Dublin City University

Data Breach Reporting Procedure

(For Internal Use Only)

Important Notice

It is crucial for all DCU employees and students to immediately report any potential or suspected Data Breach (as defined in this Procedure) to the Data Protection Officer by phone and email – contact details are set out in paragraph 3 of this Procedure. If unsure whether an incident is a Data Breach or not please refer to the guidance set out in this Procedure and consult with the Data Protection Officer.

Version Control Panel

Document Name: Data Breach Reporting Procedure – Internal
Owner: Data Protection Unit - Office of the Chief Operations Officer
Approved by: Data Protection Officer
Date of Original: Original V1.0 - May 15th 2018
Date of Revision: V1.1 – August 24th 2023

1. Introduction

1.1 Dublin City University ("**DCU**") is a Data Controller[1] for the purposes of the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**"). The GDPR imposes obligations on Data Controllers and processors to process Personal Data (as defined below) in a manner that ensures the security, confidentiality and integrity of the Personal Data by implementing appropriate technical and organisational measures. In the event of a Data Breach (as defined below) that is likely to cause a risk to individuals the GDPR requires mandatory notification to the Office of Data Protection Commissioner (the "**ODPC**") and, in some cases, an additional communication to the affected individuals. This Personal Data Security Breach Procedure (the "**Procedure**") describes the process for identifying, escalating, reporting and recording suspected or actual Data Breaches involving Personal Data in accordance with DCU's GDPR obligations.

1.2 The purpose of this Procedure is to ensure that DCU manages and contains any Data Breach quickly so that the impact of the Data Breach can be minimised and any legal obligation to report the Data Breach to a regulator and/or any individual(s) affected by the Data Breach (in accordance with the GDPR) can be complied with in good time. This Procedure is also intended to enable DCU to take appropriate measures to reduce the risks for affected individuals.

2. Who does this Procedure apply to?

2.1 This Procedure applies to all employees of DCU and the DCU Campus Companies (as defined in the DCU Privacy Policy) irrespective of which department they are assigned to and applies to all students of DCU to the extent that Personal Data is disclosed to them. This Procedure also applies to independent contractors, agency temps and staff seconded to DCU. Together all employees, students to whom Personal Data is disclosed, contractors, agency temps and staff seconded to DCU are referred to in this Procedure as "**Personnel**". All Personnel should be provided with and read a copy of this Procedure.

3. What is Personal Data?

3.1 "**Personal Data**" is any information relating to an identifiable living individual. A person is identifiable if he/she can be identified directly or indirectly, for example by reference to an identifier such as a name, address, date of birth, telephone number, account number, job title, photo, IP Address, etc. If in doubt as to whether any specific information or data may constitute Personal Data, consult with the Data Protection Officer.

4. What is a Personal Data Breach?

4.1 The GDPR defines a 'personal data breach' as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" ("**Data Breach**"). A Data Breach occurs when there is any unauthorised or accidental disclosure, loss or any other form of unauthorised, accidental or unlawful collection, use, recording,

[1] ***'Data Controller" or "Controller'*** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

storing or distributing (each being a form of "**Processing**") of Personal Data. Examples of Data Breaches may include but are not limited to:

(a) loss, theft or misplacement of IT equipment or devices containing Personal Data e.g. smartphone, laptop or USB key;

(b) loss, theft or misplacement of briefcase or folder containing Personal Data in physical hardcopy form;

(c) human error resulting in email or post containing Personal Data being sent to an unintended recipient;

(d) unauthorised access to automated or manual Personal Data as a result of a break-in to an office or building on any DCU premises;

(e) unauthorised access to Personal Data as a result of a breach of access controls;

(f) an attack by a "Hacker", i.e. unauthorised access to DCU's computer network, which may consist of a deliberate interruption to IT network services or penetration of the IT network or system, by an unauthorised party with the intention of obtaining information, destroying data or preventing access to data;

(g) unforeseen circumstances such as a flood or fire, in particular where Personal Data is not accessible either temporarily or permanently;

(h) unauthorised access to Personal Data where information is obtained by deception; and

(i) in certain circumstances, where there is a loss of access to or availability of Personal Data (temporarily or permanently), for example where Personal Data has been deleted either accidentally or by an unauthorised person and the data cannot be restored.

