ICO call for views on incident reporting thresholds under NIS Regulations 2018

Background

Currently, incident reporting thresholds for digital services providers are set out in the NIS Regulations 2018 and the European Commission Implementing Regulation 151/2018. The thresholds were established when the UK was a member of the European Union (“EU”) and were set for a market size of 28 EU member states.

Now that the UK has left the EU, it recognised that there is a deficiency in the NIS legislation surrounding the incident reporting thresholds. In July 2021, the Government launched a call for views proposing the amendment of the current legislative provisions to enable thresholds to be set which are relevant to the UK market.

The Government proposes to lay a statutory instrument which would revoke Article 4, which sets out the thresholds, from the UK retained version of the European Commission Implementing Regulation 151/2018. This would allow the Commissioner, as the competent authority for digital service providers, to set the thresholds at a more appropriate level through guidance. Digital service providers would be required to have regard to these thresholds when determining whether they are required to notify the ICO of an incident under Regulation 12(3) of the NIS Regulations 2018.

We are consulting on potential approaches to thresholds that would be set out in the Commissioner’s guidance. The consultation will run for a period of 28 days, from Thursday 9 September 2021 to Thursday 7 October 2021. We will then analyse the results and use the information provided to inform our assessment of the costs and benefits of the different options.

In addition to the questions, we would also be interested in any wider evidence or analysis of the costs associated with the management of NIS incidents, either to digital service providers or users, or of current reporting requirements.

Current reporting requirements

Under the current legislation, a digital service provider must notify the Commissioner in writing about any incident having a substantial impact on the provision of any relevant digital services. In order to determine whether the impact of an incident is substantial, digital service providers must take into account:

* the number of users affected by the incident and, in particular, the users relying on the digital service for the provision of their own services;
* the duration of the incident;
* the geographical area affected by the incident;
* the extent of the disruption to the functioning of the service; and
* the extent of the impact on economic and societal activities.

In addition, the digital service provider must assess whether one of the following situations has taken place (Article 4 of 151/2018 Regulations):

* the service provided by a digital service provider was unavailable for more than 5,000,000 user-hours, whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;
* the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100,000 users in the Union;
* the incident has created a risk to public safety, public security or of loss of life; or
* the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1,000,000.

Proposed amendments to these requirements

Under the new proposals, digital service providers would no longer be required to assess whether one of the situations referred to in Article 4 has occurred when deciding whether to notify the Commissioner about an incident. However, digital service providers would be required to have regard to incident thresholds set by the Commissioner in guidance.

We are consulting on two proposed approaches to the thresholds that would be contained within the Commissioner’s guidance. These are set out below.

Proposed incident thresholds

Proposal 1 – Revise existing thresholds so that they are applicable to UK markets

The existing incident thresholds were established taking into account a market of 28 EU member states. This proposal adopts the existing considerations but with revised numerical thresholds, to take account of the smaller UK market.

The revised numerical thresholds are intended to be proportionate to the size of the UK market.

Proposed text within guidance

How do we determine if we need to notify?

You need to assess whether the incident caused a ‘substantial impact on the provision’ of your digital service(s) in order to decide if you need to notify.

Regulation 12(7) provides further details on how you can make this determination. This refers to provisions within Article 3 of the DSP Regulation. In short, when determining the impact of an incident you must take into account:

* the number of users affected by the incident, in particular those relying on the service for the provision of their own services;
* the duration of the incident;
* the geographical spread with regard to the area affected;
* the extent of the disruption of the functioning of the service;
* the extent of the impact on economic and societal activities; and
* whether one of the thresholds specified in this guidance has taken place.

What does the ‘number of users affected’ mean?

Article 3(1) of the DSP Regulation requires you to be in a position to estimate:

* the number of affected persons you have a contract with (this includes both individuals and organisations); or
* the number of affected users determined by reference to previous traffic data.

A “user” in the context of NIS may comprise a person, organisation or other entity that uses the service(s) you provide. In some cases, you may not have visibility of every single user and Regulation 12(4) only requires you to notify where you have access to the information that allows you to assess the impact of an incident. The key is the extent to which you are aware of the type and number of users at a particular point in time.

