Data Protection
Responsibilities of Data Controllers

Under the Irish Data Protection Acts, a data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

Therefore, Chambers and businesses resident in Ireland[1] who are processing or collecting personal data are data controllers and thus required to comply with the requirements of the Data Protection Acts.

Being a data controller carries with it serious legal responsibilities. Chambers and businesses resident in Ireland who are not compliant with the requirements of the Data Protection Acts as outlined below will be subject to penalties. If you are in any doubt, or are unsure about the identity of the data controller in any particular case, you should consult your legal adviser or seek the advice of the Data Protection Commissioner.

Data controllers can be either individuals or "legal persons" such as companies, Government Departments and voluntary organisations.

All data controllers must comply with certain important rules about how they collect and use personal information.

Some data controllers must register annually with the Data Protection Commissioner, in order to make transparent their data handling practices. Please refer to guidance here to determine if you are a data controller who is required to register.

How long should personal data be held to meet the obligations imposed by the Acts?

The Data Protection Acts state that personal information held by Data Controllers (in this case Chambers and businesses resident in Ireland[1] who are members of Chambers) should be retained for no longer than is necessary for the purpose or purposes for which it was obtained. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

For example any personal data related to a member of staff should be deleted when the employee leaves the employment of the organisation. However, the Acts do not stipulate specific retention periods for different types of data, and so organisations must have regard for any statutory obligations imposed on them as a data controller when determining appropriate retention periods.

How do I make a privacy policy?

A privacy policy should reflect a detailed examination of an organisation's processing of personal data and the application of data protection law to these practices. It should be a dynamic document, regularly reviewed and updated to reflect changes in the way the organisation processes personal data.

To ensure that all aspects of data protection are covered we suggest that a privacy policy should be built around the eight data protection principles listed in "A Guide for Data Controllers" pdf booklet.

What security measures should I have in place to protect personal data from unauthorised access?

The Acts require that appropriate security measures be in place which takes account of the harm that would result from unauthorised access to the information. This should take account of available technology and the cost of installation. In addition to technical security measures, due regard should be had for physical security measures such as access control for central IT servers and local PCs.

What do I do if there is a security breach?

A Data Controller is required to have in place appropriate security measures to prevent both internal and external unauthorised access to personal data that it is responsible for. The Data Protection Commissioner has issued a Code of Practice and Guidelines on what to do if personal data is put at risk of disclosure, loss etc . Data controllers are advised to notify affected data subjects in most such cases and also to notify the Office of the Data Protection Commissioner no later than 24 hours after the first detection of the breach. If the provider is unable to provide full details on the breach at this time, further details should be provided within three days of the initial notification.

What should be contained in a contract between a Data Controller and a Data Processor?

Sometimes, an organisation will need to engage the services of a sub-contractor or agent to process personal data on its behalf. Such an agent is termed a 'data processor' under the Data Protection Acts. An example would be a payroll company. Where a data controller engages the services of a data processor, it must take certain steps to ensure that the data protection standards are maintained.

A data controller can do business with a data processor only on the basis of a written contract (or a contract in equivalent form) which includes appropriate security and other data protection

safeguards. Informal and ad-hoc arrangements will not be acceptable, where personal data is involved.

There is not a specific template on the content of such contracts as a case by case approach needs to be taken depending on the particular circumstances arising. As a general guide, the key points for consideration are:

1. The Data Protection Acts place responsibility for the duty of care owed to personal data on the Data Controller and accordingly when drawing up the contract the Data Controller should be very specific in the instructions given as to what the Data Processor can do with the personal data provided. In particular, the contract should specifically provide that the data processor will process personal data only on the basis of the authorisation and instructions received from the data controller. This provision ensures that personal data passed on to a data processor may not be retained or used by the data processor for its own purposes.

2. The contract must commit the data processor to apply appropriate security measures to the personal data to protect it from unauthorised access or disclosure. This provision ensures that the standard of security must be maintained when the personal data is passed from the data controller to its agent.

3. The deletion or return of the data upon termination or ending of the contract.

4. Any penalties in place should the terms of the contract be broken.

5. It would also be expected that the Data Controller or their agents would have a right to inspect the premises of the Data Processor as to ensure compliance with the provisions of the contract.

6. The contract should detail a retention period for the categories of personal data held on the Data Processor's systems.

7. The contract should contain a requirement on the Data Processor to notify the Data Controller, without undue delay, in the event of a data security breach affecting the personal data being processed on behalf of the Data Controller.

8. The contract should contain a requirement on the Data Processor to notify the Data Controller, without undue delay, in the event the Data Processor receives a subject access request from a relevant data subject.

9. If the Data Controller is required to register with this Office, the Data Processor must also register with this Office for the duration of the contract

Can I use a "cloud" service to process my data?

The "cloud" provider will usually be acting as a data processor for you. This means that you remain responsible for how the data is processed and that this must be spelled out in a contract that complies with the terms of Section 2C (3) of the Data Protection Acts. The contract must provide that the "cloud" provider only processes your data in accordance with your instructions and takes measures to keep the data secure.