privacy perfect

PrivacyPerfect White Paper series (4)

How to prepare for and handle data breach notifications

This whitepaper describes the steps your organisation can take in order to prepare for and handle data breach notifications under the GDPR. Articles 33 and 34 specify the cases in which your organisation has to register a breach, notify it to the supervisory authority or communicate it to the data subject (the natural persons affected by the breach).

Preparation

To introduce an internal breach notification procedure, it is first important to understand what a breach amounts to under the GDPR. Article 4, for instance, states that a personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

A procedure for breach notifications requires the firm collaboration of various areas in your organisation. Usually, the data breach procedure is embedded in or aligned with the security incident procedure. IT security specialists are necessary to assess the impact of an incident and follow up on that. Then, privacy specialists will help find out whether personal data are involved and which next steps should be taken.

Because notification of data breaches is time-sensitive (a breach must be notified within 72 hours after your organisation has become aware of it), the procedure should be as clear as possible. A customer contact center (or similar) can be used as an internal notification point. They may be instructed to ask additional questions to qualify the notification for further assessment by a centrally-appointed security or privacy professional.

If the incident is serious enough, it can be escalated to a data breach response team. Such a team can be composed of:

- Two top-level privacy specialists
- A top-level security officer
- Head of the customer contact center
- A top-level communication specialist

This team should have authority to make the necessary decisions when a (possible) data breach occurs. Otherwise, the managing director of the relevant unit should also be included in the team. In addition, there should be clear replacement procedures if any of these are on leave and an up-to-date conference call number for a first meeting by phone if a meeting in person is not possible.

Four steps in case of breach

We describe here the steps that can be taken once a notification has reached the data breach response team. First, investigate the breach; second, determine the need for notification. Third, notify the supervisory authority, where applicable; and fourth, notify the data subject if needed.

1. Investigate the breach

The GDPR emphasises the importance of identifying a breach, assessing the risk to individuals and notifying the breach. An internal breach notification needs to be followed across the 'notification funnel'. In order to do so, the data controller needs to know the following:

- An identifier for identification purposes internally and (possibly) externally;
- Where possible, a description of the issue and its consequences;
- The start and end date and times, the moment when your organisation became aware of the breach. Note that, as a controller, your organisation is supposed to be aware of any breach known by a processor or sub-processor of your organisation. So make sure your organisation contracts its (sub)processors in such a way that they notify your organisation in time too. And, of course, set up an effective procedure that reflects the agreement.

In order to further investigate the scope of the breach, one needs to know which stakeholders are involved:

- Controllers: if various controllers act as joint controllers, according to the EDPB, they should have contractual clauses in place that determine which controller takes the lead in the investigation and notification;
- (Sub)processors: Article 28(3)(f) states that the processor has the obligation to assist the controller in ensuring compliance with the obligations pursuant to Article 32 to 36. Under Article 33(2), processors must notify the controller "without undue delay";
- The data subject categories affected as well as the estimated total number of individual data subjects concerned;
- The departments in your organisation that are involved;
- Third parties involved (not processors).

Subsequently, your organisation needs to know what personal data categories and data sources are affected:

- Personal data categories and personal data items involved in the breach (e.g. check whether special personal data items are involved);
- Data sources, such as local software, local databases, local storage, SaaS solutions and cloud storage;
- The estimated number of personal data records

affected (usually the number of personal data items multiplied by the number of data subjects).

Finally, your organisation has to determine the nature and consequences of the breach and the measures to counter its effects:

- Nature of the breach: usually reading, copying, alteration, deletion, unavailability, unauthorised disclosure, or theft;
- Potential consequences of the breach for data subjects, e.g. reputational damage, discrimination, financial loss, fraud, health damage, identity theft, limitation of rights or loss of confidentiality (many other physical, material or non-material consequences are possible);
- The measures your organisation takes to counter the adverse effects of the breach, in addition to the technical and organisational measures that should already be in place in order to protect personal data. The new counter measures may be manifold. For example, in case of a breach of credit card data, your organisation should (probably) notify the issuing organisation as soon as possible to block the affected cards.

Having inventoried the scope of the breach, you can go to the next step: assessing the need for external notification.

2. Determine the need for notification

In order to determine the need for notification, you must assess the likelihood and severity of risks to the rights and freedoms of natural persons. This assessment should involve every aspect of the breach, including the type of breach, sensitivity of personal data involved, and identification of affected individuals. Below, we list the conditions under which your organisation has to notify a breach, accompanied by practical examples of such situations, taken from the EDPB Guidelines.

When it comes to determining the need for notification, Articles 33 and 34 distinguish three types of cases:

- A breach is unlikely to result in a risk to the rights a freedoms of natural persons (Article 33(1) GDPR). In this case, no notification is needed but the breach should be registered within your organisation for accountability purposes.

Breaches concerning publicly-available personal data need not be notified because their disclosure does not constitute a (new) risk to the individual. Also, the loss of a securely-encrypted mobile device may, in some circumstances, not require notification. If the copy of the personal data is not accessible by the attacker and the encryption key remains secure with the controller, then a notification to the supervisory authority or the data subject is not necessary.

