



## Anonymous Whistleblowing Systems and CNIL and European Union Data Protection Measures

### OVERVIEW

As U.S. companies move into international markets, many are confronting foreign regulations, which seem to conflict with those governing operations in the U.S. In the aftermath of several corporate debacles, the adoption of the Sarbanes-Oxley Act (SOX) in the U.S. in 2002 presented new challenges to organizations, particularly those that are publicly traded. The decline of public trust in the ethics of corporate America had a resoundingly negative economic impact not just in the U.S., but worldwide. Perhaps the most internationally challenging provision of SOX is the requirement for organizations listed on U.S. stock exchanges to provide at least one channel of communication by which employees can make anonymous reports. Now that the SOX compliance deadline has long since passed, organizations are recognizing the special challenges posed by the collision of domestic and foreign regulations, especially regarding anonymous reporting by employees.

Historically, the U.S. has provided greater employer protection in the management of employees engaging in misconduct and criminal behavior within the organization. Other countries, particularly those in the European Union (E.U.), take a decidedly pro-employee approach.<sup>1</sup> In addition, cross cultural beliefs regarding the utility of anonymity in employee reporting are markedly different. While European sensibility places great value on the rights of the accused, the American perspective lends more

credence to the reporting party and the potentially increased protection against retaliation that the option of anonymity provides. These distinct U.S./E.U. cultural differences resonate clearly in their respective employment-related laws and regulations.

### U.S. Regulations

Regulated by the Securities and Exchange Committee (SEC), the Sarbanes-Oxley Act of 2002, among other provisions, requires publicly traded organizations to establish independent audit committees to essentially provide company oversight regarding financial and accounting-related issues. In the pursuit of such responsibility, the audit committee must also implement a “whistleblower” program to enable employees, vendors, and any other stakeholders to submit complaints or knowledge of fraudulent activity in an *anonymous* and confidential fashion. Organizations are not only responsible for providing a mechanism by which such reports can be received, but must also document retention and treatment activities of submitted complaints. Failure to comply may result in SEC-enforced sanctions, civil penalties, and possible de-listing from the stock exchange.<sup>2</sup>

The intent of anonymous reporting channels is to encourage employees to report their knowledge of financial misconduct who may otherwise fear reprisal. In this way, organizations may investigate and identify potential problem areas or employees to efficiently manage and prevent organizational losses due to employee misconduct.

---

<sup>1</sup> Schreiber, M. E., Held, J. M., Bond, R. T. J., Dana, R., Runte, C., & Flower, K. (2006). *Anonymous Sarbanes-Oxley hotlines for multi-national companies: Compliance with E.U. data protection laws*. Retrieved June 5, 2006, from <http://www.theworldlawgroup.com/db30/cgi-bin/pubs/PrivacyMatters - Ch9.Anonyms>  
SOX.PracGuideSOX.Vol2.ELEC.pdf

---

<sup>2</sup> Sarbanes-Oxley Act of 2002. Available: <http://fl1.findlaw.com/news.findlaw.com/cnn/docs/gwbush/sarbanesoxley072302.pdf>.

Perhaps the most common mechanism organizations have adopted to meet the compliance requirements of SOX is the confidential fraud hotline. Many third-party hotline providers also administer an internet-based reporting portal in addition to the traditional hotline. Regardless of the method of report intake, the option of anonymity is often advertised and sometimes even encouraged, which further assists organizations in their compliance efforts.

SOX compliance, however, is not limited to only domestic locations. Multinational companies are required to implement such mechanisms throughout their organization to include those employees working in international locations. Therefore, many organizations have implemented “one-size-fits-all” reporting channels across the organization, whether domestic or international. In addition, many organizations allow their employees to make anonymous complaints about diverse forms of employee misconduct, not just those that are financial or accounting-related. For example, many employee hotlines are set up to receive reports of sexual harassment, discrimination, and unsafe working conditions. Though not mandated by SOX, organizations are quickly recognizing the benefits associated with receiving reports of all forms of employee misconduct and are opening up their reporting mechanisms to receive such employee complaints.

