Data Breach Policy

What is a Data Breach.

It is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

When does the WRC have to Notify the Data Protection Commission.

The obligation on the WRC to notify the Data Protection Commission arises in the case of any personal data breach, unless the breach is unlikely to result in "*a risk*" to the rights and freedoms of individuals.

The risk can include a broad range of physical, material and immaterial damage, such as loss of control over personal data, financial loss, identity theft and damage to reputation.

However, even where the WRC does not have to notify the Data Protection Commission the fact of the breach itself and the facts relating to the breach, its effects and any remedial action taken will be documented.

When does the WRC have to Notify the Data Subject.

The WRC must notify the data subject when a breach if it is likely to result in a "*high risk*" to their rights and freedoms and damage to the data subject. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

Identifying high risk.

The GDPR does not lay down a specific threshold as to when a breach causes a "*high risk*" to individuals and their rights. In practical terms, it can mean different things in different circumstances. For example, the disclosure of the name and address of an individual in ordinary

circumstances is unlikely to cause substantial damage. Sensitive personal data or information that could be used for identity theft are at the higher end of the risk scale, whereas contact details or similar or probably at the lower end.

When to notify.

Notifications to the DPC need to be made without undue delay, and if not made within 72 hours of the WRC becoming aware of the issue, the delay will need to be explained. Furthermore, where it is not possible to provide all relevant information at once, it may be provided in phases without undue further delay. This means that the WRC may have to consider notifying breaches before they have been able to carry out a full risk assessment, failing which they will need to explain the delay to the DPC.

Notifications to data subjects also needs to be made without undue delay, but without the 72 hour proviso. However, there are some circumstances in which no notification to individuals will be required, such as where the data has been encrypted, or steps have been taken to ensure that the high risk is no longer likely to materialise.

It is likely that the DPC will provide information either through cases or otherwise as to what will constitute a high risk. Meanwhile, the Guidelines on Personal data breach notification by the Article 29 Data Protection Working Party will be used to assess risk. The Guidelines can be accessed here http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052