4.2 Whether the incident (the "**Data Incident**") giving rise to the suspected Data Breach involves Personal Data must be determined on a case-by-case basis. If a Data Incident does not involve Personal Data, it is not a Data Breach. Furthermore, not all Data Incidents involving Personal Data will be Data Breaches. For example, the loss or compromise of Personal Data may not qualify as a Data Breach where:

(a) there is no risk to the individuals, their rights or freedoms, resulting from the Data Breach;

(b) the Personal Data is securely encrypted or anonymised such to make the Personal Data unintelligible; and/or

(c) there is a full, up-to-date back-up of the Personal Data (in cases of accidental destruction).

5. Personnel obligation to report Data Incidents to the Data Protection Officer

5.1 It is vital that all Data Incidents are immediately reported to the Data Protection Officer ("**DPO**") as soon as they are identified. It is the role of the DPO to ascertain whether the Data Incident is in fact a Data Breach. The DPO contact details are as follows:

Name	Martin Ward
Email	data.protection@dcu.ie
Phone	01 7005118 / 7008257

5.2 Prompt reporting of any Data Incidents to the DPO is crucial to ensure compliance with the GDPR, which contains a number of action points that must be put into immediate effect when DCU is alerted or notified of a suspected or potential Data Breach.

5.3 These detailed action points are comprised in the **Data Breach Response Plan** set out in Appendix 1. However, for Personnel the most important obligation to be aware of is that any Data Incident should be reported immediately to DCU's DPO. In implementing the **Data Breach Response Plan**, the DPO will investigate the Data Incident, liaising with the relevant departments as necessary to assess whether it is a Data Breach and the level of risk to the affected individuals, consider containment measures and determine whether: (i) a notification to the ODPC; and/or (ii) a communication to the affected individuals is required.

5.4 While it is important to note that not all Data Incidents will necessarily involve Personal Data, and will not require notification to the ODPC, all Personnel should note that all loss/theft/misplacement of IT equipment must be reported to the DPO and the IT Department (ISS).

6. Outsourced Activities

6.1 The GDPR requires that all Data Breaches must be reported to the relevant Data Controller without undue delay[2] as soon as the Data Processor[3] becomes aware of the incident. Where processing of Personal Data is outsourced to a third party, it is the responsibility of the Head of Unit to ensure that each Data Processor engaged by DCU: (a) has a contractual obligation to notify DCU on becoming aware of any suspected Data Breach relating to Personal Data they are processing on behalf of DCU; and (b) has been advised that they must bring any suspected Data Breaches relating to Personal Data they are processing on behalf of DCU to the attention of DCU immediately as soon as they are identified.

7. Making a Report to the Office of the Data Protection Commissioner

7.1 The DPO is responsible for making reports to the ODPC in accordance with the Data Breach Response Plan and will act as liaison between the ODPC and the relevant department in relation to requests for detailed written reports or any subsequent investigation by the ODPC.

---

[2] Article 33(2) GDPR.

[3] "Data Processor" or 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller;

8. Record of Personal Data Security Breaches in Data Breach Log

8.1 In accordance with the **Data Breach Response Plan** (set out in Appendix 1), the DPO is responsible for keeping a written record of all potential or suspected Data Breaches that are notified to him/her (including those that are not notified to the ODPC or the affected individuals). For this purpose, he/she, in conjunction with the relevant department/employee making the report, will complete the Personal Data Security Breach Incident Report contained in Appendix 3.

End.

Appendix 1 – Data Breach Response Plan

1. **Step 1: Internal report / report by processor / escalation**

1.1 Given the tight timelines within which Data Breaches must be reported to the ODPC, it is crucial that all Personnel immediately report any potential or suspected Data Breach to the DPO.

Timing: Immediately on alert or notification of suspected/potential Data Breach.

2. **Step 2: Initial Investigation**

2.1 Once reported to the DPO, there is a short period (of up to 24 hours[4]) during which DCU must determine whether the incident has given rise to a Data Breach or not (see definition above). If the DPO determines there has been no Data Breach, proceed to steps 7 and 11.

Timing: 0 hrs – 24 hours after initial alert or escalation of suspected/potential Data Breach.

