The Why and How of a Privacy Awareness Program.

For every organization, privacy awareness plays a large role in the success of risk mitigation. Whether an organization is large or small, it is essential that privacy is taken seriously. A successful privacy program requires many elements can include technical solutions - such as encryption, firewalls and virus scanners, procedural elements, processes and more. However, one of the elements that can make the biggest difference is the human one. Knowing how to deal with risks to private data and how to respond to threats is essential. The way people handle privacy can be your strongest shield. This makes an informative and engaging privacy awareness program essential.

1 Why is a Privacy Awareness Program important?

Aside from that fact that employee awareness is key for success, it is also a mandatory part of the GDPR regulation. The second subpoint under the heading 'Tasks of the Data Protection Officer' (Section 4, Article 39) in the General Data Protection Regulation (GDPR) states:

> *'to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities,* ***awareness-raising*** *and* ***training*** *of staff involved in processing operations, and the related audits;'*

The GDPR does not go into further detail regarding what awareness-raising and training should entail. This is why it is important to consider a range of factors when deciding what kind of privacy awareness program is appropriate for your organization. The privacy awareness program should, as stated, make those employees and contractors who deal with the protection of personal data aware of their responsibilities and how to execute them. However, it may also be relevant to the broader organization to have a basic awareness of privacy. Especially if the type of work done in the organization is focused around the use of personal data. By creating broader awareness, you help create a mindset that encourages people to be proactive and vigilant.

2 Who should be involved in a Privacy Awareness Program?

A privacy awareness program is specifically required for employees who are involved in processing operations and audits, but the program should span beyond just those groups. Throughout the organization there is a need to understand the importance of privacy, to support those directly responsible for delivering on those requirements.

2.1 Support of Senior Management

To get started, it is essential that there is buy-in for the initiative to ensure its success. This means that it is important to get support from senior management (or C-level). In organizations of any size, it can be complex and time consuming to secure endorsement from management. This is, however, an essential step to ensure that the required resources and time is made available. The trainings should be engaging and true-to-life to ensure that employees take the information on board; and budget and resources impact the quality of the training you are able to provide. Visible support from the C level also increases the likelihood of getting support from other departments, which helps when you need their expertise (for example, IT for technical support and marketing for communication to the organization).

One of the questions you may face from senior management will be regarding Return on Investment (ROI). You should include a reminder in your request that this is not optional, GDPR requires awareness raising and training. But you should also be prepared to show how a good privacy awareness program is a good investment, how it will save your organization money and lower risk. One approach is to reference research showing that companies in your industry with strong awareness programs have fewer reportable breaches or have fewer records lost per breach then those without, etc.

2.2 Key Departments

Once you have the support of senior management, work with other departments in the organization to leverage their expertise in creating or rolling out a privacy awareness program. The most successful awareness programs involve multiple departments to ensure buy-in from the entire organization. Some of the departments you may wish to involve include marketing, human resources, legal, compliance, privacy and physical security. For example, if your organization has a legal and/or compliance department, they can often make privacy or security awareness training mandatory (including for new hires). Also, the communications department often has control over approval and distribution of internal newsletters. Marketing is all about catching people's attention, making them aware of something new and inspiring them to action. Too often privacy and security training is created by technologists of compliance people;

why would you do this when you have potentially decades of experience available in your Marketing partner? Working together with other departments not only means expert resources are shared but also that more activities can be coordinated which often leads to better results. Of course, it may also be the case that your organization does not have all of these departments. Then it becomes key to see what you can do with the resources you have available.

2.3 Processing and Auditing Employees

As the key target of a privacy awareness program, you could involve the employees who deal with processing and auditing directly in the process of creating training material. It is a good idea to engage with your target audience to find out whether there is a preferred format for the training and also to see what level of training is required. You may also want to consider testing the material before rolling out a training to all of the employees (depending on the size of your organization).

2.4 The Wider Organization

You may want to consider sharing some key points of the privacy awareness program with the entire organization. This can be done through short online trainings, newsletter or any other format that isn't too content heavy. It is important that good privacy awareness is not just focused on the main targets of the GDPR as this can lead to a lack of understanding outside their immediate team or department. To ensure that data privacy is taken seriously, it is best to create a basic on-boarding awareness program and regular touchpoints to refresh this awareness.

3 What should be included in a Privacy Awareness Program?

Naturally, what you include in your privacy awareness program will depend on the target group. Although you may be inclined to focus on news-worthy subjects, it is actually better to take a look inside your own organization for inspiration first. A training that is based on real-life examples from within your organization will be much more impactful than examples from other companies or news stories. Risks that need to be controlled or mitigated within your own organization offer great subject material for a privacy awareness program. An example that is applicable to most organizations and is a significant risk is ransomware. Teaching employees how to detect and report ransomware is essential in mitigating risk. Your organization most likely has a range of policies; it is unrealistic to expect ALL employees to retain all the information about these policies. In many organizations, even reading and understanding them is a hard requirement. Creating targeted content for each key subject means that you can select elements for

the different awareness trainings. You can focus on a broad or specific aspect, depending on what the target of the training needs. It is important that awareness moments are scheduled regularly. Short and regular bursts of information are much more likely to be remembered and will help instill the culture of privacy awareness across the organization.

