TEMPLATE
GENERAL DATA PROTECTION POLICY

Table of Contents

POLICY STATEMENT

The General Data Protection legislation is in place to ensure that any personal information gathered and held by any business/company is collected correctly and only used for the purpose specified when collected. During the course of any company / business activity they may collect, store and process personal information about staff, clients and service providers, the company / business recognises the need to treat this data in an appropriate and lawful manner. The company/business is committed to complying with its obligations in this regard in respect of all personal data it handles.

The types of information that this company may be required to handle include:

Details of current, past and prospective employees, suppliers and customers / clients / owners.

PURPOSE OF THE POLICY

This policy sets out the company / business rules on data protection that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal and sensitive information and what procedures and protocols are in place in the event of a security breach.

If an employee considers that the policy has not been followed in respect of personal data about themselves or others they should raise the matter with their manager as soon as possible.

DEFINITION OF DATA PROTECTION TERMS

DATA is information that is stored electronically, on a computer, or in a certain paper-based filing system. This would include IT systems and CCTV systems.

DATA SUBJECTS for the purpose of this policy include all living individuals about whom the Company / Business holds personal data.

PERSONAL DATA means data relating to a living individual who can be identified from the data (or from that data and other information that is in, or is likely to come into, the possession of the data controller). Personal data can be factual (such as name, address or date of birth) or it can be opinion (such as a performance appraisal).

DATA CONTROLLERS are the individual or organisations who control and are responsible for the keeping and use of data.

DATA USERS include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the Company's / Business data protection and security policies at all times.

PROCESSING means performing any operation or set of operations on data, including:

- Obtaining, recording or keeping data
- Collecting, organising, storing, altering or adapting the data
- Retrieving, consulting or using the data
- Disclosing the information or data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the data

SENSITIVE PERSONAL DATA includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition or sexual life, criminal convictions or the alleged commission of an offense. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight principles of good practice.

These provide that personal data must be:

1. Obtained and processed fairly
2. Kept only for one or more specified, explicit and lawful purposes
3. Used and disclosed only in ways compatible with these purposes
4. Kept safe and secure
5. Kept accurate complete and up to date
6. Adequate, relevant and not excessive
7. Retained for no longer than is necessary for the purpose or purposes for which it was collected
8. Provided to data subjects on request

1. OBTAINED AND PROCESSED FAIRLY

The data subject must be told who the data controller is (business owner / secretary / Human resource manager / accountant etc) the purpose for which the data is to be processed by the company, and the identities of anyone whom the data may be disclosed or transferred. In most cases the data subject's explicit consent to the processing of such data will be required (see Appendix 1 & 2).

2. KEPT FOR ONLY SPECIFIED, EXPLICIT & LAWFUL PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Acts. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which data is processed, the data subject must be informed of the new purpose before any processing occurs. Any employee personal data collected by the company is used for ordinary Human Recourse purposes. Where there is a need to collect employee data for another purpose, the company/business will notify the employee of this and where it is appropriate will get employee consent to such processing.

3. KEPT SAFE AND SECURE

The company/business and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, an against the accidental loss of, or damage to, personal data.

Personal data may only be transferred to a third-party data processor if the third party has agreed to comply with those procedures and policies or has adequate security measures in place.

The following must be maintained to ensure the following:

Confidentiality: that only people who are authorised to use the data can access it. The company/business will ensure that only authorised persons have access to an employee's personnel file and any other personal or sensitive data held by the Company/business. Employees, Human resource managers and payroll administrators are required to maintain the confidentiality of any data to which they have access.

Integrity: that the personal data is accurate and suitable for the purpose for which it is processed.

Availability: that authorised users should be able to access the data if they need it for authorised purposes.

SECURITY PROCEDURES INCLUDE:

Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).

Methods of disposal: Paper documents should be shredded. USB sticks should be physically destroyed if they are no longer needed.

Equipment: Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

CLOUD STORAGE OF PERSONAL DATA

FIVE STEPS TO SECURE CLOUD-BASED ENVIRONMENTS

Cloud-Based environments offer many advantages to organisations. However, they also introduce a number of technical security risks which organisations should be aware of such as:

- Data breaches
- Hijacking of accounts
- Unauthorised access to personal data

Organisations should determine and implement a documented policy and apply the appropriate technical security and organisational measures to secure their Cloud-Based environments. If organisations do not implement such controls, they may increase their risk of a personal data breach[1].

Organisations should apply technical security and organisational security measures in a layered manner consisting of but not limited to:

- Access controls
- Firewalls
- Antivirus
- Staff training
- Policy development.

A layered approach to Cloud-Based security mitigates the risk of a single security measure failing which may result in a personal data breach.

Many Cloud-Based providers, such as Microsoft's Office 365 and Google's G-suite provide advanced settings and solutions which can assist organisations to appropriately secure their use of Cloud-Based services. These providers, in most cases, also offer best practice guidance to assist organisations in securing their Cloud-Based environments.

