Data Protection Policy

Document Title	Data Protection Policy
Document Owner	Information Management Group
Author	Andy Henderson
Document Version	V3.2
Approved By	Merseytravel
Created Date	December 2015
Review Date	August 2022
Renewal Date	August 2024

Uncontrolled when printed – for latest version please check OnePlace

Contents

Version	Date	Updates
V3.2	May 2022	Change references of EU GDPR to UK GDPR Added reference to statutory nature of DPO role Change reference to Information Security Incident Management Protocol to Data Breach Protocol

1. Introduction

1.1 This document sets out Merseytravel and the Liverpool City Region Combined Authority's ('the Combined Authority) policy regarding Data Protection. It is based on the Data Protection Act 2018, which came into force on 25 May 2018 and the UK General Data Protection Regulation (GDPR), which was adopted upon the United Kingdom's withdrawal from the European Union on 31 January 2020..

1.2 The purpose of the GDPR is to regulate the way in which personal information about individuals is obtained, stored, used and disclosed. The legislation grants rights to individuals to see data stored about them and to require modification if the data is incorrect, and, in certain cases, to compensation. These provisions amount to a right of privacy for the individual.

1.3 The GDPR requires that personal data must be kept and used in accordance with its provisions and that the Information Commissioner's Office (ICO) must be notified of all processing of personal data and of the GDPR (see www.ico.gov.uk for more information).

1.4 Merseytravel and the Combined Authority are a registered data controllers with the ICO (Registration Numbers Z741948X and ZA098743, respectively). The types of personal information processed by Merseytravel can be found on the ICO's website at this link, while the Combined Authority's information can be found at this link.

1.5 During the life of this policy, it is anticipated that the United Kingdom is scheduled introduce a Data Reform Bill. It is anticipated that this will remove or amend many facets of GDPR. This policy will be updated to reflect any legislative changes.

2. Policy Statement

2.1 Everyone has rights with regard to how their personal information is handled. During the course of Merseytravel and the Combined Authority's activities we will collect, store and use personal information about our staff, suppliers, contractors, customers and other parties, and we recognise the need to treat it in an appropriate and lawful manner.

2.2 The information is subject to certain legal safeguards specified in the GDPR and other regulations. The GDPR imposes restrictions on how Merseytravel and the Combined Authority uses that information.

2.3 Merseytravel and the Combined Authority support the objectives of the GDPR. This policy is designed to ensure that the confidentiality of personal data is maintained, whether held or processed on computer or

in manual files, and to increase the access given to individuals to their information.

3. Status of the Policy

3.1 This policy sets out our rules on Data Protection and the legal conditions that must be satisfied in relation to the obtaining, handling, storage, transportation and destruction of personal information.

3.2 Overall responsibility for the implementation of this policy lies with the Chief Executive. Day to day responsibility for protection of data lies with the Head of Service for each section.

3.3 Any questions or concerns about the operation of this policy should be referred to the Senior Information Management Officer in the Legal, Democratic Services and Procurement Department, who is the statutory Data Protection Officer for both organisations.

4. Definition of Data Protection Terms

4.1 **Data** is information which is stored electronically or in paper-based filing systems. The information does not have to be in a written format to be classed as data. Photographs and CCTV images are also data.

4.2 **Data subjects** include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

4.3 **Personal data** means data relating to a living individual who can be identified from that data or from that data and other information either in or likely to come into our possession. Personal data can be factual (such as a name, address or date of birth), an expressed opinion about that person, their actions and behaviour or any indications of the intentions of the data controller in respect of that person.

4.4 **Controllers** determine the purposes and manner in which any personal data is processed. They have a responsibility to establish practices and policies in line with the GDPR. Merseytravel and the Combined Authority are the data controllers of all personal data held and used in our business for our own purposes.

4.5 **Data users** include employees whose work involves processing personal data. Data users have a duty to protect the information they handle by following our Data Protection and other applicable Information Governance Policies.