## European Union Data Protection Laws

European regulations are rooted in distinctly differing cultural values related to privacy, particularly in occupational settings. As early as 1978, some European countries adopted data protection legislation governing the use, processing, and dissemination of the “personal data” of any citizen.<sup>3</sup> Any information that allows for the direct or indirect identification of individuals constitutes personal data. Generally, as applied to U.S.-based corporations with European operations, the receipt, investigation, treatment, and retention of any reports of employee misconduct, financial or otherwise, would be subject to the restrictions and

<sup>3</sup> Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties. Available: <http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf>.

mandates imposed by European data protection laws.

As E.U. Member States began adopting their own data protection measures, the flow of information across the E.U. became increasingly restricted due to conflicting mandates. The passage of E.U. Directive 95/46 EC in 1995 sought to synchronize diverging E.U. legislation and all E.U. Member States are required to implement regulations consistent with the Directive and establish a supervisory body responsible for the enforcement of data protection laws.<sup>4</sup>

The Directive principally covers the “processing” of personal data and defines the circumstances under which processing is lawful and warranted.<sup>5</sup> In order to legally process personal data, three conditions must be met: transparency, legitimate purpose, and proportionality.

- ◆ In order to meet the condition of *transparency*, the individual whose data is to be processed (“data subject”) has the right to be notified of the processing and must be given access to all personal data to be processed. The Directive further outlines six specific situations in which personal data may be processed and the data subject has the explicit right to modify any inaccuracies in the data to be processed.<sup>6</sup>
- ◆ Personal data must be collected only “...for specified, explicit and *legitimate purposes*...” In addition, the possibility that personal data may be collected through a whistleblowing system and the purpose for such a system

<sup>4</sup> European Commission Data Protection . Available: [http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm).

<sup>5</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available: [http://www.cdt.org/privacy/eudirective/EU\\_Directive\\_.html](http://www.cdt.org/privacy/eudirective/EU_Directive_.html)

<sup>6</sup> These circumstances include: (1) When the data subject provided consent for data processing, (2) when the processing is contractually required, (3) when the processing is required for legal compliance, (4) when the processing is necessary in pursuit of the public interest, (5) when the processing is for the protection of the data subject, or (6) when processing is necessary for the legitimate interests of the data controller, unless superseded by the fundamental rights and freedoms afforded to the data subject.

must be clearly communicated to those who may be identified through the reporting mechanism.

- ◆ The collection of personal data “must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.”<sup>7</sup> That is, organizations must limit the types of information collected through reporting mechanisms to only that information necessary to meet the purpose(s) set forth by the implementation of the reporting mechanism (e.g. proper corporate governance). The level of information reported must be in *proportion* to the purpose the collection of such information sets out to achieve.

Since the adoption of the E.U. Data Protection Directive in 1995, U.S.-based multinational organizations face significant challenges across all E.U. Member States, as all E.U. Member States have separate data protection laws and regulatory enforcement agencies. Such circumstances require a comprehensive evaluation of existing SOX compliance protocols implemented internationally and the local governing regulations.

Recent discussions between relevant U.S. and E.U. regulatory agencies revealed that, though U.S. and E.U. legislation appears to conflict on its face, there are no critical inconsistencies expressly precluding whistleblower compliance mechanisms from being implemented in E.U. Member States under E.U. data protection law.<sup>1</sup> Much of the work required for resolution of U.S. and E.U. regulations lies in ensuring implementation of such systems are tailored to meet the applicable legal requirements. Consequently, traditional “one-size-fits-all” systems are a solution of the past and may, in fact, expose organizations to legal liability that could have been prevented.

