Section 22 Notification of security compromises

1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify—

    1. the Regulator; and

    2. subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

2. The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

3. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

4. The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:

    1. Mailed to the data subject's last known physical or postal address;

    2. sent by e-mail to the data subject's last known e-mail address;

    3. placed in a prominent position on the website of the responsible party;

    4. published in the news media; or

    5. as may be directed by the Regulator.

5. The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

    1. a description of the possible consequences of the security compromise;

    2. a description of the measures that the responsible party intends to take or has taken to address the security compromise;

    3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

    4. if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

6. The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that

such publicity would protect a data subject who may be affected by the compromise.