TIPS FOR IMPLEMENTING EFFECTIVE PRIVACY TRAINING IN YOUR ORGANISATION

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Delphine Daversin | January 28, 2020

Human error is the primary cause of personal data breaches[1].

The consequences of a data breach can be detrimental to a company and includes, not only direct damages and sanctions, but also substantial reputational harm.

The mere occurrence of, as well as the costs and consequences of data breaches and data incidents could be drastically reduced by having appropriate awareness and training programs in place for your organisation. Having a well-crafted training program which suits your industry and organisation, as part of your privacy programme, is absolutely crucial.

Moreover, training your staff is part of your obligations under data privacy laws and is one of the measures demonstrating your compliance[2].

Here are a few tips to create an effective privacy training programme for your team.

1- Know your audience

To be effective, training should not be a “tick-the-box” exercise and should be tailored to fit the needs of your audience. It is far more effective to provide role-specific training as opposed to generic training.

The training can extend beyond your employees and in certain instances, it is advisable to train your suppliers and business partners as well.

2- Avoid generic training packages

Remember that training is meant to communicate the organisation’s privacy policies and processes (such as data collection and retention, access control, data subject access requests, breach or incident reporting, etc.).

Therefore, your training content should be tailored to your organisation's privacy statement, corporate culture and specific policies and processes. The cookie-cutter approach will have less impact on your team: we strongly recommend crafting a customised training programme for your organisation.

A customised training program will make it more relevant and more attractive to your audience. For example, you could leverage privacy incidents which occurred in your own organisation.

3- Use multiple channels and resources

Classroom training is the most common means of training but should be reinforced by various complementary channels, such as:

– Online learning through streaming, videos and websites

– Workshops and simulations

– Posters, Newsletters and emails campaigns

– Booklets, Pamphlets, FAQs, and stickers can also be a cool way to convey a few simple but necessary messages regarding privacy at the office.

The more creative and varied the communication channels are, the more effective it is at conveying the message to the organisation. However, irrespective of the variety of channels, the communication should be consistent at all levels.

It may be also beneficial to establish a privacy community to deliver privacy messages throughout the organisation. This can be done, for example, by appointing a "privacy champion" in each department, who follows up on training and awareness within his/her own department and reports difficulties or specificities. This makes it easier for the information officer to refine or accurately customise the privacy training.

4- Keep training

Privacy awareness amongst your team is an ongoing effort. The privacy training should be part of the induction process in your organisation. Each member of your team should receive an initial training, and this training should be regularly refreshed and updated.

5- Track attendance and results

Although privacy training has cost implications for your organisation, it will most certainly reduce risks. It therefore makes sense to implement methods to measure effectiveness of these programs.

As an example, a simple dashboard of your training and awareness could include the following metrics:

– Percentage of the workforce which received training during a given period;

– Type of training received;

– Percent of training completed;

– Evolutions of results to quizzes or simulation exercises; and

– Evolution of the number of privacy incident reports.

We can help you design and implement a fully customised training programme for your organisation in 2020! Please do not hesitate to contact us for Good, Clear, Precise Advice.

[1] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[2] Article 39, Regulation (EU) 2016/679, General Data Protection Regulation, ("**GDPR**") or Article 8 of Protection of Personal Information Act, 4 of 2014 ("**POPIA**")