

Quick Guide to GDPR Breach Notifications



Co-funded by the Rights, Equality and Citizenship
Programme of the European Union (2014-2020)

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS,
EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT
N°874524.



Quick Guide to GDPR Breach Notifications

This quick guide is intended primarily to help SMEs better understand their obligations regarding notification and communication requirements – covering both notification to the relevant Data Protection Authority (DPA), 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 SMEs understand their basic obligations under this regime.

There are two primary obligations on SMEs under this regime: (a) notification of any personal data breach to the relevant DPA, 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 SMEs understand and comply with both of these obligations.

SMEs 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 relevant DPA.

It is recommended that SMEs 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

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. SMEs should be aware that a personal data breach can cover a lot more than just ‘losing’ personal data. Personal data breaches include incidents 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 SME is unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 GDPR.

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’.

Whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

When does an SME have to notify the DPA of a data breach under the GDPR?

An SME is obliged to notify the relevant DPA 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 SMEs is that all data breaches should be notified to the relevant DPA, except for those where the SME has assessed the breach as unlikely to present any risk to data subjects, and the SME can show why they reached this conclusion. In any event, for all breaches – even those that are not notified to a DPA, on the basis that they have been assessed as being unlikely to result in a risk – SMEs 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 an SME 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 relevant DPA 'without undue delay'; where feasible, not later than 72 hours from when the SME became aware of the breach. An SME 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), SMEs should be able to demonstrate to the relevant DPA when and how they became aware of a personal data breach. It is recommended that SMEs, 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 an SME fails to notify the relevant DPA within 72 hours, they must provide a reason for the delay along with the late notification to the DPA, 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 DPA 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 SME 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 an SME, must notify the SME of any personal data breach without undue delay after becoming aware of the breach. This is of key importance in enabling the SME to comply with their notification obligations. The requirements on breach reporting should also be detailed in the contract between the SME and processor, as required under Article 28 GDPR.

³ See Recital 85 and Article 33(1) GDPR

What should a notification to a DPA contain?

A notification of a personal data breach by a SME to the relevant DPA 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 SME to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

To assist the DPA in assessing compliance with the requirement to notify 'without undue delay', as well as the principle of accountability, it is recommended that SMEs 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 an SME have to communicate a personal data breach to data subjects?

SMEs 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 relevant DPA 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 relevant DPA. 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 SMEs 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

⁴ See Article 33(3) GDPR

⁵ See Article 33(4) GDPR

⁶ See Recital 86 and Article 34(1) GDPR

⁷ See Article 34(3) GDPR

a) the SME 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;

b) the SME 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, SMEs 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 SME to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

Whilst there is no obligation on SMEs to communicate a personal data breach to affected data subjects where it is not likely to result in a high risk to them, SMEs 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.