4.6 **Processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded

from this definition, but it would include contractors who handle personal data on our behalf.

4.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4.8 **Special category personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life. Sensitive personal data can only be processed under strict conditions as defined by Article 9 of the GDPR (such as the data subject's explicit consent).

5. Data Protection Principles

5.1 Anyone processing personal data must comply with the six enforceable principles set out by Article 5 of the GDPR. These provide that personal data must be:

a) processed fairly, lawfully and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) processed for specified, explicit and legitimate purposes and not further processed in a manner that is incomparable with those purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and up to date ('accuracy');
e) 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 ('storage limitation');
f) 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 ('integrity and confidentiality');

5.2 Merseytravel and the Combined Authority, as data controllers, are responsible for, and must be able to demonstrate compliance with, the above Principles.

6. Lawfulness, Fairness and Transparency

6.1 The GDPR is intended to ensure that the processing of personal data is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this

case Merseytravel and the Combined Authority), the purpose for which the data is to be processed by Merseytravel and the Combined Authority, and the identities of anyone to whom the data may be disclosed or transferred.

6.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the GDPR. These are set out in Article 6 of the GDPR and include the data subject's consent to the processing, the performance of a contract with the data subject, and the processing being necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (such as Merseytravel and the Combined Authority's public functions). When special category personal data is being processed, additional conditions must be met (see Article 9). When processing personal data as data controllers in the course of business, Merseytravel and the Combined Authority will ensure that those requirements are met.

6.3 Article 13 of the GDPR states that Merseytravel and the Combined Authority will inform data subjects about:

- Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer
- Purpose of the processing and the legal basis for the processing
- The legitimate interests of the controller or third party
- Description of the categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

6.4 We will ensure that this Fair Processing Notice is concise, transparent, intelligible and easily accessible. It will be written in clear and plain language and provided free of charge.

6.5 If the personal data is collected directly from data subject then notice should be provided at the time of collection.

6.6 Furthermore, Article 14 of the GDPR states that if the personal data is received from another data controller (i.e. not directly from the data subject), the fair processing notice will be provided

- Within a reasonable time (i.e. one month)
- If data is being used for communication purposes then no later than the first communication
- If data is being shared further, then before the first disclosure takes place

7. Purpose Limitation

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

8. Data Minimisation

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

9. Accuracy

Personal data must be accurate and kept up to date. When information is incorrect or misleading, steps should be taken to remedy this. Checks should be carried out at regular intervals after the data has been collected. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Storage Limitation

Personal data should not be kept longer than is necessary for the purpose. We will take all reasonable steps to destroy or erase from our systems all personal data that is no longer required. Merseytravel and the Combined Authority's Record Retention Schedule & Guidance should be consulted when determining how long certain data should be retained.

11. Integrity and Confidentiality

11.1 Merseytravel and the Combined Authority must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of

personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 We will, at all times, have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

a) **Confidentiality** means that only people who are authorised to use the data can access it.

b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

11.4 Security procedures include, but are not limited to:

a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold personal information.

c) **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs and other removable storage devices should have data permanently deleted from them where possible and otherwise be physically destroyed when they are no longer required.

d) **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock or turn off their PC when it is left unattended.

11.5 In the event of a security breach (i.e. unauthorised access or loss of data or equipment) being discovered, consult the Data Breach Protocol (formerly the Information Security Incident Management Protocol). The organisation's response will include:

a) **Containment and recovery of data**; it must established who will lead the investigation into the breach, who should be informed and what steps are required to contain and recover the lost data. In serious cases it may be appropriate for the Police to be notified.

b) **Assessment of the risk**; the consequences of the breach are and how the data could be used should be determined. This will be influenced by the type and sensitivity of the data. It will be necessary to assess the effectiveness of any protections that were in place, such as encryption of devices.

c) **Notification of breaches**; impacted individuals should be informed that a breach has occurred to allow them take steps to mitigate the risks posed to them (i.e. cancelling bank cards). When a large number of people are involved or there are serious consequences we must report the breach to the ICO. The decision on whether to report a breach will be made by the Legal, Democratic Services and Procurement Department.

d) **Evaluation and response**; Merseytravel and the Combined Authority must investigate not only the cause of the breach, but also the effectiveness of our response to it. This is likely to involve a review of relevant policies and procedures to identify any weaknesses, establishing what personal data is held, where and how it is stored and assessing where risks lie. This may include increased staff training and guidance.