3. **Step 3: Risk assessment and containment (simultaneous to step 2):**

3.1 If the DPO determines that incident does or may amount to a Data Breach, the next step is to assess the risks to individuals (for example, identity theft, fraud, reputational damage). This assessment should, in particular, consider the likelihood of risks taking place and the severity of such risks is to be categorised as ***no risk / risk / high risk*** in accordance with the detailed criteria below:

(a) **Type of breach:** A Data Breach may include any unauthorised or accidental disclosure, loss, destruction, damage or any other form of unauthorised, accidental or unlawful access to, collection, use, recording, storing or distributing of Personal Data. What type of Data Breach has or may have occurred? Does the breach consist of a breach of confidentiality relating to Personal Data? Is there a temporary or permanent lack of availability or access to Personal Data and if temporary, how long will it be before it is restored?

(b) **Nature of Personal Data:** Is the relevant Personal Data sensitive in nature? The more sensitive the Personal Data the higher the risk of the Data Breach. The utility of the relevant information may also indicate a higher risk to the affected individuals.

(c) **Scale and volume of Personal Data affected:** The higher the volume of the Personal Data records and the number of individuals potentially affected will usually create a higher risk.

(d) **Ease of identification:** The ease of identifying the relevant individuals based on the Personal Data will likely increase the risk of identity theft, fraud and reputational damage in particular.

[4] Article 29 Working Party Guidelines on Personal data breach notification suggest that the initial investigation undertaken by the Data Controller should be completed within 24 hours. This is only a guideline.

(e) **Security measures:** 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?

(f) **Containment measures:** Have any containment measures been implemented which mean that the Data Breach is unlikely to present a risk to the individuals affected?

(g) **Other factors:** Other relevant factors in assessing the risk to individuals is whether those individuals affected by the Data Breach have any special characteristics (for example children or vulnerable adults).

(h) **Severity of risk:** Based on the above criteria and any other relevant factors, the DPO should assess the severity of the risk in terms of the potential consequences to the individuals affected by the Data Breach.[5]

(i) **Likelihood of the risk(s) materialising:** Once the Data Breach has occurred, the DPO must objectively assess the likelihood of the potential risks actually materialising[6] and this should form part of the risk assessment.

3.2 The assessment of the Data Breach based on the above criteria should be an objective assessment focused on the risks likely to result from the Data Breach. Once it has been established with "a reasonable degree of certainty" that a Data Breach has occurred, DCU is considered to be "aware" of the Data Breach[7]. Unless the Data Breach is "unlikely to result in a risk to individuals" (having carried out the assessment above) then a notification to the ODPC is **mandatory** under the GDPR (see **Step 5**).[8] Consideration should be given as to whether communications in this phase are or should be subject to legal privilege so consult with the DPO (and external legal advisors if necessary).

Timing: 0 hrs – 24 hours (ideally) provided that any report is made within 72 hours from the end of that initial 24-hour period.

4. Step 4: Containment (simultaneous to step 3)

4.1 Simultaneously, DCU, with the assistance of the departments (such as the IT Department) and appropriate external advisors, will consider what measures should be taken to contain the Data Breach in order to mitigate the risks to the affected individuals

[5] For example, a low risk is where individuals will either not be affected or may encounter minor inconveniences which they can over-come without any problem (such as time spent re-entering information). A very high risk may be where individuals may suffer significant, or even irreversible consequences, which they may not be able to overcome, such as financial distress, long term psychological impact etc.

[6] Physical, material and non-material.

[7] Article 29 Working Party Guidelines on Personal data breach notification provides that a Data Controller will be considered to be 'aware' of a Data Breach once the Data Processor is has informed it of that breach. Once a Data Processor period becomes aware of a Data Breach (i.e. has established with a reasonable degree of certainty that a Data Breach has occurred) it must promptly notify the Data Controller, with further information about the Data Breach to be provided in phases as it becomes available. The Data Processor does not need to assess the likelihood of risk arising from the Data Breach before notifying the Data Controller.

[8] For example, if the data is already publicly available and disclosure will not give rise to any risk to the individual. However, given that there is no penalty for reporting an incident that ultimately transpires not to be a Data Breach, any such determination should be exercised with caution.

and the adverse effects of the Data Breach. These measures should be implemented without delay.

Timing: 0 hrs – until Data Breach has been contained.

5. **Step 5: Notification to ODPC**

5.1 If it has been established that there exists ***a risk*** to the rights and freedoms of individuals as a result of the Data Breach (which may include identity theft, fraud, reputational damage), then DCU's DPO is required to report the Data Breach to the ODPC without undue delay and within 72 hours from DCU becoming aware of the Data Breach (see **Step 3** above).

