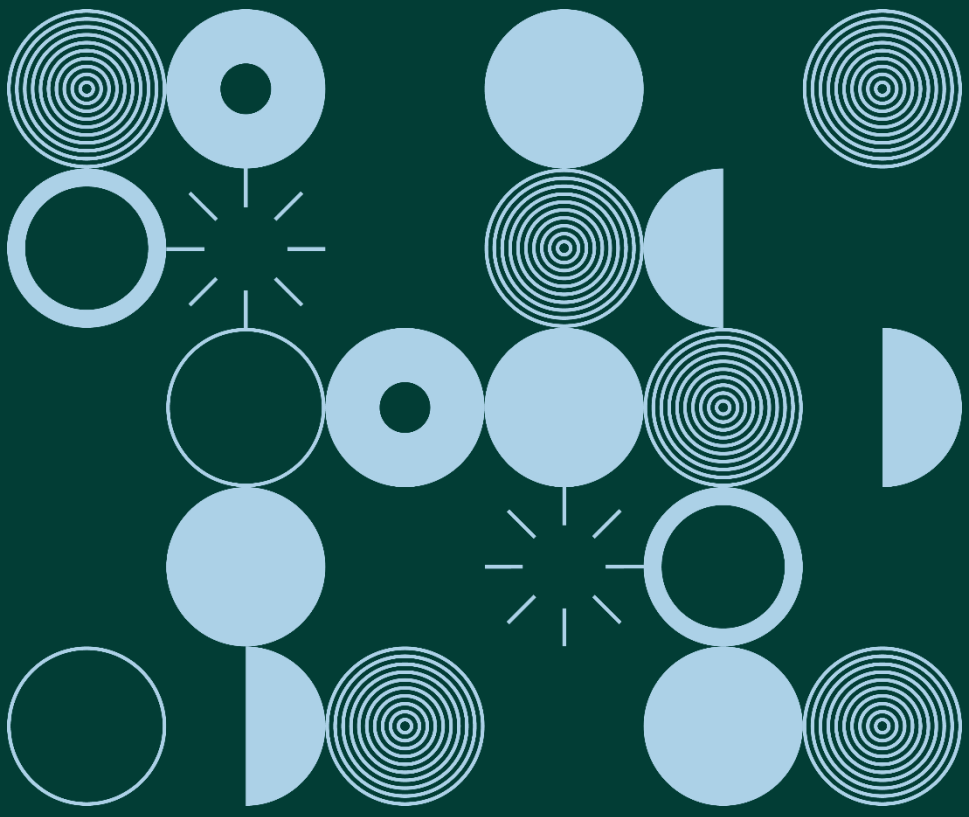
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

A Practical Guide to Personal Data Breach Notifications under the GDPR

October 2019



A Practical Guide to Personal Data Breach Notifications under the GDPR

Contents

Introduction

This guidance note is intended primarily to give data controllers some practical advice on how to handle data breaches and navigate the mandatory data breach notification regime, which was introduced by the General Data Protection Regulation (GDPR) in May 2018. This guidance may also be of assistance to the public at large where concerns arise regarding compliance with the breach notification regime.

This guidance was produced following an analysis of the trends and statistics observed by the Data Protection Commission (DPC) during the first year of the GDPR mandatory breach reporting regime. The statistics and trends analysed covered data breach notifications received in the first year since 25 May 2018, the details of which are set out in a separate information note on breaches trends and statistics published by the DPC.

The DPC's Breach Assessment Unit undertook an analysis of breach notifications received from various areas within the public and private sector, including: banking and finance; insurance; telecommunications; healthcare; and law enforcement.

Some of the trends and issues identified by the Breach Assessment Unit whilst conducting these reviews and from the handling of breach notifications included: late notifications; difficulty in assessing risk ratings; failure to communicate a breach to data subjects, where applicable; repeat breach notifications; and inadequate reporting.

The guidance below has been designed to help controllers better understand their obligations with regards to notification and communication requirements – covering notification to the DPC, and also communication to data subjects, where applicable – and to clarify some of the most common issues encountered during the first year of the GDPR data breach notification regime.

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]

[1] The Article 29 Working Party has since been replaced by the European Data Protection Board (EDPB), which has endorsed these guidelines.