12. Processed in Line with Data Subjects' Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- be informed of any data held about them by a data controller and to be provided with copies by making a subject access request (Article 15);
- rectification of inaccurate personal data (Article 16)
- erasure of personal data no longer necessary for the purpose for which it was collected, where consent is withdrawn, where the data subject objects to the processing (and there is no overriding legitimate grounds),where the personal data has been unlawfully processed (Article 17)
- restriction of processing by the data controller (Article 18)
- portability of their data that has been provided to the data controller in a commonly used, machine-readable format (Article 20)
- object to processing based on the public task or legitimate interests condition of Article 6 (Article 21)
- object to any decision that significantly affects them being taken solely by a computer or other automated process (Article 22).

13. Dealing with Subject Access Requests

13.1 Individuals (whether Merseytravel and the Combined Authority employees or members of the public) have the right to be informed

whether their personal data is being processed by a data controller, the purpose of the processing, whether their data has been disclosed to anyone and for copies of their data to be provided to them. This is the right of subject access as stipulated by Article 15 of the GDPR.

13.2 Any request must be made in writing (a pro forma is available from the Legal, Democratic Services & Procurement Department), specify the data being requested and be accompanied by adequate proof of identification. Once all necessary information and the fee have been received, a response must be issued within one calendar month.

13.3 Requests can be made either by the data subject, or by someone acting on their behalf (i.e. a solicitor). Merseytravel and the Combined Authority must be satisfied that the third party has the proper authorisation from the data subject to receive their data.

13.4 When a request is received it should be forwarded to DPO@liverpoolcityregion-ca.gov.uk or, if received by post, forwarded to the Senior Information Management Officer, who will co-ordinate the response with the department(s) who holds the data.

13.5 Some exemptions do apply, meaning that in certain scenarios a requester might not be entitled to be informed that their data is being processed and would not receive copies of it. Examples of this include data held for the purposes of crime and taxation, employment references provided (but not received) by Merseytravel and the Combined Authority, management forecasting and negotiations. The Senior Information Management Officer will be able to advise if any exemptions are applicable to the requested information.

13.6 For further guidance please see the 'How To Identify Information Requests' flowchart at Appendix One and the ICO's website.

14. Providing Information to Third Parties

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us. In particular they should:

a) check the identity of the person making the enquiry and ensure that they are legally entitled to receive the information requested;

b) instruct the third party to put their request in writing, explaining why they require the information and which provision of the GDPR they are relying upon;

c) keep a record of what information has been provided and Merseytravel and the Combined Authority's justification for doing so, and

d) refer to the Senior Information Management Officer for assistance if they have any queries.

15. Training

15.1 Merseytravel and the Combined Authority are committed to its aim that all staff will be properly trained and fully informed of their obligations under the GDPR.

15.2 The e-learning portal includes Data Protection modules, which should be completed by all officers.

15.3 Bespoke training sessions are available from the Senior Information Management Officer, and can be tailored to suit the particular needs of a department.

16. Disciplinary Action

Merseytravel and the Combined Authority expects all of its staff and members to comply fully with this Policy and the GDPR. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this Policy.