---

<sup>7</sup> Article 29 Data Protection Working Party. (2006). *Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*. Available: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp117\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf)

## The French Data Protection Model and Overarching E.U. Implications

Founded under the Act of January 6, 1978, the *Commission nationale de l'informatique et des libertés* (CNIL) is the administrative body established for the enforcement of E.U. and State data protection laws in France. In 2005, France enacted legislation making the implementation of anonymous incident reporting systems by any employer in France unlawful in the absence of certain precautions.<sup>1</sup> The specific provisions and dual compliance options will be discussed in detail below. However, in general, administrative and judicial decisions in France dictate anonymous whistleblowing systems must have a specific and narrow scope with regard to the type of data collected. In addition, such mechanisms must be submitted to the CNIL for authorization prior to implementation. Other provisions mandate that individuals accused of misconduct must have access to the data retained by the organization and must have the opportunity to correct any inaccuracies once the data has been sufficiently preserved for investigative or evidentiary purposes.

It is important to understand the adoptions of the CNIL regarding the compliance expectations of U.S.-based multinational companies because many of the existing data protection laws across the E.U. resemble those in France and are rooted in very similar philosophical values. Many E.U. countries, including Germany and the United Kingdom, are rapidly adopting approaches comparable to those in France regarding the use of anonymous incident reporting systems in those Member States. Therefore, such specialized and dual U.S. and E.U. compliance is not likely to remain limited to U.S.-based operations in France.

## Striking a Balance

Recognizing the need to come to some compromise between U.S. and E.U. regulations regarding the use of anonymous whistleblower systems, the CNIL recently published guidelines establishing suggested compliance techniques to assist multinational organizations confronting these apparent conflicts.<sup>8</sup> In addition, a

---

<sup>8</sup> Commission nationale de l'informatique et des libertés (CNIL). (2005). *Guideline document*. Available: <http://www.cnil.fr/index.php?id=4>

Frequently Asked Questions document is now available to clarify previously confounding interpretations of the law.<sup>9</sup> The CNIL has ultimately determined that whistleblowing systems, such as those mandated in the U.S. under SOX, are “neither allowed nor banned under the provisions of the French Labor Code.”<sup>8</sup> Furthermore, the CNIL does not prohibit the use of a third-party service supplier, as long as the service provider contractually agrees to comply with French and European data protection laws. However, these decisions were based upon reporting mechanisms collecting only certain types of personal data, specifically “...in the fields of accounting, financial audit, fight against bribery or banking areas...”<sup>9</sup> In addition, data of a particularly serious nature, outside of financially-related incidents, may be collected. Seriousness is defined as any facts that “affect the vital interests of the company or its employees’ physical or mental integrity.”<sup>9</sup> Some examples of serious issues that would be considered acceptable data include threats to the safety of employees, moral and sexual harassment, discrimination, threats to public health, and insider trading.

Regardless, the organization wishing to implement SOX-compliant anonymous reporting mechanisms in France is required to have that system authorized by the CNIL. The CNIL has established two authorization processes, depending upon the type of facts the organization is requesting authorization to collect and process.

◆ *Single/Unique Authorization:* This authorization procedure was established to expedite the process and allow E.U.-compliant organizations to implement SOX-compliant anonymous reporting mechanisms in a timely manner. The CNIL should receive a filing acknowledgement within one to two weeks of submission.<sup>1</sup>

The single authorization process, known as a unilateral commitment to comply, is an internet-based process that requires the organization to submit the following information:

- the name, address, and contact details of the person responsible for compliance in general,
- the name, address, and contact details of the person responsible for the right to access personal data,
- the name, address, and contact details of the person whom the CNIL can contact, and
- a purpose section indicating what service provider or software is utilized, how many persons are covered by the program, implementation year, and whether data will be transferred outside of the E.U. (and if so, a list of the countries involved must be included).

◆ *Standard Authorization:* Organizations wishing to implement an anonymous incident reporting system to collect data outside the scope of that described above (e.g. financially related concerns) and that does not expressly meet the CNIL’s requirements must submit a complete application to the CNIL for examination at a plenary session of the CNIL. The CNIL is mandated to review the application within two months of the filing, provided that no additional information is needed by the CNIL to make a determination.

