Context and overview

Introduction

Celebrity International Movers SA needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact. This policy describes how this personal data is collected, handled and stored to meet the company's data protection standards (set out in the company's Data Security & Access Control Policy) and to comply with local and EU data protection and GDPR laws. This policy is reviewed yearly on 1st June by the CQO and the CIO.

Why this policy exists

This data protection policy ensures Celebrity International Movers SA:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Right to choose

Celebrity International Movers SA respects the moral and legal obligation it has to all personal information it may handle. Therefore:

- All individuals have the express right to **opt-out** of Celebrity International Movers SA gathering and/or sharing their personal information with third parties (e.g. vendors, etc.).
- Celebrity International Movers SA never shares any information unless it is mission critical and will never lease, distribute or sell personal information to third parties unless we have express permission or the law requires us to.
- In instances where Celebrity International Movers SA needs to share **sensitive** personal information (such as medical data) it will require the individual to **opt-in** by providing express consent.
- Celebrity International Movers SA will always inform the individual if their choice to optout or not opt-in will hinder the completion of any/all work assigned.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Celebrity International Movers SA

- The warehouse of Celebrity International Movers SA
- All staff and volunteers of Celebrity International Movers SA
- All contractors, suppliers and other people working on behalf of Celebrity International Movers SA

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks

This policy helps to protect Celebrity International Movers SA from some very real data security risks, including:

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

Responsibilities

Everyone who works for or with Celebrity International Movers SA has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data always ensures that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- The **CEO** is ultimately responsible for ensuring that Celebrity International Movers SA meets its legal obligations.
- The **CQO** is responsible for:
  - o Keeping the CEO updated about data protection responsibilities, risks and issues.
  - o Reviewing all data protection procedures and related policies. o Arranging data protection training and advice for the people covered by this policy. o Handling data protection questions from staff and anyone else covered by this policy. o Dealing with requests from individuals to see the data Celebrity International Movers SA holds about them (also called 'subject access requests').
  - o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

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

- The **Marketing Manager** is responsible for:
  - o Approving any data protection statements attached to communications such as emails and letters.
  - o o Addressing any data protection queries from journalists or media outlets like newspapers.
  - o o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

These guidelines are in place to make sure that all staff and partners adhere to the Data Protection Policy properly:

- The only people able to access data covered by this policy are those who **need it for their work**.
- Data **is not shared informally**. When access to confidential information is required, employees request it from their supervisors and third party contractors request from their Celebrity staff contact and are provided with it according to the necessities of the service they are providing
- **Celebrity International Movers SA provides training** to all employees to help them understand their responsibilities when handling data.
- Employees keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords are used,** are never shared and are mandatorily changed every 180 days.
- Personal data **is not disclosed** to unauthorised people, either within the company or externally.
- Data is **regularly reviewed and updated** if it is found to be out of date or if no longer required, it is deleted and disposed of.
- Employees **request help** from their supervisor or the CIO if they are unsure about any aspect of data protection.
- When this policy is sent to third party contractors (as data processors), they agree to our (as data controllers) policies and to be GDPR compliant for all data shared with them by us (past, present or future). Specifically, they agree forthwith as data processors to:

- process 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 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
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- takes all measures required for the security of processing (GDPR Article 32)
- not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor
- take into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights
- assist the controller in ensuring compliance with their obligations pursuant to Security and Prior consultation
- at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data
- make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this policy and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

Data storage

These rules describe how and where data is safely stored. Questions about storing data safely are directed to the CQO. Personal data is stored for no more than 3 years or as long as there is a legal obligation to do so, after which it is destroyed either by shredding (hard copy), deletion (electronic) or anonymised.

When data is **stored on paper,** it is kept in metal filing cabinets inside the secure Head Office of Celebrity International Movers SA (security doors & windows, theft and fire alarm system, 24 hour CCTV surveillance) where unauthorised 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 are kept **in a drawer or filing cabinet**.
- Employees always make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts are destroyed** and disposed of securely when no longer required.

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

- Data is **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is ever **stored on removable media** (like a CD or DVD), these are encrypted and/or kept locked away securely when not being used.
- Data is only stored on **designated drives and servers**, and is only uploaded to **approved GDPR compliant cloud computing services**.
- Servers containing personal data are **sited in a secure location**, away from general office space.
- Data is **backed up frequently**. Those backups are tested regularly, in line with the company's standard backup procedures.
- Directly saving data to mobile devices like is **avoided where possible**. All mobile devices are keycode/password protected, trackable and encrypted.
- All servers and computers containing data are protected by **approved security software and a firewall**.

Data types, usage and disclosure

Celebrity International Movers SA will only gather data relevant to the successful and efficient completion of the services for which it has been hired. This data may include but is not limited to: Name, Address, DOB, Phone number, Email, Passport/ID info, Tax info, etc. This data is used **strictly** for the completion of the job at hand and any other usage is **strictly forbidden** both by company policy and national/international law.

