This document is not intended to be a GDPR tutorial, nor provide advice or recommendation; it is information for organisations to consider.

WHAT?

The General Data Protection Regulation (GDPR) is a European Union regulation scheduled to go into effect on 25 May 2018.

GDPR aims to standardise and strengthen data protection policies for residents of EU member nations. It replaces the prior Data Protection Directive (95/46/EC) of 1995 and will apply immediately on the enforcement date. This means that it applies immediately, in every Member State, from that date.

The term 'data' refers to any personal information you store. This includes staff, volunteers, suppliers, customers and anyone else related to your business or organisation, or who receive its function or service. If you have employees, then you will hold their contact and bank details – that's data. Staff performance reviews, attendance records, volunteer names and addresses, lists of people you've helped or want to contact - it's all data and it all counts!

Ignoring the requirements of GDPR legislation risks a fine of up to £20 million or 4% of your annual turnover – whichever is the greater.

WHO DOES THIS AFFECT?

Everyone.

GDPR applies to all organisations. There is a misconception that if organisations are small, or volunteer based or only have paper records, they are exempt. This is not true. No data controller or data processor is exempt.

You must be careful not to mistake **business conducted from home** for **household activity**. GDPR does not apply to people using personal data in the course of **exclusively** personal or household activity. For clarity: if you hold personal details that you use in relation to any activities (paid for or free of charge) that form part of your business or on behalf of The British Horse Society, then you must comply with GDPR legislation.

WHAT DO I NEED TO KNOW?

The data you hold belongs to the data subject (the person) and that data subject has the **absolute right** to say what happens to their information - and seek compensation if it is wrongly used or used without proper explicit consent.

GDPR applies to all personal data that you currently hold. It does not just apply to data collected after May 2018.

What Do I Need To Do?

Here are some of the things you need to do immediately:

- Create a register of the personal information you hold, where it came from and who you share it with
- Review your current **Privacy Notice** & ensure it is GDPR compliant
- Decide and document the **Lawful Basis** your organisation has for holding and processing each individual piece of personal data
- Get consent to store, manage, use and maintain personal data, where appropriate
- Check that you can respond to a 'Subject Access Request' – where someone asks for a copy of their data. You MUST be able to provide this to them in a secure, standard format.
- If you are asked to remove data or consent, do it, and make sure you can prove that you've done so
- Have a process and plan for dealing with data breaches – in case you lose data or someone steals it
- Consider nominating someone within your organisation as a Data Protection Officer

Here are just two ways in which you can be financially and reputationally exposed:

1. Breaching the requirements of GDPR such that the Information Commissioner imposes a fine and terms. Fines are up to £20 million or 4% of gross global turnover – whichever is greater.

2. That you are pursued by an individual data subject (horse owner/parent etc) because they allege you have used their data in a way which has no legal basis or which they have not consented to. We mention this because of the unique PPI claims culture in the UK, which is drawing to an end. The PPI lawyers have now identified GDPR as the next opportunity to make money by pursuing individuals' rights and because of the low awareness of charities and small organisations of their obligations in law, they could be highly vulnerable to being targeted. The cost of meeting any compensation claims could be enough to see many organisations out of business, so the time to act is now.

What Is The British Horse Society Doing?

The BHS is currently working towards compliance and is making changes to its policies, procedures and systems. We will be offering data protection training to all staff before 25th May and we will also make information and on-line training available to volunteers and associates. More details will follow.

DEFINITIONS

DATA CONTROLLER

A **Data Controller** is a person or organisation who determines the purposes for which, and the manner in which, any personal data is processed.

EXAMPLE: The British Horse Society is a Data Controller because it holds information about staff, volunteers, members and individuals who are part of its education programme. It uses this information to run the organisation and provide the services offered by the Charity.

DATA PROCESSOR

A **Data Processor** is a person or organisation which carries out the act of processing data on behalf of the **Data Controller**.

EXAMPLE: The British Horse Society uses an external organisation to send out magazines to its members. This organisation is a Data Processor.

LAWFUL BASIS

Lawfulness, transparency, and fairness are the key ingredients to the first principle of data processing in the General Data Protection Regulation (GDPR). This means that you must have legitimate grounds for collecting and using personal data. Other than Consent, all other lawful bases for data processing require the processing to be **necessary**. This means that organisations should only be collecting and processing information for a specific purpose.

The GDPR legislation sets out 6 possible options for Lawful Basis. These are:

Consent	Legitimate Interest
Public Task	Legal Obligation
Contract	Vital Interest

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

EXAMPLE: The British Horse Society sends magazines to its members. The lawful basis of this is **Contract**, because the member expects to receive the magazine as part of their membership benefit and could not receive it without his/her personal data (name, address) being used.

EXAMPLE: The British Horse Society sends salary details about its employees to HMRC. The lawful basis of this is **Legal Obligation**: it must do this to comply with tax laws.

EXAMPLE: The British Horse Society keeps details about individuals who have attended a fun ride, with the intention of using some of the names and photographs taken on the day to promote other upcoming rides. The lawful basis for this is **Consent**, because The BHS has contacted each individual and obtained specific consent from them to hold their information for this purpose.

PRIVACY NOTICE/PRIVACY POLICY

A privacy notice is externally facing (usually it is displayed on an organisation's website), telling customers, regulators and other stakeholders what the organisation does with personal information & why.

A privacy policy is a statement that discloses some or all of the ways an organisation gathers, uses, discloses, and manages personal information. A privacy policy is internally focused, telling employees what they may do with personal information.

If you/your organisation has not done so already, visit the ICO website (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) for information and advice. It contains all the information you need to understand what is happening, quite how different GDPR is from the existing Data Protection Act (DPA) and how important it is that you do not inadvertently fall foul of its increased powers.