s. 22

[redacted]

OAIC guidance – Assessment

Assessment of serious harm - general

Entities should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm. The NDB scheme includes a non-exhaustive list of 'relevant matters' that may assist entities to assess the likelihood of serious harm.

Assessment of serious harm – scale of breach

If the breach involves the personal information of many individuals, the scale of the breach should affect an entity's assessment of likely risks. Even if an entity considers that each individual will only have a small chance of suffering serious harm, if more people's personal information is involved in the breach, it may be more likely that at least some of the individuals will experience serious harm.

Assessment of serious harm – time of exposure

The time between when the data breach occurred and when the entity discovers the breach will be relevant to the entity's consideration of whether serious harm is likely to occur. For example, if personal information is publicly accessible for a significant period before the entity is aware of the data breach, it may be more likely that the personal information have been accessed in ways that will result in serious harm to the individuals affected.

Assessment of serious harm - Lack of evidence

Entities should be cautious about relying on a lack of evidence that data has been accessed. Some threat actors are careful to delete evidence of their actions within a system, limiting the reliability of a lack of evidence, particularly where an entity does not have adequate audit and activity logs. Entities need to consider the reliability or credibility of the evidence on which their findings are based.

s. 22

[redacted]