What does the ‘duration of the incident’ mean?

Article 3(2) of the DSP Regulation states that this refers to the period of time from the disruption of the service until its recovery.

You must assess the disruption on the basis of availability, authenticity, integrity and confidentiality of the digital data you process.

What does the ‘geographical spread with regard to the area affected’ mean?

Article 3(3) of the DSP Regulation clarifies that this refers to your ability to identify whether the NIS incident affects the provision of your services in other countries – in other words, you need to determine if the incident has cross-border impact.

You are required to provide the ICO with sufficient information for us to assess the significance of any cross-border impact.

What does the ‘extent of the disruption’ mean?

Article 3(4) of the DSP Regulation requires you to be able to measure whether the NIS incident has impaired one or more of the following:

* the availability of data or related services;
* the authenticity of data or related services;
* the integrity of data or related services; and
* the confidentiality of data or related services.

What does the ‘extent of the impact’ mean?

Article 3(5) of the DSP Regulation requires you to be able to conclude whether the incident has:

‘caused significant material or non-material losses for the users in relation to health, safety, or damage to property.’

You should reach this conclusion by indications such as the nature of your contractual relations with your customers (ie the type of customer your digital service serves) and, where appropriate, the potential number of affected users.

Importantly, under Article 3(6) of the DSP Regulation, for the purposes of the above, DSPs:

‘shall not be required to collect additional information to which they do not have access’

What other thresholds apply?

When assessing the above, you need to take into account whether one of the following situations has occurred. If any one of these thresholds is met, the you should regard the incident as ‘substantial’:

* the service was unavailable for more than 750,000 user hours. User-hour refers to the number of affected users in the UK for a duration of 60 minutes;
* the incident resulted in a loss of confidentiality, integrity and authenticity for data or related services where this affects more than 15,500 users in the UK;
* the incident created a risk to public safety, security or of loss of life; or
* the incident caused material damage to at least one user in the UK £850,000.

An incident is considered substantial when **at least one** of the above has taken place.

It is important to understand that if the NIS incident results in a personal data breach, the above factors and thresholds do not apply. Essentially, the incident may not meet any of the thresholds above, but if personal data was compromised, you need to assess whether this could result in a risk to the rights and freedoms of individuals.

If that is the case you are required to notify the ICO of a personal data breach, even if you may not have to tell us about the NIS incident.

Proposal 2 – Replace numerical thresholds with a risk-based indicative and relative thresholds

In developing this proposal, we have sought to identify thresholds that have broader application to all services. It is recognised that numerical thresholds may have limited application to some digital services, dependant on the size of the service provider and nature of the service being provided.

We have sought to take into account established international cyber security requirements and practices.

The proposed framework would require a digital service provider to undertake an assessment of the impact of the incident on the function of the service, on information and on resources required to recover from the incident.

Proposed text within guidance

How do we determine if we need to notify?

You need to assess whether the incident caused a ‘substantial impact on the provision’ of your digital service(s) in order to decide if you need to notify.

Regulation 12(7) provides further details on how you can make this determination. This refers to provisions within Article 3 of the DSP Regulation. In short, when determining the impact of an incident you must take into account:

* the number of users affected by the incident, in particular those relying on the service for the provision of their own services;
* the duration of the incident;
* the geographical spread with regard to the area affected;
* the extent of the disruption of the functioning of the service;
* the extent of the impact on economic and societal activities; and
* whether one of the thresholds specified in this guidance has taken place.

When assessing the above, you should consider:

* the impact the incident has on the functions of your service. For example, whether it means you are unable to provide a critical service to a subset of your users for a period of time, or cannot provide them to any user;
* the impact the incident has on the information your service stores, transmits or otherwise processes. For example, whether it impacts the confidentiality, integrity, availability and authenticity of the digital data concerned; and
* the resources and time you are likely to need to recover from the incident. For example, if you need specific additional resources to recover beyond those in your incident management and business continuity processes. This does not include instances where you request advice from the NCSC or other bodies, but where you need specific technical assistance to restore your service.