Additional information, advice, and best practice regarding security of Cloud-Based environments is also provided by agencies such as the European Union Agency for Network and Information Security ("**ENISA"**) https://www.enisa.europa.eu/, and the US-based National Institute of Standards and Technology (**"NIST"**) https://www.nist.gov/topics/information-technology.

The DPC has listed five key ways organisations can secure their Cloud-Based environments to mitigate their risk of a personal data breach.

1. Access control and authentication

Organisations should implement strong password polices to ensure that users accessing personal data within Cloud-Based environments do so in a secure manner.

Organisations should implement two-factor authentication. Two-factor authentication is an effective way to further enhance Cloud-Based security and is available from most Cloud-Based providers.

Organisations should be aware of and document user access privileges within their Cloud-Based environments. User access control is particularly important where group mailboxes or shared folders are utilised. Organisations should also document each user's specific access requirements and ensure that these are supported by an appropriate change control process.

Security measures applied by an organisation must be supported by regular reviews of user access to ensure that all authorised access to personal data is strictly necessary and justifiable for the performance of a specific function.

2. Review default security settings

Organisations should **not** rely on Cloud-Based service providers' default security settings. Organisations should review the Cloud-Based security features available from the Cloud-Based service provider to ensure that they are applied appropriately and in a layered manner. Examples of security settings and controls provided by Cloud-Based service providers often include:

- Centralised administration tools
- Mobile device management
- Multifactor authentication
- Login alerts
- Encryption during message send and receive
- Encryption of message content
- Account activity monitoring and alerts
- Data loss prevention
- Malware protection
- Spam and spoofing protection
- Phishing protection

Organisations should also be aware that Cloud-Based services might be publicly accessible and organisations should review and implement the appropriate security settings to secure remote access.

3. Seek assurances from your ICT service provider

Organisations may utilise external ICT services providers to implement their Cloud-Based environments. It is vital during such engagements that organisations seek formal assurances from their ICT service provider that the security controls which have been implemented meet an organisation's specific security requirements and protect the organisation's personal data.

Organisations should proactively engage and conduct regular security reviews with their ICT service providers to ensure the security controls in place are up-to-date and are effective to protect the organisation in an evolving threat landscape.

4. Clear Policies and staff training.

Organisations should ensure that staff receive appropriate training on social engineering attacks, phishing attacks and security threat practices. Such training should be supported by refresher training/awareness programmes to mitigate the risk posed by an evolving threat landscape.

Organisations should have clear policies in place with respect to the usage and security of Cloud-Based services, especially where these services are being accessed outside of the organisation corporate network under Bring Your Own Device ("BYOD") policies.

Organisations should have clear "employee leaver" and "succession" policies in place and these should be applied to an organisations Cloud-Based environment.

Organisations should have a clear policy in place for data retention and conduct regular reviews to ensure that personal data is not retained longer than necessary or where the original purpose for the use of the personal data has ceased.

5. Know your data and secure it

Organisations should understand and monitor the types of data that is stored in their Cloud-Based environments. Knowing the types of data stored in the Cloud enables an organisation to ensure the appropriate security and access controls are applied to protect the data.

Organisations should utilise data classification methods to identify the data which they store and process within Cloud-Based environments. The process of data classification enables an organisation to categorise their stored data in order to determine the appropriate security controls.

Organisations should carefully evaluate Cloud-Based vendors based on the security features they offer and how they specifically meet with their organisational requirements.

Who has access to your data, how is it secured, how often is the data backed up and if the Cloud-Based environment aligns to your organisational policies are all vital questions to ask of both your Cloud-Based service provider and / or the ICT service provider charged with implementing your environment.

Applying the appropriate security measures is not a once off "Set and forget" exercise. Cloud-Based security settings should be reviewed on a regular basis to ensure that they are still appropriate and up-to-date.

4. ACCURATE AND COMPLETE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out of date data should be destroyed. Employees should ensure that they notify their manager of any relevant changes to their personal information so that it can be updated and maintained accurately. Example of changes to data would be a change of address.

5. TIMELY PROCESSING

Personal data should not be kept longer than necessary for the purpose. In compliance with the General Data Protection Regulation and other regulations (e.g. WRC) the data is retained for the following periods of time:

Documentation	Min. Period to be retained	Notes
List of Employees	Current	WRC may request to see a list of all Employee including full names, address and PPS numbers
Commencement/Termination Dates	Current	Dates of commencement and dates of termination of Employees
Written Terms of Employment /Contract (including Boarding Contracts)	Current and for 1 year after termination	Employer must retain a copy of this statement throughout the Employee's employment and for one year after termination. Stud must retain a copy of the Client Contract for one year after departure of horse.
Young Persons (Under 18)	3 years	Need to retain records for 3 years to demonstrate that Employer has complied with Protection of Young Persons (Employment) Act 1996.