4 When should you implement a Privacy Awareness Program?

A privacy awareness program should not be a one-time initiative. It is an exercise that will need to be repeated on a regular basis to keep the knowledge of employees up-to-date and top of mind. The training program specifically for employees who directly involved with processing and audits should be repeated regularly. More general awareness initiatives can be bolstered by related events in the real world – security breaches, stolen logins or ransomware for example. Informing employees as to the best way to deal with these threats when they are currently in the news makes the information more engaging and successful. Another example is Data Protection Day (or Data Privacy Day in some parts of the world) which occurs every year on the 28th of January. This is an ideal moment to give employees throughout the organization a refresher – whether that is in the form of a newsletter, a short quiz or other engaging content.

Aside from this, new employees can join the organization at any time. This is an ideal moment to share the organizational mindset regarding privacy awareness. So, a privacy awareness introduction is a valuable addition to your onboarding program. This can be supplemented, depending on the role of the individual, with specific training if needed.

5 How should you create and deliver a Privacy Awareness Program?

As a general rule, people don't take well to being told what they can or cannot do. In this respect, it is highly advisable to focus on how to conduct actions safely, rather than a "Do Not Do" list. Also, ideally, an awareness program should not be limited to the office. By helping employees understand how to deal with information safely at home as well, you are actively helping them at a personal level and are instilling a mindset that will help at work. Consider social networks. Rather than telling employees they are not allowed to access a social network, teach them how to safely use it instead. The key is to help enforce positive habits. Although many aspects of security are seen as common sense, without some understanding of the rationale, it's often not so common at all. It is crucial to deliver a privacy awareness

program in a way that is accessible and realistic. Talking down to employees or making the content too dry will not serve you well and will most likely decrease the success of your program.

5.1 Creating the Program.

Before you start to put together your privacy awareness program, you will need to take some information into consideration. The size of your organizations will impact the resources and scale of the program. It is easy to take the data protection objectives as the focus of your campaign. But try to combine them with the wants/needs of the employee – otherwise engagement will be low.

5.1.1 Target Audience.

If you are creating an awareness program that covers multiple target groups, remember that different groups will respond better to different formats and styles and that you may need to try multiple approaches or provide multiple options. For example, senior management may appreciate a newsletter or short articles whilst employees in the wider organization, particularly younger ones, may prefer a video or more interactive content.

5.1.2 Format.

There is a wealth of privacy awareness information available and some of it is specifically designed for training use. Below is a (by no means exhaustive) list of possible options to consider:

- Computer-based training;
- Games;
- Phishing simulations;
- Videos;
- Newsletters;
- Blogs;
- Posters;
- Team security/privacy champion programs.

Aside from the format, it is also important to remember that you must package the content in a way that is appealing. If you can work together with a marketer, designer or other content specialist to create the program materials, it could significantly increase engagement.

5.2 Communicating.

Before rolling out your privacy awareness program you should communicate the launch date and the activities that will be part of the program. Make sure to include any information about whether activities are mandatory or not. This will give employees a clear idea of what to expect and what is expected of them. It is essential that employees are adequately informed, so consider communicating through multiple communications platforms if appropriate (i.e. company e-mail, team chat, home page notice, intranet etc.)

5.3 Recording & Improving.

Once the campaign is launched, you may need to keep record of who attended which mandatory activity. This is important when it comes to showing that you are fulfilling the requirement of the GDPR. This is also an ideal moment to engage with the employees who were the audience of the awareness campaign. A short online survey is ideal to find out what people thought of the campaign and to give the opportunity for feedback and points of improvement.

5.4 Validating.

It is important to monitor the results of your awareness program. It is also beneficial to be able to report on the success of program. The best way to do this is to start by identifying a baseline before you begin your efforts. This should include both quantitative and qualitative measures. For example, comparing the number of privacy-related incidents before and after the awareness program as a quantitative measure and comparing the satisfaction of individuals with their knowledge about privacy awareness as a qualitative measure. For the quantitative metrics, it is important to check the status at regular intervals to identify the success of both the initial program and any refresher sessions. In this respect it's also possible to set targets for any subsequent activities such as increasing reporting of phishing attempts by 20%. This is an excellent way of using data to indicate the success of your program.

Summary

A privacy awareness program is an essential part of the GDPR requirements.

- It is important to carefully consider the needs of your organization and audience so that the effectiveness of your program is guaranteed.
- Using a variety of engaging content to bring the message of privacy awareness to employees in an accessible way is essential.

- The more employees can relate to the information you are sharing with them the more likely they are to take on board the messaging of your content.
- It is a good idea to start with a baseline of quantitative and qualitative data to be able to show the effectiveness of your program.
- Taking the time to measure the effect of your efforts will ensure you are able to steer your organization and its employees towards a positive mindset in relation to privacy awareness.