Office of the
Information and Data Protection Commissioner

REPORT A DATA BREACH - FIELDS MARKED IN RED ARE MANDATORY

0. Data breach notification	
a) Type of notification.	
b) IDPC file reference number of previously notified breach (applicable to complementary/amended notifications).	
c) Date of previous notification (applicable to complementary/amended notifications).	
d) Brief description of previous notified breach (applicable to complementary/amended notifications).	
1. About you	
1.1 Contact details - UNLESS PROVIDED IN A PRELIMINARY NOTIFICATION	
a) Organisation officially registered number.	
b) Name of the organisation.	
c) Organisation registered address and any relevant contact details of the organisation.	

d) Address of the establisment concerned with the breach.	
e) Identity and contact details of the data protection officer or other contact point where more information can be obtained (email address, phone number, address of the location from which he/she carries out his/ her activities).	
f) Reporting person's contact details (if different from the one above).	
g) Sector of activity of the organisation.	
1.2 Involvement of other entities outside the data controller for the service concerned by the data breach	
a) Involvement of others outside the data controller for the service concerned by the data breach? (joint controllers, processors, other autonomous data controllers).	
b) Contact details and role of the other enties involved (email address, phone number, address of the location from which they carry out their activities).	

2. Timeline	
a) Date of breach.	
b) Date of awareness of breach.	
c) Means of detection of breach (describe how you became aware of the breach).	
d) Date of notification by processor (if applicable).	
e) Reasons for late notification of breach (if breach is not notified within the 72 hours).	
f) Other comments on the time line (if required).	
3. About the breach - Tick as appropriate	
a) Confidentiality (where there is an unauthorised or accidental disclosure of, or access to, personal data).	☐
b) Integrity (where there is an unauthorised or accidental alteration of personal data).	☐
c) 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 the incident - Tick as appropriate	
a) Paper lost or stolen or left in insecure location.	☐
b) Device lost or stolen or left in insecure location.	☐
c) Mail lost or opened.	☐
d) Hacking.	☐
e) Malware (e.g. ransomwares).	☐
f) Phishing.	☐
g) Incorrect disposal of personal data.	☐
h) E-waste (personal data still present on obsolete device).	☐
i) Unintended publication.	☐
j) Data of wrong data subject shown.	☐
k) Personal data sent to wrong recipient.	☐
l) Verbal unauthorized disclosure of personal data.	☐
m) Other.	☐
n) Summary of the incident that caused the personal data breach including the storage media involved.	

3.2 Cause of the breach - Tick as appropriate	
a) Internal non malicious.	☐
b) Internal malicious.	☐
c) External non malicious.	☐
d) External malicious.	☐
e) Unknown.	☐
f) Other.	☐
g) Description of other cause of the breach (if applicable).	

4. Type of breached data - Tick as appropriate	
4.1 Regular data	
a) Data subject identity.	☐
b) National identification number.	☐
c) Contact details.	☐
d) Identification data.	☐
e) Economic and financial data.	☐

f) Official documents.	☐
g) Criminal convictions, offence or security measures.	☐
h) Other.	☐
i) Description of other (if required).	

4.2 Special categories of data	
a) Data revealing racial or ethnic origin.	☐
b) Political opinions.	☐
c) Religious or philosophical beliefs.	☐
d) Trade union membership.	☐
e) Sex life data.	☐
f) Health data.	☐
g) Genetic data.	☐
h) Biometric data.	☐

5. About the data subjects - Tick as appropriate	
a) Employees/staff.	☐
b) Current customers/subscribers.	☐
c) Students.	☐

d) Patients.	☐
e) Minor.	☐
f) Vulnerable individuals.	☐
g) Former customers and/or subscribers.	☐
h) Others.	☐
i) Description of other (if required).	
j) Approximate number of data subjects concerned by the breach.	
6. About the measures in place BEFORE the breach	
a) What technical and organizational measures did the organisation have in place to prevent an incident of this nature from occurring?	
b) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these related to such measures were implemented at the time this incident occurred. **Please provide the dates on which they were implemented and any other proof of implementation.**	

c) As the data controller, does the organisation provide its staff with training on the requirements of the GDPR and of the Data Protection Act? If so, please provide any extracts relevant to security incident here.	
d) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?	
e) 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 - Tick as appropriate	
7.1 Breach of confidentiality	
a) The data involved in the breach was accessed by recipients other than authorised.	☐
b) If the data was accessed by third party was there the consent of the Data Subject?	☐
c) Data may be linked with other information of the data subjects.	☐
d) The personal data may be further processed for other purposes different from the original ones.	☐
e) Other.	☐
f) Description of other confidentiality consequence.	

7.2 Breach of integrity	
a) Data may have been modified and used even though it is no longer valid.	☐
b) Data may have been modified into otherwise valid data and subsequently used for other purposes.	☐
c) Other.	☐
d) Description of other integrity consequence.	
7.3 Breach of availability	
a) Loss of the ability to provide a critical service for the affected data subjects.	☐
b) Alteration of the ability to provide a critical service to the affected data subjects.	☐
c) Other.	☐
d) Description of other availability consequence.	
7.4 Physical, material or non-material damage or significant consequences to the data subjects	
a) Nature of the potential impact for the data subject.	

b) Description of the other impacts for the data subject.	
c) Severity of the potential impacts.	

8. Taking action

8.1 Communication to data subjects

a) Information to data subjects.	
b) Date of when information was given to data subjects if they already have been informed.	
c) Date of future information of the data subjects if they have not been informed yet.	
d) Unknown date of future information of the data subjects.	☐
e) Reason for not informing data subject.	
f) Number of data subjects informed.	
g) Means of communication used to inform the data subject.	
h) Content of the information delivered to the data subjects Attach sample copy of the communication delivered to the Data Subject.	
i) Public communication or similar measure.	

8.1.1 Description of measures allowing to skip information of data subjects (tick as appropriate).	
a) 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.	☐
b) 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.	☐
c) It would involve disproportionate effort to inform each data subject individually.	☐
8.2 Measures taken to address the breach	
a) Measures taken by the controller to address the breach.	
8.3 Cross border and other notifications	
a) Is this notification a cross border notification?	
b) Is this Office the Organisation's lead authority?	
c) List of other Member States concerned by the breach.	

d) 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.	
e) 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.	
f) 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.	