



SOKE EDUCATION TRUST
SUSTAIN • EMPOWER • TRANSFORM

Personal data breach notification procedure

April 2021

How ready are you?

What is a personal data breach?

The GDPR defines a personal data breach as:

“...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”.

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



The C.I.A.

(no, not that one!)



The C.I.A.

Confidentiality

Integrity

Availability



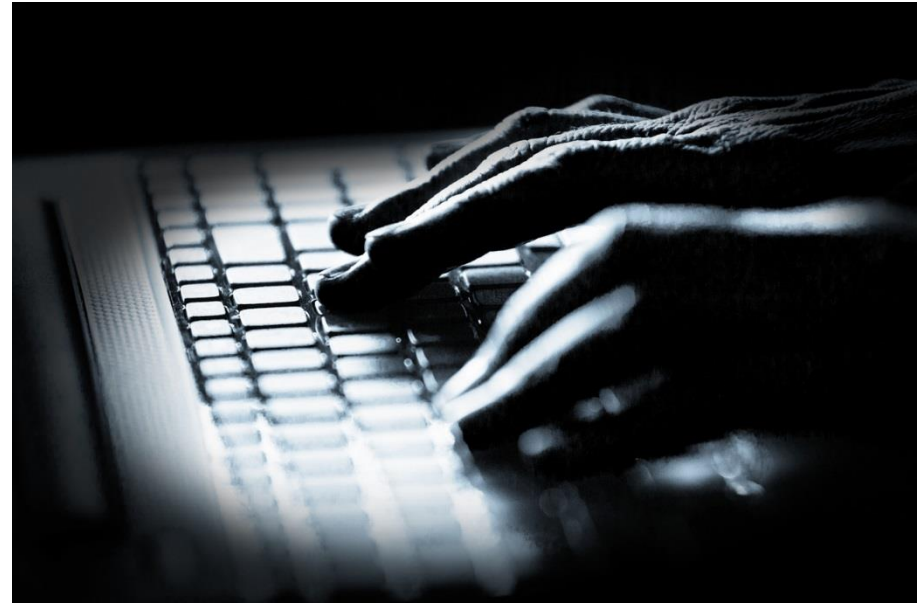
A personal data breach **can** be broadly defined as a security incident **that has** affected **the** confidentiality, integrity or availability of personal data **(or a combination of these)**.



In short, there will be a
personal data breach
whenever:



someone accesses the
data or passes it on
without proper
authorisation



the data is (maliciously
or accidentally)
corrupted, lost, or
destroyed



or if the data is made
unavailable
(eg encrypted by
ransomware, or lost)



Awareness

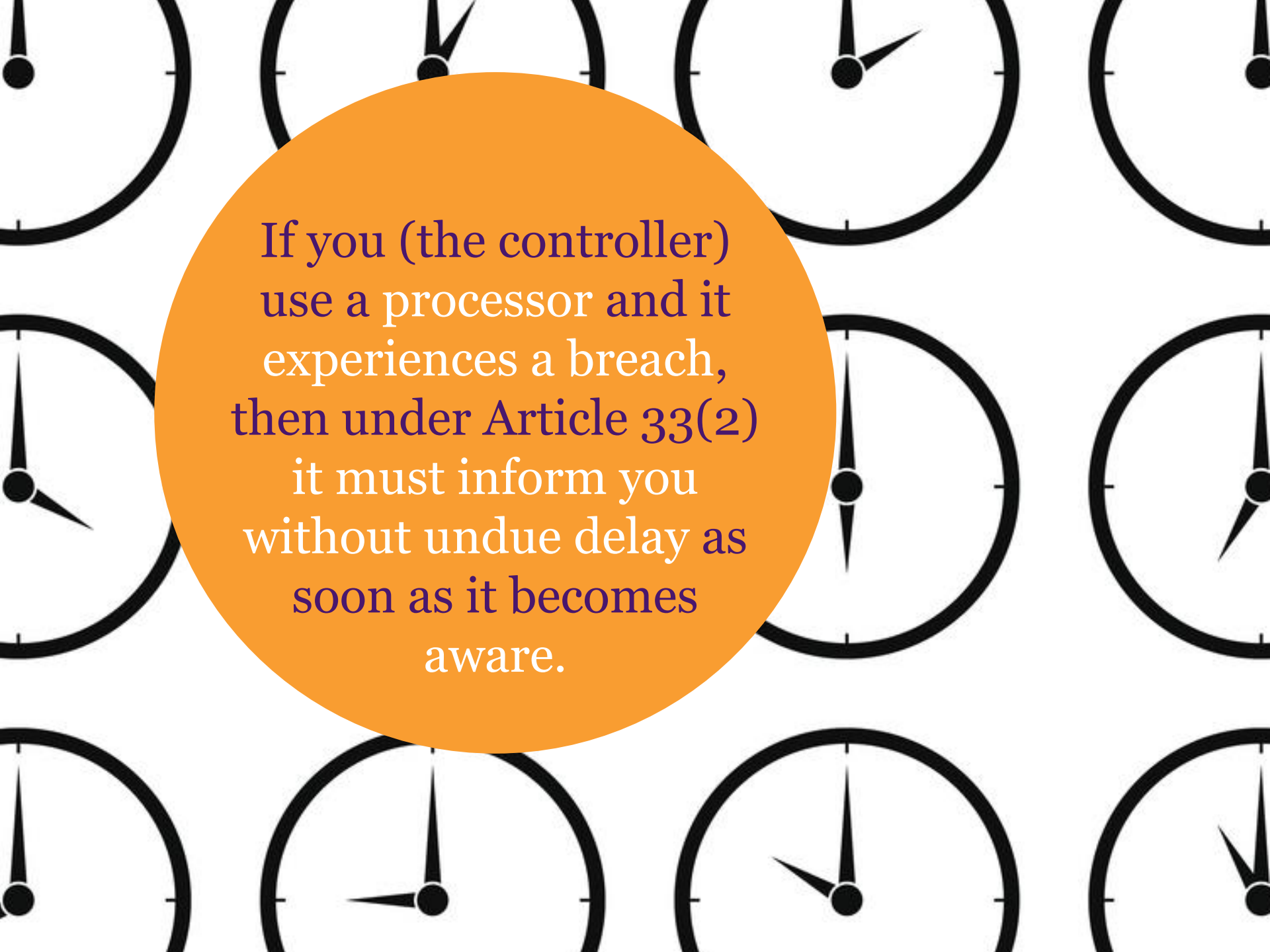
The Article 29 Working Party considers that a controller has become aware of a breach when it has a “reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised”.

