CONTROLLED DOCUMENT

N.B. Colleagues should be discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.

Personal Data Breach Procedure

CATEGORY:	Procedure
CLASSIFICATION:	Information Governance
PURPOSE:	To set out the procedure and related guidance for reporting and dealing with a personal data breach
CONTROLLED DOCUMENT NUMBER:	BC/IG/010a *(replaces Guidance on identifying and Reporting and Information Governance Incident*)
VERSION NUMBER:	V003
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	GDPR Advisor
APPROVED BY:	Director of Corporate Services
APPROVED ON:	V002 - October 2024 V003 – September 2025
IMPLEMENTED ON:	October 2024
REVIEW PERIOD:	Every 3 years - unless changes to legislation, best practice or internal roles and responsibilities
REVIEW DATE:	Reviewed in September 2025 – to reflect new Executive Team Structure Next full review: October 2027
ASSOCIATED DOCUMENTS:	Data Protection Policy Personal Data Breach Policy
Essential Reading for:	Trustees and all colleagues

Document Consultation and Review Process

Groups/Individuals who have overseen the development of this Procedure:	**Corporate Governance Team, Senior Leadership Team**
Groups/Individuals Consulted:	**Corporate Governance Team, Senior Leadership Team**

Document version control:

Date	Version	Amendments made	Amendments Approved by
October 2024	V002	Fully updated procedure following data protection review and approval of related policy.	Director of Corporate Governance (policy approved by Board in September 2024)
September 2025	V003	Updated to reflect new Executive Team structure and adoption of the term colleague for employee	Director of Corporate Services

For the Use of the Corporate Services Team only:

Date added to Register:	**October 2024**
Date published on Hub:	**V002 – October 2024** **V003 – September 2025**
Does it need to be published on website:	**No**

CONTENTS

1. INTRODUCTION

1.1 The purpose of this procedure is to provide further guidance on our Personal Data (PD) Breach response plan as described in the Personal Data Breach Policy.

1.2 The sections of this procedure contain:

1.2.1 a summary of the PD Breach response plan;

1.2.2 guidance on how to assess the risk to the rights and freedoms of individuals;

1.2.3 a flowchart illustrating notification requirements under the GDPR;

1.2.4 guidance on the notification and communication procedures, including when a notification is – and is not – required; and

1.2.5 [1]further examples of when a notification or communication is – and is not – required.

1.3 A template Personal Data Breach Record is provided separately, which must be completed when we suspect a PD Breach or a PD Breach in fact occurs.

2. SCOPE OF PROCEDURE

2.1 This procedure applies to any suspected or actual Personal Data Breach relating to any Information processed by Brunelcare and, as appropriate, those acting on its behalf.

3. DEFINITIONS

3.1 See the Personal Data Breach Policy for definitions of capitalised terms.

4. DETAILED PROCEDURE

Breach

4.1 If you become aware of a breach of this procedure, you must report it promptly to the Corporate Services Team at dataprotection@Brunelcare.org.uk.

Enforcement

4.2 All Brunelcare's employees (colleagues) bear responsibility for their own compliance with this procedure. Breach of this procedure is ground for disciplinary proceedings against an colleague, which may result in disciplinary action including termination of employment. Breach of this procedure by any non-employee such as a temporary worker, contractor or

[1] Examples have been taken from the Article 29 Working Party a European body that provided guidance on data protection law, particularly the GDPR.

supplier may be a breach of their contract with Brunelcare and grounds for damages or termination.

Ownership

4.3 The Corporate Services Team is responsible for maintaining this procedure and related training and awareness programs.

5. SUMMARY OF PD BREACH RESPONSE PLAN

5.1 Should a PD Breach occur, the response plan set out in this procedure must be implemented to:

- **detect** a suspected or actual PD Breach and **confirm** if a PD Breach has occurred;
- **escalate** a suspected or actual PD Breach to the relevant stakeholders;
- **contain** the breach and prevent recurrence;
- **assess** the risk to individuals;
- **consider notification** - determine whether notification to the regulator or individuals is necessary and make any required notification; and
- **document** the breach throughout, including timings, actions taken, and lessons learned.