Overview of Breach Notification Regime

Before moving on to the practical guidance on common issues encountered in the context of data breach notifications, it is worth setting out an overview of the breach notification regime itself, in order to ensure that all controllers are aware of their basic obligations under this regime. Controllers can also find information on breach notifications, as well as the link to the breach notification form, on the breach notification page of the DPC's website.

There are two primary obligations on controllers under this new regime: **(a)** notification of any personal data breach *to the DPC*, unless the controller can demonstrate that the breach 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 the utmost importance that controllers understand and comply with *both* of these obligations.

A further key obligation of controllers in the context of a personal data breach arises out of the principle of accountability, set out in Article 5(2) GDPR, as well as the requirements of Article 33(5). Under Article 5(2) GDPR it is the responsibility of controllers to demonstrate their compliance with the other principles of data protection, including the principle of 'integrity and confidentiality', and under Article 33(5) controllers must document relevant information to enable the DPC to verify their compliance with their obligations under Article 33.

Controllers must document all personal data breaches, including the facts relating to the personal data breach, when and how they became aware of the 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. This documentation should include the details of how the controller assessed the likelihood of risk and severity of risk to the rights and freedoms of the data subject.

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. Personal data breaches include incidents that are the result of both accidents (such as sending an email to the wrong recipient) and deliberate acts (such as phishing attacks to gain access to customer data).

[2] See Article 4(12) GDPR for the definition of 'personal data breach'.

A personal data breach occurs in incidents where personal data are lost, destroyed, corrupted, or illegitimately disclosed. This includes, for example, situations 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, with the consequence that the controller is unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 GDPR. It is important to note that 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 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 being 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 that may result in any risk to the rights and freedoms of data subjects, they must make a notification to the DPC 'without undue delay', or 'as soon as possible',[4] and, 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' of the breach when they have a reasonable degree of certainty that a security incident has occurred and compromised personal data.[5]

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 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

[3] See Recital 85 and Article 33(1) GDPR
[4] Article 29 Working Party Guidelines, p.20
[5] Article 29 Working Party Guidelines, p.10

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, it must provide a reason for the delay along with the late notification to the DPC, and may, in these circumstances, be in breach of its 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, which may arise in more complex breaches, the initial notification should be lodged and then information may be provided in phases, provided it is done without undue delay and provided the controller can give reasons for the delay in accordance with Article 33(1).

In relation to the timeline for notification, the Article 29 Working Party Guidelines recommended that when the controller first notifies the breach, it should inform the supervisory authority that it does not yet have all of the required information and that it will provide further information later on.

Similarly, per Article 33(2) GDPR, a processor, processing personal data on the direction of a controller, must notify the 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 its 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:[6]

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.

[6] See Article 33(3) GDPR

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 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.[7]

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'.[8] This obligation is in addition and separate to the obligation to notify the DPC of personal data breaches, and sets a higher threshold before the 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 and which are likely to result in a high risk to them.

Such communications to data subjects should be made without undue delay, in many cases in close cooperation with the DPC, 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:[9]

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;

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

---

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

c) it would involve disproportionate effort. In such a case, however, data 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.

Assessing Risk

One of the main areas in relation to which controllers have raised queries to the DPC concerns the assessment of risk. As both **(a)** the threshold for notification to the DPC, and **(b)** the threshold for communication of a breach to affected data subjects, involve an assessment of the potential or likely risk posed by the breach, failure to adequately assess risk (or failure to attempt to assess risk at all) may result in controllers failing to meet their obligations under the GDPR.

In some cases, controllers, in their breach notifications to the DPC, have rated the risk to the rights and freedoms of affected data subject(s) as being lower than would be expected, taking into account the nature of the breaches concerned. Controllers may fail to give sufficient weight to certain criteria when assessing the likelihood and gravity of any potential risk to data subjects. Factors that controllers should take into account when engaging in such an assessment include, but are not limited to:

- the type and nature of the personal data (including whether it contains sensitive, or 'special category' personal data);
- the circumstances of the personal data breach;
- whether or not personal data had been protected by appropriate technical protection measures, such as encryption or pseudonymisation;
- the ease of direct or indirect identification of the affected data subjects;
- the likelihood of reversal of pseudonymisation or loss of confidentiality;
- the likelihood of identity fraud, financial loss, or other forms of misuse of the personal data ;
- whether the personal data could be, or are likely to be, used maliciously;
- the likelihood that the breach could result in, and the severity of, physical, material or non-material damage to data subjects; and
- whether the breach could result in discrimination, damage to reputation or harm to data subjects' other fundamental rights.