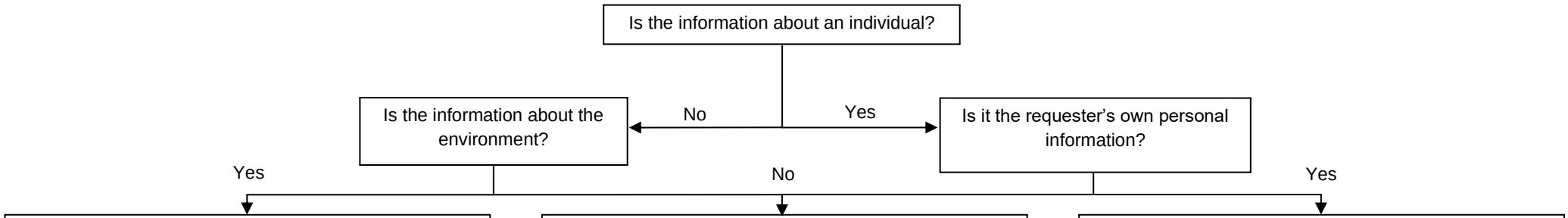
17. Monitoring & Review of the Policy

17.1 This policy will be reviewed regularly by the Legal, Democratic Services and Procurement Department to ensure it is updated in line with any legislative updates.

17.2 Merseytravel and the Combined Authority will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

Appendix One

How to Identify Information Requests



Environmental Information Regulations 2004

- Includes recorded information held by some public bodies relating to the elements, emissions, policies & reports, buildings and health & safety
- 20 working days to respond
- Requester must provide their name and an address for correspondence; there is no standard fee
- There is no strict limit on the time it would take to respond; requests can be refused if it would be 'manifestly unreasonable' to reply, but the burden for responding can be higher than under FOI
- Information must be supplied unless an exception applies, such as: information is in draft; internal communications; commercial sensitivity; prejudice to a fair trial; information is confidential
- All exceptions subject to a public interest test, which balances the arguments for disclosure against the factors in favour of refusal
- Reasons for withholding information differ from FOI, so it is important to apply the correct legislation
- Third party personal information can be asked for, but will only be disclosed if doing so is in accordance with Data Protection legislation
- The Information Commissioner's Office investigates complaints, and can overturn our decision

Freedom of Information Act 2000

- Includes recorded information held by all public bodies such as printed documents, computer files, letters, emails, photographs, and sound or video recordings
- 20 working days to respond
- Requester must provide their name and an address for correspondence; there is no standard fee
- If responding would take the organisation over 18 hours of work, there is no obligation to provide the information. We must, however, suggest what we could provide within the time limit.
- Information must be supplied unless an exemption applies, such as: information will be published; disclosure would prejudice the conduct of public affairs; commercial sensitivity; information is confidential
- Most exemptions subject to a public interest test, which balances the arguments for disclosure against the factors in favour of refusal
- Reasons for withholding information differ from EIR, so it is important to apply the correct legislation
- Third party personal information can be asked for, but will only be disclosed if doing so is in accordance with Data Protection legislation
- The Information Commissioner's Office investigates complaints, and can overturn our decision

General Data Protection Regulation

- Includes information held by anybody that allows the individual to be identified, such as their health records, completed application forms, and images or recordings of them
- one calendar month to respond
- Requester (or advocate) must provide proof of their identity and body holding the data can charge for postage
- There is no strict limit on the time it would take to respond; requests can be refused if it would require a 'disproportionate effort', but this only applies to physically providing the information (i.e. considerable amounts of physical files that cannot be posted).In practical terms, this is rarely applicable
- Requester can be asked to assist in reducing the scope of their enquiry to aid our searches
- Information must be supplied unless doing so would have a negative impact on crime & taxation, management planning & forecasting, on-going negotiations or legal professional privilege
- Third party personal information contained in the same record should be anonymised where possible, but disclosure may be allowed
- The Information Commissioner's Office investigates complaints, and can overturn our decision

If you have any questions, or have received an information request, please contact
Andy Henderson, Senior Information Management Officer (x1679, andrew.henderson@liverpoolcityregion-ca.gov.uk) or
FOI@merseytravel.gov.uk / FOI@liverpoolcityregion-ca.gov.uk / DPO@liverpoolcityregion-ca.gov.uk