|  |  |  |
| --- | --- | --- |
| **AGL23** | **AGL Training Ltd** | **Data Breach Notification Process** |
|



|  |  |  |
| --- | --- | --- |
| **Author:** | **Gary Biggam** | **Version 001** |
| **Authorised:** | **Aaron Biggam** | **Date: 25-05-2018** |

|  |  |  |
| --- | --- | --- |
| **SOP - 13.14** | **AGL Training Ltd** | **Data Breach Notification Process** |
|
| **Appendix 1** |  |  |  |  |  |  |  |
| **ICO notification requirements** |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| As part of the data breach notification process, the directors and GDPR manager is to prepare an informed opinion as to whether the ICO are required to be notified and this decision is to be formally approved by the directors. The decision on whether to notify the ICO must be made with all relevant information available and must be informed via a thorough understanding of the reporting requirements. |
|
|
|
| When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However. if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it. |
|
|
|
| In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that: |
|
| "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned" |
|
|
|
| This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors. |
|
|
|
| **Data Subject notification requirements** |
| The convened privacy team must also prepare a recommendation as to whether and in what format data subjects are required to be notified, the directors will formally approve this decision as part of the breach notification, to inform this decision, the following guidelines from the ICO must be considered: |
|
|
| If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible. |
|
| A 'high risk' means the threshold for informing individuals is higher than notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In, risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach. |
|
|
|
|

|  |  |  |
| --- | --- | --- |
| **Author:** | **Gary Biggam** | **Version 001** |
| **Authorised:** | **Aaron Biggam** | **Date: 25-05-2018** |