The PD Breach Report must be completed for each reported, suspected or actual PD Breach and will help guide you through the process.

6. GUIDE TO ASSESSING THE RISK TO INDIVIDUALS

6.1 Guidelines produced by a Working Party to look at Article 29 of the GDPR and compliance with it, states that:

*'A breach can potentially have a range of significant adverse effects on individuals, which can result in **physical, material, or non-material damage**. The GDPR explains that this can 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 can also include any other significant economic or social disadvantage to those individuals …*

When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.'

6.2 A Data Protection Impact Assessment ('**DPIA**') may have already been carried out on the processing activity in question. While the PIA or DPIA may be helpful, that assessment was a review of hypothetical situations, whereas the assessment in a PD Breach must be

of the specific facts of the breach and the risks from that breach to the rights and freedoms of individuals.

6.3 In assessing the risk, and to make the assessment as objective as possible, we will therefore take into account the following factors (Art 29 WP):

6.3.1 The **likelihood** and the **severity** of the risk. If either one is high, the risk is heightened.

6.3.2 The **data processing context**

<u>The nature, sensitivity, and volume of personal data:</u>

- e.g. is the personal data public? Is it low level, 'business card' data?
- Risk of harm increases with increased sensitivity of the data involved. Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft.
- However, personal data that is not itself sensitive can also have serious consequences and the more personal data involved, the higher the risk. A combination of personal data (or sources of personal data) is typically more sensitive than a single piece of personal data.

<u>The number of affected individuals:</u>

- Generally, the larger the number of data subjects involved, the higher the risk; but a small amount of sensitive personal data can have a high impact on an individual.

<u>The severity and permanence of consequences for individuals:</u>

- The potential damage to individuals from unauthorised disclosure or use of special categories of personal data can be especially severe, in particular identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation.

<u>Special characteristics of the individual:</u>

- The breach may involve personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual(s) that affect the level of impact of the breach, e.g. if a list of telephone numbers includes known members of the national parliament.

<u>Special characteristics of the controller:</u>

- e.g. the risk to individuals is likely higher from disclosure of a customer list from an online pharmacy than from a stationery shop.

6.3.3 The **ease of identification** of individuals. Encryption and pseudonymisation are effective measures to reduce the risk from a PD Breach.

