| REF: | AP_HR_0034 | ISSUE | 001 | ISSUE DATE | Mar 2018 | PAGE | 1 OF 5 |
|---|---|---|---|---|---|---|---|
| AREA: | HR | ***General Data Protection Regulation (GDPR)*** | | | | | |
| DOC: | Policy | | | | | | |

**Introduction**
This policy describes how personal data must be collected, handled and stored to meet the company's data protection standards – and comply with the law. Primeline needs to gather and use certain information collated about individuals including customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

The General Data Protection Regulation (GDPR) was ratified by the European Union during April 2016 and has now become law. This means that companies such as Primeline will be expected to be fully compliant from May 25th 2018.

**Why this policy exists**
This GDPR policy ensures Primeline:

- 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 individual's data
- Protects itself from the risks of a data breach

**General Data Protection Regulation (GDPR)**
The GDPR describes how organisations – including Primeline – 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 regulation, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by seven important principles which are set out below.

1. Transparency – Data processing should be lawful, fair and done in a transparent manner.
2. Purpose Limitation – The collection of data should only be for a specified, explicit and legitimate purpose. Processing should not be incompatible with that specific purpose.
3. Data Minimisation – Processing of data should be limited to only what is necessary to achieve the purpose.
4. Accuracy – Inaccurate or incorrect personal data should be corrected or deleted as soon as possible.
5. Storage Limitation – Data should only be held in a form that allows identification of the individual for as short a time as possible. Following this time it should then be anonymised or erased.
6. Integrity and Confidentiality – The security and integrity of the data should be protected via both technological and organisational structures.
7. Accountability – The Data Controller must be able to actively demonstrate compliance with the Regulation.

**People, Risks and Responsibilities**
**Policy Scope**
This policy applies to:

- The head office of Primeline Group (Units 3, 9 & 12)

- All branches of Primeline Group, including Primeline Logistics, Primeline Sales & Marketing ROI & UK, Primeline Express (ROI and NI), Primeline VNE
- All staff and volunteers of Primeline
- All contractors, suppliers and other people working on behalf of Primeline

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

**Data Protection Risks**
This policy helps to protect Primeline 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 company uses data relating to them.
- **Reputational Damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

**Responsibilities**
Everyone who works for or with Primeline 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, the following people have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that Primeline meets its legal obligations.
- The Data Protection Officer within HR is 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 staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Primeline 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.

- 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.

**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.
- Primeline **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.
- 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 Group HR manager.

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 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 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.

- 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 Primeline 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 authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area** (EEA).
- 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 Primeline 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 Primeline will put into ensuring its accuracy.

It is the responsibility of all employees who work with the 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.
- Primeline will make it **easy for data subjects to update the information** Primeline holds about them. For instance, via the self-service tool in the HRIS.
- 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 Primeline 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 protection officer.

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 GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Primeline will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the Board and from the company's legal advisers where necessary.

**Providing Information**
Primeline aims to ensure that individuals are aware that their data is being processed, and that they understand:

- The identity and contact details of the organisation behind the data request
- The purpose of acquiring the data and how it will be used
- Whether the data will be transferred internationally
- The period for which the data will be stored
- Their right to access, rectify or erase the data
- Their right to withdraw consent at any time
- Their right to lodge a complaint

**Rules for Enforcement of GDPR**
**For managers**
An employee must provide consent for personal data to be disclosed to you, their manager. An 'Access Request Form' must be completed in full, identifying what information is requested and why. This form must then be signed by the employee. No employee personal data will be disclosed to you or any member of the management team without receipt of this form.