Bluecode Labelling Technology Ltd

Personal data breach notification policy

Recognising a personal data breach

A personal data breach is:

"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 in connection with the provision of a public electronic communications service".

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by the controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing data without permission
- Loss of availability of personal data

What we must do if a breach is identified?

- Investigate the breach and establish the likelihood and severity of the risk to people's rights and freedoms
- If a risk is likely: we must inform the ICO and the affected individuals within 24 hours of the breach being identified
- If a risk is unlikely: we will document our investigation findings and our justification for not notifying the ICO

How we will notify the ICO if required?

We will complete and submit the ICO breach notification form to the ICO. Where applicable we will attach supporting documents to the form.

This notification must include at least:

- our name and contact details;
- the date and time of the breach (or an estimate);
- the date and time we detected it;
- basic information about the type of breach; and
- basic information about the personal data concerned.

If possible, we will also include full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about our notification to customers. If these details are not yet available, we will provide them as soon as possible. We will submit a second notification form to the ICO within three days, either including these details, or advising how long it will take us to get them.

We understand that failure to submit breach notifications can incur a £1,000 fine.

When and how we will notify our customers

If the breach is likely to adversely affect the personal data or privacy of our customers, we will notify them of the breach without unnecessary delay.

We will tell them:

- our name and contact details;
- the estimated date of the breach;
- a summary of the incident;
- the nature and content of the personal data;
- the likely effect on the individual;
- any measures we have taken to address the breach; and
- how they can mitigate any possible adverse impact.

We are not required to tell subscribers about a breach if we can demonstrate that the data was encrypted (or made unintelligible by a similar security measure).

If we do not tell our customers, the ICO can require us to do so if they consider the breach is likely to have an adverse effect on our customers.

What are we required to record in our data breach log?

We will keep our own record of all personal data breaches in an inventory or log.

It must contain:

- the facts surrounding the breach;
- the effects of the breach; and
- remedial action taken.