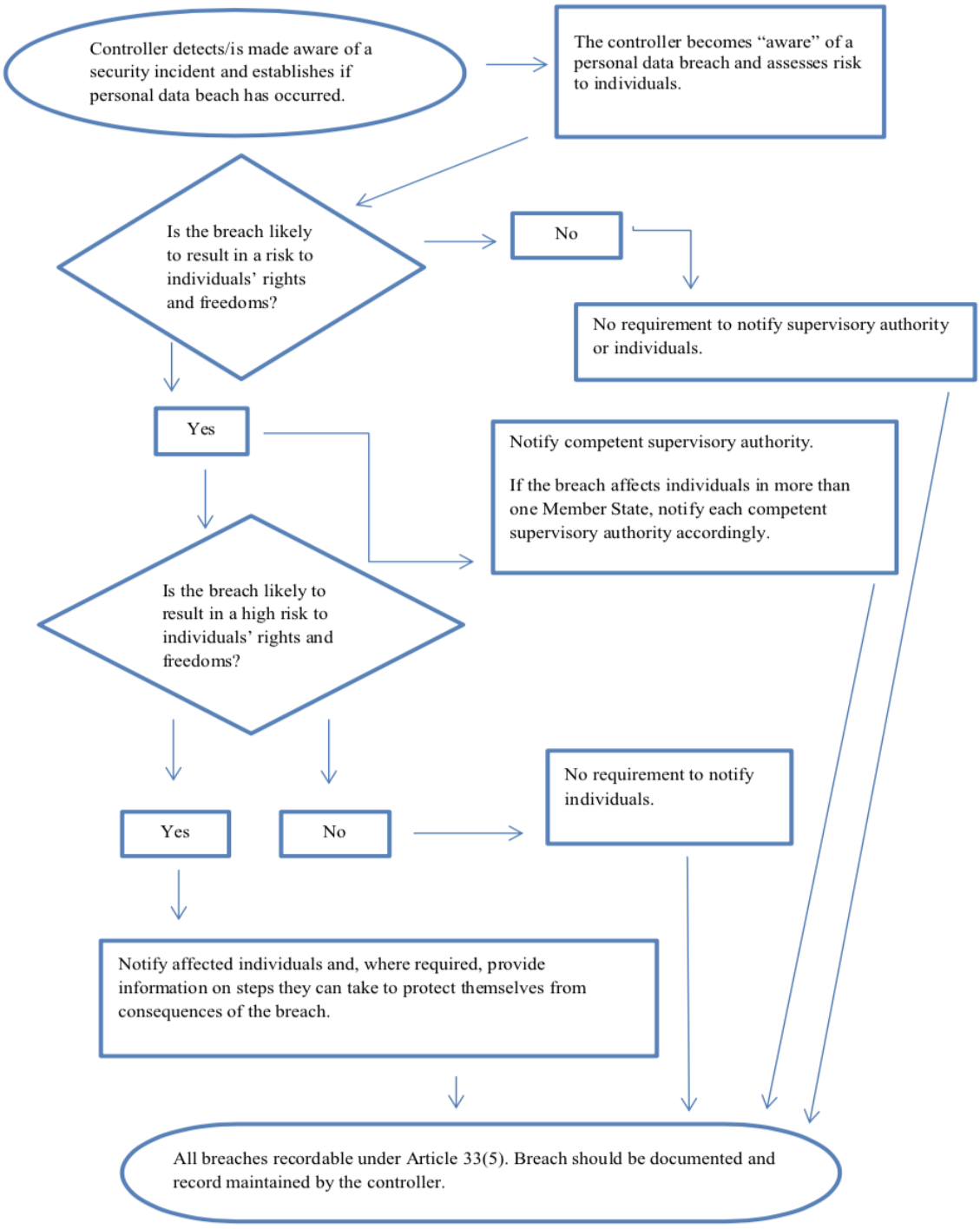
6.3.4 The **circumstances of the breach**

i. Loss of confidentiality, which varies by the scope of disclosure (i.e. the potential number and type of parties that may have unlawful access to the information).
ii. Loss of availability (temporary or permanent loss of use of data).

iii. Loss of integrity, which is most severe when there are serious possibilities that the altered data has been used in a way that could harm the individual.
iv. Malicious intent. Was the breach due to an error or mistake (human or technical) or by an intentional action of malicious intent?

7. FLOWCHART

7.1 This flowchart (by the Article 29 Working Party illustrating notification requirements under the EU GDPR) applies equally to the UK GDPR with references to the EU/Member States replaced with the UK, until disapplied by the UK ICO.



8. GUIDANCE ON NOTIFICATIONS

Notification to the Competent Supervisory Authority

8.1 If you have carried out a risk assessment and reviewed the PD Breach Policy and the guidance in this procedure on when a notification is – and is not – required and you have determined that a notification to the supervisory authority is required because there is a likely risk to the rights and freedoms of data subjects, the notification will be made by the Director of Corporate Services, or their delegate.

8.2 A notification must contain:

8.2.1 a description of the nature of the PD Breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

8.2.2 the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

8.2.3 a description of the likely consequences of the PD Breach; and

8.2.4 a description of the measures taken or proposed to be taken by the controller to address the PD Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.3 As one of the purposes of notification is limiting damage to individuals, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories.