Employment Permits	5 years	Records on employment permits for Non-EEA nationals must be retained for 5 years or for the duration of the employment.
Parental Leave Records	8 years	Records of Parental Leave taken must be retained for 8 years. Copies of notices required under the Parental Leave Acts 1998 and 2006 must be retained for 3 years.
Force Majeure Leave Records	8 years	Records of Force Majeure Leave taken must be retained for 8 years.

6. PROCESSING IN LINE WITH DATA SUBJECTS RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

7. DEALING WITH SUBJECTS ACCESS REQUESTS

A formal request from a data subject for information that the company/business holds about them must be made in writing. Data subjects should be provided their data in accordance with any such request within 40 days of retrieving the request.

8. PROVIDING INFORMATION OVER THE TELEPHONE

Any data controller or employee who is dealing with telephone enquiries should be very careful about disclosing any personal information held by the business / company over the phone. In particular the data controller should:

1. Check the identity of the caller to ensure that information is only given to a person who is entitled to that information.
2. Suggest that the caller put their request in writing if the data controller is not sure about the identity of the caller and in circumstances here the identity of the caller cannot be identified.
3. Refer the request to their manager for assistance in difficult situations. No employee/data controller should feel forced into disclosing personal information.

SECURITY BREACH PROCEDURE

PERSONAL DATA SECURITY BREACH CODE OF PRACTICE

[Approved by the Data Protection Commissioner under Section 13 (2) (b) of the Data Protection Acts, 1988 and 2003]

1. The Data Protection Acts 1988 and 2003 impose obligations on data controllers [1] to process personal data entrusted to them in a manner that respects the rights of data subjects to have their data processed fairly (Section 2(1)).Data controllers are under a specific obligation to take appropriate measures to protect the security of such data (Section 2(1)(d)).This Code of Practice does not apply to providers of publicly available electronic communications networks or services.[2]

2. This Code of Practice addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. The focus of the Office of the Data Protection Commissioner in such cases is on the rights of the affected data subjects in relation to the processing of their personal data.

3. Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller must give immediate consideration to informing those affected.[3] Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

4. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the data controller may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures(such as encryption) were of a high standard.

5. 5.All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident.

6. All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial nature.[4] In case of doubt- in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner.

7. Data controllers reporting to the Office of the Data Protection Commissioner in accordance with this Code should make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data. The Office of the Data Protection Commissioner will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

8. Should the Office of the Data Protection Commissioner request a data controller to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

    - a chronology of the events leading up to the loss of control of the personal data;

- the amount and nature of the personal data that has been compromised;
  the action being taken to secure and / or recover the personal data that has been compromised;

- the action being taken to inform those affected by the incident or reasons for the decision not to do so; the action being taken to limit damage or distress to those affected by the incident; and

- the measures being taken to prevent repetition of the incident.

9. Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where a data controller has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

10. Even where there is no notification of the Office of the Data Protection Commissioner, the data controller should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records should be provided to the Office of the Data Protection Commissioner upon request.

11. This Code of Practice applies to all categories of data controllers and data processors to which the Data Protection Acts 1988 and 2003 apply.

REVIEW OF POLICY

The business/company will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account changes in law and organisational or security changes.

Appendix 1

EMPLOYEE INFORMATION

Name _____ whose contact details are as follows:

Address ……..

……..

……

Phone number ……

Emergency contact name & number ……

Email address ……

Commencement date of employment ……

Date of Birth ……

PPS No. ……

Medical conditions ……

☐ In accordance to the General Data Protection Regulations 2018 and the Stud's Data Protection Policy you are required to [√] tick this box **IF YOU CONSENT** to your information being held by the Trainer / Trainer's personnel and used for correspondence from the Trainer / Trainer's personnel only in relation to your employment.

☐ You are required to [√] tick this box **IF YOU CONSENT** to your information being given by the Trainer to other persons for employment purposes, i.e. Revenue, Accountant and Payroll outsourcing.

SIGNED for and on behalf of the Trainer ……

SIGNED for and on behalf of the Employee ……

Date ……

Appendix 2

OWNER AND BOARDING AGREEMENT

THIS AGREEMENT is dated _____ **AND MADE BETWEEN**

(1) **_____** of_____ **('the trainer');** and

(2) **_____** **('the Owner')** whose contact details are as follows:

Address ……..

……..

Invoicing address ……

(if different) ……

……

Phone number ……

Emergency contact number ……..

Email address ……

Equine Premises No. …… (for compliance with Dept. of Agriculture records)

☐ In accordance to the General Data Protection Regulations 2018 and the Stud's Data Protection Policy you are required to [√] tick this box **IF YOU CONSENT** to your information being held by the Trainer and used for correspondence from the Trainer and the Trainers' personnel only.

☐ In accordance to the General Data Protection Regulations 2018 you are required to [√] tick this box **IF YOU CONSENT** to your information being given by the Trainer / Trainer's personnel to other persons for billing purposes, i.e. Veterinary Practice, Farrier, Equine Hospital, HRI and / or Weatherbys.

SIGNED for and on behalf of the Trainer ……

SIGNED for and on behalf of the Owner ……

Date ……