Data Breach Policy

Template GDPR-115

(V1.02)

Version: 1.02 Release date: August 2020 Review date: August 2021
Authorised by: Martin Long
Location: Shared policy, please contact gdpr@turniton.co.uk

GDPR Data Breaches

These guidelines have been summarised from Article 29 Data Protection Working Party revised and adopted on 6th February 2018, titled "Guidelines on Personal Data Breach notification under regulation 2016/679".

What is a personal data breach?

'A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.'

A data breach can include digital, verbal and paper-based records.

For example, loss of personal data can include where a device such as a laptop has been lost or stolen. A further loss may be where the only copy of a set of personal data has been encrypted by ransomware.

Types of data breach

Breaches can be categorised to the following three well-known information security principles:

- **Confidentiality** breach – where there is an unauthorised or accidental disclosure of, or access to personal data;
- **Integrity** breach – where there is an unauthorised or accidental alternation of personal data;
- **Availability** breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data."

The CIA (Confidentiality, Integrity and Availability) security triangle is an important security concept because all security controls, mechanisms, and safeguards are implemented to provide one or more of these protection types. All risks, threats, and vulnerabilities are measured for their potential capability to compromise one or all the CIA triad principles. This triad is the basis for creating a holistic security plan to protect all your organization's critical and sensitive assets.

For example, loss of availability includes where data has been deleted accidentally or where securely encrypted data cannot be accessed due to a lost encryption key. Another loss of availability may also occur where there has been a significant disruption of service due to a power failure or a denial of service attack rendering personal data unavailable.

Examples of personal data breaches and who to notify (guidance only)

The following non-exhaustive examples will assist controllers and processors 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.

Data processors must notify the data controller if a data breach occurs. Data processors must have a data breach reporting process in place.

Example	Notify the Supervisory Authority	Notify the Data Subject	Notes and recomendations
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 is 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 functionality was to encrypt the data, and that there was no other malware present in the system.	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 consequences.	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 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 controls user	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay.	If there is likely no high risk to the individuals, they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations

authorisation. The effect of the flaw means that any user can access the account details of any other user.	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.		(e.g. under the NIS 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 is 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 is 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.

Data breach Process – Response Flow Example

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO as the relevant supervisory authority. Not every data breach will be so severe that it requires reporting to the ICO. In the first instance the data breach should be reported to the DPO who will support in assessing it needs to be esculated. You must do this within 72 hours of becoming aware of the breach, where feasible. This is a significant undertaking for any organization and involves the development and provisioning of a comprehensive containment plan.

Simple containment plan example:

1. Carry out a thorough investigation
2. Inform regulators and impacted individuals of the breach
3. Identify what personal data has been impacted and how
4. Draft a comprehensive containment plan

