Data Protection & Privacy Essentials

A Quick Guide for Staff – Provided by Alpha IT Solutions

Introduction: Our Legal & Ethical Duty

Organisations in Ireland are legally required to protect personal and sensitive data under the **GDPR** and the **Data Protection Act 2018**. Strong security and clear privacy practices are essential to maintain the trust of our clients and partners.

1. Understanding Sensitive Data

Not all data is equal. Certain categories require enhanced protection:

- **Personally Identifiable Information (PII):** Names, addresses, email addresses, and PPS numbers.
- **Special Categories (GDPR Article 9):** Health data, biometric data, racial/ethnic origin, and religious beliefs.
- **Financial & Health Info:** Bank details, transaction histories, and medical records.
- **Business Confidentiality:** Strategic plans, trade secrets, and customer lists.

2. Core Data Protection Principles

Every employee must adhere to these fundamental GDPR principles:

- **Lawfulness & Transparency:** Data must be processed fairly and explained clearly in privacy notices.
- **Purpose Limitation:** Use data only for the specific, legitimate purpose for which it was collected.
- **Data Minimisation:** Collect only the information that is absolutely necessary.
- **Accuracy:** Ensure records are kept up to date; rectify or erase inaccuracies promptly.
- **Storage Limitation:** Retain data only for as long as needed, adhering to documented retention schedules.
- **Integrity & Confidentiality:** Protect data against unauthorised access or accidental loss using strong technical measures.

3. Practical Steps for Daily Safety

- **Access Control:** Follow the 'principle of least privilege'—only access data you need for your specific role. Always use strong passwords and **MFA**.
- **Secure Disposal:** Shred physical documents and use certified wiping tools for digital data. Never put sensitive documents in a general waste bin.
- **Encryption:** Ensure sensitive data is encrypted both when stored (at rest) and when sent (in transit).
- **Report Breaches Fast:** If you suspect a data breach, report it immediately. The organisation may be legally required to notify the **Data Protection Commission (DPC)** within **72 hours**.
- **Regular Training:** Stay updated on GDPR obligations and learn to recognise social engineering attempts.

"Data protection is not a one-off task—it is an ongoing commitment to vigilance."

For technical assistance or to report a suspected breach, contact the Alpha IT Solutions team.

Call: +353 (0)23 881 0061 | **Email:** support@alphait.ie

Scan Me