What does the ‘number of users affected’ mean?

Article 3(1) of the DSP Regulation requires you to be in a position to estimate:

* the number of affected persons you have a contract with (this includes both individuals and organisations); or
* the number of affected users determined by reference to previous traffic data.

A “user” in the context of NIS may comprise a person, organisation or other entity that uses the service(s) you provide. In some cases you may not have visibility of every single user, and Regulation 12(4) only requires you to notify where you have access to the information that allows you to assess the impact of an incident. The key is the extent to which you are aware of the type and number of users at a particular point in time.

What does the ‘duration of the incident’ mean?

Article 3(2) of the DSP Regulation states that this refers to the period of time from the disruption of the service until its recovery.

You must assess the disruption on the basis of availability, authenticity, integrity and confidentiality of the digital data you process.

What does the ‘geographical spread with regard to the area affected’ mean?

Article 3(3) of the DSP Regulation clarifies that this refers to your ability to identify whether the NIS incident affects the provision of your services in other countries – in other words, you need to determine if the incident has cross-border impact.

You are required to provide the ICO with sufficient information for us to assess the significance of any cross-border impact.

What does the ‘extent of the disruption’ mean?

Article 3(4) of the DSP Regulation requires you to be able to measure whether the NIS incident has impaired one or more of the following:

* the availability of data or related services;
* the authenticity of data or related services;
* the integrity of data or related services; and
* the confidentiality of data or related services.

What does the ‘extent of the impact’ mean?

Article 3(5) of the DSP Regulation requires you to be able to conclude whether the incident has:

‘caused significant material or non-material losses for the users in relation to health, safety, or damage to property.’

You should reach this conclusion by indications such as the nature of your contractual relations with your customers (ie the type of customer your digital service serves) and, where appropriate, the potential number of affected users.

Importantly, under Article 3(6) of the DSP Regulation, for the purposes of the above, DSPs:

‘shall not be required to collect additional information to which they do not have access’

What other thresholds apply?

When making your assessment in line with the above requirements, you should assess the level of impact using the matrix below to determine whether the impact is ‘substantial’:

|  |  |  |  |
| --- | --- | --- | --- |
| **Criterion** | **Impact level** | | |
| Functioning | Low (1) | Medium (2) | High (3) |
| Information | Low (1) | Medium (2) | High (3) |
| Recoverability | Low (1) | Medium (2) | High (3) |

These represent the extent of the disruption the incident causes. You should incorporate the number of users affected and the duration of any disruption or reduction into these calculations. For example, when considering the impact level terms of the functions your service provides and the information you process, you should regard the impact level as high where the incident:

* affects [10%] or more of your users; and
* results in a reduction or disruption in functionality, or impact on information, for a significant period of time [(eg a duration of 60 minutes or more).]

The ICO considers an incident is substantial when, after all criteria are considered, it meets or exceeds a threshold score of three. Therefore, any incident that has a high impact level in any category is automatically ‘substantial’ and requires notification.

**Example: Notification required**

An RDSP assesses the impact of an incident using the above matrix. It judges that:

* the impact on functioning is high (3);
* the impact on the information it stores, processes or transmits is low (1); and
* the recovery requirement is low (1).

This results in a ‘score’ of 3, meaning the threshold is met and the impact is substantial. Notification is required.

**Example: Notification not required**

An RDSP assesses the impact of an incident using the above matrix. It judges that:

* the impact on functioning is low (1);
* the impact on information is medium (2); and
* the impact on recovery is low (1).

The threshold score is not met, and therefore the impact is not substantial and notification is not required.

In cases where notification is not required, you should retain relevant documentation about the incident itself and the decisions you took in relation to it.

It is important to understand that if the NIS incident results in a personal data breach, the above factors and thresholds do not apply. Essentially, the incident may not meet any of the thresholds above, but if personal data was compromised, you need to assess whether this could result in a risk to the rights and freedoms of individuals.

If that is the case you are required to notify the ICO of a personal data breach, even if you may not have to tell us about the NIS incident.