**Describe and critically analyse how the Data Protection Acts 1988 and 2003 are enforced.**

## General

Under the current Irish framework for data protection follows 8 principles. To obtain and keep data fairly, to keep personal information only for awful purposes, to use and dispose personal information only in ways compatible with the reason they are stored, to keep all personal data secure, to keep all personal data accurate and up to date, to ensure that personal data is relevant and not excessive for the purpose, to retain personal information for no longer than is necessary and to provide a copy of the data to the relevant individual on request.

## Question specific

The data protection commissioner enforces these principles. If any of the above principles are seen to have been breached, then a complaint with the data protection commissioner and under section 10 of the Data protections acts the DPC must carry out investigation of any complaints made. The DPC has the right, under section 12 to require any person or entity to provide him with the information required for the investigation, under section 24, he may also appoint an authored officer to enter and examine the premises of the data controller should it be required.

Should a breach of the data protection acts be found to have happened then the DPS is initially obliged to seek amicable resolution but failing this may make a ruling on the complaint and has the power to require a data controller to comply with the DP acts and may prosecute under the 2001 Electronic Communications regulations.

**Evaluate whether the current Data Protection legislation achieves a satisfactory balance between the rights of data controllers and data subjects.  20 Marks**

The balance between the rights of the data subject and the data controller is a delicate one. On one hand a subject must be protected from misuse of their information and have access to it while on the other the data controller’s business is likely dependant on the information they store and is extremely value to them so their interests must be protected assuming they are complying with regulations.

Current legislation in the Data protection acts 1988, 2003 favours the data subject in that, to protect their information, the data controller must be seen to be fully compliant with regulations following any investigating by the Data protection commissioner meaning that the risk to data controllers data is at greater risk than the subjects.

An example of this is with the right to be forgotten which protects the data subject from having sensitive or defamatory data form appearing in search results online. In the Costeja case in 2014, a Spanish man complained that the notice of the auction of his repossessed house was on Google which infringed his privacy under EU law. The EU court of Justice ruled in favour of the man much to Google chagrin and this case has been used as a judicial precedent in similar cases since. This ruling ensures that data subjects are protected against outdated or harmful information but at what cost? The business model of Google Search, for example, is search result. If things are removed from the results then their product is less valuable so this may harm the data controller.

A balance is necessary to ensure that each case is handled with care and consideration is given to both sides of the case and ensure that frivolous requests are not approved.

**Discuss the legal rules governing the transfer of personal data from Ireland to a jurisdiction outside of the European Union.**

Section 11 of the data protection acts 1988 and 2003 state that conditions must be met before personal data may be transferred outside of the EU, namely that the destination country provided a sufficient level of data protection. If they do not, then the irish data controller, the origination of the data, must rely on another method approved by irish law to determine if the transfer is legal. None the less the DPC has the right to prohibit transfers if he considers the data protection rules are likely to be contravened.

In the past the above regulations were handled under safe harbour when the data was being transferred to the US. In these case the data controller only had to self-certify that they complied with the EU regulations so were somewhat immune to investigation. The safe harbour arrangement was deemed insufficient by the CJEU following a ruling in the Max Schrems case.

In this case, after becoming aware of Edwards Snowdens claims that Facebook and other companies were being forced to make user data available to US intelligence, brought tit to the attention of the Irish Data protection commissioner. Initially the DPC ruled that he could not investigate as the companies were protected by safe harbour. Max appealed this case and it was eventually referred to the CJEU as it was deemed an issue of EU law. The CJEU rules that safe harbour was invalid and did not ensure the correct level of data protection.

Because of this ruling, transfer of personal data to the US is not prohibited.