Where controllers fail to consider, or give sufficient weight to, all of the relevant criteria regarding the assessment of potential risk to data subjects, this may result in 'under-reporting' – failure to notify the DPC of a data breach where notification is required. Controllers should bear in mind that they are required to notify the DPC of a personal data breach, unless they can demonstrate that it is unlikely to result in *a risk* to the rights and freedoms of data subjects.

On the other hand, in a small number of cases, controllers have been identified as reporting data breaches that do not result in *any* risk to the data subjects, which has led to some cases of 'over-reporting'.

It is important that immediately upon becoming aware of a personal data breach, controllers should in addition to seeking to contain the incident, carry out an assessment of the risk that could result from it. Under Article 33 GDPR, no notification is required where the breach is assessed as being '*unlikely to result in a risk*' to the rights and freedoms of data subjects. This assessment of risk should be undertaken and documented in the case of all personal data breaches.

Once the personal data breach has been assessed as not unlikely to result in a risk to data subjects, then the second, and separate, assessment which the controller should undertake is whether or not the risk is such that the controller is also under an obligation to communicate it to the affected data subjects.

The details of what should be communicated are set out above, under the heading '*When does a controller have to communicate a personal data breach to data subjects?*', but the same guidance with regards to the assessment of risk applies – controllers should take all relevant criteria into account when assessing whether the breach is '*likely to result in a high risk to the rights and freedoms of the natural person*', and should keep a record of this assessment.

To demonstrate compliance with their obligations, controllers are recommended to keep a record of how and when assessments are carried out.

For further information on how to assess risk in the context of a personal data breach, the DPC recommends that controllers consult Section IV, 'Assessing Risk and High Risk', of the Article 29 Working Party 'Guidelines on personal data breach notification'.

Case Studies – Under-Estimation of Risk

Vulnerable Data Subjects

A controller notified the DPC of a potential breach experienced by a healthcare provider which had been the victim of a ransomware attack. It was outlined that the compromised laboratory system and its backups were attacked and encrypted. It was specified that personal data of approximately 50,000 data subjects could potentially be affected.

In its notification to the DPC, the controller indicated that there was not a 'High' level of risk to data subjects.

However, following the DPC Breach Assessment Unit's analysis of the initial notification and review of supporting documentation provided by the controller, and in light of the categories

of personal data potentially affected, and the vulnerability of data subjects, it was determined that the breach was 'likely to result in a high risk to the rights and freedoms of data subjects'.

Not only was this breach notifiable to the DPC, but, due to the high risk, it would necessitate a communication to the affected data subjects.

Breach Resulted in Fraud

A controller notified the DPC that an unauthorised third party had gained access to an employee email account due to an incident of phishing/hacking. Contained in the account was the personal data of approximately 400 data subjects.

As a result of this incident, one data subject was actually the victim of financial fraud. Nevertheless, in its notification to the DPC, the controller indicated that the level of risk to data subjects was 'Low'.

However, following the Breach Assessment Unit's analysis and review of supporting documentation, particularly in light of the nature of the personal data affected, and the fact that actual harm had been suffered by a data subject, it was determined that the breach was 'likely to result in a high risk to the rights and freedoms of data subjects'.

Not only was this breach notifiable to the DPC, but due to the high risk, it would necessitate a communication to the affected data subjects.

Case Study – Over-Estimation of Risk

No Identifiable Risk

On a number of occasions, a particular controller submitted a personal data breach notification that involved supporting documentation being scanned to their system, but subsequently being saved to the incorrect data subject's electronic folder.

The personal data was retained, unaltered and not disclosed to any unauthorised parties and when the error was detected the personal data was moved to the correct electronic folder – the incident was therefore unlikely to result in any risk to data subjects.

Following a review of these incidents it was concluded that they would not warrant notification under Article 33(1) GDPR, on the basis that there was no identifiable risk, and the incidents were 'unlikely to result in a risk to the rights and freedoms of natural persons'.

Late Notifications or No Notification

As addressed above, under the heading '*Assessing Risk*', where controllers have misunderstood the threshold for notification or communication of a personal data breach, or have even failed entirely to conduct a risk assessment of that breach, this has on occasion resulted in no notification being made to the DPC or a failure to communicate the breach to data subjects, where notification was in fact required. Further, in a number of cases, controllers have notified the DPC of a personal data breach, but have failed to do so within the appropriate time limit, and have failed to provide a sufficient justification for late notification.