8.4 The UK ICO recognises that it will not always be possible for an initial notification to be comprehensive. The UK ICO: '*will not expect to receive comprehensive reports at the outset of the discovery or detection of an incident – but we will want to know the potential scope and the cause of the breach, mitigation actions you plan to take, and how you plan to address the problem*.'

8.5 As a UK entity, the UK GDPR applies to us and our regulator is the UK ICO. Where the EU GDPR also applies to us, we will also consider notification to regulators in Member States of the EEA.

8.6 If Brunelcare does not make a notification within 72 hours, we will state the reasons why.

8.7 Notifications may be updated, even to include that there was no PD Breach after all, as the Art 29 WP notes: '*A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended*.'

8.8 As the GDPR does not define categories of data subjects, the Art 29 WP suggests this refers to the various types of individuals whose personal data has been affected by a breach and, depending on the descriptors used, this could include:

8.8.1 children and other vulnerable groups,

8.8.2 people with disabilities,

8.8.3 colleagues, and/or

8.8.4 customers.

8.9 Similarly, for categories of Personal Data records, the Art 29 WP suggests this refers to the different types of records that the controller may process, such as:

- health data,
- educational records,
- social care information,
- financial details,
- bank account numbers,
- passport numbers

……..and so on.

8.10 Where we are the controller, it is our responsibility to notify the supervisory authority of a breach. While a processor could make a notification on our behalf, our policy is that this should not happen. Likewise, where we are a processor, our policy is that we will meet our obligation to notify the controller and that it remains for the controller to notify the regulator and individuals.

Communication to Data Subjects

8.11 If you have carried out a risk assessment and reviewed the guidance in this procedure on when a communication to data subjects is – and is not – required and you have determined that a communication is required because there is a likely high risk to the rights and freedoms of data subjects, the communication will be made by the Director of Corporate Services, or their delegate.

8.12 Communications to UK data subjects must usually be carried out in consultation with the UK ICO, our competent supervisory authority, and will describe, in clear and plain language:

8.12.1 the nature of the PD Breach;

8.12.2 the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

8.12.3 description of the likely consequences of the PD Breach; and

8.12.4 description of the measures taken or proposed to be taken by Brunelcare as controller to address the PD Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.13 Communications to data subjects in the EEA will usually be carried out in consultation with the relevant supervisory authority.

8.14 In addition, the communication might:

8.14.1 state that, after having notified the breach to the relevant supervisory authority, we have received advice on managing the breach and lessening its impact; and

8.14.2 where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

8.15 Communication should be:

8.15.1 to the affected data subject(s) directly, unless doing so would involve a disproportionate effort. In such a case, the GDPR requires instead 'a public communication or similar measure whereby the data subjects are informed in an equally effective manner'.

8.15.2 clear and transparent, so they should be in a dedicated message, not sent with other information such as regular updates, newsletters, or marketing messages; and

8.15.3 if appropriate, by means that maximise the chance of properly communicating information to the affected individuals, which may require using more than one means of communication. In cases of large breaches, care should be taken to plan for sufficient resources to deal with data subjects' enquiries, and a dedicated, regularly updated web page is a good additional practice.

8.16 On transparent communication methods, the Art 29 WP:

8.16.1 gives examples of direct messaging such as email, SMS, direct message, prominent website banners or notification, postal communications, and prominent advertisements in print media; and

8.16.2 notes that a '*notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual*'.

When Notification and/or Communication are Not Required

8.17 The Art 29 WP gave the following examples in their GDPR-focussed guidance on PD Breaches in 2017:

8.17.1 '[If] personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority.'

8.17.2 ‘Article 33(1) makes it clear that breaches that are “unlikely to result in a risk to the rights and freedoms of natural persons” do not require notification to the supervisory authority. An example might be where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual.’

