details in combination with addresses, CVs etc.
Low	The category contains personal data which the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorized access to the data is not likely to result in a high risk to the rights and freedoms of natural persons.	• All other forms of personal data including names and contact details

Note: The risk level should always be considered in light of the nature of the data, the purposes of the processing and the impact that any unauthorised access, loss or destruction would have on the relevant individuals. address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.2 Data handling rules

The following defines the minimum handling requirements for each Personal Data classification. Note that all personal data (regardless of its format), may only be processed in line with Data retention requirements:

	Low	Medium	High
Storage on Laptops	Laptops must not be used as a storage location		
Storage on Public Shared Drives	Must not be stored on public shared drives.		
Storage on Work Drives	May be stored in line with data retention requirements set out in the [Dublin Bus Data retention policy]. All Personal Data must be restricted on need to know basis.		
Storage on SharePoint	May be stored in line with data retention requirements set out in the [Dublin Bus Data retention policy]. All personal data must be restricted on need to know basis.		
Storage on OneDrive	May be stored in line with Data Retention Requirements set out in the [Dublin Bus Data retention policy]. All Personal Data must be restricted on need to know basis.		
Storage on Private/Home Drives	May be stored however should be structured in such a manner/ system which ensures implementation of the data retention policy.		
Email Transfer. 1.1Note: Email is a method of communication and must not be used as a storage location.	May be used for the transfer of information only. Email must not be considered as an area in which to store information for the long-term. Emails which are important must be saved into an appropriate storage area with other records on the same topic. This will ensure a full and complete record is kept and that emails are not 'lost' or hard to retrieve should they be deleted or archived as part of auto archiving. The contract must be in place for all recipients with whom Dublin Bus transfers Personal Data and appropriately risk assessed.		
	Consider encryption of email based on risk.	Must be encrypted if transferred via email.	

	Low	Medium	High
Processed within Dublin	May be stored in line with Data retention requirements set out in the [Dublin Bus Data retention policy]		Should not be stored in CRM.
Bus structured applications (e.g. Microsoft CRM).	Retention Policy]. However, Dublin Bus must minimise the information stored, and restrict on "need-to-know" basis.		
CCTV footage	Must not be disclosed unless: • A contract is in place • Legally required to disclose the footage (such as official investigation by Gardai where formal, written request by a data subject has been made) Must only be reviewed by authorised persons. Must be securely destroyed in line with recommended data retention guidelines set out in the [Dublin Bus data retention policy].		
Paper-based files – access control and transfers	The contract must be in place for all recipients with whom personal data is shared, and the sharing of the data must be appropriately risk assessed. Must be restricted on a need to know and minimum rights basis.		
	Must not be stored in public/common areas. Should not be stored or processed offsite except for absolute business requirement and the risk appropriately assessed.		
Everything Else (Including Spoken Communications etc.)	Must not be disclosed unless contract in place. Processed on Dublin Bus controlled systems and within Dublin Bus physical location.		
Reports		All reports should be anonymised, masked or pseudonymised.	
Data Destruction	Must be securely destroyed in line with Data Retention requirements set out in the [Dublin Bus Data Retention Policy].		

The above identifies minimum handling requirements only. Additional controls may be put in place for certain personal data types if required in addition to the above.

Information correct at time of print. October 2019

Version	2
Approved by Dublin Bus board	28 August 2019

Dublin Bus
59 Upper O'Connell Street,
Dublin 1,
Ireland,
D01RX04

T: 01 8734222
W: www.dublinbus.ie

Dublin Bus