GRA
GIBRALTAR REGULATORY AUTHORITY

(8) Guidance on Personal Data Breach Notification

Guidance on the General Data Protection Regulation

5th December 2018

Guidance Note IR03/18

CONTENTS

SUMMARY

- The General Data Protection Regulation (the "GDPR") introduces the requirement for a personal data breach to be notified to the relevant supervisory authority (or in the event of a cross-border data breach, to the lead supervisory authority).

- A personal data breach is considered a type of security incident.

- A personal data breach can have significant adverse effects on individuals, which may result in physical, material, or non-material damage.

- Data controllers and data processors should have appropriate technological protection and organisational measures implemented to establish immediately whether a personal data breach has taken place.

- Once the data controller becomes 'aware' of a data breach, it should assess the likely risk to individuals to determine whether the requirement for notification to the relevant supervisory authority (within 72 hours) has been triggered and take appropriate remedial action to address the data breach.

- In certain cases, as well as notifying the relevant supervisory authority, the data controller will also need to communicate a data breach to the affected individuals.

- When assessing the risk to individuals as a result of a data breach, data controllers should consider the specific circumstances of the data breach, including the severity of the potential impact and the likelihood of this occurring.

- Regardless of whether or not a data breach needs to be notified, data controllers are required to document all data breaches.

- **Annex A** provides examples to assist data controllers determine whether they need to notify a personal data breach to the relevant supervisory authority and/or the individuals affected by the data breach.

- **Annex B** provides a flowchart which illustrates the notification requirements under the GDPR.

- **Annex C** provides a 'data breach notification form' for organisations to use should they be required to notify the relevant supervisory authority of a personal data breach.

1. INTRODUCTION

The GDPR introduces the requirement for a personal data breach to be notified to the relevant supervisory authority (or in the event of a cross-border data breach, to the lead supervisory authority) and, in some cases, to communicate the data breach to individuals whose personal data have been affected by the data breach.

The new notification requirement has several benefits. For example, when notifying the Information Commissioner[1] (the "Commissioner") of a personal data breach, a data controller may obtain advice on whether the affected individuals need to be informed. Further, communicating a data breach to individuals may allow the data controller to provide information on the risks presented to individuals because of the data breach and the steps they can take to protect themselves from its potential consequences.

Data controllers and data processors should therefore have procedures in place to be able to detect and promptly contain a data breach, assess the risks to individuals, and determine whether it is necessary to notify the Commissioner and communicate the data breach to the individuals affected. It is important to note that the focus of any data breach notification plan should be on protecting individuals and their personal data.

Data controllers should view data breach notification as a tool for enhancing compliance with the GDPR. However, under the GDPR, failure to report a data breach to either the Commissioner and/or the individuals affected by a data breach, may result in a possible sanction to the data controller, as well as a sanction for the data breach itself.

This guidance note aims to provide advice on the GDPR's data breach notification requirements and provides examples to assist data controllers determine whether they need to notify a personal data breach to the Commissioner and/or the individuals affected by the data breach (see **Annex A**). Further, the guidance note includes a flowchart which illustrates the notification requirements under the GDPR (see **Annex B**) and a 'data breach notification form' for organisations to use should they be required to notify the Commissioner (or other supervisory authority), of a personal data breach (see **Annex C**).

Note: *the guidance in this document largely aims to provide advice based on the European Data Protection Board's guidelines on personal data breach notification under the GDPR[2]. For more detailed guidance, it may be useful for a controller to consult said guidelines separately.*

Acknowledgements

Where appropriate Gibraltar's Information Commissioner will seek to ensure that locally published guidance notes are consistent with others made available by fellow Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the European Data Protection Board and the UK's Information Commissioner's office.

[1] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

[2] European Data Protection Board, 'Guidelines on Personal data breach notification under Regulation 2016/679' (6 February 2018) < https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 > Accessed 23 November 2018.

2. PERSONAL DATA BREACH NOTIFICATION

What is a personal data breach?

GDPR - Article 4(12)

'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 transmitted, stored or otherwise processed.

