G.D.P.R. breaches in small organisations

Nicky Ackerley BA(Hons)

Nicky Ackerley BA(Hons)

Nicky is the owner of HR Support Consultancy. She has a BA(Hons) in Business Studies, is a member of the Chartered Institute of Personnel and Development and has been a practising HR manager for more than 20 years. HR Support Consultancy has provided the BVNA Members Advisory Service (formerly known as the Industrial Relations Service) since it began in 2002.
Email: nickyackerley@hrsupportconsultancy.co.uk

You have your G.D.P.R. policy in place, staff have been trained, you are complying with all good practices regarding data protection, and then… there is a breach of personal information.

Data breaches can occur for a number or reasons, it could be access by an unauthorised third party; it could be deliberate or accidental action (or inaction) by a controller or processor; personal data could have been sent to the wrong recipient, a lap top could have been stolen from a car, an operator may have altered records unlawfully, but whatever the cause, the reporting requirements remain the same. 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'.

The process to report a data breach is the same whatever the size of the organisation.

You might be the Data Protection Officer, or your organisation might not have this post and you are the person with responsibility for data protection, do you know what to do?

The first thing to do is to find out what has happened. You may or may not have to report the breach to the Information Commissioners Office (ICO) and you may or may not have to inform the individuals concerned.

If you are required to report the breach to the ICO, this has to be done within 72 hours of you knowing about the breach.

If you have good systems in place to detect breaches, for staff to internally report breaches and for you to investigate, this will help you decide on what action you need to take. Do you have a response plan in place to help you manage a breach?

As an organisation you need to keep a record of any personal data breaches, whether or not you are required to report the breach to the ICO or to individuals. You should investigate the cause and put safeguards in place to prevent a reoccurrence.

You do not need to report every breach to the ICO.

You need to assess whether the breach that has occurred poses a risk to people 'the likelihood and severity of risk to people's rights and freedoms'. If it is likely there will be a risk, then you should report this to the ICO. If it is unlikely, then you do not have to report it to the ICO (but you do need to keep a record yourself). There is an assessment tool on the ICO website that will help you to decide if you need to report it https://ico.org.uk/for-organisations/report-a-breach/ The ICO can also advise you about any further steps you might need to take and can support you if you are not sure if you need to report the breach or are doing this for the first time.

If you decide you do need to report the breach to the ICO you can do this online or by telephone, the number is 0303 123 1113 and the link to the website is https://ico.org.uk/for-organisations/report-a-breach/

The information you will need to have available is:

- What has happened;
- When and how you found out about the breach;
- The people that have been or may be affected by the breach;
- What you are doing as a result of the breach; and
- Who they should contact if they need more information and who else you have told about the breach.

What if you decide there is a high risk to the rights and freedoms of individuals? In this case you should notify these people 'without delay'. This is *in addition* to notifying the breach to the ICO. (The ICO can compel you to notify individuals if necessary).

In summary, it is best to be prepared for a potential data breach and have plans in place in case it happens. Record the incident internally, assess the risk and notify the ICO within 72 hours if necessary. Take advice from the ICO if you are unsure.

For further support with this or any other HR issue, BVNA members can call the BVNA Advisory Service Helpline on 01822 870270 or email AdvisoryService@bvna.co.uk

DOI: 10.1080/17415349.2020.1826769