DATA PROTECTION LEGISLATION
Compliance self-help checklist

information commissioner
Barrantagh Fysseree

This self-help checklist is to assist you formulate a clear policy on data protection compliance.

It examines the issues in a structured manner in relation to compliance with the legal requirements of the data protection legislation and with the principles of data protection. The amount of detail you find useful will depend on the size of your organisation and the amount of personal information you hold.

If you can answer 'yes' to all these questions then your business is in good shape with regard to data protection. If not, it should help you pinpoint the areas that need improvement.

Compliance with the Legal Requirements

- ☐ Does the organisation need to register with the Information Commissioner?
  - o If so, is the register entry kept up to date?
  - o Do we advise the Information Commissioner of any changes as soon as practicable?
- ☐ Does the organisation require a Data Protection Officer (DPO)?
  - o Are all staff aware of who the DPO is and know how to contact them?
- ☐ Does the organisation keep some form of record showing what personal data is processed, why, and how the processing complies with the data protection legislation?
  - o Is this reviewed and updated as necessary?
- ☐ Are there formal data protection compliance review mechanisms in place within the organisation?
- ☐ Are staff aware of their responsibilities under the data protection legislation?
- ☐ Is data protection included as part of the regular training programme for staff?
  - o Is a senior member of staff responsible for ensuring that training is provided and completed?
- ☐ Does the organisation know:
  - o the legitimate uses of personal data and how it flows in and out?
  - o the minimum personal data needed in order to fulfil each of the different purposes?
  - o whether it is kept accurate and up-to-date?
  - o how long is personal data kept for the particular purpose(s)?
  - o what security measures are needed to protect the personal data (this may vary depending on the particular purposes and what type of personal data is being processed)?
  - o whether any personal data is disclosed to named third parties, and in what circumstances;

Compliance with the Principles of Data Protection

1. Lawfulness, fairness and transparency

Lawfulness

- ☐ Have we identified the lawful basis for each purpose for which we process personal data?
- ☐ If we rely on consent as the only lawful basis for processing:
    - can we demonstrate that we obtained the client's consent and that it was freely given, specific and informed?
    - Are procedures in place to record and demonstrate that the client consented by way of a clear indication to the processing of their data?
    - Are procedures in place to permit an individual to withdraw their consent to the processing of their data?
    - If automated decision-making is used, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected?
    - Are procedures in place to verify age and get valid consent of a parent or guardian, where required?
- ☐ If we rely on 'legitimate interests', can we demonstrate that:
    - There is a valid legitimate interest and reliance on this legal basis is appropriate; and
    - The data processing is strictly necessary in pursuit of that legitimate interest;
    - The processing is not prejudicial to, or overridden by, the rights of the client?

Fairness

- ☐ Do we have a privacy notice or fair processing notice available for our clients and staff?
    - Do we provide them with this at the time we collect their personal information?
    - Does it include details of any disclosures of their personal information to third parties?
- ☐ Have we made information about rights and how to exercise them available in an easily accessible and readable format?
- ☐ Are procedures in place to proactively inform individuals of their rights?

Transparency

- ☐ Are employees, volunteers, members and clients fully informed of how we use their data in a concise, transparent, intelligible and easily accessible method using clear and plain language?
- ☐ Are our personal information collection processes open, transparent and up-front?
- ☐ Have we obtained the client's consent (if necessary) for any secondary uses of their personal information that might not be obvious to them, e.g. direct marketing?

- Are details published of our data protection officer or other contact for data protection matters?

2. Purpose limitation

- Is personal data only used for the purposes for which it was originally collected?
- If personal data is used for other purposes:
  - are they closely connected to the original purpose for collection?
  - Have we obtained consent (if necessary) for any secondary uses of their personal information that might not be obvious to them, e.g. direct marketing?
- Is the personal data disclosed or shared with any other party?
  - If so, can you identify every other party?

3. Data minimisation

- Is the personal data obtained limited to what is necessary for the purposes for which it is processed?

