Thoroughbred Breeders' Association Employment Law Fact Sheet No. 23

General Data Protection Regulations ('GDPR'): what employers need to know

GDPR takes effect from 25 May 2018 – this is regulation said to be in order to 'strengthen and unify' data protection within EU and replaces the Data Protection Act. The UK Government has committed to the regulations despite leaving the EU.

As under the Data Protection Act, it applies whenever a "data controller" "processes" "personal data".

Personal data is information, relating to a living individual (human being) who can be identified directly or indirectly from that data. For example, information about an employee's salary and bank account details, an email about an incident involving a named worker.

Data is information processed automatically by equipment (e.g. information held on a computer or recorded by a CCTV camera) or information that forms part of a relevant (organised and structured) filing system.

A data controller is anyone who determines the purposes for which, and the manner in which, any personal data is, or is likely to be processed (for example, an employer).

A data processor is a person who processes the data on behalf of the data controller. Processing covers any use of personal data, from collecting the data, storing it, sharing it and using it to destroying it.

A data controller must:

- Notify the Information Commissioner of their identity and provide details of the purposes for which personal data is to be processed. There is a fee to pay. The process can be started by telephone call to the Notification Helpline on 01625 545740 or by visiting www.ico.org.uk

- comply with general principles of the legislation including requirements that the data must be:

    - Fairly and lawfully processed
    - Collected for specified and legitimate purposes
    - Limited to what is necessary
    - Accurate, up to date, held for the purposes they are kept for
    - Data kept for no longer than necessary
    - Processed with appropriate security
    - Must be able to demonstrate compliance

- Must identify the 'lawful basis' for processing and set this out in a privacy notice. Normally in the case of an employee an employer will say that it is necessary for the purposes of legitimate interests (e.g. for the purposes of the payment of salary or administration of benefits).

- If consent is relied upon it must be freely given, specific, informed and unambiguous and separate from other terms and conditions. It must be simple to withdraw consent.

- Meet special additional requirements when dealing with sensitive personal data (personal data consisting of information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health and sexual life, criminal records).

- Provide the data subject with information about the purposes of processing. This information can be given in a privacy notice, application forms or terms and conditions and must include information such as the identity of the data controller, the purposes for which the data is to be processed.

- put in place adequate security measures to safeguard personal data from destruction, loss, unauthorised access or disclosure.

- The new accountability principle requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility. You may be required to document more information than you previously had done and appoint a Data Protection Officer.

A data processor must:-

- Process personal data in accordance with the controller's instructions.
- Be governed by a contract with regard to the controller. The binding obligations on the processor must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the controller.
- Maintain a record of all categories of processing activities.
- Implement appropriate security measures.
- Notify their relevant controller of any breach without undue delay after becoming aware of it.

Data subjects may:

- access the data held by making a request in writing – usually there is no fee for this
- prevent processing which is likely to cause damage or distress
- take action for compensation and to rectify, block, erase or destroy inaccurate data

What information must be included in an employee privacy notice?

The mandatory information "types" that must be set out in a Privacy Notice include:

- The identity and contact details of the employer;
- A description of the personal data that is collected;
- The purposes for processing the data;
- The legal basis on which the processing will take place;
- Who the personal data is shared with;
- Whether personal data is transferred outside of the EEA and if so, details of the safeguards that are in place to protect the security of the data;
- How long the personal data will be kept for; and
- Details about the rights that employees have in relation to that personal data, for example the right to request that the employer rectify any incorrect information

The Privacy Notice must be "meaningful". Essentially this means that it must be tailored to reflect the structure of the employer's business, the types of personal data that the employer processes and the nature of the processing (amongst other things). As such, whilst a template privacy notice is a useful starting point for an employer, it will only become a purposeful document, when it is specifically tailored to reflect the relevant processing of employees' personal data within the organisation.

Non-compliance

Under GDPR, action can be taken against both a data controller and a data processor. The ICO may choose to take action against both data controller and data processor if it believes both have played a role in breaching the legislation.

The fines are significant and much more than under the previous legislation - the ICO can impose up fines of up to 20 million Euros or 4% of group worldwide turnover (whichever is greater) against both data controllers and data processors.

In addition to the imposition of fines, the ICO may choose to conduct audits, review certifications, issue warnings and reprimands to controllers and processors that have breach GDPR and impose limitations and restrictions around the breaching party's ability to process data. Reputational damage could also be significant.

Recruitment issues

- Explain on adverts/application forms what applicants' data will be used for and if it will be transferred to third parties
- Only seek relevant information: only seek information on criminal convictions if this can be justified e.g. because the employee will be working with disabled/vulnerable people or because the employee may be working in the Accounts office and have access to significant amounts of money.
- Only request sensitive information if one of the sensitive data conditions satisfied (e.g. it is required for the purposes of complying with employment law, it is necessary to establish, exercise or defend legal rights and/or the applicant has given his explicit consent).
- Explain to applicants if verification/vetting procedures will be used
- Ensure interviewers know their notes may be subject to a Subject Access Data Request. Only keep notes that are necessary to the recruitment process.

Employment records

Ensure

- There is a clear and foreseeable need for collection of personal data
- There is in place a data protection policy for staff which covers privacy issues re clients/customers
- Any personal data is kept secure

Retaining employment records

No prescribed timescale, but suggest:

- Job application/recruitment records (unsuccessful candidates) - six months.
- Written particulars of employment/contracts of employment/changes to terms and conditions – six years after employment ceases
- Personnel and training records (job applications/interview records, qualifications/references, annual assessment reports, job history, disciplinary/grievance procedures, resignation, termination and/or retirement letters – six years after employment ceases.

Action points

- Ensure there is a clear and foreseeable need for any personal data collected.
- Consider your privacy notices and policies for the retention and storage of data.
- Comply with your need to notify to the ICO. The following guidance may assist: https://ico.org.uk/for-organisations/register/

Further sources of information

Information Commissioner's website:

https://ico.org.uk/

Data Protection: Sector specific and small business guidance:

https://ico.org.uk/for-organisations/business/

This information and draft documentation is provided by the TBA as a guide to members and does not constitute legal or other professional advice. It is not a substitute for individual legal advice and members are recommended to seek advice on their own circumstances from a specialist employment lawyer. The TBA does not accept liability for any loss sustained by members in reliance on the information published on this website.