



INTERNATIONAL REMOVALS, RELOCATIONS & STORAGE

DELAHAYEMOVING

DEMENAGEMENTS INTERNATIONAUX & GARDE-MEUBLES



Data Protection Policy

Version : 2020 05

TABLE OF CONTENT

| | |
|---|---|
| 1. Introduction..... | 3 |
| 2. Objectives..... | 3 |
| 3. Roles and responsibilities..... | 3 |
| 4. General staff guidelines | 4 |
| 5. Data gathering | 4 |
| 6. Data storage..... | 5 |
| 7. Use of Data..... | 5 |
| 8. Data retention..... | 6 |
| 9. Data accuracy | 6 |
| 10. Subject access requests..... | 6 |
| 11. Disclosing data for other reasons | 7 |
| 12. Providing information | 7 |
| 13. Document Control | 7 |

1. Introduction

Delahaye Moving needs to gather and use certain information about individuals, these may include customers, suppliers, business contacts, employees and other people Delahaye Moving has a relationship with or may need to contact.

This policy describes how this personal data must be gathered, handled, and stored to meet Delahaye Moving's data protection standards and to comply with the law. This policy applies to all businesses that trade under the name "Delahaye Moving" and all personnel employed directly or indirectly by these businesses.

This Data Protection Policy ensures Delahaye Moving

- Complies with data protection law and follows best practice
- Protects the rights of its staff, customer, and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of a data breach

The Data Protection Act 1998 describes how organisations, including Delahaye Moving, must collect, handle and store personal information; these rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act 1998 is underpinned by eight important principles, these state that personal data must:

1. Be processed fairly and lawfully
2. Be obtained for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not to be transferred outside the European Economic Area, unless that country or territory also ensures an adequate level of protection

2. Objectives

This policy aims to protect Delahaye Moving from some very real security risks, including of breaches of confidentiality and reputational damage.

3. Roles and responsibilities

Everyone who works directly or indirectly for Delahaye Moving has some responsibility for ensuring data is collected, stored and handled appropriately. Everyone that handles personal data must ensure it is handled and processed in line with this policy and with data protection principles.

While being everyone's responsibility some people have key areas of responsibility:

- The CEO is ultimately responsible for ensuring that Delahaye Moving meets its legal obligations. He is responsible for reviewing data protection issues and to ensure that any issue is adequately resolved. The CEO approves any contract or agreement with any third party that may handle the company's sensitive data.
- The Branch managers are responsible for ensuring compliance in their branch with the current policy and in particular
 - Arrange training as required for their direct and indirect staff
 - Deal with requests from customers to see the data Delahaye Moving holds about them
- The IT management is outsourced with Techxcellent, they are responsible for
 - Ensuring all systems, services, and equipment for storing data meet acceptable security standards
 - Performing regular checks and scans to ensure security hardware and software is functioning properly.

4. General staff guidelines

The following guidelines apply to all staff employed directly or indirectly by Delahaye Moving:

- Access to Delahaye Moving premises is controlled and only authorised people should be in our offices, we refer to our staff handbook for more details.
- The only people to access data covered by this policy should be those who require the access for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Employees must keep all data secure, by taking sensible precautions and following the guidelines below:
 - Employees are to use strong passwords and they should never be shared
 - Private data should not be disclosed to unauthorised people, either within Delahaye Moving 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 manager if they are unsure about any aspect of data protection.

5. Data gathering

Our customers understand that we will need some of their personal information to contact them and to provide our service. We may obtain their personal information directly from them or from our partners.

Because the gathering of our customer's private information is inherently required to the service, we provide it is assumed that we implicitly receive the customer's authorisation to use and share that information as required for the delivery of our services.

Similarly, for employees, by the nature of their employment by Delahaye Moving they are implicitly agreeing with Delahaye Moving storing and using their personal details.

6. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to our IT support, Techxcellent or to the branch managers.

When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed for some reason.

- When not required, all paper and files should be kept in a locked drawer or in a filing cabinet
- When no longer required all papers need to be disposed of in an appropriate way to prevent any unauthorised person to have access to the information.

When data is stored electronically it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts.

- Data should be protected by passwords that are changed regularly and never shared between employees.
- Data should not be stored on removable media like DVD or USB memory stick and these are not to be used to exchange information with any 3rd party.
- Data should be stored on the shared drives and not on the local drive or desktop unless agreed with our IT supplier.
- Data is replicated on live basis amongst servers that communicate in safe and secure way.
- All servers and computers should be adequately protected by security software, firewalls and other measures as required.
- Remote access is to be arranged by our IT supplier who will make sure that all data is adequately protected before such access is being granted.
- Offices located out of the EEA will only have access to the Delahaye Moving IT environment through the “remote” or “virtual” desktop applications.

7. Use of Data

While personal data is of no value to Delahaye Moving but for the execution of its moving and storing activities it is extremely important to Delahaye Moving’s reputation that, when data is being used, it is done so in a safe and secure manner. To protect the customer’s information against the risks of loss, corruption and theft the following guidelines apply:

- When leaving their desks, employees should ensure the screens of their computers are always locked and “auto-lock” after a brief period when left unattended.
- In the process of delivering a service an employee may have to share our customer’s personal details and passport information with an agent based outside of the EEA. Giving the nature of the services provided our customers

provide us implicitly with their agreement for us to share those details with the agent selected to represent Delahaye Moving at origin or destination.

- Data must be encrypted before being transferred electronically.

8. Data retention

Delahaye Moving will archive electronic data on a regular basis, keeping a maximum of three years of moves directly accessible to its employees.

All records will be kept for up to 24 months above the legally required minimum holding period and will be adequately disposed of to ensure confidentiality to the data being maintained till destruction.

9. Data accuracy

The law requires Delahaye Moving to take reasonable steps to ensure our data is kept accurate and up-to-date; the more important it is that the personal data is accurate the greater the effort that Delahaye Moving 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.

Below guidelines will help Delahaye Moving to keep its data up to date:

- Data will be held in as few places as necessary; the company has a move management software which is the single point of data for all customer related information.
- Delahaye Employees should take every opportunity to ensure data is updated.
- Data should be updated as inaccuracies are discovered.

10. Subject access requests

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

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

If an individual contact the company requesting the above information, this is called a subject access request.

Subject access requests from customers should be made by an email to the Delahaye Moving Branch manager where the individual has a relationship with or to the CEO. The Delahaye Moving CEO and Branch Managers will always verify the identity of anyone making a subject access request before handing over any information. All other subject access requests are to be directed to the CEO.

11. Disclosing data for other reasons

In certain circumstances the law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under such circumstances Delahaye Moving will disclose the requested data however, before doing so, Delahaye Moving will ensure the request is legitimate, seeking external legal advice where necessary.

12. Providing information

Delahaye Moving aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used. For this purpose, Delahaye Moving employees will explain to our customers why certain personal data above standard contact details are required to allow Delahaye Moving to provide its services.

Customers will receive upon simple request a copy of the current Delahaye Moving Data Protection Policy.

13. Document Control

The present policy will be reviewed and updated at least annually. Below table will help Delahaye Moving to keep track of changes made.

| Version Control | | | |
|-----------------|-------------|---------------------------|---------------|
| Version | Author | Date | Changes made |
| 2017 02 | J-C Maerten | 15 February 2017 | New draft |
| 2018 05 | J-C Maerten | 2 nd May 2018 | No changes |
| 2019 05 | J-C Maerten | 14 th May 2019 | No changes |
| 2020 05 | J-C Maerten | 06 May 2020 | Minor updates |