It's therefore important for organisations to have in place measures to detect and establish if a breach has occurred and a process for escalating the matter to the relevant person or team responsible for addressing a breach.



Do you use a
processor?





If you (the controller)
use a processor and it
experiences a breach,
then under Article 33(2)
it must inform you
without undue delay as
soon as it becomes
aware.

If you use a processor the requirements about breach reporting should be detailed in the contract between you and your processor, as required under Article 28.



Reporting 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, where feasible.**

If you take longer than this, **you must give reasons for the delay.**





Reporting a breach

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



Reporting a breach

- 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.

Reporting a breach

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 you can provide the required information in phases. We will discuss the timescales for providing further information with you when you first report the breach to us.



If you engage in cross-border processing and a breach occurs, you need to notify your lead supervisory authority – this might not be the ICO.

You should establish who your lead supervisory authority is as part of your breach management plans.



Risk assessment

Not every breach needs to be reported...

...but you will need to notify unless it's unlikely to result in a risk to individuals' rights and freedoms (and you can demonstrate this).



When assessing risk, you should be considering a combination of the severity and the likelihood of the potential negative consequences of a breach.

Some factors to consider include:

- the type of breach
- the nature, sensitivity and volume of personal data
- the ease of identification of individuals
- the severity of the consequences
- any special characteristics of the individual / controller

CHECKLIST





Contacting individuals

If there is a high risk to individuals' rights and freedoms then you will need to inform them too.



A high risk means the potential or actual consequences for individuals is more severe. This is part of the reason for telling individuals about a breach involving their personal data – to help them take steps to protect themselves from its effects.

When telling individuals about a breach you need to 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 (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 and including, where appropriate, of the measures taken to mitigate any possible adverse effects.



Contacting individuals

- Be clear on what you need to tell them and when.
- Informing individuals can help them to take steps to protect themselves from the effects of a breach.
- You should tell individuals what you're doing to mitigate the breach, and how they can protect themselves from the impact of the breach.

The background of the slide is a photograph of a row of metal lockers. The lockers are in shades of beige and brown, with silver-colored handles. A dark teal speech bubble with rounded corners is overlaid on the right side of the image, containing the main text.

Even if you don't need to notify a breach, remember the GDPR requires you to document:

- the facts relating to the breach
- its effects; and
- the remedial action taken.

This helps you to meet your accountability obligations.



If you fail to report...

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2% of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58.

So it's important to make sure you have a robust breach-reporting process in place to ensure you can detect and notify a breach, on time; and to provide the necessary details.

A hand is holding a stack of white leaflets. The leaflets have a red and orange graphic and text that reads "How much do I need to know about data protection?" and "ico." Below this, there are four bullet points: "Data Protection", "Data", "Data Protection", and "Data Protection". The background shows stacks of other leaflets in blue, green, and yellow, suggesting a public information event.

Further information is available!

Pick up some leaflets on your way out!

More resources are available on the ICO
website: ico.org.uk

