|  |  |  |  |
| --- | --- | --- | --- |
| **Ref # \_\_\_\_\_\_\_\_\_\_\_** | | | |
| **Incidents involving DCU** **as Data Controller** | | | |
| 1 | Name of DCU Department / Unit |  | |
| 2 | Name of Employee(s) or Student involved |  | |
| 3 | Date and Time of Incident |  | |
| 4 | Describe the incident or breach |  | |
| 5 | Date and Time Incident Reported to the DCU Data Protection Unit |  | |
| 6 | Type / categories of personal data involved, if any |  | |
| 7 | Description of the incident |  | |
| 8 | Date and Time Incident Resolved |  | |
| **Incidents involving Data Processors** | | | |
| 9 | Name of Data Processor |  | |
| 10 | Name of DCU Department / Unit which has oversight of the Data Processor |  | |
| 11 | Name of DCU employee dealing with the Data Processor |  | |
| 12 | Date of Incident |  | |
| 13 | Date and Time Incident Reported to DCU |  | |
| 14 | Type / categories of personal data involved, if any |  | |
| 15 | Description of the incident or breach |  | |
| 16 | Date and Time Incident Resolved |  | |
| 17 | Has the Data Processor reported the incident to the Data Protection Commission? |  | |
| **Summary Details of Incident** | | | |
| 18 | Root Cause(s) of Incident |  | |
| 19 | Summary of Actions Taken to Remediate |  | |
| 20 | Root Cause Corrective Action Plan |  | |
| 21 | Planned Date of Root Cause Remediation |  | |
|  | **Risk Assessment** | | Yes/No |
| 22(a) | Is the breach likely to result in a risk to the rights and freedoms of individuals? Recitals 75 and 85 GPDR and the Article 29 WP Guidance suggests the following risks should be specifically considered:   In the wrong hands could the data give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, psychological distress, humiliation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage?   Does the data reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or data concerning sex life or criminal convictions or offences?   Does the data reveal the evaluation of personal aspects such as analysing or predicting performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?   Does the data relate to vulnerable natural persons, such as children?   Does the breach involve a large amount of personal data and affect a large number of data subjects? | |  |
| 22(b) | Risk mitigations:   Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact and the data is unintelligible to a third party?   Containment measures: Have any containment measures been implemented which mean that the Data Breach is unlikely to present a risk to the individuals affected? | |  |

|  |  |
| --- | --- |
| **To be Completed by Data Protection Officer or DPU Staff Member** | |
| 1. **Report to the DPC** | |
| **Is the incident reportable to the Data Protection Commissioner (DPC)?** | Yes/No |
| **If the breach is reportable to the DPC state the date & time the report was made via the DPC’s website.** |  |
| **State reason(s) for determining that the DPC was or was not informed as the case may be.** |  |
| 1. **Inform the Data Subjects** | |
| **Has the breach been notified to the Data Subjects affected?** | Yes/No |
| **If notification took place state the date & time of notification and how it took place.** |  |
| **State reason(s) for determining that notification to the Data Subjects was necessary or not necessary as the case may be.** |  |
| **Any other comments?** | |
| **Follow-Up Action** | |

Signed by Data Protection Officer (DPO) or DPU Staff Member & date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Definitions**

**Personal Data**

Personal data means any information concerning or relating to an living person who is either identified or identifiable (such a person is referred to as a ‘data subject’).

An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

**Sensitive Personal**

Sensitive personal data is defined as Personal Data which refers to:

 the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject

 whether the data subject is a member of a trade union

 the physical or mental health or condition or sexual life or sexual orientation of the data subject

 genetic or biometric data

 the commission or alleged commission of any offence by the data subject, or

 any proceedings for an offence committed or alleged to have any committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

**Personal data of a financial nature** means an individual’s last name, or any other information from which an individual’s last name can reasonably be identified, in combination with that individual’s account number, credit or debit card number.

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Name** | Data Incident Report Template | |  |
| **Owner** | Data Protection Unit | |
| **Version Reference** | **Original Version – 1.0** | **Reviewed Version – V1.2** |
| **Approved by** | Data Protection Officer | Risk & Compliance Officer |
| **Effective Date** | May 15th 2018 | 24th August 2023 |

