General Data Protection Regulation (GDPR)

1) Definition:

"The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier."

2) The data protection principles:

Under the GDPR, the data protection principles set out the main responsibilities for organisations:

- **Fair, lawful and transparent:**
  - We must be open and honest about who we are and how we will process someone's personal data. We must only handle it as they would reasonably expect and we mustn't have an unjustifiably negative effect on them.
  - A clear and complete privacy notice tells people exactly how we will use their data.
  - We must have a legal basis before we can process personal data. These include:
    - Consent: the individual has consented.
    - Contractual necessity: it's necessary so an individual can enter into a contract or in relation to an existing contract.
    - Legal compliance: it's necessary for our compliance with legal obligations.
    - Vital interests: it's necessary to protect the vital interests of the data subject or another natural person e.g. in cases of life or death.
    - Public interest: it's necessary to deliver justice, or to exercise statutory, governmental, or other public functions.
    - Legitimate interests: it's in accordance with the data controller's legitimate interests, e.g. a finance company who use an agency to locate a client.

- **Purpose limitation principle:**
  - Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.
  - Be clear and transparent about why you are collecting the data.
  - Don't use the data for anything else without consent.

- **Data minimisation principle:**
  - Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
  - Is this the minimum amount of data I need?
  - Do I have enough information?
  - Does it all apply directly?
  - Is any of this information ‘just in case’ or ‘might be useful’?

- **Accuracy principle:**
  - Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.
  - Whether the data is likely to change?
  - How often it might and therefore how often you should check?
  - How you can maintain accuracy efficiently and reliably?

- **Data retention principle:**
  - Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
  - When and how should personal data you collect be destroyed?
  - Should data be retained or disposed of?
  - Destroy files containing personal or corporate data when it is no longer required.
  - Manual files must be destroyed using confidential waste facilities.

- **Data security principle:**
  - Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
  - Read your IT policy.
  - Follow procedures such as setting safe passwords to make sure you keep information secure and confidential.

- **Accountability:**
  - The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.
  - Follow data protection and information security policies.
  - Maintain data protection documentation precisely.

3) The GDPR provides the following rights for individuals:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

4) How to stay compliant:

- **Never:**
  - Allow others to know your system logins or passwords.
  - Leave files or documents containing personal data or sensitive corporate information visible.
  - Forward information to anyone that does not have a valid reason for seeing it.
  - Use personal data in a manner that is inconsistent with the privacy policy.

- **Be aware of:**
  - The information contained within an email trail before forwarding; even if you are forwarding an email sent to you.
  - Your surroundings when working with personal data, particularly in public areas.

- **Always:**
  - Be clear and transparent about the purposes for which you use or disclose or share personal data.
  - Keep personal data accurate and up to date.
  - Consider whether an individual would consider the purpose for which you intend to use their data as being fair.
  - Destroy files containing personal or corporate data when it is no longer required.
  - Save personal data in a secure place.
  - Choose the most secure route for sharing data.

5) The consequences of non-compliance (the organisation):

- An investigation by the UK Information Commissioner.
- Reputational damage caused by bad publicity.
- Compensation claims against the organisation for the damage and distress.
- A fine imposed by the UK Information Commissioner.

Further information:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- https://www.sportandrecreation.org.uk/pages/gdpr
- https://www.englandathletics.org/clubs--community/club-management/gdpr-and-data-protection-advice?utm_source=Sported+Master+List&utm_campaign=b4363fe77c-EMAIL_CAMPAIGN_2018_03_19&utm_medium=email&utm_term=0_86227d8202-b4363fe77c-1203793917