- A breach is likely to result in a risk to the rights and freedoms of natural persons (Article 33(1) GDPR). In this case, a notification to the supervisory authority is necessary.

A website hosting company (a data processor) has found an error in the code which regulates user authorisation. The problem implies that any user can access the account details of a different user. In this case, the processor must notify the controllers without undue delay, and after conducting their own investigations, the controllers must notify the supervisory authority. If there's no high risk to the data subject, they do not need to be notified.

- A breach is likely to result in a high risk to the rights and freedoms of natural persons. In this case, in addition to the notification to the supervisory authority, the data subject also needs to be notified (Article 34(1) GDPR).

Due to a cyber-attack, medical records in a hospital are unavailable for 45 hours, which poses an immediate threat to patients being treated there. This should be reported by the hospital to the supervisory authority and to the affected individuals.

The third case is said to be subject to three exceptions (Article 34(3) GDPR):

- The personal data have been rendered in such a manner that they are unintelligible. This means that the controller implemented all the necessary technical and organisational measures which ensure nobody can access the personal data without authorisation (e.g. because of the use of effective encryption);
- The high risk is unlikely to materialise because of subsequent measures (this is good proof of the existence of an efficient incident response plan);
- The notification would require disproportionate effort. This involves situations where it is not possible to identify all the individuals that are affected by the breach. For example, a fire occurred in the archive of a hospital and all the documents containing personal data are lost. In this case, a public statement can be more effective than trying to contact individual data subjects.

Please take into account that the supervisory authority might decide on the necessity of a data subject notification. If your organisation decides to notify the supervisory authority and not (yet) the data subject, the supervisory authority can still interpret the term 'high risk' and the exceptions differently and force your organisation to notify the data subject.

Of course, no organisation likes to 'admit' to the general public that they've had a breach (which will usually be the consequence of notifying individual data subjects). However, it is better to be safe than sorry. Remember the Yahoo case in 2014 in which the breach of 500M user accounts became known to the general public only in 2016? This is a perfect example of how concealing a data breach might cause greater reputation damage.

3. Notify the supervisory authority

Article 33 describes the notifications to the lead supervisory authority, which are usually sent through a web form published on the website of the relevant supervisory authority. According to this Article, a notification must contain:

- The nature of the breach, including, where possible:

  - The categories and approximate number of data subjects involved;
  - The categories of personal data and the number of personal data records concerned;
- The name and contact details of the data protection officer or other contact person;
- A description of the likely consequences of the breach for the data subject;
- Measures taken to address the consequences of the data breach, including mitigating measures to counter adverse effects for the data subject;

If the notification is not made within 72 hours after the controller became aware of the breach, the reasons for the delay should be provided.

4. Notify the data subject

Article 34(2) requires that the content of a data breach communication, as detailed below, be expressed in clear and plain language:

- The name and contact details of the data protection officer or other contact person;
- A description of the likely consequences of the breach for the data subject;
- Measures taken to address the consequences of the data breach, including mitigating measures against the adverse effects for the data subject;

If the notification is not made within 72 hours after the controller became aware of the breach, the reasons for the delay should be provided.

The above requirements mirror those of Article 33(3), except for the nature of the breach. This is strange, as one might expect the data subject to be informed about the categories of personal data affected, so that the data subject can act upon that (e.g. by changing a password that was leaked).

Notifications must be addressed to the data subject; in other words, the notification should be specific and it should not be combined with regular newsletters or standard messages. The EPDB Guidelines on Personal data breach notification under Regulation 2016/679 suggest that the communication be made in a transparent manner, e.g. a direct message, postal communication or prominent website banner. It further suggests to controllers that they choose ways to maximise the chance of properly communicating information to all affected individuals.

It is important to realise that the supervisory authority may have more requirements than those literally stated in the GDPR. Although Articles 33 and 34 do not allow for deviations in national legislation, the supervisory authorities are free to ask what they deem necessary. The supervisory authorities should provide a way to notify breaches to them, such as (web) forms. In practice, this might result in more questions being asked than those which are included in Articles 33 and 34.

Conclusion

It is important to have an established procedure for investigating and notifying breaches. As described in this whitepaper, once a breach is brought to your attention, if your organisation is the controller, it will only have a short time to carry out a first investigation. That's why it's advisable to establish a data breach response team in anticipation of a possible breach, and if a breach actually occurs, do follow the four steps above: investigate the breach, determine the need for notification, and where applicable, notify the supervisory authority and notify the data subject.

About PrivacyPerfect

PrivacyPerfect is an easy-to-use GDPR compliance toolkit. It provides a natural flow between the three administrations required by the new regulation: data protection impact assessments, processing activities (including transfers), and data breaches. The user-friendly tool allows for maintaining all necessary privacy records and leading them through workflows to meet the needs of both SMEs and large companies.

More info

Do you have any questions regarding this whitepaper or would you like to get more information about the PrivacyPerfect tool?
Please visit www.privacyperfect.com or contact us via info@privacyperfect.com.

Transparency

Compliance

Accountability

Do you want to know what our clients say about us?

Ask for a webinar

Contact us

info@privacyperfect.com

+31 10 310 07 40