A personal data breach is considered a type of security incident. Because of a data breach, a data controller will be unable to comply with the principles relating to the processing of personal data under Article 5 of the GDPR. However, it is important to note that not all security incidents are personal data breaches[3]. The GDPR only applies where there is a breach of personal data.

Personal data breaches can be categorised according to the following:

- **Confidentiality breach** – where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **Integrity breach** – where there is an unauthorised or accidental alteration of personal data.
- **Availability breach** – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, or a combination of these.

Consequences of a personal data breach

A personal data breach can have significant adverse effects on individuals, which may result in physical, material, or non-material damage. This may include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It may also include significant economic or social disadvantage to individuals (see Recitals 75 and 85 of the GDPR). Assessing risk is a fundamental part of any personal data breach notification arrangements.

[3] It is important to note that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but also includes incidents from internal processing that breach security principles.

3. NOTIFYING THE COMMISSIONER

When to notify?

GDPR - Article 33(1)

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Data controllers should have appropriate technological protection and organisational measures implemented to establish immediately whether a personal data breach has taken place and to promptly inform the Commissioner and the individuals concerned. A data controller would be considered as being 'aware' of a data breach when it has a reasonable degree of certainty that a security incident has occurred that has resulted in personal data being compromised.

Once the data controller becomes 'aware' of a data breach, it should assess the likely risk to individuals to determine whether the requirement for notification to the Commissioner (within 72 hours) has been triggered and take appropriate remedial action to address the data breach.

Controllers should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data. It is important that when a breach is detected it is reported upwards to the appropriate level of management.

Data processors

Article 33(2) of the GDPR states that the data processor shall notify the data controller without undue delay after becoming aware of a personal data breach. However, the data processor does not need to make the first assessment of the likelihood of risk arising from the data breach before notifying the data controller. It is the data controller's responsibility to make the assessment on becoming aware of the data breach. The data processor is only required to establish whether a data breach has occurred.

The information that should be provided to the Commissioner

GDPR - Article 33(3)

The notification referred to in paragraph 1 shall at least:

(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 or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(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.

The GDPR does not define categories of data subjects or personal data records. However, the Commissioner suggests that categories of data subjects refer to the various types of individuals whose personal data have been affected by a data breach (for example, children and other vulnerable groups, individuals with disabilities, employees, customers etc). Categories of personal data records can refer to the different types of records that the data controller processes (for example, health data, educational records, social care information, financial details, bank account numbers, passport numbers etc).

If the types of data subjects or types of personal data indicate a risk of damage occurring to individuals as a result of a data breach (for example, identity theft, fraud, financial loss, threat to professional secrecy), then the notification should include these categories (see Recital 85 of the GDPR).

Notification in phases

GDPR - Article 33(4)

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

When a breach is identified, but the extent is not yet known and is subject to further investigation, a notification in phases is a safe way to meet the notification obligations. In these cases, the Commissioner recommends that when the data controller first notifies his office, the data controller informs that it does not have all the required information and that it will provide more details later on.

Delayed notifications

Article 33(1) of the GDPR makes it clear that where notification to the Commissioner is not made within 72 hours, it shall be accompanied by reasons for the delay in notifying of the data breach.

Data breaches involving cross-border data flows

In the context of cross-border processing within the EU, Article 56(1) of the GDPR states that the supervisory authority of the main establishment or of the single establishment of the data controller or data processor shall be competent to act as lead supervisory authority. Further, Article 56(6) of the GDPR states that the lead supervisory authority shall be the sole interlocutor of the data controller or data processor for the cross-border processing carried out by that data controller or data processor.

The above means that where a data breach has taken place in the context of cross-border processing, and notification is required, the data controller will need to notify the lead supervisory authority[4]. Therefore, data controllers must make an assessment to determine which supervisory authority is the lead supervisory authority that they will need to notify in the event of a data breach[5].

If a data controller has doubts as to who is the lead supervisory authority, then it should notify the local supervisory authority where the data breach has taken place.

Data breaches at establishments outside of the EU

GDPR - Article 3

1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.

