BREACH OF DATA PROTECTION – PCC INTERNAL POLICY

At a glance

ICO website refers:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

- The GDPR introduced on 25 May 2018 a duty on all organisations - the OPCC Chief Executive Officer (CEO) as Data Controller and the Joint Data Protection Officer (OPCC and Constabulary) - to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.
- This policy sets out our obligations and how we intend to meet them.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.
- We must ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.
- We must also keep a record of any personal data breaches, regardless of whether we are required to notify.

We will use the below checklist to prepare for a personal data breach

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ We have prepared a response plan for addressing any personal data breaches that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We know who is the relevant supervisory authority for our processing activities.

☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

☐ We know what information we must give the ICO about a breach.

☐ We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

☐ We know we must inform affected individuals without undue delay.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't all need to be reported.

In brief

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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so we will document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. We will assess this case by case, looking at all relevant factors.

Example

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, we would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.
So, on becoming aware of a breach, we will try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party guidelines on personal data breach notification.

What role do processors have?

We organisation does use a data processor, if this processor suffers a breach, then under Article 33(2) it must inform us without undue delay as soon as it becomes aware.

The requirements on breach reporting will be detailed in the contract between us and our processor, as required under Article 28. For more details about contracts, please see our draft GDPR guidance on contracts and liabilities between controllers and processors.

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have “become aware” of a breach.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) 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, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

We will do this.

What if we don’t have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows us to provide the required information in phases, as long as this is done without undue further delay.

However, the ICO expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. We must still notify the ICO of the breach when we become aware of it, and submit further information as soon as possible. If you know you won’t be able to provide full details within 72 hours, we will explain the delay to the ICO and tell the ICO when we expect to submit more information.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see the ICO pages on reporting a breach.

In the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of our breach response plan, we will establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the Article 29 Working Party guidance on identifying your lead authority.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. Again, we will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, we will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

What information must we provide to individuals when telling them about a breach?

We will describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer (Joint DPO) 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, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Does the GDPR require us to take any other steps in response to a breach?

We will ensure that we record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires us to document the facts relating to the breach, its effects and the remedial action taken. This is part of our overall obligation to comply with the accountability principle, and allows the ICO to verify our organisation’s compliance with our notification duties under the GDPR.

As with any security incident, we shall investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What else should we take into account?

The following aren’t specific GDPR requirements, but we will take them into account when we’ve experienced a breach.

We are aware that we may have additional notification obligations under other laws if we experience a personal data breach.

We will consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

The European Data Protection Board, which will replace the Article 29 Working Party, may issue guidelines, recommendations and best practice advice that may include further guidance on personal data breaches. We shall look out for any such future guidance. Likewise, we will be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements that your organisation may be subject to.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of our global turnover. The fine can be combined the ICO's other corrective powers under Article 58. So it's important to make sure we have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Further Reading

- Relevant provisions in the GDPR - See Articles 33, 34, 58, 83 and Recitals 75, 85-88

In more detail - ICO guidance

See the following sections of the Guide to the GDPR:

- Security
- Accountability and governance

GDPR 'in more detail' guidance:

- Draft GDPR guidance on contracts and liabilities between controllers and processors

Existing DPA guidance:

- Encryption
- A practical guide to IT security: ideal for the small business

Other related guidance:

- Guide to PECR
- Notification of PECR security breaches
- Guide to eIDAS

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Following the consultation period, the Article 29 Working Party has adopted final guidelines on personal data breach notification.

The Article 29 Working Party has published guidelines on lead supervisory authorities and lead supervisory authority FAQs.

Other resources

- Report a security breach

For organisations