Crises control

Keep your
business safe
from regulatory fines

Keep your business safe from regulatory fines

Introduction

As the Owner or Director of a small business you can often feel exposed in the face of regulatory requirements for which you become responsible upon taking up your position. As an office-holder you immediately become responsible in law for a whole range of duties, in particular if you hold personal data and employ team members.

The obligations placed upon you are likely to include informing and training your employees, recording compliance related incidents, reporting incidents to regulators within certain time limits and being able to prove that you have done all of the above. If you fail to meet these compliance requirements then regulators typically have the powers to fine you, impose restrictions on your business or even prosecute you.

The two biggest areas of regulatory reporting for SMEs are related to information security, and health and safety. If you hold any personal data within your systems, or if you employ any team members or are responsible for any work premises, then you will fall within regulatory legislation, certainly within the UK and within most other jurisdictions also.

This range of duties can be onerous and intimidating, but there are a number of software solutions available which can help you to both meet these regulatory requirements and, just as importantly, prove that you have met them if you are threatened with sanctions. This paper looks at five ways that such solutions, delivered through the software-as-a-service model, can help you to meet your regulatory compliance requirements.

Executive summary

An incident notification solution is piece of software, available for a monthly subscription fee, which will allow a business to communicate with all of its key audiences through its own secure cloud-hosted communication channel, via e-mail, SMS, phone call and mobile app push notification.

There are five main ways in which an incident notification solution can help you to meet and prove that you meeting your regulatory compliance requirements.

1. Creation of a process to respond to regulatory incidents quickly and effectively
2. Notification of your team, your customers and the regulators of an incident, quickly and reliably
3. Distribution of legal and response documents to your team, as part of their education or in response to an incident
4. Placing an obligation on recipients to acknowledge delivery of your message and any accompanying documents
5. Automatically creating a detailed audit trail of your actions, messages, documents and who has received them, to show to regulators

Compliance regulations

There are many areas of regulation that place compliance obligations on businesses of any size. Of these, by far the most significant relate to information security and to health and safety.

Information security

The General Data Protection Regulation (GDPR) comes into force across the EU from May 2018 and applies to any 'personal data' relating to identifiable EU citizens, including names, ID number, location data, contact data and online identity. It applies to any company or organisation which holds personal data in either automated or manual filing systems.

The Regulation defines a 'personal data breach' very widely, as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. It could also result where personal data has been inappropriately access accessed due to a lack of appropriate internal controls.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to €10 million or 2 per cent of a company's global turnover. This means that companies must have in place the following procedures:

- Rapid notification of the Company Directors of a personal data breach
- Rapid notification of the Regulator of a personal data breach
- Possible notification of customers of a personal data breach
- Procedures to record an audit trail that all of this has been done

Case study

A UK firm of solicitors discovers that its IT network has been hacked into after an employee opened a phishing e-mail with a link to a malware virus. The IT network is isolated from the internet, but the firm does not know what data might have been stolen.

The firm is required to notify the Information Commissioner's Office within 24 hours of becoming aware of the data breach. Within 72 hours it is required to tell the ICO how it has notified its clients of the breach, since the firm holds sensitive personal data, including bank details.

Failure to submit breach notifications can incur an immediate fine of £1,000 from the ICO.

Health and safety

In the UK the Health and Safety at Work Act places a responsibility on employers for health and safety management. It is an employer's duty to protect the health, safety and welfare of their employees and other people who might be affected by their business. Employers must do whatever is reasonably practicable to achieve this.

Employers must assess health and safety risks in the workplace, inform their employees about these risks and also instruct and train them on how to deal with the risks. These communications must be recordable to ensure that the business can demonstrate to the Health and Safety Executive (HSE) it has complied with the legislation.

The company must also report a wide range of health and safety incidents to the HSE, including accidents requiring hospital treatment and dangerous occurrences. The report must be submitted without delay and has to be completed within 10 days of the incident. They must also keep records of any reportable injury, over three day injury, disease or dangerous occurrence. This includes the date and method of reporting; the date, time and place of the event; personal details of those involved; and a brief description of the nature of the event or disease.

Failing to meet these health and safety legal requirements can result in a prosecution by the HSE with resulting fines or even imprisonment. Company directors can also be disqualified from holding office. This means that companies must have in place the following procedures:

- Notification to employees of workplace risks and safety instructions
- Rapid notification of the Company Directors of a health and safety incident
- Timely notification of the Regulator of a health and safety incident
- Procedures to record an audit trail that all of this has been done

Case study

An employee of a UK supermarket suffers a workplace injury when a pallet of groceries falls on him as he is unloading them in the warehouse. The employee suffers a broken ankle, requiring hospital treatment and is off work for three months.

