Process Id# :: **0000**
Process Name :: **NSSO Data Breach Reporting Process**
Date Last Updated :: **8/11/2019**

Description :: Where the NSSO (processor) is made aware of a breach arising from an error made by the NSSO, it will enact the following agreed breach reporting process on behalf of the controller Public Service Body (PSB). The Article 29 Data Protection Working Party Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01), particularly under Section II.A.4 list obligations under Article 33 – Notification to the Supervisory Authority. This guidance (page 14) states that; processors can make a notification on behalf of a controller if the controller has given the processor the proper authorisation and this forms part of the contractual arrangements between controller and processor. Such notifications must be made in accordance with Article 33 and 34 of the GDPR. This process is considered to form such proper authorisation.

Stage 1 :: Breach Awareness & Investigation

1. Once the NSSO is alerted to a breach incident a 72 hour window commences, in line with Art 33(1).
2. All breaches will be notified to the information governance team (IGT) after which the standard IGT investigation process begins. This guidance should supplement the investigation process.
3. Within 24 hours IGT need to have a clear picture of the nature of the breach, even if the circumstances of why it happened and how to prevent it reoccurring is not resolved.
4. IGT will issue a CAPA (breach incident report) form to the section where the breach occurred.
5. The section will populate the breach incident report and return to IGT for a risk evaluation.

Stage 2 :: Breach Classification (Risk vs. No Risk)

6. The IGT will use criteria from page 9 of the DPC "breach notification form" and prior advices received from the Data Protection Commission (DPC) to determine if there is -
    a. risk or no risk,
    b. If there is a risk then to set which level of risk should apply.
7. The NSSO DPO will be made aware and consulted on all breaches at this point to make a determination on the appropriate risk level and course of action.
8. If there is a risk, then IGT will populate the DPC's "Breach Notification Form" (in line with the 2019 website submission process) within 24-48 hours of the breach being notified to them and send to the NSSO DPO and appropriate line managers for review.
9. The NSSO DPO will consult with the team and others as appropriate to finalise the wording of the breach notification form.
10. While the IGT are empowered to make determinations on such matters, particularly if the NSSO DPO is unavailable, where there is a different interpretation on any matter and especially on if a breach needs to be reported, the final determination rests with the NSSO DPO.
11. Also to be noted and connected with (10) is that a DPO has legal protections under GDPR and the Data Protection Act that other staff do not have (Art 38). Staff are encouraged to consult with the DPO if they have any concerns or wish guidance on any matters related to data protection and reporting.

Stage 3 :: Breach Notification :: DPC & controller DPOs

12. Breach notifications had issued to breaches@dataprotection.ie, but due to revisions to the DPC process are now submitted via the DPC website. This makes circulation and tracking more challenging.
13. The DPC will reply shortly with a receipt and breach code, eg BN—18-7-621.
14. Document this in your records and ensure the NSSO DPO is forwarded the notification email.
15. Any correspondence with the DPC must issue from dataprotection@pssc.gov.ie, dataprotection@peoplepoint.ie, or dataprotection.finance@nsso.gov.ie it is not to issue from personal email addresses.
16. You should always cc dpo@nsso.gov.ie on all DPC emails.

17. Any breach being notified to the DPC shall also be submitted to the controller DPO at the time of submission. The NSSO DPO will be cc'd on all PSB DPO correspondence.

Stage 4 :: Breach Notification :: Controllers :: All Breaches to LHR

18. All breaches irrespective of risk must be notified to the controller PSBs.
19. IGT will issue weekly reports, via the secure Document Management System (DMS), to the data controllers Local HR units providing details of breaches which occurred in a particular week and also provide reports where no breaches have occurred. This was previously limited to breaches in the HRSS.
20. IGT have now added breaches that occur in the payroll shared service to the DMS upload so that the report will now include all breach incidents in the NSSO.
21. LHR's who receive the secure DMS uploads will notify their DPO's or finance unit officials as appropriate.

Stage 5 :: Breach Notification :: Data Subjects

22. The NSSO will notify data subjects of a breach where the risk is deemed as high or severe, in line with data protection law, DPC advice and best practice. Attention is particularly drawn to Article 34(1).
23. The NSSO will not be notifying data subjects of a breach where the risk is deemed as non-existent, low or medium, as a matter of routine. Attention is particularly drawn to Article 34(3)(b).
24. Where a DPO of a client PSB requests that data subjects are notified of a no/low/medium risk breach, the NSSO will issue agreed correspondence in line with Article 34(2).

Assessing Risk ::

The NSSO is obliged to report a breach where is presents a risk to the affected individual. Risk should be determined by the impact it could have on the data subject. In assessing the potential impact you should consider the type of breach, to who the data is exposed, if the data has been accessed and/or contained.

- No Risk : The breach will not have an impact on individuals, the data has been contained and in a Civil Service context the DPC have advised :: *'if you consider the recipient "trusted", this may eradicate the severity of the consequences of the breach but does not mean that the breach has not occurred. However, this in turn may remove the likelihood of risk to data subjects, thus no longer requiring notification to the DPC'.*

- Low : The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal
- Medium : The breach may have an impact on individual, but the impact is unlikely to be substantial
- High : The breach may have considerable impact on affected individuals
- Severe : The breach may have a critical, extensive or dangerous impact on affected individuals.

Risk Summary ::

- No risk breaches will be notified to the LHR only via the weekly DMS upload.
- Low & Medium risk breaches must be reported to the DPC and will be notified to the LHR and PSB DPO.
- High & Severe must be communicated to the DPC and to the data subject and will be notified to the LHR and PSB DPO