2.This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the EU, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the EU.

3.This Regulation applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

Where a data controller is not established in the EU but is subject to Article 3(2) or Article 3(3) of the GDPR, it will be bound by the notification obligations under Articles 33 and 34 of the GDPR.

Article 27 of the GDPR requires a data controller or data processor to designate a representative in the EU where Article 3(2) of the GDPR applies. In these cases, the Commissioner recommends that notification should be made to the supervisory authority in the Member State where the data controller's representative in the EU is established (see Recital 80 of the GDPR).

Further, where a data processor is subject to Article 3(2) of the GDPR, it will be bound by the obligations on data processors, including the duty to notify a data breach to the data controller under Article 33(2) of the GDPR.

[4] See the GRA Guidance Note IR02/17 Guidance on the General Data Protection Regulation: (2) Lead Supervisory Authority.

[5] Please see list of contact details for all European national data protection authorities, found at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

Conditions where notifying the Commissioner is not required

Article 33(1) of the GDPR makes it clear that data breaches that are unlikely to result in a risk to the rights and freedoms of individuals do not require notification to the Commissioner (for example, when personal data are already publicly available, and a disclosure of such data would not constitute a likely risk to individuals).

A breach of personal data that were effectively encrypted is a personal data breach. However, if the confidentiality of the encryption key is intact and the key is not compromised then the data would be considered in principle unintelligible. As a result, the data breach is unlikely to adversely affect individuals and would not require notification.

It should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.

Further to the above, even where personal data is encrypted, a loss or alternation may have negative consequences for individuals where the data controller has no adequate backups. In these cases, notifying the Commissioner (and individuals) would be required.

4. NOTIFYING INDIVIDUALS

Informing individuals

GDPR - Article 34(1)

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The above means that, in certain cases, as well as notifying the Commissioner, the data controller will also need to communicate a data breach to the affected individuals. The threshold for communicating a data breach to individuals is therefore higher than for notifying the Commissioner and not all data breaches will therefore be required to be communicated to individuals. This will protect individuals from unnecessary notification fatigue.

The main objective of informing individuals of a data breach is to provide specific information about the steps they should take to protect themselves from any negative consequences which may result from a data breach (see Recital 86 of the GDPR).

Information to be provided

GDPR - Article 34(2)

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

When notifying individuals, the data controller should at least provide the following information:

- a description of the nature of the data breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken by the data controller to address the data breach and where appropriate, to mitigate its possible adverse effects[6].

Data controllers should communicate a data breach to the affected data subjects, unless doing so would involve a disproportionate effort (Article 34(3)(c) of the GDPR). In such cases, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent. However, a controller should be wary of using a contact channel compromised by the breach as this channel could also be used by attackers impersonating the controller.

Notifying individuals of a breach is not required if any of the following conditions are met:

- 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 those that render the personal data unintelligible to any person who is not authorised to access it. For example, the data controller protected personal data with state-of-the-art encryption, or by tokenization.

- The controller has taken measures which ensure that the high risk to the rights and freedoms of data subjects are no longer likely to materialise. For example, a data controller has immediately identified and taken action in regard to the individual to whom information was erroneously sent before they were able to do anything with it.

- It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the data breach or are not known in the first place. For example, a data controller's office has flooded and the documents containing personal data were stored only in paper form. In this case, the data controller must make a public communication or take a similar measure, whereby the individuals affected are informed in an equally effective manner.

[6] Where relevant, this should include advice to individuals on how to protect themselves from possible adverse effects of the data breach, such as resetting passwords in the case where access credentials were compromised.

In accordance with the accountability principle, data controllers should be able to demonstrate to the Commissioner that they meet one or more of the above conditions (Article 5(2) of the GDPR).

5. ASSESSING RISK AND HIGH RISK

Risk as a trigger for notification

Notification about a personal data breach –

(a) to the Commissioner is required, unless the data breach is unlikely to result in a risk to the rights and freedoms of individuals; and
(b) to the individual, if the breach is likely to result in a high risk to their rights and freedoms.