The supermarket is required to notify the Health and Safety Executive as soon as possible after the incident has taken place. It must supply full details of what happened and when and the personal details of the injured employee. It must also keep its own records of the incident

Failure to submit an incident notification, or to comply with other requirements, including proper risk assessment and training, can lead to a prosecution by the HSE, resulting in a fine, disqualification from office, or even imprisonment.

Five ways an incident notification solution can help you to meet your regulatory compliance requirements

1. Creation of a process to respond to regulatory incidents quickly and effectively

The first way in which an incident notification solution can help you with your compliance requirements is to facilitate the development of a set of procedures for you or your team to respond to regulatory incidents.

The best notification solutions will be based on the premise that you identify your corporate risks and then build incident specific responses around them. This will allow you to create an action plan or standard operating procedure to handle the incident when it occurs, as well as providing communications channels and pre-prepared messaging to send out.

The leading solutions in the field, such as Crises Control, have additional functionality such as a task manager that will allow you to build a task list to respond to a compliance event, allocate tasks to named individuals and set deadlines for them to complete the task. This will not only standardise and speed up your incident response, but will also provide a detailed audit trail of the actions your team has taken, for later review by regulators if needed.

2. Notification of your team, your customers and the regulators of an incident, quickly and reliably

The main functionality of a notification solution is, of course, to send out communications to your employees, customers and other stakeholders, such as regulators. The best solutions will provide multi-channel communications to ensure that your message gets through as quickly and reliably as possible.

Crises Control, for example, offers four different communications channels, e-mail, SMS, phone call and push notification. You can choose to use some or all of these channels to communicate and the end result is a message that the recipient cannot ignore. So long as they have at least a phone signal, an internet connection or access to Wi-Fi they will receive at least one of the modes of communication.

Most solutions will also allow you to onboard your recipients in groups, departments or locations, so that you can choose to send to your message to many people at the same time, rather than having to rely on old-fashioned, complex and time consuming call trees. You can recreate your entire organisational chart on the platform if you wish.

3. Distribution of legal and response documents to your team, as part of their education or in response to an incident

A vital part of your preparation for, or response to, a compliance event will be the distribution of key documents associated with that incident. These might be pre-event safety instructions to your team as part of your information and education process. Or they might be post-event reporting forms sent to the regulator, or standard operating procedure sent to your incident response team.

Whether they are legal or operational documents, they will all be vital in meeting your regulatory compliance requirements. You will also need to be able to prove to the regulator that you have sent them or made them available to the right people at the right time.

Sophisticated notification solutions, such as Crises Control, will allow you to upload and store these vital documents on their cloud hosted platform. This means that they will always be available to you and your team, even when your own networks might be compromised, on account, for example, a cyber security attack. This always-available feature is an important benefit of software-as-a-service cloud-hosted solutions.

4. Placing an obligation on recipients to acknowledge delivery of your message and any accompanying documents

In addition to notifying employees, customers and regulators of compliance events, Directors also need to be able to confirm that they have received and, if necessary, acted on the notification.

Some notification systems, like Crises Control, require that message recipients acknowledge receipt of a notification. This provides a clear route to confirm that notifications and documents have been received and instructions acted on. The acknowledgement receives a time and date stamp that cannot be tampered with and so provides formal proof, if needed, of the transaction.

Where a regulatory compliance event has taken place that requires notification to the authorities within a specified time limit, such formal proof of reporting is extremely valuable.

5. Automatically creating a detailed audit trail of your actions, messages, documents and who has received them, to show to regulators

The most sophisticated incident notification solutions will time and date stamp all messages and actions that have been executed using the platform. Thus means that an audit trail is automatically generated. Such an audit trail is of great value if a compliance event leads to a regulatory investigation.

The leading solutions in the field, such as Crises Control, also have the additional functionality of a task manager that will provide a detailed and timed audit trail of all actions undertaken by named response members, which will be available for later review by regulators if needed.

Crises Control not only provides this automatically generated audit trail of all notifications and actions, but it also creates, as standard, graphic performance reporting at incident, group or individual user levels. This means that managers can very easily assess the responsiveness of their team members to compliance events and even conduct regular testing of their teams in preparation for real life events.

Author

Tim Morris is Director of Marketing for Crises Control. He has worked in the field of corporate communications and disaster recovery for over 20 years. His roles have included the 24/7 press office at New Scotland Yard and being the Head of Communications and Community Engagement at Sussex Police. He has been personally involved in the operational response to a number of major incidents including the Southall rail crash, the Heathrow Terminal One fire and the terrorist bombing of Canary Wharf. He has lectured and conducted research in the field of communications in a variety of academic settings, including the University of the Arts, London and the Chartered Institute of Public Relations.