Data Privacy Policy & Procedure

PURPOSE

All employees of Delight International Movers (DIM) who process personal data must comply with the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

SCOPE

This Procedure & policy applies to:

- All branches of DIM
- All employee and volunteers of DIM
- All contractors, suppliers and other people working on behalf of DIM

It applies to all data that the DIM holds relating to identifiable individuals, even if that information technically falls outside of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 this can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Documents like Passport and Visa copies.
- Any other information relating to individuals

RESPONSIBILITIES

Everyone who works for or with DIM has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Top Management** is ultimately responsible for ensuring that DIM meets its legal obligations.
- All employee who deals with data are responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from employee and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data DIM holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the DIM's sensitive data.

- The **IT personnel,** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the DIM is considering using to store data. For instance, cloud computing services.
- The **sales & marketing personnel,** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Is responsible for communicating the data protection policy to the customer and obtaining their consent
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other employee to ensure marketing initiatives abide by data protection principles.

TERMS AND DEFENITIONS

- **Data Protection Officer** – means a person in DIM who decides the purposes for which and the way in which personal data is collected and used. The DIM HR Dept head, is the Data Protection Officer in respect of employee and Employee personal data.
- **Personal Data** – means information about a living person who can be identified by that information or by that information together with other information that the Data Protection Officer has or is likely to obtain.
- **Data Subject** – all employee of the DIM are data subjects under the Act. Other definitions are set out in the body of the text where appropriate.

DATA PROTECTION PRINCIPLES

All personal data must be processed in accordance with *CHAPTER II* ***Principles*** *Article 5* **Principles relating to processing of personal data of the** REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

The essence of these principles is set out below together with brief, non-exhaustive practical examples of when these principles may have relevance to you.

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) Be collected with the consent of the individual after explaining the purpose and the necessity of the data.

(c) The individual will have the right to refuse the collection or processing of his personal data unless it is required by the Law.

(d) Be obtained only for one or more specified or lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;

(e) Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

(f) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(g) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

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

(i) 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; personal data may be stored

for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(j) 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').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

In accordance with the above principles DIM Employees are strictly follow the below instructions.

- Employees should collect only the relevant minimum data from the customer which is essential to ensure that the services solicited by the customer is delivered at the best possible manner. The customer should be clearly explained the purpose and reason for the collection of these data. They also should be informed about our data Privacy policy and where it is available for their reference.
- Employees should immediately update any of the customer records if they have been advised of any changes by the customer via phone, email of any other medium of communication.
- Employee must notify changes of name, address, telephone number, bank and marital status to the HR Department soon as possible. The HR Department will endeavor, periodically, to ask employee to confirm that such personal data held by the DIM is accurate. Employees should advise the DIM of any changes to their contact details or to any other details that may be of relevance.

- All Employees of DIM, required to delete any personal data from their computer or destroy the files (if manually recorded) at the end of the sixth year following the year in which the service was provided to the person. In case of information regarding the employees held by the HR Department all the personal data other than what is required by Law is destroyed at the end of the sixth year following the year in which the data subject ceased to be an Employee of DIM. The reason that the DIM retains this information for this duration is to assist in establishing facts in the event of a dispute.

- All individuals have a right of access to the information that the DIM holds about them. Upon receipt of a written subject access request DIM shall disclose all the information that it is required to do so by law

- If any employee receives any request from a customer, business contact, other employee or any other third party requesting any information about them then they must pass the request to the Data Protection Officer immediately.

- Employees should, if they are making a data access request of a DIM customer, send their access request to the Data Protection Officer

- Access to personal data must be restricted to authorised individuals for approved purposes

- The DIM must take steps to put in place technical methods (i.e. firewalls, encryption, password protection, etc.) or organisational methods (hierarchy of access to personnel files, locking cabinets etc.) of protecting personal data where the importance of the personal data makes this appropriate.

- All Employees who have access to personal data controlled by the DIM whether or not on computer, and whether in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that neither the DIM, nor any individual employed by the DIM, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data. All individuals must fully comply with all DIM procedures and requirements in this regard.

- Laptops are particularly vulnerable to theft, especially when used outside of DIM premises. In these circumstances, employee must keep laptops in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe.

- Personal data should not be stored on laptops unless this is unavoidable and appropriate security measures have been implemented following a risk assessment. This will comprise an encryption and security system. These measures will apply to portable data storage media such as DVDs, mini hard disk drives and USB flash memory data sticks. • Personal data must not be transmitted over the Internet unless appropriate encryption methods are used.

