Guidance v2.0

Appendix D – ICO guidance on assessing disclosure to individuals affected by a data breach

* Are there any legal or contractual requirements? Service providers have an obligation to notify the Commissioner in certain circumstances, in other areas sector specific rules may lead you towards issuing a notification.
* Can notification help you meet your security obligations with regard to the sixth data protection principle?
* Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
* If a large number of people are affected, or there are very serious consequences, you should inform the ICO.
* Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.
* Have you considered the dangers of ‘over notifying’. Not every incident will warrant notification and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.
* What type of data is involved?
* How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
* If data has been lost or stolen, are there any protections in place such as encryption?
* What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
* Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
* How many individuals’ personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
* Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks.
* What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
* Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
* If individuals’ bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use