Data breach policy

Finding out about a data breach

If in doubt the ICO's guidance is worth reading. They define a data breach as:

> *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.*
>
> *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.*

There are many possible ways to find out about a breach, from causing it yourself to being told that a 3rd party has had a breach we're affected by or by discovering a hack of our systems.

As soon as finding out about a data breach

All important to do quickly, but in no specific order (depending on the situation, use your judgement)

Tell others

- Tell Sym right away, using a method of communication they are likely to be checking (or as many methods as you have)
- Let the other core team members know
- Make sure the board knows (get Sym to contact them)

Start investigating the breach

Make some initial attempts to find out:

- What information was compromised
- If other data is at risk or compromised
- How many people's data is affected
- Other things that might have lead to the breach
- If it was caused by a 3rd party (because a service we use was compromised)

Make notes about everything, they will be needed later by you and others.

Next steps

Once we have told everyone and done the initial work of finding out what happened and who is affected, we need to start telling others and investigating fully.

Tell others

The people affected need to know what has happened. We should be open and honest with them about what's gone on, even if we don't yet know all the details. Better to alert someone quickly than wait longer before giving them 100% of the information. We can always update them later.

This policy goes beyond the GDPR requirements as they don't require us to notify affected people in all cases. See the "When do we need to tell individuals about a breach?" section of the ICO guide.

Find out more about the nature of the breach

Exactly what information was compromised and how many people were affected?

Decide if the breach needs reporting to the ICO

If it needs reporting then it must be done within 72 hours of discovering the breach. They will need the details from the notes and investigation above, contact information for someone to talk to about the breach and some idea of mitigation and next steps, where possible.

This should be a conversation with Sym (and maybe someone from the board, if time allows).

If the decision is taken not to report to the ICO then notes on why must be kept.

Debrief

- Think about limiting any future risk, is the something that could have been avoided?
- Did this process work well? What needs changing?