NOTIFICATION BREACH FORM

0. Data Breach Notification

Type of notification:

IDPC file reference number of previously notified breach:

Date of previous notification:

Brief description of previous notified breach:

1. About you

1.1 Contact Details

Organisation officially registered number:

Name of organisation:

Organisation registered address and any relevant contact details of the organisation:

Address of the establisment concerned with the breach:

Identity and contact details of the data protection officer or other contact point where more information can be obtained:

Name:
Surname:
Email Address:
Phone number:

Address of the location from which he/she carries out his/ her activities:

Reporting person contact details:

Email address:
Phone number:
Address:

Sector of activity of organisation:

1.2 Involvement of other entities outside the data controller for the service concerned by the data breach

Involvement of others outside the data controller for the service concerned by the data breach?

Contact details and role of the other entities involved

Contact Person:
Email Address:
Phone Number:
Address:

2. Timeline

Date of breach:

01-01-1970

Date of awareness of breach:

01-01-1970

Means of detection of breach:

Date of notification by processor:

01-01-1970

Reasons for late notification of breach:

Other comments on the timeline :

3. About the breach

	Confidentiality (where there is an unauthorised or accidental disclosure of, or access to, personal data)
	Integrity (where there is an unauthorised or accidental alteration of personal data)
	Availability (where there is an accidental or unauthorised loss of access to, or destruction of, personal data and data are not made available)

3.1 Nature of incident

	Paper lost or stolen or left in insecure location
	Device lost or stolen or left in insecure location
	Mail lost or opened
	Hacking
	Malware(e.g. Ransomware)
	Phishing
	Incorrect disposal of data
	E-waste (Personal data is still present on obsolete device)
	Unintended publication
	Data of wrong data subject shown
	Personal data sent to wrong recipient
	Verbal unauthorized disclosure of personal data
	Other

Summary of the incident that caused the personal data breach including the storage media involved:

3.2 Cause of breach:

	Internal non malicious
	Internal malicious
	External non malicious
	External malicious
	Unknown
	Other

Description of other cause of the breach:

4. Type of breached data

4.1 Regular data

	Data subject identity
	National identification number
	Contact details
	Identification Data
	Economic and financial data
	Official Documents

	Criminal convictions, offence or security measures
	Other
Description of other:	

4.2 Special categories of data

	Data revealing racial or ethnic origin
	Political Opinions
	Religous or philosophical beliefs
	Trade union membership
	Sex life data
	Health data
	Genetic data
	Biometric data

5. About the data subjects

	Employees/staff
	Current customers/subscribers
	Students
	Patients
	Minor/s
	Vulnerable individuals
	Former Customers
	Others
Description of other:	
Approximate number of data subjects concerned by the breach:	

6. About the measures in place BEFORE the breach

Did the organisation have technical and organizational measures to prevent an incident of this nature from occuring ?
If yes please indicate the measures:
Please provide extracts of any policies and procedures considered relevant to this indicent, and explain which of these related to such measures were implemented at the time this incident occured. Please provide the dates on which they were implemented and any other proof of implementation.
As the data controller, does the organisation provide it's staff with training on the requirements of the GDPR and of the Data Protection Act? If so, please provide any extracts relevant to the security incident here.
Please confirm if the training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?
As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in the processing operations that led to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

7. Consequences

7.1 Breach of Confidentiality

	The data involved in the breach was accessed by recipients other than authorised
	If the data was accessed by a third party, was there the consent of the data subject?
	Data may be linked with other information of the data subjects?
	The personal data may be further processed for other purposes different from the original

Other confidentiality consequence/s

7.2 Breach of integrity

	Data may have been modified and used even though it is no longer valid
	Data may have been modified into otherwise valid data and subsequently used for other purposes

Other integrity consequence/s

7.2 Breach of availability

	Loss of the ability to provide a critical sercive for the affected data
	Alteration of the ability to provide a critical service to the affected data

Other availability consequence/s

7.4 Physical, material or non-material damage or significant consequences to the data subjects

Nature of the potential impact for the data subject:
Description of other: (If applicable)
Description of the other impacts for the data subject:
Severity of the potential impacts:

8. Taking Action

8.1 Communication to data subjects

Information to the data subject:

Date of when information was given to data subjects if they already have been informed:

Date of future information of the data subjects if they have not been informed yet:

☐ **Unknown date of future information of the data subjects**

Reason for not informing data subject:

Means of communication used to inform data subject:

Content of the information delivered to the data subjects.
Attach sample copy of the communication delivered to the Data Subject

Public communication or similar measure

8.1.1 Description of measures allowing to skip information of data subjects

☐ **The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it**

☐ **The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise**

☐ **It would involve disproportionate effort to inform each data subject individually**

8.2 Measures taken to address the breach

Measures taken by the controller to address the breach

8.3 Cross border and other notifications

Is this notification a cross border notification?
Is this Office the Organisation's lead authority?
List of other Member States concerned by the breach
☐ **Has the breach been, or will it be notified, directly to other concerned Member States Supervisory Authority ?**
If YES, list the Member States Supervisory Authority to which the breach has been or will be notified
☐ **Has the breach been, or will it be notified, to Data Protection Authorites in third countries?**
If YES list of the other third country data protection authorities to which the breach has been or will be notified
☐ **Has the breach been, or will it be notified, to other Member States regulators (not related to Data Protection) because of other legal obligations (NIS directive eIDAS regulation)?**
If YES list of other Member State regulators to which the breach has been or will be notified