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

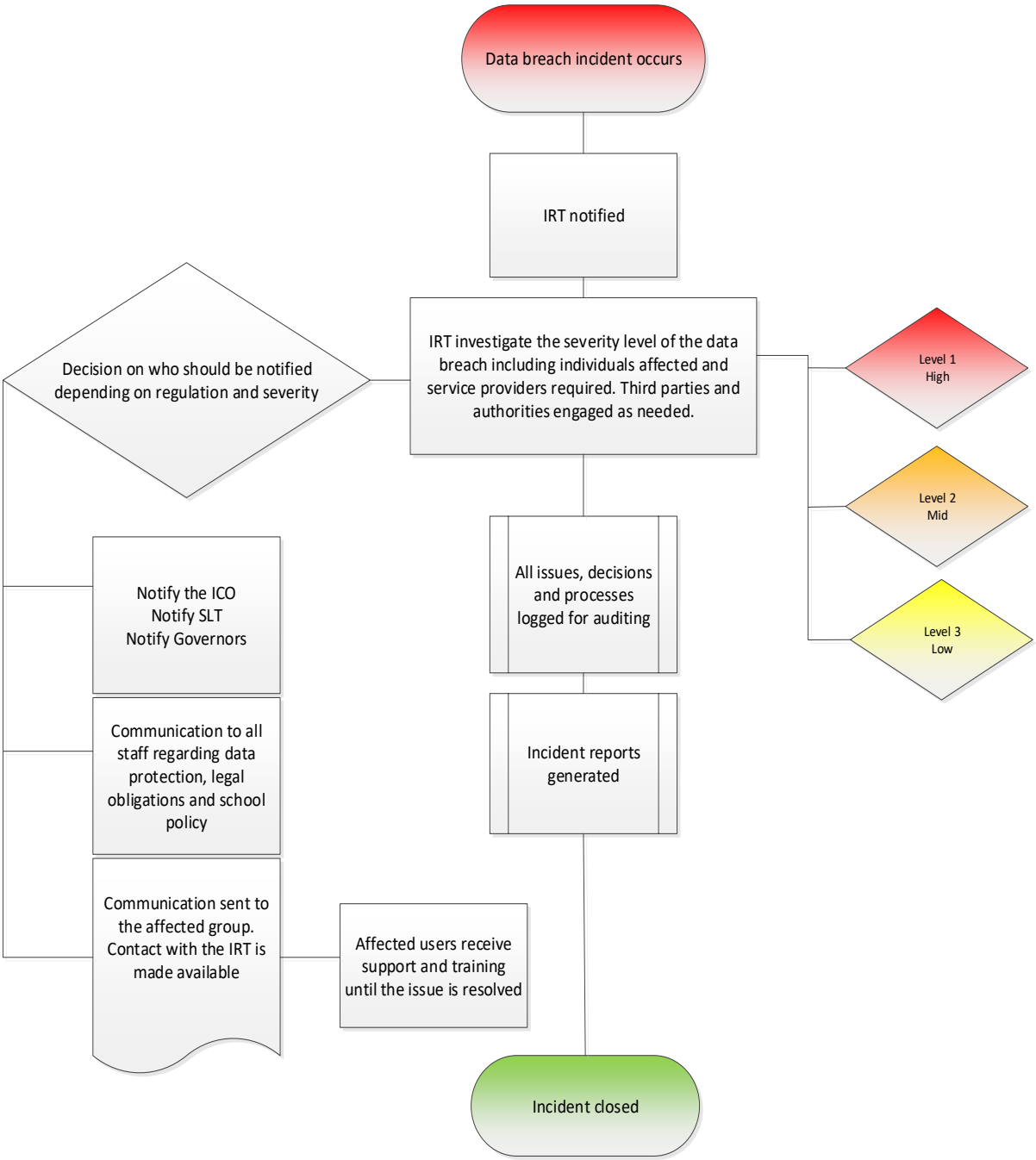
The school should ensure it has a robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

It is good practice to have a data breach incident response team made up of the following roles, the list below is just for reference and should be amended to suit the staff structure in school.

Role	Involvement
Head Teacher	
School Manager	
Admin Manager	
Bursar	
School Business Manager	
School Data Manager	
MIS Manager	
ICT Manager\Network Manager	
Governor (with GDPR responsibility)	
Data Protection Officer (internal or External)	

The following flow diagram is an example of good practice when dealing with a data breach.



Associated Documents

- GDPR 134 - School data protection contact information poster PDF.
- GDPR 127 – Data Breach Guidance for School Staff

Policy update information (policy number GDPR-115)

This policy is reviewed annually and updated in line with data protection legislation.

Policy review information

Review date	Reviewed by
02-05-2018	turn IT on
08-08-2019	turn IT on
01-08-2020	turn IT on

Policy update information

Review date	Revision	Description of change	By
02-05-2018	1.00	Draft release	turn IT on
03-05-2018	1.00	Full release	turn IT on
08-08-2019	1.01	Full release	turn IT on
01-08-2020	1.01	Full release review	turn IT on