GDPR Checklist

DATA PROTECTION COMMISSION CHECKLIST

MAIN RESPONSIBILITIES

Rule 1: Fair obtaining:

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with the Data Protection Commissioner, does our register entry include a

proper, comprehensive statement of our purpose? *[Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]*

- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Rule 3: Use and disclosure of information

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.
- If we are required to register with the Data Protection Commissioner, does our register entry include a full list of persons to whom we may need to disclose personal data? *[Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.]*

Rule 4: Security

- Is there a list of security provisions in place for each data set?

- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorised people?

Rule 5: Adequate, relevant and not excessive

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Rule 6: Accurate and up-to-date

- Do we check our data for accuracy?

- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Rule 7: Retention time

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 8: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the Act's requirements?

Registration

- Are we clear about whether or not we need to be registered with the Data Protection Commissioner?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? *[Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]*
- Is a named individual responsible for meeting our registration requirements?

Training & Education

- Do we know about the levels of awareness of data protection in our organisation?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training programme for our staff?

Co-ordination and Compliance

- Has a data protection co-ordinator and compliance person been appointed?
- Are all staff aware of his or her role?

- Are there mechanisms in place for formal review by the co-ordinator of data protection activities within our organisation?