The above means that upon becoming aware of a breach, the controller needs to assess the risk that could result from the data breach. Assessing risk will allow data controllers know the likelihood and the potential severity of the impact on individuals (which will help determine the actions that are appropriate to contain and address the breach) as well as determine whether notification is required.

Assessing risk

When assessing the risk to individuals as a result of a data breach, data controllers should consider the specific circumstances of the data breach, including the severity of the potential impact and the likelihood of this occurring.

When assessing risk, data controllers should consider the following:

- **The type of data breach that has occurred**. This may affect the level of risk presented to individuals (for example, loss of data, "internal" unauthorised access, external disclosure).

- **The nature, sensitivity and volume of personal data.** The more sensitive the personal data, the higher the risk of harm will be to the individuals affected by a data breach. However, consideration should also be given to other personal data that may already be available about an individual.

  Data breaches involving health data, identity documents or financial data can all cause harm on their own. However, if used together, they could be used for identity theft. Therefore, a combination of personal data is typically more sensitive than a single piece of personal data. Further, a small amount of highly sensitive personal data can have a high impact on individuals, and a large amount of details can reveal a greater range of information about individuals.

- **Ease of identification.** Data controllers should consider how easy it will be for someone, who has access to compromised personal data, to identify specific individuals or match the data with other information to identify individuals.

- **Severity of consequences for individuals.** These will depend on the nature of the personal data involved in a data breach. For example, where a personal data breach concerns special categories of personal data, the potential damage to individuals that could result may be especially severe, in particular where the data breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation.

  Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk.

- **Special characteristics of the individual.** For example, personal data relating to children or other vulnerable data subjects, who may be placed at greater risk as a result of a data breach.

- **Special characteristics of the data controller.** The nature and role of the data controller, and its activities, may affect the level of risk to individuals as a result of a personal data breach.

- **The number of individuals affected**. The higher the number of individuals affected, the greater the impact of a data breach can have. However, it is important to note that a data breach can have a severe impact on just one individual, depending on the nature of the personal data and the context in which it has been compromised.

When designing a data breach management response plan, data controllers and data processors may want to consider the recommendations for a methodology of assessing the severity of a data breach produced by the European Union Agency for Network and Information Security (ENISA)[7].

6. ACCOUNTABILITY

Documenting data breaches

GDPR - Article 33(5)

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Regardless of whether or not a data breach needs to be notified, data controllers are required to document all data breaches. This requirement is linked to the accountability principle of the GDPR and relates to the data controllers' obligations under Article 24 of the GDPR.

[7] ENISA Recommendations for a methodology of the assessment of severity of personal data breaches: https://www.enisa.europa.eu/publications/dbn-severity

The Commissioner can request to see records or documentation from a data controller regarding a data breach. Therefore, the Commissioner recommends that data controllers establish an internal register of data breaches that includes the following details –

- its causes,
- what took place,
- the personal data affected,
- the effects and consequences of the breach,
- the remedial action taken by the controller,
- the reasoning for the decisions taken in response to a breach, and
- where relevant the reasons for any delay in the response to a breach.

The Data Protection Officer ("DPO")

In regard to breach notification and the role of the DPO –

- it is the DPO's task to inform and advise the controller on its data protection obligations;
- the DPO is responsible for monitoring data protection compliance;
- the DPO acts as a contact point for the Commissioner and their details are to be included in breach notifications; and
- the DPO could be tasked with maintaining the records of data breaches.

The above means that the DPO should play a key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach, and during any subsequent investigation by the supervisory authority. The DPO should therefore be promptly informed about the existence of a breach and should be involved throughout the breach management and notification process.

ANNEX A – EXAMPLES TO ASSIST DATA CONTROLLERS DETERMINE WHETHER THEY NEED TO NOTIFY A DATA BREACH TO THE COMMISSIONER AND/OR INDIVIDUALS AFFECTED.

Example 1

A data controller stored a backup of files containing personal data of customers encrypted on a USB key. The USB key is stolen.

