DATA SECURITY POLICY

Document Control History

Title	**Data Security Policy**
Version no.	1.0
Date of publication	May 2018
Author(s)	Stephen Lynas, Business Development Director
Next review date	May 2021

Introduction

Hadden Group is committed to a policy of protecting the rights and privacy of individuals, our workforce and others on how it collects and uses the personal data of its workforce, and to meeting its data security obligations in accordance with the General Data Protection Regulation (GDPR) May 2018. This policy sets out the Hadden Group's commitment to data security protection.

The new regulatory environment demands higher transparency and accountability in how we manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) we will ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all Hadden Group Staff. Any breach of this policy or of the Regulation itself will be considered an offence and disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with Hadden Group and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

1. Data protection principles

Hadden Group processes personal data in accordance with the following data protection principles:

- Hadden Group processes personal data lawfully, fairly and in a transparent manner.
- Hadden Group collects personal data only for specified, explicit and legitimate purposes.
- Hadden Group processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Hadden Group keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Hadden Group keeps personal data only for the period necessary for processing.
- Hadden Group adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

Hadden Group will ensure that all personal data is accessible only to those who have a valid reason for using it.

We have in place appropriate security measures including:

- ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

  password protecting personal data held electronically. Strong passwords must be used and should never be shared

- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.
- Ensuring all systems, service & 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 so that they are fit for purpose. For example: cloud computing services or project management portals
- Employees should make sure paper and printouts containing data are not left where unauthorised people could see them. For example: on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- Data stored electronically must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- If data is stored on removable media e.g USB Stick or CD these should be kept locked away securely when not in use.
- Data should only be stored on designated drives and servers and should only be uploaded to 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 back-ups should be tested regularly in line with company IT back-up protocols
- 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
- Personal data should not be shared informally. In particular, it should never be sent un-encrypted by email
- Data must be encrypted before being transferred electronically

- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data

In addition, Hadden Group will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically.

This policy also applies to staff who process personal data 'off-site', e.g. when working at home or on construction sites, and in these circumstances additional care must be taken regarding the security of the data.

2. Data security

Hadden Group takes the security of personal data seriously. Hadden Group has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where Hadden Group engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

3. Data breaches

If Hadden Group discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Hadden Group will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

4. International data transfers

Hadden Group will not transfer HR-related personal data to countries outside the EEA.

5. Individual responsibilities

Individuals are responsible for helping Hadden Group keep their personal data up to date. Individuals should let Hadden Group know if data provided to Hadden Group changes, for example if an individual moves to a new house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, Hadden Group relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to only access data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

6. Training

Hadden Group will provide training to all individuals about their data security responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.