5.2 If the relevant details surrounding the Data Breach are not clear within the initial 72-hour notification period, an initial notification should be made to the ODPC. Subsequent notifications can be made to the ODPC in phases. Consideration as to whether a communication to affected individuals is required should be addressed when notifying the ODPC.

Timing: Within 72 hrs of becoming aware of the breach.[9]

6. **Step 6: Notification to individuals affected**

6.1 Based on the risk assessment carried out in Step 3, where the DPO assesses that there is ***a high risk*** to rights and freedoms of individuals as a result of the Data Breach, then the existence of the Data Breach should be communicated to the affected individuals without undue delay. Any such communication should inform the affected individuals on relevant measures that they can take to reduce the risks to them and any negative consequences arising from the Data Breach. The DPO should determine the most appropriate and effective means of communicating the Data Breach to the affected individuals, if necessary engaging the assistance of communications advisors.

Timing: Without undue delay (to be determined on a case-by-case basis and after consultation with the OPDC if appropriate).

7. **Step 7: Other Notification requirements**

7.1 DCU should consider whether, and seek advice as appropriate, as to whether there are any other relevant notification requirements are required (such as to the Gardaí etc.).

Timing: will depend on the Data Breach and the legal advice provided in relation to the Data Breach.

8. **Step 8: Further investigation**

8.1 Certain Data Breaches will require further detailed investigation after the initial investigation period, which may involve external IT, legal and other support, as appropriate to ascertain the full extent of the Data Breach, its causes, likely consequences and in order to effectively contain the breach. The effect of the Data Breach must be monitored and the risks re-evaluated throughout this period. It may be necessary to agree a phased notification program with the ODPC in these cases.

[9] If there is any delay beyond this 72-hour period, the notification must provide reasons for that delay

Timing: After initial 72 hrs (as appropriate).

9. **Step 9: Phased notification**

9.1 Once all relevant details have been obtained in the further investigation phase (see **Step 8** above), DCU should consider whether further notification to the ODPC is appropriate. For example, a further notification may state that the Data Breach has been effectively contained or that on further investigation, no Data Breach had actually occurred.

Timing: After initial notification (as appropriate).

10. **Step 10: Post-Breach investigation detailed review and recommendations**

10.1 Once the Data Breach has been contained and relevant engagement and/or ODPC investigations have concluded, DCU should conduct a post-Data Breach review including detailed recommendations to be implemented to reduce the recurrence of similar Data Breaches and to ensure that appropriate organisational and technical security measures are put in place.

Timing: Once the Data Breach has been contained.

11. **Step 11: Recording of Data Breach in Data Breach Log**

11.1 DCU is required to maintain a log of all Data Breaches and Data Incidents (including those not requiring notification to the ODPC and/or a communication to individuals). The log entry must specify at least: (i) the facts relating to the Data Breach or Data Incident; (ii) its effects; and; (iii) the remedial action taken by DCU. The Article 29 Working Party Guidelines also recommend that any decisions taken not to report a Data Incident to the ODPC and/or to communicate it to individuals should also be recorded, including the reasons for such decision (as part of the risk assessment undertaken at **Step 3** above and for accountability purposes).

Timing: Once the Data Breach has been contained and the investigation is complete.