### The Governance of Cross-Border Data Transfer – Safe Harbor

In addition to the mandates and regulations described above, organizations implementing anonymous incident reporting systems internationally must be cognizant of restrictions regarding the cross-border transfer of data originating in the E.U. to countries outside of the E.U. Many organizations may find it necessary for U.S. management representatives or audit committee members to be made aware of and even investigate employee misconduct occurring in the E.U. that is reported through their whistleblower system. However, portions of the E.U. Directive 95/46 EC discussed above also limit the ability to transfer personal data outside of the E.U. and explicitly prohibit data transfer to countries that do not adequately meet E.U. privacy protections. After negotiations between E.U. and U.S. officials, the Safe Harbor Arrangement was delineated to make data

<sup>9</sup> Commission nationale de l’informatique et des libertés (CNIL). (2006). *Frequently asked questions*. Available: <http://www.cnil.fr/index.php?id=4>

transfer across the boundaries of the E.U. possible.

Safe Harbor went into effect in 2000 and prevents multinational organizations from experiencing business interruptions as a result of seemingly conflicting, yet equally applicable, cross-border regulations.<sup>10</sup> Organizations can join the Safe Harbor by a self-certification process, renewed annually, in which they agree to comply with the requirements of Safe Harbor and publicly declare that they do so. In order to join, there are seven Safe Harbor requirements to which organizations must comply:

- ◆ *Notice:* Organizations must notify individuals that they may collect and use personal information, the purpose for which they would do so, and any third parties with whom their information may be shared. In addition, individuals must be provided with a means by which they can contact the organization.
- ◆ *Choice:* Individuals must be given the opportunity to authorize the organization to disclose personal data to third parties or to use the information in a manner diverging from the purposes for which the information was originally collected.
- ◆ *Onward Transfer:* In order to transfer personal information to a third party, the organization must first apply the *Notice* and *Choice* principles and must further ensure that the third party also subscribes to Safe Harbor principles. In so doing, the organization may obtain written agreement from the third party that it provides at least the same level of privacy protection as the applicable regulations dictate.
- ◆ *Access:* With some exceptions, individuals must be granted access to the information the organization retains about them and must have the opportunity to modify, delete, or otherwise edit inaccuracies.
- ◆ *Security:* Reasonable precautionary measures must be undertaken to prevent “the loss, misuse, and unauthorized access,

disclosure, alteration, and destruction” of personal information retained by the organization<sup>10</sup>

- ◆ *Data Integrity:* Organizations must take reasonable steps to ensure the data collected is that which is necessary to meet the purpose for which it was collected and to ensure that it is accurate and reliable.
- ◆ *Enforcement:* Adequate and non-burdensome recourse mechanisms must exist for the appropriate investigation and resolution of individual complaints and damages awarded where applicable under the relevant law. In addition, there must be a means for verifying organizational adherence to the Safe Harbor principles as well as accountability for problems resulting from a failure to comply. Furthermore, consequences for failure to comply must be “sufficiently rigorous” to encourage consistent compliance.<sup>10</sup>

Organizations reap many benefits for joining the Safe Harbor and maintaining their compliance. First and foremost, perhaps, is the ability to ensure seamless and efficient organizational communication internationally. In addition, Safe Harbor participation satisfies the adequacy standard for all 25 E.U. Member States, who all have very similar data protection regulations. Also, prior approval for data transfers will be automatically approved or waived and, subject to limitations, all complaints made by E.U. citizens against U.S. companies will be heard in the U.S.

---

<sup>10</sup> U.S. Department of Commerce. (n.d.) *Welcome to Safe Harbor*. Available: <http://www.export.gov/safeharbor/index.html>

## MYSAFEWORKPLACE® SUGGESTED COMPLIANCE TECHNIQUES

With the advent of the recent CNIL regulations regarding whistleblower protocols, much of the literature has focused on compliance overlap between SOX and CNIL regulations. For multinational organizations, this may initially appear as a burdensome task. However, it appears the discrepancy lies within company-specific compliance strategies and implementation choices versus a direct conflict of laws. *So what should an organization do?* Organizations should ascertain how E.U. data protection laws apply to those states in which the organization operates.<sup>1</sup> Organizations should carefully follow any developments in regard to whistleblower statutes in each of those E.U. Member States and consider establishing relationships with the appropriate local data protection authorities.<sup>1</sup> Furthermore, organizations should consider the following convenient guidelines to minimize the possibilities of violating relevant data protection laws<sup>1</sup>:

