

ETHICS IN HEALTHCARE INDUSTRY

XX How New Technologies can Bring Value to Ethics and Compliance Professionals



SUE EGAN,

*Founder of Sue Egan Associates Ltd,
Board and Strategic Committee Member of ETHICS*

THOMAS K. HAUSER,

*Global Governance, Risk Management and Compliance Practice Leader
for Guidehouse Life Sciences, Guidehouse Europe Ltd,
Board and Strategic Committee Member of ETHICS*

Il existe aujourd'hui un large éventail d'outils informatiques permettant d'accompagner les compliance officers. Le nombre de fournisseurs est infini et le choix d'un outil adapté à l'entreprise peut s'avérer compliqué. Le point le plus important reste que ces outils ne remplaceront jamais un compliance officer avec son bon sens et son expérience eu égard aux décisions qu'il a pu prendre dans le passé. Pour autant, ces outils peuvent lui être d'une aide considérable et améliorer sa productivité. En outre, l'expert compliance peut, grâce à ces solutions informatiques, prendre connaissance de tendances ou de risques spécifiques, l'analyse des données n'étant souvent possible qu'à l'aide de l'intelligence artificielle. Cet article donne un aperçu des principaux domaines dans lesquels les outils informatiques aident les compliance officers du monde entier à être plus performants et plus efficaces dans leurs missions.

1. Data Privacy Tools

Today, privacy extends to a wide range of personal data and information that may be stored on personal digital devices, in corporate data centres, and in multiple cloud platforms. Compounding that complexity are ever - demanding data privacy regulations and consumer views on privacy - all of which need to be aligned with as companies look to avoid the penalties of getting privacy wrong, from heavy fines (up to 4% of global turnover) to angry customers.

At this point, compliance is simply the cost of doing business. The question on the mind of companies should be how to align compliance with their business roadmaps and to turn privacy into a business driver.

Data privacy management software provides comprehensive solutions for users to manage their company's privacy program, including the ability to reply to consumer requests, or data subject requests (DSR/DSAR), and mapping sensitive data.

Data privacy management software is used to achieve and maintain compliance with privacy laws and regulations. Employees such as privacy managers are the typical users of data privacy management software; however, these robust solutions offer workflows to enable other employees across the business, such as IT teams, to work collaboratively on consumer or DSR/DSAR requests for data access, amendment, or deletion.

Businesses use data privacy management software to automate manual processes, provide visibility, and leverage reporting tools to manage their company's privacy program.

These platforms include a centralized dashboard and have modules related to DSR/DSAR management, incident management, data discovery, and data mapping. For data discovery, some software solutions offer automated data discovery methods, others may offer workflow to manage manual, survey-based data discovery methods, and some software providers may offer both manual and automated discovery methods.

Many data privacy management software also includes identity verification software within the application, privacy impact assessment (PIA) software, privacy policy generation tools, cookie and website tracking compliance, and data breach notification functions.

Regardless of the level of sophistication of software used by companies, data privacy experts and/or business ethics and compliance professionals are still needed to determine how to implement the software, and what to do with the information provided by the software.

2. Speak-Up Hotline and Case Management Tools

Any company's hotline value exceeds the box-checking regulatory requirement that it fulfils. It can provide insight into compliance issues, give your team an opportunity to resolve issues before they spill into the press or social media, and prepare you to deal with risk. However, it can only do all of the above if you are capturing an appropriate number of reports - and that is where a company's speak-up culture, or lack thereof, becomes its biggest asset, or its biggest missed opportunity.

An effective hotline that is part of a healthy "speak-up ecosystem" can help companies to prepare for challenges like litigation or external investigation. The hotline is not just an expensive messaging service; it is a portal to case management that should capture a detailed record of complaints, and the associated documentation and actions taken. That audit trail is an essential element of the company's defence when a regulator comes knocking.

Best practices for employers to create such a healthy speak-up culture include:

- "listen up" before expecting people to "speak up";
- take all reports of retaliation seriously;
- include specific examples of retaliation in the anti-retaliation policy that managers and supervisors may not have otherwise realized were legally actionable;
- provide regular training to management of all levels, and senior leadership;
- create a mechanism through which employees can report concerns and instances of retaliation, anonymously if necessary;
- make it clear that retaliation will be subject to discipline, up to and including termination;
- campaign success stories; and,
- promote civility, which can help reduce incidents of retaliatory behavior.

A case management system enables tracking of the number of substantiated investigations resulting from employees speaking up. The tool used should be thorough enough to provide

the who, what, why, when, where, and how of each reported concern. Who knew? When was the report raised? What was the response to the report? Who did not report incident who may have known about it (and why didn't they)? What lessons were learned? How did the incident occur? All of these factors should be measured and investigated to learn what exactly is happening, or not happening, in the organization.

The most important element in any speak-up programme is the integrity of the person conducting the investigation into the alleged incident or behaviour that led to the report. Without business ethics and compliance professionals of high personal integrity, these speak-up lines are worthless.

3. Third Party Due Diligence Tools

The evolution of due diligence is at the stage where it is no longer sufficient to focus on a narrow range of risks. A much more holistic view is needed to understand what risks are present when considering business dealings with a third party.

In the eyes of the law, third parties (suppliers, distributors, and other business partners) are considered an extension of the hiring company, so it is in the best interests of companies that use such third parties to build third party due diligence into their compliance program.