4. Accuracy

- Are procedures in place to ensure personal data is kept up to date and accurate and any necessary changes are made without delay?
- Where personal data are obtained from a third party, are there processes in place to verify the accuracy of that data before further processing occurs?

5. Storage limitation

- Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected?
- Is your business subject to rules that require a minimum retention period (e.g. tax/NI returns, AML/KYC records)?
- Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies?

6. Integrity and confidentiality

- Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?
- Do you have a documented security policy that describes the technical, administrative and physical safeguards for personal data?
- Have you designated an individual with responsibility for information security including the investigation of security incidents and breaches?
- Do you have documented processes and procedures for investigating and resolving security related complaints and issues?
- Can access to personal data be restored in a timely manner in the event of an incident?

- Is personal data systematically destroyed, erased, or anonymised in accordance with retention policies when no longer required?
- Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records?
- If you process special category data, such as health data, do you employ encryption techniques to transfer, store, and receive such data?

7. Accountability

- Does any individual, or role, within the organisation have overall responsibility for information security and ensuring that staff understand their responsibilities?
- Have we designated a Data Protection Officer (DPO)?
    - If not, are we able to demonstrate the rationale for not having a DPO?
- Are appropriate data protection policies implemented?
- Are records of processing activities maintained?
- Do we review records on a regular basis?
- Are the arrangements with any joint controllers documented?
- Are there written contracts in place with any processors?
- Are records of system testing maintained?
- Are security policies and procedures in place?
    - Are they reviewed on a regular basis?
- Are there security measures in place to protect the personal information we hold and use?
    - Are these provisions appropriate?
    - Do we have additional provisions in place for special categories of personal data?
- Are computers, servers, paper client files etc., secured from unauthorised physical access?
- If third parties process personal information on our behalf, do we have written agreements in place?
- Is there an information security/ information governance policy in place that staff are aware of and receive regular training in?
  Does this include:
    - The need for the use of password protection and/or encryption to current standards if necessary, particularly if personal information is emailed, taken off-site or portable devices are used?
    - Arrangements for the use of personally owned portable and mobile devices for work purposes either in the workplace or at home? (Bring Your Own Device)
- Do we regularly transfer personal information to third countries?
    - If so, are we confident that there are appropriate security measures in place, and what steps do we take to check those measures?

Compliance with the Rights of Individuals

Right to information about processing - Articles 13 & 14

- ☐ Do we provide privacy information:
  - in a concise, transparent, intelligible and easily accessible form?
  - in clear, plain language adapted as necessary to meet the target audience needs, especially where children, or other vulnerable groups, are concerned?
  - in conjunction, if needed or desirable, with standardised icons to give an easily visible, intelligible and clearly legible overview of the intended processing?

Right of access - Article 15

- ☐ Can we recognise a subject access request?
- ☐ Is any individual, or role, within the organisation responsible for handling subject access requests?
- ☐ Is there a documented policy/procedure for handling requests to access personal data?
  - Are these policy/procedures clear for dealing with such requests in accordance with the data protection legislation?
- ☐ Have we established processes to fully respond within one month to an individual exercising any of their rights?

Right to rectification - Article 16

- ☐ Are there controls and procedures in place to allow personal data to be rectified when necessary?

Right to erasure 'right to be forgotten' - Article 17

- ☐ Are there controls and procedures in place to allow personal data to be deleted when necessary?

Right to restriction of processing - Article 18

- ☐ Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?

Right to data portability - Article 20

- ☐ Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine-readable format?

Right to object to processing - Article 21

- Have we made individuals aware of their right to object to certain types of processing such as:
  - direct marketing;
  - where the legal basis of the processing is based on legitimate interests or for a task carried out in the public interest?
- Are there controls and procedures in place to halt the processing of personal data where an individual objects to the processing?
- Where an automated decision is made (which is necessary for entering into, or performance of a contract, or based on the explicit consent of an individual) are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?
- Do we give clients the right to object to direct marketing?
- Do we give clients the right to opt out with every electronic marketing communication?

Further guidance is available on the website.

May 2020