

DATA BREACH MANAGEMENT FLOWCHART

Club members/
other
stakeholders

START

Incident is identified/
detected and reported

END

Analyses the
preliminary
information provided
by the source

Does the
incident classify
as a security
incident?

NO

The report
incident was a
false alarm

Log the incident
(or false alarm)
in the
incident register

YES

Does the
incident
involve
personal
data?

NO

Treat and respond
to the incident as per
the club incident
response policies

YES

Is the club
a 'Controller'
or 'Processor'
of the data
involved?

Log the incident
in the register

Inform the data
controller without
delay

END

CONTROLLER

Consult ICO guidance on how to
assess the severity of the incident
(i.e. based on the number and type of
personal data compromised)

Consult ICO guidance on whether to
inform ICO (within 72 hrs after
becoming aware of the incident) and/
or data subjects about the data
breach (i.e. this depends on the
severity of the incident, the controls
implemented and mitigations efforts)

Do you need
to notify
the ICO?

YES

Notify the ICO about the
data breach. Refer to ICO
guidance on what
information needs to be
provided pertaining to the
data breach

NO

Do you need
to notify
the affected data
subjects?

YES

Notify the data subjects
about the data breach.
Refer to ICO guidance on
what information needs to
be provided pertaining to
the data breach

NO

Consult ICO guidance (and/or
internal incident response
policies) and respond to the incident
in order to mitigate the risk

Information Security/Data Privacy Team (of a club)