Controllers should note that the requirements to notify or communicate a personal data breach must be complied with '*without undue delay*', and that any delay in notification or communication must be justified. As is outlined above, this will also apply where the controller is not in a position to provide all of the information to the DPC within the first 72 hours.

Any controllers encountering a pattern in their notifications being late should consider revising their breach notification policy and procedures, ensuring that any delay in notifications is with due reason and considering whether information should be provided in phases where full notification is not possible right away.

As noted above, in order to demonstrate compliance with the requirements of the GDPR, in particular the requirement to notify breaches to the DPC or communicate with data subjects '*without undue delay*', controllers should keep a record of how and when they first became aware of the personal data breach.

Case Study – No Communication

Failure to Communicate to Data Subjects

The DPC was notified of a breach by a public body which involved its website experiencing a cybersecurity incident. Due to the nature of the services provided through the website and the security incident experienced, a significant volume of personal data had the potential to be exposed.

The controller assessed the risk to data subjects as 'Low'. However, following the DPC Breach Assessment Unit's analysis and review of the supporting documentation, the categories of data potentially affected, the reported impact on data subjects, and the actions/measures undertaken, it was determined that the breach was 'likely to result in a high risk to the rights and freedoms of data subjects' and none of the exceptions of Article 34(3) applied.

In this case, the controller had failed to adequately assess the risk likely to result to data subjects, and had therefore failed to make a communication to the affected data subjects as required by Article 34 GDPR, and was subsequently directed to make the required communication.

Inadequate Reporting

In some cases, controllers have been identified as not providing the DPC's Breach Assessment Unit with adequate information concerning the personal data breach incidents which they have experienced. Inadequate reporting can take the form of controllers providing incomplete notifications, omitting relevant information, or failing to complete adequate risk assessments. This can lead to significant delays, and may, in some cases, even constitute failure by the controller to fulfil its obligations to provide information as required by Article 33(3) GDPR.

Controllers should ensure, by means of their own internal policies and procedures, that when filling out the DPC's online breach notification form, all of the required and relevant information about a personal data breach is notified to the DPC – both at the initial notification stage, and when providing any subsequent updates, if applicable.

Controllers should seek to include, at the very least, all of the information mentioned in Article 33(3) GDPR and discussed under the heading '*What should a notification to the DPC contain?*' above.

Similarly, where it is appropriate to do so, controllers should also ensure that when communicating a personal data breach to affected data subjects, they communicate all of the required information to the data subjects , including, at least, the information listed above under the heading '*What should a communication to a data subject contain?*' and in Article 34(2) GDPR.

Case Study – Inadequate Reporting

Missing Information

The DPC Breach Assessment Unit identified certain obstacles in processing and evaluating notifications received from certain public bodies, where initial notifications contained limited information concerning the breach itself, how it occurred, and the categories of data affected.

Follow-up requests for further information took a considerable amount of time in some cases. The reasons provided for the delays were often that further investigation was required into the incidents.

In cases such as these, the correct approach is that interim updates should be provided to the DPC, with as much relevant information being provided to the DPC '*without undue delay*', rather than providing no information or limited information until explicitly requested to do so.

Technical Knowledge

One of the frequent obstacles which the DPC has noted from its interaction with controllers in the context of personal data breach notifications regards the level of technical knowledge that controllers possess. Controllers should ensure that an appropriate level of technical knowledge is available to them, in order to enable them to identify, without undue delay,:

a) that they have been the victim of a security incident, such as a cyber-attack;

b) the measures and actions which should be taken immediately after a breach of this nature has occurred; and

c) the appropriate safeguards which should have been employed to reduce the risk of incidents of this nature occurring.

This issue is of particular relevance to smaller to medium sized controllers, who may only have access to limited resources and knowledge in terms of IT.

Under the principle of 'integrity and confidentiality' (one of the key principles of data protection found in Article 5 GDPR), there is a requirement that controllers must, using appropriate technical or organisational measures, process personal data in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Compliance with this requirement will both protect the personal data and will also assist a controller to quickly establish whether a personal data breach has taken place and to promptly notify the DPC.

To achieve this end, controllers must utilise appropriate technical or organisational measures. Where controllers themselves do not have the necessary level of technical knowledge, they should seek appropriate training or external advice or ICT support.

