HARD HAT
logistics ltd

POLICY

GDPR
COMPLIANCE STATEMENT & POLICY

Context and overview

At Hard Hat Logistics Ltd, we are committed to our obligations for GDPR compliance on two fronts: our responsibilities as an organisation that processes personal data; our role as a data processor on behalf of our clients.

Hard Hat Logistics Ltd needs to gather and use certain information about individuals through the normal course of business. Hard Hat Logistics Ltd will process individual data subject's information on behalf of our clients. We take the personal and commercial sensitivity of this data very seriously and have processes in place to ensure that data is safe and secure in our care. This includes (but not limited to) data used for operations and project planning, data for processing employees and data used through the provision of support.

These can include customers, suppliers, business contacts, employees and other people the organisation 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 GDPR legal requirements — and to comply with the law.

Why this policy exists

This data protection policy ensures Hard Hat Logistics Ltd

- Complies with data protection law and follows 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

Data Protection Law

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully, it must also not be retained without good cause.

The law is underpinned by important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

The above applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR requirements. This can include, but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photographs
- Personal files, copies of personal documentation

Data Protection Risks

This policy helps to protect (Company Name) and its clients from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Hard Hat Logistics Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

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

The Managing Director is ultimately responsible for ensuring that Hard Hat Logistics Ltd meets its legal obligations. These are:

- Being aware of 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 staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Hard Hat Logistics Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The IT manager is responsible for:

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

The Sales manager is responsible for:

- Approving any statements attached to communications such as emails and letters.
- Addressing any queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by sound principles.

General Staff 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.
- Hard Hat Logistics Ltd 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 unauthorised people, either within the company or externally unless specifically authorised.
- 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 if they are unsure about any aspect of data protection.

Data Storage

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 out for some reason:

- When not in use, 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 unauthorised 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 unauthorised 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 company's standard backup procedures.
- 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 Hard Hat Logistics Ltd 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. 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 authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- 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 Hard Hat Logistics Ltd 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 Hard Hat Logistics Ltd 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. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Hard Hat Logistics Ltd will make it easy for data subjects to update the information Hard Hat Logistics Ltd holds about them. For instance, via the company 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.

Subject Access Requests

All individuals who are the subject of personal data held by Hard Hat Logistics Ltd 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 should be made by email, addressed to the data controller. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for the subject access request. The data controller will aim to provide the relevant data within 30 days.

The data controller 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, Hard Hat Logistics Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing Information

Hard Hat Logistics Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand: days

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

Encrypted restorable backups are made at regular intervals. Hard Hat Logistics Ltd has a business continuity plan in the event of a total loss of the data.

Hard Hat Logistics Ltd does not share clients' data with any third parties without our client's express instruction. Any such data transfer between organisations will always be in accordance with GDPR standards and our own documented processes.

In the event of a data breach, Hard Hat Logistics Ltd has processes in place to report a data breach to our clients and where necessary, the ICO within 72 hours of discovering the breach. Our priority will be to restrict the risk and minimize the impact on the individuals and organisations concerned. Responsibility for a breach will be determined once the circumstances are understood.

Signed.....

Ross Ferguson

Managing Director

Date: 01/04/2019