- Personal data must not be sent to a third party on portable storage media or in paper form by conventional post. A secure delivery service must be used.

Employees should ensure the security of employment or employee records (whether paper records or computerised) at all times, including when out of the DIM premises. Employee must not leave personal data on screen or on desk tops when they are not at their desks. Paper records should be stored securely unless under active consideration. A clear desk policy should be observed.

DATA PROTECTION RISKS

This policy helps to protect DIM from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the DIM uses data relating to them.
- **Reputational damage.** For instance, the DIM could suffer if hackers successfully gained access to sensitive data.

GENERAL EMPLOYEE GUIDELINES

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **DIM will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorized people, either within the DIM or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or Data Protection Officer.
When data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot see it.
These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorized people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the DIM's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

DATA USE

Personal data is of no value to DIM unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorized external contacts.
- Personal data should **never be transferred outside of the DIM** without permission of Top Management.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

DATA ACCURACY

The law requires DIM to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort DIM should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Employee should not create any unnecessary additional data sets.
- Employee should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- DIM will make it **easy for data subjects to update the information** DIM holds about them. For instance, via the DIM website.

- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by DIM are entitled to:

- Ask **what information** the DIM holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the DIM is **meeting its data protection obligations**.

If an individual contacts the DIM requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at [email address]. The Data Protection Officer can supply a standard request form, although individuals do not have to use this.

The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, DIM will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from the DIM's legal advisers where necessary.

PROVIDING INFORMATION ABOUT THE POLICY

DIM aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the DIM will provide an individual with access to view this document by publishing this in our website.

SECURITY

Data Breech and reporting

Any breaches of this Procedure in relation to personal data security will result in disciplinary action and, in serious cases, may result in the dismissal or the expulsion of an Employee.

Employees will be authorised to gain access to certain computer systems, programs and data in accordance with the necessity of their activities. No employee must attempt, alone or with others, to gain access to data or programs to which they have not been authorised to gain access.

Employees must not disclose personal details of other employee or Employees to unauthorised third parties where this information is personal data in respect of which the DIM is the Data Protection Officer.

Any Data breech or unauthorized access to any personal Data if found to be immediately informed to the data controller and the data controller should notify the competent Government authorities (UAE Police) within 72 hrs. of discovering the breech.

The notification shall at least:

(a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) Describe the likely consequences of the personal data breach;

(d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The Data protection officer shall 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 with this Article.

The data protection officer shall communicate to the data subject or subjects about the data breech of the data that was stored by DIM without any delay once the authorities have given their, “no objection”, to inform the data subjects.

SURVEILLANCE AT WORK

The DIM has a legitimate interest in monitoring the behavior of its employee and Employees that attend the DIM. For instance, DIM may wish to carry out monitoring in order to:

- Detect harassment or other inappropriate behavior;
- Monitor performance of its employee or of Employees where this is appropriate;
- Monitor and detect the outward transmission of confidential information;

- Prevent and detect theft of DIM property;
- Prevent or detect any unlawful act;
- Monitor adherence to this and other policies;

Monitoring can take several forms. It can involve monitoring by way of Closed Circuit Television (CCTV), e-mail and Internet monitoring or telephone monitoring. More detailed information about the monitoring of Internet and e-mail activity can be found in the DIM IT Policy. The DIM holds information on the destination and duration of calls made from the DIM telephone system and may use this information if misuse of the system is suspected. Below, the DIM sets out its policy with regard to the use of CCTV cameras.

CCTV CAMERAS

In carrying out such monitoring the DIM may use CCTV cameras in what are considered to be "public" areas of the workplace. Generally, the use of such CCTV Cameras shall be notified by using suitable signage at obvious places at the entrance to the monitored areas, however, (even in the absence of such signage) Employees and employee should be aware that public space within DIM premises may be monitored in this way.

The DIM may also monitor through the use of covert CCTV but it shall only do so where specific criminal activity has been identified. Before starting any use of covert CCTV the DIM will have made an impact assessment concluding that notifying employee of the use of such covert monitoring would prejudice the investigation and that the use of covert monitoring techniques is a proportionate response to the behavior in question. Where appropriate, (but at its absolute discretion) the DIM may involve the law enforcement authorities in such monitoring.

REFERENCE

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016
THE EU DATA PROTECTION DIRECTIVE 95/46/EC.
THE UK DATA PROTECTION ACT 1998,
UAE FEDERAL LAWS

Approved by

Zulfiker Abdul Hasis

Managing Director

Date: - 10th Jan 2019

****