Case Study – Inadequate Technical Knowledge

Inability to Identify Vulnerability

On foot of a notification from a concerned citizen, the DPC Breach Assessment Unit contacted a controller in relation to customers receiving spam email that appeared to come from the controller. It appeared the controller was unaware that a potential breach of their IT infrastructure had occurred which had led to spam emails being sent without their authority.

Subsequently, the controller notified customers by utilising its social media presence. However, the controller had difficulty identifying the source of the breach, and in ensuring that appropriate technical measures were introduced to reduce the risk of incidents of this nature reoccurring.

Controllers need to ensure a level of technical knowledge, whether through in-house or external expertise, to allow them to identify likely security threats, mitigate against them, and prevent future reoccurrence.

Repeat Breach Notifications

The DPC has noted, in the case of certain controllers, a pattern whereby the same controller experiences the same category of data breach on a number of occasions. A pattern of repeated personal data breaches is a matter of particular concern, particularly where the breaches have continued over an extended period and where they demonstrate that the controller has inadequate technical and organisational measures in place to prevent recurrence.

Where patterns like this arise, it is particularly important that controllers take steps to improve their policies and technical knowledge and/or engage expert support to mitigate vulnerabilities.

Case Study – Repeat Breach Notifications

Repeated Failures to Mitigate

One controller reported a total of 7 incidents to the DPC where email accounts of staff members had been potentially compromised. A significant amount of personal data was involved, with various levels of risk presented to affected data subjects.

These breaches, particularly their continued reoccurrence, were the result of the controller's failure to have the appropriate technical and organisational measures in place to ensure the security of personal data stored within their IT environment.

Social Engineering

Certain controllers, particularly within the telecommunications sector, have been identified as being increasingly vulnerable to incidents of 'social engineering', which in turn, have resulted in unauthorised access to data subjects' communications accounts and, in some cases, have left those data subjects susceptible to fraud.

This is another area in which sufficient technical knowledge and technical and organisational measures are vital, and such knowledge and measures must be kept up to date with the evolving technological and risk landscape.

Case Study – Social Engineering

Repeated Phishing Incidents

One controller reported multiple incidents involving social engineering, where the perpetrator contacted the controller to initiate a SIM change, using legitimate customer details, to pass the validation process and ultimately obtain control over the legitimate customer's account.

In this example, a more robust validation process could reduce the potential for controllers and their customers experiencing such incidents.

Data Accuracy

A common type of personal data breach, particularly in certain industries which engage in large volume email or postal communications, involve 'unauthorised disclosure' of customers' personal data, due to inadequate data accuracy in the recording of contact data.

The vast majority of these cases can be avoided by controllers taking basic steps, such as ensuring that customer data is accurate and up to date, and having appropriate review mechanisms in place to check correspondence before it issues.

Although a very simple error can lead to an incorrect recipient receiving another individual's personal data, the consequences for affected data subjects arising from such unauthorised disclosure can be serious.

Furthermore, the circumstances that lead to such incidents can be an indication that the controller does not have sufficient technical and organisational measures in place to protect the security and integrity of the personal data under their control.

Case Study – Data Accuracy

Incorrect Contact Details

Certain large financial institutions have reported a significant volume of personal data breaches resulting from inaccuracies in recorded contact data. These breaches include correspondence being sent to incorrect addresses or incorrect customers, or incorrect customer records being attached to outgoing correspondence.

As a result, personal data contained in bank statements, mortgage information, loan information, payment cards, and assurance policies have potentially been incorrectly disclosed.

These types of breaches could be reduced, or eliminated, by taking steps to ensure customer data is up to date and that mechanisms and procedures are in place to review correspondence before it is issued.

In certain sectors, personal data breaches of this nature account for the vast majority of breaches notified to the DPC. Appropriate steps taken to prevent such unauthorised disclosure could significantly reduce the number of data breaches affecting data controllers and data subjects in these sectors.

Conclusions and Recommendations

Having regard to the experience of the DPC's Breach Assessment Unit, the statistics gathered to date on breach notifications under the GDPR mandatory notification regime, and some of the key issues outlined above, there are a number of important considerations which controllers should keep in mind when dealing with personal data breaches. A synopsis of the key points is set out below:

Obligations to Notify and Communicate – Articles 33 and 34

Controllers should ensure that they understand, and reflect in their policies and procedures, that there are two distinct primary obligations, with differing tests, in the context of the GDPR notification regime for personal data breaches, namely:

a) **Notification** of a data breach **to the DPC**, unless the controller can demonstrate that the breach is unlikely to result in a risk to data subjects; and

b) **Communication** of the breach **to data subjects**, where the breach is likely to result in a high risk to data subjects.

