GDPR Readiness: Getting the Message Out

Creating a Communication Plan

Once good privacy policies and procedures have been developed, a plan must be put in place to communicate this information to everyone in the organization. Even a complete and well-written policy cannot be effective if the people in your organization have not been made aware of it.

Having a clear communication plan will ensure that everyone in the organization is properly informed. Your communication plan should have four different parts: **who, why, what,** and **how**.

- First, you need to list **who** in your organization needs to be communicated with.

- Then, identify **why** each separate group of employees needs to be informed.

- Next, write out **what** exactly will be communicated with each group of employees, whether this is a new procedure, certificate, schedule, or announcement.

- Finally, identify **how** this information will be communicated.

- In your communication, it is important to identify a person or office where questions and concerns can be referred.

Specific Policy Training

Specific groups of employees should also receive additional training about the organization's privacy policies and procedures as they pertain to the scope of their work. The policies covered by different groups of employees may vary, based on the work they do. Certain groups of employees may only need awareness training. There are a variety of methods to deliver training, including:

- Face-to-face training sessions

- Computer-assisted training / eLearning

- Induction training

- Toolbox / tailgate training

- Mentoring

- Privacy bulletin board

- Meetings (e.g. to explain upcoming workplace changes)

- Outside meetings / conferences

Customer Notification

Whenever any significant changes are made to the privacy policy, customers must be notified. This shows transparency on the part of the organization and ensures that all customers are informed about the way their personal data is being collected and used. This kind of notification often takes the form of an email sent to all customers that includes a link to the updated privacy policy.

Internal Audits

A great way to monitor an organization's privacy practices is through regular internal audits. An internal audit aims to improve an organization's privacy system by identifying how the organization is meeting privacy objectives and pointing out non-compliant actions or processes. A widely used method to administer an internal audit is through one-on-one interviews with employees to gauge their knowledge of the privacy system and the ways they implement it. The questions used for an audit interview should be open-ended to allow the auditee to answer the questions their own way. Some examples:

Open-ended (preferred) questions	Closed-ended (poor) questions
What do you do if you receive a customer complaint?	*Do you record customer complaints in the Customer Complaint Logbook?*
How did you find out what the organization's personal data protection policy was?	*Were you made aware of the organization's personal data protection policy during your orientation?*
What is the standard procedure for an information request?	*Do you follow the written procedure for information requests?*
What is the reporting procedure for a data breach?	*Do you have to inform your supervisor when a data breach occurs?*
What do you do if you identify a way to improve a process within your job?	*If you identify a way to improve a process within your job, do you fill out a Process Improvement Form?*