St Bridgets C.E. School

GDPR Data Breach Incident Management Policy

Summary

Data breach reporting was only mandatory under the DPA98 if the breach was also covered by the Privacy and Electronic Communications Regulations 2011 (PECR covering any data security breach at telecoms providers or ISP). Otherwise, breach reporting was only considered advisory. Under GDPR, breach reporting is now mandatory and in many cases there is also an obligation to inform Data Subjects in specific circumstances as well.

Initial notification to the Supervising Authority (SA), normally the ICO, Information Commissioners Office, must come from the Data Controller **within 72 hours** of the discovery. Processors must notify any data breach to the Data Controller, and without delay.

A Data Breach Information Security Incident is an event, or chain of events, that could compromise the confidentiality, integrity or availability of information. Examples of information security incidents can include but are not limited to:

- *Potential and suspected disclosure of school information to unauthorised individuals.*
- *Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored.*
- *Disruption to systems and business processes.*
- *Inappropriate access controls allowing unauthorised use of information.*
- *Attempts to gain unauthorised access to computer systems, e.g. hacking.*
- *Records altered or deleted without authorisation by the data 'owner'.*
- *Virus or other malicious (suspected or actual) security attack on IT equipment systems or networks.*
- *'Blagging' offence where information is obtained by deception.*
- *Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing school sensitive information left unlocked in accessible area.*
- *Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.*
- *Human error such as emailing data by mistake.*
- *Covert or unauthorised recording of meetings and presentations.*
- *Damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges.*
- *Deliberate leaking of information.*

- *Insider fraud.*

Data Breach Transparency

The Data Controller is obliged to notify both the Data Protection Officer (DPO) and the Data Subjects about data breaches in certain circumstances.

1) If a data breach is likely to result in harm to the Data Subjects or it is likely to result in a risk to the rights or freedoms of the individuals, then the Data Controller must report this to the Supervisory Authority(ICO) in less the 72 hours of the breach being discovered.

2) Where there is a high risk, Data Subjects need to be informed immediately.
    a. If possible directly
    b. Otherwise, the controller should consult the Supervisory Authority to determine the best way forward

3) We shall ensure that any incident that could potentially affect the security of information is identified and managed appropriately.
    - The incident shall be reported to the DPO via telephone
    - The process shall be simple, clear and easy to follow. It should follow the below guidelines:
    - Use a single point of contact for telephone reporting of incidents with internal and external telephone number
    - We use a simple reporting form for incident reporting and capture the required information, which is suggested to be no more than:
    - Date
    - Location
    - Short summary of what occurred
    - Type of incident – e.g. e-mail, lost USB device or paper
    - Contact details for obtaining further information
    - The DPO within St Bridgets C.E. School is responsible for reporting security incidents. All personnel shall be made aware of what constitutes an incident and how to report them to the DPO via the Education and Awareness process.
    - Information security incident management shall be incorporated into all third party and outsourced contracts.

Ways to Minimise Breach Impact

The Data Controllers and Processors are required to put in place appropriate technical and organisational measures to ensure a level of security proportional to the risk. This can be done in the following ways:

- Including the ability to restore availability and access personal data in a timely fashion in the event of an incident
- The regular testing and evaluation of technical and organisational measures is intended to ensure security of data processing
- Pseudonymisation and encryption
- Guaranteeing confidentiality, integrity, availability, and resilience of processing systems and service