Notification to the Commissioner and individuals would not be required if the personal data are encrypted with a state-of-the-art algorithm, a backup of the data exists, the unique key is not compromised, and the data can be restored within a reasonable period. However, if the key is compromised, notification will be required.

Example 2

There is a brief power outage lasting an hour at a data controller's call centre meaning that customers are unable to call and access their records.

Notification to the Commissioner or individuals would not be required. However, the data controller should record the incident to comply with Article 33(5) of the GDPR.

Example 3

A data controller suffers a ransomware attack which results in all data being encrypted. No backups are available, and the data cannot be restored.

The data controller should report the data breach to the Commissioner as this has resulted in a loss of availability. Further, notification to individuals may be required depending on the nature of the personal data affected and the consequences which may result due to the lack of availability of the data. However, if a backup exists and the data could be restored within a reasonable period of time, the data controller would not be required to notify the Commissioner, or the individuals affected, as there would have been no permanent loss of availability or confidentiality.

Notwithstanding the above, the data controller should consider undertaking an investigation to assess compliance with the security requirements under Article 32 of the GDPR.

Example 4

A cyber-attack in a public hospital results in medical records not being available for a period of two hours.

The hospital is obliged to report the data breach to the Commissioner as the loss of availability to personal data is likely to result in a high risk to patient's well-being and privacy. The hospital should also communicate the data breach to the individuals affected.

Example 5

A bank accidently discloses a customer's monthly statement to a third party. The bank undertakes a short investigation and establishes that a data breach has occurred. The bank decides to undertake a more detailed investigation to determine whether it has a systematic flaw that may have or might affect other customers.

The bank is required to notify the Commissioner of the data breach. However, the bank is not required to notify all its customers of the data breach. They should only notify the individuals affected if there is a high risk and it is clear that other customers have not been affected.

Notwithstanding the above, if after further investigation, the bank identifies that more customers have been affected by the data breach, they should update the Commissioner and notify other customers affected if there is a high risk.

Example 6

A university mistakenly sends personal data of a large number of students to the wrong mailing list. The mailing list consists of more than 1500 recipients.

A personal data breach has occurred, and the university is required to notify the Commissioner. The university should also notify the students affected depending on the scope and type of personal data disclosed, and the possible consequences which may result from the data breach.

Example 7

An organisation operates an online marketplace and has customers across several EU Member States. The marketplace suffers a cyber-attack which results in usernames, passwords and purchase histories being published online.

The organisation must notify the lead supervisory authority[8] if the data breach involves cross-border processing. Customers affected by the data breach should also be notified of the data breach as this may result in a high risk to their rights and freedoms. Further, the organisation should take appropriate action to minimise the risks which may result from the data breach (for example, force password resets).

In addition, the organisation should consider other notification obligations such as those under the NIS Directive[9], as a digital service provider.

[8] See the GRA Guidance Note IR02/17 Guidance on the General Data Protection Regulation: (2) Lead Supervisory Authority.

[9] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6th July 2016 concerning measures for a high common level of security of network and information systems across the Union.