8.17.3 *Accidentally sending Personal Data to the wrong department or external organisation with appropriate follow-up* – A common example provided by the Art 29 WP is a Confidentiality Breach where personal data is ‘sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered “trusted”. In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on a case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches.’

8.18 The Art 29 WP gave the following examples in their 2014 guidance on PD Breaches which was also drafted with GDPR in mind:

8.18.1 *Loss of an encrypted laptop* - The Art 29 WP also considered the loss of an encrypted laptop: ‘The encrypted laptop of a financial adviser has been stolen from the boot of a car. All the details of financial assessments - e.g. mortgage, salary, loan applications of 1000 data subjects were affected. The encryption key, the passphrase, is not compromised but no backup is available. … Depending on the exact nature of the data that was breached, misuse of the data may have various impacts on the data subjects. However, as the laptop had full disk encryption (state of the art) enabled with a strong passphrase which has not been compromised, no unauthorised disclosure occurred.’

8.18.2 *Encryption* - A personal data breach only relating to confidentiality, where data was securely encrypted with a state of the art algorithm, the key to decrypt the data was not compromised in any security breach, and the key to decrypt the data was generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key. Indeed, such measures make the data unintelligible to any person not authorised to access it.’

8.18.3 *Cryptographic hashing* – 'Data, such as passwords, were securely hashed and salted. The hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not been compromised in any security breach, and the key used to hash the data had been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access the key.'

8.18.4 *Accidentally placing personal data in non-secure disposal facilities* - The Art 29 WP considered where personal data had been sealed in envelopes and simply thrown in the trash: 'If the envelope had been recovered by the data controller from either of the waste bins and the envelope or otherwise remained unopened it is unlikely that this would adversely affect subscribers; therefore the breach would not need to be notified to the data subjects.'

8.19 If either of these 2 conditions are met (Art 34(3)) then no communication to data subjects is required:

8.19.1 the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data before the PD Breach - in particular measures that render personal data unintelligible to any person who is not authorised to access it (such as state-of-the-art encryption); or

8.19.2 the controller has taken measures after the PD Breach which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise (for example, depending on the circumstances of the case, immediately identifying and taking action against the individual who has accessed personal data before they were able to do anything with it).

8.20 The UK ICO has provided the following examples on GDPR and PD Breaches:

8.20.1 'A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.'

8.20.2 'A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.'

9. IMPLEMENTATION AND TRAINING

9.1 Brunelcare will establish effective arrangements for communicating the requirements of this procedure. This will include:

- All new starters being briefed on the requirements of this procedure as part of their induction to Brunelcare.

- An annual reminder of the existence and importance of this procedure via internal communication methods.

9.2 All colleagues will undertake mandatory training on information governance and security which they will re-take every year. In addition, all colleagues will be required to attend a more detailed data protection training protection training module as part of their induction.

10. MONITORING AND REVIEW

10.1 The implementation of this procedure, and the effectiveness of the arrangements detailed within it, will be monitored by the Director of Corporate Services.

10.2 This procedure will be reconsidered against any legislative changes and reviewed at least every three years.

APPENDIX 1: Schedule 5, Article 29 WP Examples of Personal Data Breaches and Who to Notify

Example	Notify the Supervisory Authority?	Notify the Data Subject?	Notes/Recommendations
A controller stored a backup of a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required.
A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable personal data breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
An individual phones a bank's call centre to report a data breach. The	Yes.	Only the individuals affected are notified if there is high	If, after further investigation, it is identified that more individuals are

Example	Notify the Supervisory Authority?	Notify the Data Subject?	Notes/Recommendations
individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.		risk and it is clear that others were not affected.	affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to the lead supervisory authority if it involves cross-border processing.	Yes, as could lead to high risk	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having “become aware” once they have been notified by the hosting company (the processor).	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.

Example	Notify the Supervisory Authority?	Notify the Data Subject?	Notes/Recommendations
	The controller then must notify the supervisory authority.		
Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to the supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.