In some instances this data may be passed on to third parties, **strictly** for the completion of the job at hand. These third parties usually include but are not limited to: Customs Brokers, Destination/Origin Agents, Container Transportation Companies, Transport/Machinery Providers, Technicians/Service providers. *Example: a client may request a maid service. In this instance Celebrity will provide the client's name and address so the service provider can complete their duties.*

Data processing steps

Personal data can be received and shared at various stages of a project. These stages and the parties involved can be traced in detail by referring to the project diary. The general outline follows the following structure which can better guide data tracing an retrieval.

Export/Import Projects	**Data shared:**
First Contact	from Agent/Client
Move Booked	from Agent/Client
Instructions to Agent	with Agent
Insurance	with Insurance Carrier
Order to Freight Forwarder	with Shipper
Customs Cleared	with Customs Broker

DSP Projects	**Data shared:**
DSP Booked	from Agent/Client
Instructions to 3rd Party	with 3rd Party

Data use

Personal data is of no value to Celebrity International Movers SA 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 ensure **the screens of their computers are always locked** when left unattended.
- Personal data **is not shared informally**.
- Data is **encrypted before being transferred electronically**.
- Employees **do not save copies of personal data to their own computers.** They always access and update the central copy of any data (server).

Data 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 is held in **as few places as necessary**. Staff do not create any unnecessary additional data sets.
- Staff **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.

- Celebrity International Movers SA makes it **easy for data subjects to update the information** Celebrity International Movers SA holds about them by simply sending a request email to contact@celebrity.gr.
- Data is **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it is removed from the database.
- The Marketing Manager ensures **marketing databases are checked against the suppression list** every six months.

Subject access requests

All individuals who are the subject of personal data held by Celebrity International Movers SA are entitled to:

- Ask **what information** the company 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 company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals are made by email, addressed to the CQO at contact@celebrity.gr. Individuals will be charged **EURO 20** per subject access request. The CQO will aim to provide the relevant data within **14 days**. The CQO always verifies the identity of anyone making a subject access request before handing over any information. If a complaint is received concerning Data Protection, the Complaints & Claims Procedure will be followed by staff to resolve this.

Disclosing data for other reasons

In certain circumstances personal data may be disclosed to law enforcement agencies without the consent of the data subject if Celebrity International Movers SA is legally obliged to do so.

Under these circumstances, Celebrity International Movers SA will disclose requested data. However, the CQO will ensure the request is legitimate, seeking assistance from the CEO and from the company's legal advisers where necessary.

Data Breach Procedure

In the highly unlikely event of a data breach (a breach of security leading to the destruction, loss, alteration or unauthorised disclosure of or access to personal data) or **even the suspicion of one**, the following procedure shall be followed.

1. Immediately inform the PO or, in their absence, the CEO or CIO or CFO, providing the following information
    a. When the breach occurred (time/date)
    b. Description of the breach including type of personal information involved
    c. Cause of the breach and/or how it was discovered
    d. Which systems are affected
    e. What corrective action has been taken to remedy or contain the breach
2. Assess the impact
    a. Is personal data involved
    b. Is the personal data sensitive
    c. What kind of breach has occurred
    d. How many individuals have been affected
    e. Was the data protected and if so how
    f. Who has access now
    g. Could there be a real risk of serious harm (physical or emotional) to the affected individuals
    h. Could there be media attention as a result of the breach
3. Manage the breach
    a. Ensure immediate corrective action is taken, including retrieval or recovery of the data, ceasing the unauthorised access, shutting down or isolating the affected system
    b. Evaluate the risks associated with the breach, including collecting and documenting all evidence of the breach
    c. Consult with the relevant staff in these particular circumstances
    d. Engage an independent cyber security, forensic expert or private detective if appropriate
    e. Make a recommendation to the Privacy Officer whether this breach constitutes a breach under GDPR Art. 4, par. 12 thus requiring a mandatory reporting to the DPA and the practicality of notifying affected individuals
    f. Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media.
    g. submit a report via the Privacy Officer within 48 hours of receiving instructions under containing the following:
        i. Description of breach or suspected breach
        ii. Action taken
        iii. Outcome of action
        iv. Processes that have been implemented to prevent a repeat of the situation.
        v. Recommendation that no further action is necessary

4. Notify all relevant parties and/or authorities where applicable
    - The data processor shall inform the data controller as soon as possible and without delay
    - The data controller shall inform the supervisory authority not later than 72 hours after having become aware of the breach
    - The data controller shall inform the data subjects where needed

Independent complaints body

If for some reason you wish to make a complaint concerning the way we collect, process and/or handle your data and feel that our response has been unsatisfactory, you may at any time turn to the **EUROPEAN DATA PROTECTION SUPERVISOR**. All relevant information can be found at the following link: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en

Providing information

Celebrity International Movers SA 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 company has a Privacy Policy, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]