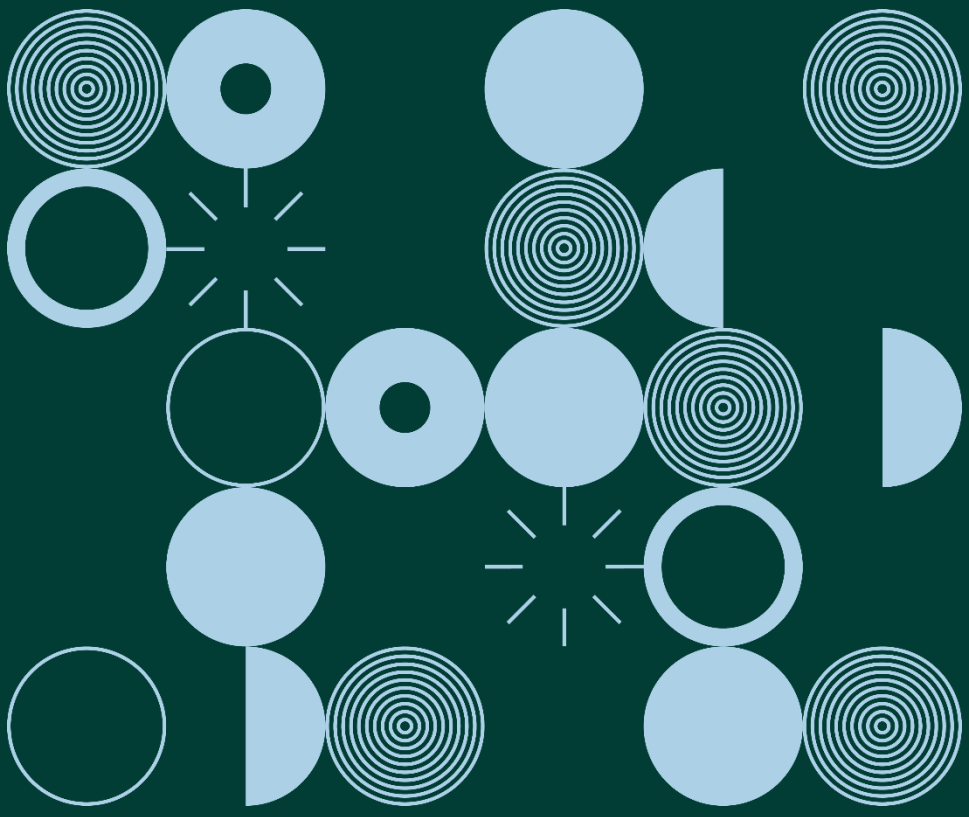
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

A Quick Guide to GDPR Breach Notifications

August 2019



This quick guide is intended primarily to help controllers better **understand their obligations** regarding notification and communication requirements – covering both notification **to the DPC**, but also communication **to data subjects**, where applicable.

The key questions covered below should give an overview of the GDPR breach notification regime, to assist controllers understand their basic obligations under this regime. Information on breach notifications, as well as the link to the **breach notification form**, can also be found on the breach notification page of the DPC's website.

There are **two primary obligations** on controllers under this regime: **(a)** notification of any personal data breach ***to the DPC***, **unless** they can demonstrate it is **unlikely to result in a risk** to data subjects; and **(b)** communication of that breach ***to data subjects***, where the breach is **likely to result in a high risk** to data subjects. It is of utmost importance that controllers understand and comply with *both* of these obligations.

Controllers must also ensure, in line with the **accountability** principle set out in Article 5(2) GDPR, as well as the requirements of Article 33(5), that they **document any and all personal data breaches**, including the facts relating to the personal data breach, its effects and the remedial action(s) taken – this will enable them to demonstrate compliance with the data breach notification regime to the DPC.

The DPC also recommends that controllers read the detailed guidance provided on topics including the definition of a personal data breach, assessing risk notification and communication requirements, and accountability, found in the Article 29 Working Party 'guidelines on personal data breach notification'.[1]

For the separate rules regarding breach notifications under the ePrivacy Regulations (SI 336/2011), concerning providers of publicly available electronic communications networks or services to report a breach, see the DPC's guidance on telecoms/ISP providers data security breach notifications.

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.[2] The term 'personal data' means **any information** concerning or relating to an **identified or identifiable** individual. Controllers should be aware that a personal data breach can cover a lot more than just 'losing' personal data. Personal data breaches include incidents

[1] The Article 29 Working Party has since been replaced by the European Data Protection Board (EDPB), which has endorsed these guidelines.
[2] See Article 4(12) GDPR for the definition of 'personal data breach'.

that are the result of both **accidents** (such as sending an email to the wrong recipient) as well as **deliberate** acts (such as phishing attacks to gain access to customer data).

A personal data breach occurs in incidents where personal data are lost, destroyed, corrupted, or illegitimately disclosed. This includes situations such as where someone accesses personal data or passes them on **without proper authorisation**, or where personal data are **rendered unavailable** through encryption by ransomware, or accidental loss or destruction.

In short, a personal data breach is a security incident that **negatively impacts** the **confidentiality**, **integrity**, or **availability** of personal data; meaning that the controller is **unable to ensure compliance** with the principles relating to the processing of personal data as outlined in Article 5 GDPR. Whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

When does a controller have to notify the DPC of a data breach under the GDPR?