It is important that controllers understand that once they have been made aware of a personal data breach, a timetable is set in motion. Controllers must comply with Article 33(1) GDPR in notifying the DPC without undue delay (not later than 72 hours under the GDPR). In addition, where applicable, controllers must also communicate the data breach to the affected data subjects without undue delay, to comply with Article 34(1).

Controllers should also ensure that, in line with their obligations under the principle of accountability and the requirements of Article 33 GDPR, they are able to demonstrate, through appropriate records and procedures, their compliance with the notification obligations, particularly the timelines for notification to the DPC '*without undue delay*'.

Controllers should be aware that in notifying the DPC of a personal data breach, they may provide, if necessary, further information and updates to the DPC following their initial notification. However, controllers must be in a position to give reasons for the delay in providing all of the relevant information at the outset, in accordance with Article 33(1).

In relation to this, the Article 29 Working Party Guidelines[10] recommended that when the controller first notifies the breach, it should inform the supervisory authority that it does not yet have all of the required information and that it will provide further information later on. This does not detract from the obligation to provide as much relevant information as possible in the initial report and without undue delay to the DPC.

[10] Article 29 Working Party Guidelines, pp. 14-16

Assessing Risk

When assessing a personal data breach, the controller should consider a number of criteria in determining the risk to the rights and freedoms of affected data subjects, including:

- the nature and circumstances of the breach;
- the type of personal data affected (including whether it contains sensitive, or 'special category' personal data);
- the volume of personal data involved;
- the potential for the personal data to be used maliciously;
- the potential damage or harm to data subjects; and
- steps taken or the possibility to mitigate the harm or damage;

Controllers should place particular emphasis on considering whether personal data could be, or are likely to be, used in a malicious manner when assessing the potential risk to affected data subjects. In cases where the potential for the malicious use of data has been identified, the controller should provide the affected data subject(s) with details of the specific mitigating actions taken and any relevant advice as to how the data subjects can protect themselves against the adverse consequences of the breach.

The controller should review all notified breach incidents where the potential for data to be used maliciously has been identified, with the aim of confirming whether attempts have been made to use any personal data inappropriately. Details of such reviews should be provided to the DPC as updates to reported breach notifications.

If, after careful consideration and appropriate mitigating steps, a data controller concludes that a breach would be '*unlikely to result in a risk to the rights and freedoms of data subjects'*, the data controller may only then make the decision not to submit a breach notification to the DPC. Risk assessments should be considered on a case-by-case basis and a record should be kept as part of the general duty to maintain records of breaches.

Information to Be Provided

When notifying the DPC of a personal data breach, in order to assist the DPC in reviewing the notification, the controller should be in a position to provide the following:

- a detailed description of how the breach occurred;
- a record of how and when they became aware of the breach;
- a detailed description of the source of the breach;

- how many data subjects have been affected;
- the specific categories of data affected;
- what immediate steps were undertaken upon discovery of the breach;
- any further plans/steps to be taken and the timeframe for their introduction;
- whether all relevant records, such as audit logs, have been retained;
- a record of processing; and
- relevant policy and procedures documentation.

Should further information need to be submitted to the DPC in relation to a breach, it should also be provided without undue delay. Should the DPC issue further specific queries in relation to a breach incident, responses should be provided within the deadline set out by the DPC.

Should the controller rate the risk to the rights and freedoms of data subjects as 'High', the controller must communicate the personal data breach to affected data subjects without undue delay. A communication to affected data subjects should describe in clear and plain language the nature of the personal data breach and contain at least:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach; and
- 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.

Personal Data Breach Policy and Procedure

Controllers should develop their own internal policies and procedures in relation to dealing with personal data breaches. In doing so, controllers may wish to give consideration to developing and utilising a standard operating procedure for breaches, to act as the organisation's response guide to personal data breach incidents and to outline its internal breach procedure.

A controller's standard operating procedure could set out the risk profile of the personal data in each part of the controller's system and have the necessary information to hand to enable the controller to carry out the two steps of the risk assessment. This will help to identify what the organisation should do before, during, and after a breach incident.