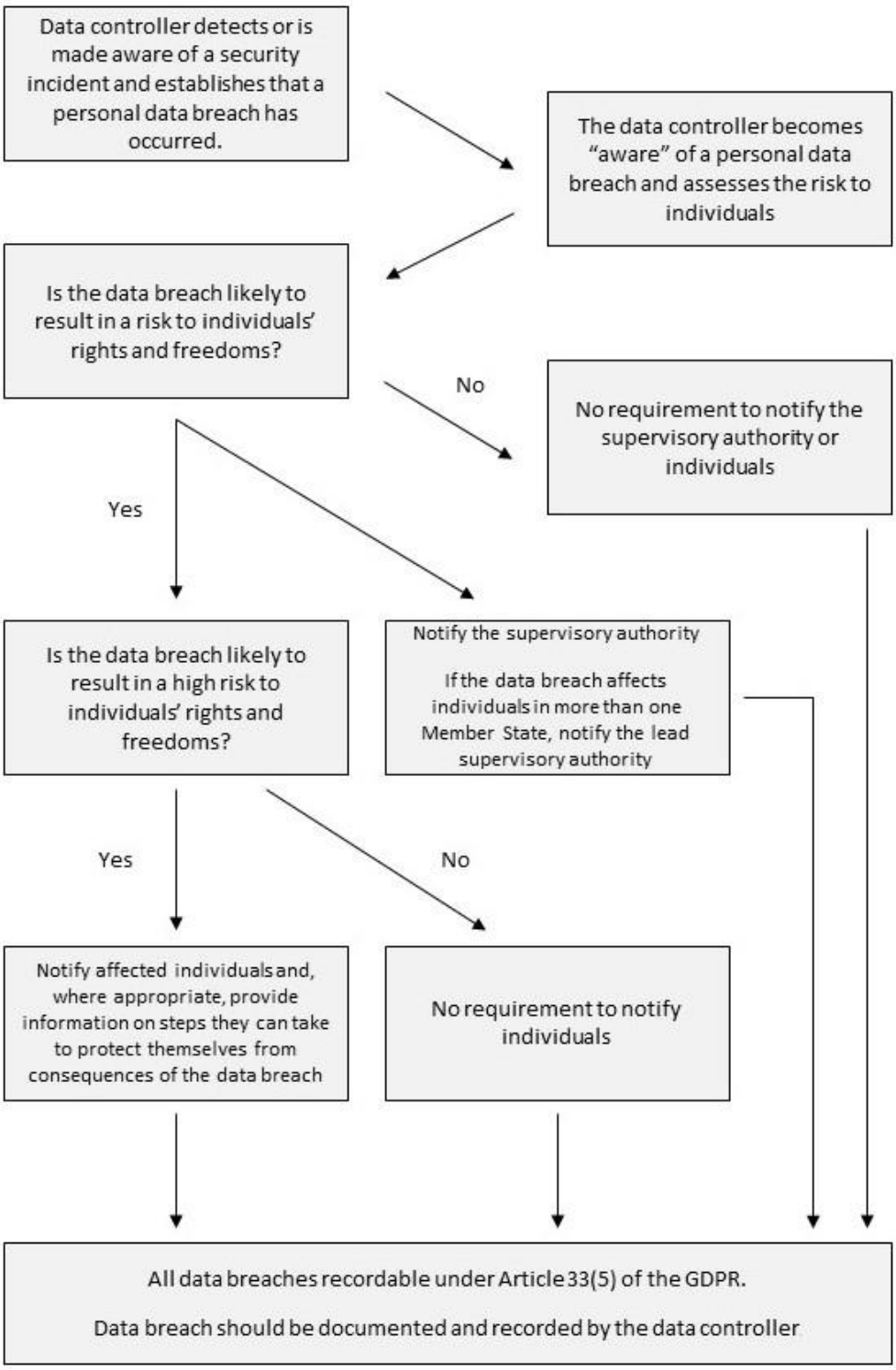
Example 8

A website operator, acting as a data processor, identifies an error in the code which controls user authorisation. As a result, any user can access the account details of any other users of the website.

The website operator must notify the affected clients (the data controllers) without undue delay. On the assumption that the website operator has conducted its own investigation, the affected clients should be reasonably confident as to whether the data breach has affected them, and therefore are likely to be considered as having become 'aware' once they have been notified by the website operator. Each client must then notify the relevant supervisory authority.

Further, if the data breach is unlikely to result in a high risk to the users affected, they would not need to notify the users of the data breach. The website operator should consider other notification obligations such as those under the NIS Directive, as a digital service provider.

ANNEX B – THE FOLLOWING FLOWCHART ILLUSTRATES THE NOTIFICATION REQUIREMENTS UNDER THE GDPR



ANNEX C – DATA BREACH NOTIFICATION FORM

This form should be used by organisations that have become 'aware' of a personal data breach and, having undertaken an assessment of the data breach, are required to notify the Information Commissioner[10] (the "Commissioner"), as the supervisory authority, in accordance with Article 33(1) of the General Data Protection Regulation ("GDPR").