A controller is obliged to **notify the DPC** of any personal data breach that has occurred, ***unless*** they are able to demonstrate that the personal data breach is **'unlikely to result in a risk** to the rights and freedoms of natural persons'.[3] This means that the **default position** for controllers is that all data breaches **should be notified** to the DPC, except for those where the controller has assessed the breach as unlikely to present any risk to data subjects, and the controller can show why they reached this conclusion. In any event, for **all breaches** – even those that are not notified to the DPC, on the basis that they have been assessed as being unlikely to result in a risk – controllers must **record at least the basic details** of the breach, the assessment thereof, its effects, and the steps taken in response, as required by Article 33(5) GDPR.

Where a controller becomes aware of a personal data breach which may result in any risk to the rights and freedoms of data subjects, they must make a notification to the **DPC 'without undue delay'**; where feasible, **not later than 72 hours** from when the controller became aware of the breach. A controller should be regarded as having become 'aware' when they have a reasonable degree of certainty that a security incident has occurred and compromised personal data.

In order to comply with their obligations under the Article 5(2) **principle of accountability** as well as the requirement to **record relevant information** under Article 33(5), controllers should be able to **demonstrate to the DPC when and how they**

[3] See Recital 85 and Article 33(1) GDPR

became aware of a personal data breach. The DPC recommends that controllers, as part of their internal breach procedures, have a system in place for recording how and when they become aware of personal data breaches and how they assessed the potential risk posed by the breach.

If a controller **fails to notify** the DPC within 72 hours, they must **provide a reason** for the delay along with the late notification to the DPC, and may be in breach of their obligation to notify without undue delay – unless the reason given is sufficient to justify the delay. Where it is not possible to provide all of the relevant information to the DPC within the 72 hour period, the **initial notification** should be lodged and then **information may be provided in phases**, as long as it is done **without undue delay** and provided the controller can give reasons for the delay in accordance with Article 33(1).

Similarly, per Article 33(2) GDPR, a **data processor**, processing personal data on the direction of a data controller, **must notify their data controller** of any personal data breach **without undue delay** after becoming aware of the breach. This is of key importance in enabling the controller to comply with their notification obligations. The requirements on breach reporting should also be **detailed in the contract** between the controller and processor, as required under Article 28 GDPR.

What should a notification to the DPC contain?

A notification of a personal data breach by a controller to the DPC (which can be done through the breach notification form on the DPC's website) must at least:[4]

a) describe the **nature of the personal data breach**, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the **name and contact details** of the **data protection officer** (DPO) or other **contact point** where more information can be obtained;

c) describe the **likely consequences** of the personal data breach; and

d) describe the **measures taken or proposed** to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

To assist the DPC in assessing compliance with the requirement to notify 'without undue delay', as well as the principle of **accountability**, the DPC recommends that controllers

[4] See Article 33(3) GDPR

include, in their initial notification, **information on how and when they become aware** of the personal data breach, along with an explanation for any delay, if applicable.

As mentioned above, where, but only in so far as, it is not possible to provide all of the required the information at the same time, the information may be provided in phases, as long as it is done without undue further delay.[5]

When does a controller have to communicate a personal data breach to data subjects?

Controllers are also obliged to communicate to the data subject a personal data breach, **'without undue delay'**, where that personal data breach is **'likely to result in a high risk to the rights and freedoms** of the natural person'.[6]

This obligation **is in addition and separate to the obligation to notify the DPC** of personal data breaches, and sets a **higher threshold** before this obligation to inform the data subject applies. The intention behind this requirement is to **ensure that data subjects can take the necessary precautions** where incidents have occurred which are likely to result in a high risk to them.

Such communications to data subjects should be made **without delay**, where appropriate in close cooperation with the DPC, and in line with guidance provided by the DPC or by other relevant authorities such as law-enforcement authorities. In cases where there is a need to mitigate an immediate risk to data subjects, prompt communication with data subjects will be necessary.

There are, however, circumstances where controllers **may not be required** to communicate information relating to a data breach to data subjects, even where the breach may be likely to result in a high risk to the rights and freedoms of the natural person. These circumstances are where any of the **following conditions** are met:[7]

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 measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

[5] See Article 33(4) GDPR
[6] See Recital 86 and Article 34(1) GDPR
[7] See Article 34(3) GDPR

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;** or

c) it **would involve disproportionate effort**. In such a case, however, controllers **must still ensure**, by way of a public communication or similar measure that the **data subjects are informed** in an equally effective manner.

What should a communication to a data subject contain?

The communication of a personal data breach to the affected data subject(s) should **describe the nature** of the personal data breach as well as **recommendations** for the data subject concerned to mitigate potential adverse effects of the breach.

This communication to the data subject should describe in **clear and plain language** the nature of the personal data breach and should include at least the following information (as required by Article 34(2) GDPR):

- the **name and contact details** of the **data protection officer** or other **contact point** where more information can be obtained;
- a description of **the likely consequences** of the personal data breach; and
- a description of the **measures taken or proposed** to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Can controllers notify data subjects of a breach even if the risk is not assessed as high?

Whilst there is **no obligation** on controllers to communicate a personal data breach to affected data subjects where it is not likely to result in a high risk to them, controllers are nevertheless **free to communicate** a breach to data subjects where it may still be in their **interests or appropriate** to do so anyway, **in the context** of that particular breach.