As companies turn to third parties with whom they have not previously engaged, it is important to have a process to both vet and monitor them to make sure they do not have a history of bribing government officials that hold the power over necessary approvals or those who have purchasing authority at hospitals, for example. Third parties must be vetted to make sure that do not engage in any activities that could tarnish the reputation of the hiring company or its products. For example, the practice of buying brand name parts from a company and mixing them with cheaper parts of other companies, or even fake products, to maximize profits, and many other corrupt practices.

Organizations are responsible for the compliance of third party partners, as they represent the company, and therefore must perform appropriate compliance due diligence and monitoring during contracting. That means companies must decide which policies and procedures their third party partners will follow, train them through main policy procedures, and ensure that risk is minimized as much as possible.

Compliance onboarding software is available that incorporates and accommodates the recommended best practice elements for engaging with new third parties. These software platforms help streamline the onboarding process and improve data collection and record-keeping by enabling dashboards, reporting tools, automation, approval workflows, built-in risk scoring and analysis, as well as robust audit trails, among other features.

For companies that have limited internal resources, some third parties now also supply complete onboarding services for third party management so that companies do not need to purchase onboarding software and/or conduct the onboarding activities themselves.

4. Risk Management

Kicking off a compliance program with an objective risk assessment helps to create a proactive, preventive program. By helping uncover and rank current and potential risks, a risk assessment activity will identify the highest likelihood and highest impact risks that the company should focus its attention on mitigating. For example, most companies that engage third parties to work on their behalf know that their third party due diligence program is one of their highest priority activities to mitigate by tailoring and customising to the needs of the organization.

Risk management tools allow the uncertainty to be addressed by identifying and generating metrics, parameterizing, prioritizing and developing responses, and tracking risk. These activities may be difficult to track without tools and techniques, documentation, and information systems.

Again, it is the interpretation of the data by highly skilled professionals that really makes the difference for companies. Without deep insights into the company's business models and core activities, it would be easy to blindly implement a series of suggested actions without fully thinking through the consequences for the company. For example, is it worth spending 100k € to mitigate the risk to part of the business that generates 50k € of revenue, or that would attract a maximum fine of 50k € if it went wrong?

5. Policy and Procedure Management

The complexity of managing policies across the range of regulations, geographical regions, languages, and digital platforms has become inefficient, unscalable for businesses of all sizes.

Companies need to be able to identify web forms, policies and disclosures that exist across their digital properties, and update and publish them within specific time periods to adhere to the range of global privacy regulations. This includes the need to set expiry dates for policies and procedures and update them before they expire. Tracking the status of hundreds of policies, procedures, and associated forms and checklists can be extremely complex.

Many software policy and notice management solutions on the market can simplify the complex process of creating, updating, and monitoring policies across websites and applications into one central location while eliminating the need for complex development work.

Businesses can also enable policies with multilingual capabilities to display in local languages based on browser preferences.

It is important that updates of policies, procedures and associated forms and checklists are properly controlled so that specific team members have access rights to collaborate on these documents during updating periods. Owners must be triggered when a policy or procedure is due for an update and companies must maintain version control for all such documents, including publicly available policies. There must also be a full audit log of changes.

6. Consent Management

Today's marketers, advertisers, and publishers must respect their customers' privacy while also driving opt-ins, marketing consent, and preferences, collecting first party data, and delivering compelling user experiences.

However, consumers are increasingly concerned with protecting their personal data whilst also demanding more personalized experiences.

Managing marketing consents and preferences, and the specific consents to collect sensitive data is a major concern for organizations, focusing on building trust with their audiences. Technology tools can empower companies to manage the choices professionally.

Increasingly, it is also important to help customers to understand the data that companies hold on them, how additional personal data may be collected, and the policies and procedures in place to protect that data.

7. Workflow Management Tools

These tools enable specific workflows to be virtually enforced by ensuring that each step in a process is completed before the next step is begun. It is important when implementing these tools to work out the most efficient route through each process, including identifying those steps that can be worked at the same time, or in parallel.

All previous parallel and sequential steps must be completed before the next sequential step begins, thus providing some control over the end-to-end process. The audit trail that these systems provide includes a record of who performed which steps within the system, and when each step was flagged as complete, which is valuable when tracing activity flows.

These tools have some important limitations. For example, they do not necessarily link directly to other systems where individual steps are performed, so they can quickly become out of step with reality unless strict oversight is maintained to ensure that no steps are missed. Such systems can sometimes be seen as a "tick box" exercise that drains resources with no value added to the overall process. However, in controlled environments, such as the manufacture of medicines or medical devices, where controlled repetition is needed, they really are a valuable and valued tool.

Conclusion

Technology can be helpful to ethics and compliance professionals but must not be used as a substitute for personal interactions with individuals.

Companies sometimes get caught up with the difficulties of implementing expensive technology and forget to train people. Any technology is only as good as the training that its users have received. This training needs to be repeated often and must include an overview of why the technology is important to the company.

Remember that people will make the technology work or fail depending on how they feel about it, including whether it is user friendly or not, so where several alternative options are available, companies should choose the most appropriate systems for their staff based on their levels of technical expertise and understanding of technology.

While all of the tools discussed in this article can support business ethics and compliance professionals in performing their roles, these tools cannot be a substitute for a well thought out and well executed compliance programme led by a competent ethics and compliance professional.