GENERAL DATA PROTECTION REGULATION (GDPR) 12 STEP CHECKLIST[1]

Step 1 – Awareness

- **GDPR change:** The GDPR will significantly amend current data protection law, effective 25 May 2018.
- **Action to be taken**: Make the GDPR reforms known to key people in the business (e.g. those with supervisory or decision making powers), and make them aware of the effects of such reforms.

Step 2 – Information you hold

- **GDPR change**: Businesses must show how they comply with the data protection principles. If a business has shared inaccurate personal data with another organisation, it must notify that other organisation.
- **Action to be taken**: Businesses should consider undergoing an information audit which documents the personal data held by them, the source of such data and details of with whom they share the data.

Step 3 – Communicating privacy information

- **GDPR change**: Additional information must be given to individuals when personal data is obtained.
- **Action to be taken**: Review current privacy notices/policies and identify those areas which will require updating to ensure compliance with the GDPR.

Step 4 – Individuals' rights

- **GDPR change**: Individuals will have enhanced rights to:
    - access their information
    - have inaccuracies corrected
    - have information erased
    - data portability
    - prevent direct marketing
    - prevent automated decision making and profiling
- **Action to be taken**: Review privacy/data protection procedures and policies to ensure that they provide for each enhanced right under the GDPR.

Step 5 – Subject access requests

- **GDPR change**: Timescales for compliance reduced, fees no longer chargeable and additional information must be provided to individuals (e.g., data retention periods, correction of inaccuracies).
- **Action to be taken**: Review and update current procedures for handling subject access requests.

[1] This information is not intended to offer legal advice. Users should seek legal counsel for guidance in their own situations. Adapted from "ICO's 12 Steps Checklist: How to Prepare for EU Data Protection Reforms." (22nd March, 2016). David Gourlay. https://www.macroberts.com/icos-12-steps-checklist-how-to-prepare-for-eu-data-protection-reforms/?utm_source=Swiftpage&utm_medium=Email&utm_content=ICO%2012%20Steps&utm_campaign=IPTC%20eupdate%20160322?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

Step 6 – Legal basis for processing personal data

- **GDPR change**: Legal basis for processing must be explained in privacy notices and when responding to subject access requests. Rights afforded to individuals vary depending on legal basis for data processing.
- **Action to be taken**: Review the data processing done by the business, identify and document legal basis.

Step 7 – Consent

- **GDPR change**: Consent must be freely given, specific, informed, and unambiguous. The recording of consent is important as data controllers must be able to demonstrate that consent was given.
- **Action to be taken**: Review methods for seeking, obtaining and recording consent to ensure compliance.

Step 8 – Children

- **GDPR change**: Parental or guardian consent must be obtained to process personal information of children (i.e., those under 13 in UK). Consent must be verifiable and written in child friendly language.
- **Action to be taken**: Create and implement new practices for (i) verifying the age of individuals and (ii) obtaining parental or guardian consent when processing the data of children.

Step 9 – Data breaches

- **GDPR change**: Widens the number of businesses obliged to notify the relevant DPA and private individuals of data breaches. Failure to comply with this obligation may lead to significant fines.
- **Action to be taken**: Ensure procedures are in place to detect, investigate and report on personal data breaches. Assess types of data held; document which ones would trigger notification if a breach occurs.

Step 10 – Data protection by design and data protection impact assessments

- **GDPR change**: Organisations must adopt 'privacy by design'. Organisations should also carry out a Data Protection Impact Assessment ("DPIA") in high-risk situations. Consult with the relevant DPA as needed.
- **Action to be taken**: Know when DPIAs should be used, who should be involved and the process to be adopted. Look at the UK Information Commissioner's Office guidance on Privacy Impact Assessments for further information.

Step 11 – Data protection officers

- **GDPR change**: Public authorities and large businesses are required to appoint a Data Protection Officer.
- **Action to be taken**: Identify and designate a Data Protection Officer to ensure compliance with GDPR. This can be someone within or outside the organisation. Select someone with suitable experience.

Step 12 – International

- **GDPR change**: The GDPR creates a system for determining which data protection supervisory authority takes the lead when investigating a complaint which is international in nature.

- **Action to be taken**: If operating internationally, determine which data protection supervisory authority will be the lead for the business. Map out where most significant decisions are made to determine this.