Impact of Data Breaches

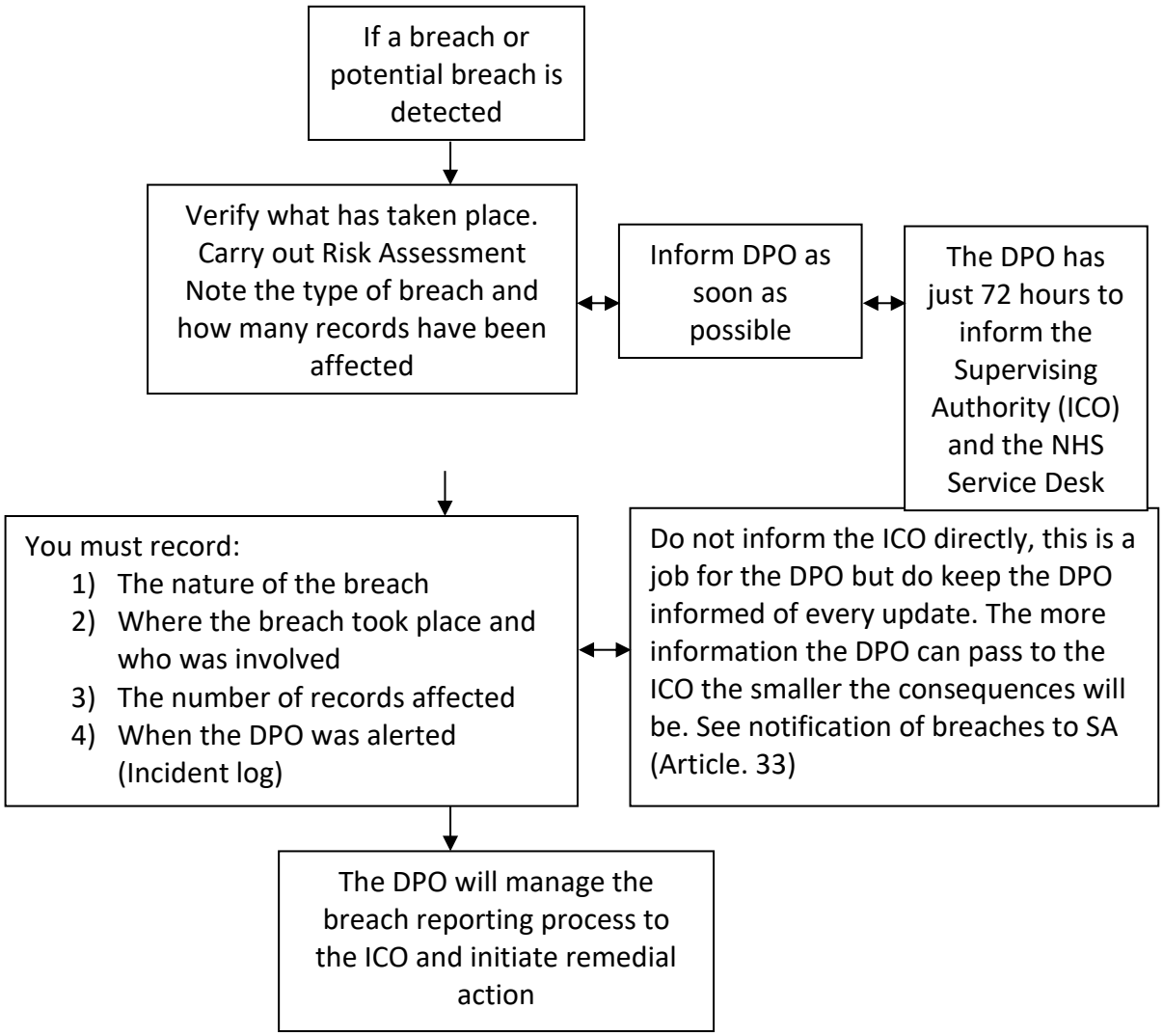
- If the data subject's rights are breached they can sue you in your country, or theirs, for material and non-material damage – there is no upper limit set by GDPR. They can also sue individually and or collectively (class actions)
- Administrative fines will be levied by the supervisory authority for data breaches

St Bridgets C.E. School

GDPR Data Breach Incident Management Policy

It is a legal requirement that the Data Processor only performs processing as defined by the Data Controller.

This is a flow diagram of the data security breaches reporting process adopted by St Bridgets C.E. School.



Make sure the Data Protection Officer is kept informed at all stages and is kept up to date throughout the whole process; the DPO will be able to advise and assist if required.