Organisations should not include any of the personal data involved in the data breach when completing this form (for example, do not provide the names and contact details of the individuals affected by the data breach). Should this information be required, it will be requested by our office.

Reporting a Personal Data Breach

1. Contact with the Commissioner

Have you already spoken to a member of staff of the Commissioner's office about this data breach? If so, please provide below the name of the member of staff you spoke to:

2. Your details

The organisation:

Name

Address

Contact details

Person submitting this report:

Full Name

Title within the organisation

[10] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

Contact number

Contact email address

3. Details of the data breach

Please explain and provide details of the data breach, including what happened, what went wrong and how it happened.

How did the organisation become 'aware' of the data breach?

When did the organisation become 'aware' of the data breach?

Date:	Time:

When did the data breach take place?

Date:	Time:

If there has been a delay in reporting the data breach, please explain why.

What categories of personal data have been affected by the data breach? (For example, basic personal identifiers, identification data, official documents, financial details, educational records, health data, criminal data, biometric data etc.)

How many personal data records have been affected?

How many data subjects could be affected by the data breach?

What categories of data subjects have been affected? (For example, customers, employees, patients, children, vulnerable adults, individuals with disabilities etc.)

4. Impact on data subjects

Please describe the possible impact on data subjects, as a result of the data breach (For example, loss of control over their personal data, limitation of their rights, discrimination, identity theft, fraud, financial loss, damage to reputation, threat to professional secrecy, psychological distress etc.)

Has there been any actual harm to data subjects? If so, please elaborate and describe the harm that has occurred.

What is the likelihood that data subjects will experience significant consequences as a result of the data breach? Please give details.

5. Cyber incidents (Please fill in this section if the data breach concerns a cyber incident)

Has the confidentiality, integrity and/or availability of the organisations' systems been affected?

☐ Yes
☐ No
☐ Unknown

If yes, please describe how the organisations' systems have been affected.

What is the impact on the organisation? (For example, has the organisation lost the ability to provide services to all users?)

Has the organisations' systems been recovered?

☐ Yes
☐ No
☐ Unknown

If no or unknown, how long does the organisation predict it will take to recover its systems?

6. Action taken

Please describe the measures in place at the organisation, before the data breach, aimed at preventing a data breach of this nature.

What action has the organisation taken, or proposes to take, as a result of the data breach? (This should include details of the actions taken to mitigate any adverse effects and/or the additional measures implemented by the organisation to prevent future reoccurrences).

Has the organisation informed the data subjects affected by the data breach?

☐ Yes
☐ No
☐ No, but are in the process of notifying them

If no, please explain the reasons for not notifying the data subjects affected.

Has the organisation reported or planning to report the data breach to other organisations? (For example, other regulators or supervisory authorities).

☐ Yes
☐ No
☐ Unsure

If yes, please specify.

7. Submitting this form

Please send the completed form to privacy@gra.gi, with 'Personal data breach notification' in the subject line.

Alternatively, you can post the form to:

FAO: Information Rights Division
Gibraltar Regulatory Authority
2nd Floor, Eurotowers 4,
1 Europort Road
Gibraltar
GX11 1AA

Please note that the Commissioner cannot guarantee security of forms or any attachments sent by email or post.

8. After submitting this form

Our office will review the information provided and provide a response within two weeks from the date the form is submitted. However, organisations should read our guidance to determine what steps it should take in response to a personal data breach and ensure compliance with the requirements of the GDPR and Data Protection Act 2004.

If you require assistance to complete this form, please contact our office on 20074636 (from 9am to 5pm Monday to Friday) or email us at privacy@gra.gi

IMPORTANT NOTE

This document is purely for guidance and aims to supplement the European Data Protection Board's Guidelines on Personal Data Breach Notification[11]. The document does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the Data Protection Act 2004 ("DPA") will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions lies with the organisation.

Where necessary, the Information Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR and the DPA, the GDPR and the DPA will take precedence.

[11] European Data Protection Board, 'Guidelines on Personal data breach notification under Regulation 2016/679' (6 February 2018) < https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 > Accessed 23 November 2018.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi