FOCUS

DATA PROTECTION TRAINING AND COMPLIANCE

When DPOs become teachers

Data protection training is important for several reasons. Training is a legal requirement to ensure that an organisation complies with the data protection and security obligations under the General Data Protection Regulation (*679/2016/EU*) (GDPR). Furthermore, an organisation needs to train its staff to ensure that everyone plays their part in ensuring compliance and to prevent human errors: a compliance chain is only as good as the weakest link.

Every controller must respond to data protection requests from individuals without delay and within a month of receipt of the request. However, if staff are not trained on what is and what is not a request, it will be difficult for an organisation to comply with this requirement. Records of processing activities will not be updated if staff are not trained on which information to report. Incident response plans may not work in practice without training.

When investigating a complaint, the regulator may ask to see proof of training. Fines for a breach of the accountability principle under the GDPR attract the higher of €20 million or 4% of group worldwide annual turnover. Claims for compensation will likely be upheld if the data controller fails to demonstrate that it has trained staff and that it is "not in any way responsible for the event giving rise to the damage". The lack of a comprehensive training programme can aggravate any fines or damages awards against a data controller.

Under the GDPR, certain organisations are required to designate a data protection officer (DPO), who must fulfil certain responsibilities and undertake tasks, including monitoring compliance. The DPO therefore has a significant role in ensuring that an organisation provides adequate training.

Training needs

In practice, most organisations will be unable to demonstrate compliance without a training programme. An organisation needs to consider the following key questions in compiling an adequate training programme.

Who to train. A failure to train staff that contributes to a personal data breach will not go unnoticed by the regulator. For this reason, data protection training should be mandatory for all relevant members of staff. Training needs to be relevant to a person's role. General training can be given to all staff, but it is essential that teams receive specific training, so that people can understand what they need to do when going about their day-to-day work.

Organisations need to think about attendance lists and make sure that the training is mandatory. Reminders should be sent out for anyone who should have attended the training but did not.

What is the training. Each part of the content should attempt to deliver a key message with impact. A good starting point is the saying that "less is more"; in other words, training should not bore people with too much regulatory text with which they are unlikely to engage.

General data protection training should be high level and include images and examples (*see box "Content of training"*). Most people will bring their prejudices to the training and may expect it to be boring. Anything that dispels this view is useful: staff are more likely to respond to a headline from the newspapers, a quote or an image. The customer services team may be more interested to hear a recording of a person who managed to circumnavigate a customer authentication process than looking at a bare list of data protection principles.

Specialist training could include an analysis of legal text, case law or regulatory opinions. Nevertheless, images, sounds and videos that set the scene can help to capture the level of attention that is needed to deliver the underlying narrative to the audience.

When to give training. Training should be given as soon as the need for training arises. General security and data protection training should be given during induction in the first week after joining the organisation. Teams should receive appropriate training before starting any activity that may involve data processing.

Regular refreshers will be required to keep the training effective. Awareness-raising initiatives can help to keep the sometimes complex data protection rules in peoples' minds: without a constant dialogue, people are likely to forget.

As a rule of thumb, a person should receive training on joining a new role, and then refresher training should be given at least once every two years or if there is a change in the processing, such as new systems, a change of responsibilities, a change in procedures or policies, or new acquisitions.

How to deliver training. The form of training will be determined by the type of audience and the training objectives. Training has to be delivered in a way that ensures that knowledge is retained but the number of training sessions and content must not be overwhelming. The training has to be effective: if it is a mere tick-box exercise, the GDPR requirements will likely not be complied with.

General training

To catch peoples' attention, training should be simple, playful and relatable. Most DPOs never imagined that they would have to try capturing their colleagues' attention in a similar way to how they may try to entertain their children when teaching them at home. A way to get attendees' attention is to mention

something from the news that everyone has heard about, explain its relevance to data protection and how it may relate to the organisation and the staff's daily tasks.

Quizzes are a well-known technique to reinforce learning, but they should be entertaining. Asking "which policy says that staff must..." will probably not be well received. A different approach is to ask which celebrity used facial recognition in a bid to detect stalkers or how much large technology companies got fined for identifying users' friends in photos. Using things like prizes for winners may help with encouraging staff to engage with the training, but ideally everyone should be rewarded.

Trainers should find ways to engage the audience using interaction. Workshops, Q&As, games or inviting external speakers will help. A "true or false" game where everyone has to put their hand up usually gets people thinking and then talking about what went wrong, what went well and who deserves a commendation. Trainers should encourage members of the audience to give their opinions and engage in the conversation.

Training may be more effective when testing is included. A minimum pass rate should be set where it is critical that everyone gets the message. Simple testing should always be considered to measure the success of training and to assess future training needs.

In a smaller organisation, it may be best to get everyone in a room, whereas larger organisations will benefit from online solutions. However, online training alone may not achieve the training objectives in practice. To be effective, staff should experience real-life examples from their daily work environment and develop an understanding of how data protection applies to them. Remember that staff without access to devices also need to be able to complete the training.

While organisations are operating remotely due to the 2019 novel coronavirus disease pandemic, online presentations with quizzes can prove successful. Thousands of employees can join a virtual training session and recorded sessions can be distributed to those who could not attend.

Content of training

The content will depend on the audience, objectives and the form of training. However, general data protection training should attempt to cover:

- What is data protection and the General Data Protection Regulation (*679/2016/EU*)?
- The risk of investigations, fines and claims for compensation.
- What is personal data?
- Controllers and processors.
- Data protection principles in practice.
- Accountability including data protection impact assessments and record keeping.
- Data sharing.
- Data transfers.
- Requests from individuals.
- Security best practices, common risks and failings.
- Data breach escalation.
- Records management.

Key messages should be included throughout the content and they should also be summarised at the end.

Department-specific training

Department-specific training should be heavier on content but generally easier to deliver. The training should focus on everyday activities in the department and content should be relatable. Participants should be encouraged to ask questions and share their experiences.

Trainers should talk about common use cases. For example, they should anticipate what requests the customer services team may face and teach them how to distinguish between a data protection request and a service request. If a customer is trying to resolve a billing issue and asks questions about their account, this may not necessarily constitute an access request. It is often best for both parties to resolve requests informally and even if the customer uses data protection language, perhaps fulfilling the service query in a satisfactory manner will diffuse the situation. However, if the customer still insists on making an access request, the employee should pass the request to the privacy team.

Specialist training and DPO training

Specialists, including DPOs, will often already hold data protection certificates and they will have a natural interest in data protection. Based on the job role, individuals who are in positions such as DPO, chief information security officer, risk owner, record manager or information security professional should engage in continued education by attending external events and continuing professional development.

While tabletop event simulation exercises can be effective for incident response planning, most specialist training and DPO training will have to be provided externally by law firms or information security firms.

The DPO must possess professional qualities, including expert knowledge of data protection law and practices, and the ability to fulfil their tasks. One of these tasks is awareness raising and training, which suggests that the DPO should have experience or be trained in presentation and teaching skills, so it is not just about data protection.

Open a channel of communication

Training is a great way for the data protection team or DPO to introduce themselves and start a conversation with staff. People should have a means to give feedback, ask questions and understand how they can communicate with the team.

Online platforms

Organisations should consider a suitable platform for delivering external training, hosting training prepared internally, distributing recorded sessions, and testing and keeping participation records. They should designate specific individuals to keep appropriate records.

For communications, organisations should consider a platform that can help with frequently asked questions and that can effortlessly connect staff with the member of the data protection team who is available at the time. In a busy work environment, email may not be the best way to achieve this.

Raising awareness and a culture of compliance

Awareness campaigns should coexist alongside the training programme to help staff remember that there are real consequences if the organisation fails to comply with its GDPR obligations. Leaflets on information boards, informative emails or prize draws are all tactics that can be deployed. A monthly data protection newsletter could inform staff about data protection developments around the world with a focus on topics that are relevant to the organisation's biggest risks. To attract readers, topics of popular culture and interesting news with a connection to data protection could be included. Significant days in the calendar could be repurposed for awareness raising; for example, the annual Data Protection Day on 28 January should have a place in an organisation's privacy calendar.

Governance

Data protection training requires evaluation, effort and commitment. Training programme governance should ensure that:

- The need for training is properly assessed.
- Training strategies are in place to meet training needs within agreed timescales.
- Execution is measured through key performance indicators.
- Training is provided to all relevant staff, including officers, temporary staff and contractors.
- Content is carefully crafted including business function and sector-specific requirements.
- The training programme is approved by senior management.
- There are dedicated resources assigned to deliver training.
- Participation is mandatory and enforced by HR.
- Responsibilities are assigned for managing and co-ordinating training.
- Appropriate records are kept.

Marta Dunphy-Moriel is a partner, and Alex Dittel is a senior associate, at Kemp Little LLP. *The authors would like to thank Ben Westwood, Regulatory Compliance Officer at IHS Markit for his input.*