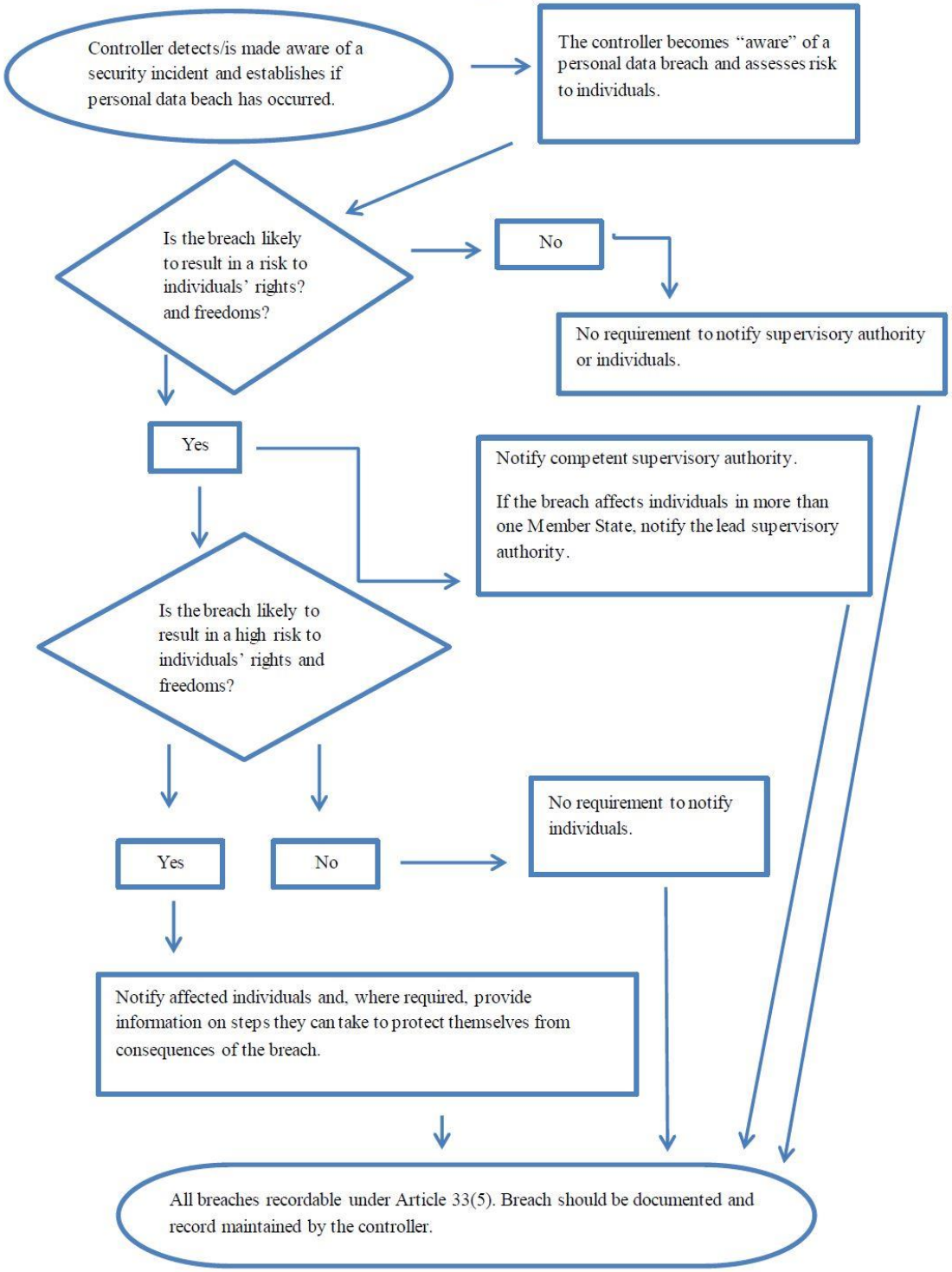
12. **Step 12: Implementation of recommendations**

12.1 The recommendations identified in **Step 10** should be implemented without delay. The recommendations may include revising and updating of data protection and IT security policies and/or technical measures.

Timing: Once the Post-Breach investigation (see **Step** 10) has been concluded.

Appendix 2 - Breach Notification Guidance

A. Flowchart showing notification requirements



B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or

functionality was to encrypt the data, and that there was no other malware present in the system.		consequences.	confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii. A website hosting company acting as a data processor identifies an error in the code which	As the processor, the website hosting company must notify its affected clients (the controllers) without	If there is likely no high risk to the individuals they do not need to be	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS

controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	notified.	Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Appendix 3

Data Breach Incident Report			
Incidents involving DCU as Data Controller			
1	Name of Department		
2	Name of Employee(s) involved		
3	Date and Time of Incident		
4	Date and Time Incident Reported		
5	Date and Time Incident Resolved		
Incidents involving Data Processors			
6	Name of Data Processor		
7	Name of Department which has oversight of the Data Processor		
8	Name of DCU employee dealing with the Data Processor		
9	Date of Incident		
10	Date and Time Incident Reported to DCU		
11	Date and Time Incident Resolved		
12	Has the Data Processor reported the incident to the Data Protection Commissioner?		
Summary Details of Incident			
13	Root Cause of Incident		
14	Summary of Actions Taken to Remediate		
15	Root Cause Corrective Action Plan		
16	Planned Date of Root Cause Remediation		
	Risk Assessment		Yes/No
17(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?	
17(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	
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.	
2) 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	

Signature of Data Protection Officer _____

Definitions

Sensitive Personal 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.