- ◆ Consult with appropriate data protection personnel prior to establishing whistleblower protocols.
- ◆ Ensure employees' due process rights are maintained.
- ◆ Ensure that the implemented compliance programs include methods beyond standard whistleblower practices, to include such options as employee training.
- ◆ Ensure that data alleging wrongdoing is preserved for only as long as necessary and that this data is stored separately from the individual's personnel file, unless the allegations result in some form of disciplinary action.
- ◆ Ensure that the appropriate steps are taken to guarantee proper transfer of data outside of the E.U. (e.g. Safe Harbor certification).<sup>1</sup>

These recommendations, based on best practices, will help organizations be compliant with applicable state laws and regulations. The following details more specific CNIL regulations

and how organizations, as well as the MySafeWorkplace solution, comply.

### Scope of incidents reported and necessary filing procedures

Professional, or external, whistleblower systems should be authorized by the CNIL prior to implementation. The types of incidents reported upon will direct the authorization process. Your organization may choose to adopt only a SOX-type focused code of conduct and whistleblower mechanism. If this is the choice, your organization may file with the CNIL through the online CNIL single authorization process with no further subsequent CNIL review. This process will require submission of the following information: legal nature of organization; name, address, and contact details of the entity responsible for the implementation; name, address, and contact details for the person responsible for compliance in general; name, address, and contact details for the person responsible for the right to access personal data; name, address, and contact details for the person whom the CNIL can contact. In addition, the notification must include a section that iterates which software is used, how many persons are concerned with the whistleblower system, the year of its implementation, and whether data will be transferred to countries outside of the E.U. (Chapter 8). Once the on-line application is received, the CNIL will send an acknowledgement receipt approximately two weeks from the time of submission. Once received, the organization can implement its whistleblower hotline immediately without any additional review by the CNIL.

The other option is for an organization to adopt a more inclusive whistleblower system, which encompasses broader reporting than that of SOX-related issues. This will require the organization to undergo the standard CNIL review process, which typically consists of a case-by-case review by the CNIL regarding the legitimacy of the program's purposes, the "proportionality" of the contemplated program as well as its transparency to all parties involved. Approval may take months.

---

**MSW and Organizational Compliance:** It is ultimately the organization's decision if they would like to implement a broad or narrow whistleblower system. The MSW system has the capability to accommodate both. Under the single authorization code for CNIL, titration of only SOX-related incident reports is the most efficient compliance strategy. These may include, but are not limited to, financial, banking, accounting, anti-bribery, or other vital corporate interests related to such categories.

MSW provides an all-inclusive list of approximately 60 incident types to all client organizations, in turn allowing the organization to limit the incidents types.

---

#### **Anonymity cannot be required or “actively encouraged”**

Anonymity is allowed by CNIL as long as it is not made compulsory and is not actively encouraged by the company. Furthermore, the reporting party has a choice regarding his/her anonymity. CNIL requests that, prior to submission of the report, the reporting party be informed that he/she will not suffer or be retaliated against for the report. Furthermore, the reporting party's identity must be kept confidential and not disclosed to third parties such as the incriminated person and the employee's line supervisor. The CNIL believes non-anonymous reports offer the following advantages: 1) to avoid or at least limit false and/or intentionally slanderous accusations; 2) to organize the protection of the whistleblower against retaliation; 3) to ensure a better handling of the report, with the option of requesting additional details on the alleged facts from the author of the report.<sup>2</sup>

---

**MSW and Organizational Compliance:** MSW is unique in that it employs three anonymity options: do not care about anonymity, remain completely anonymous, and remain anonymous toward your organization. MSW accepts a neutral stance regarding anonymity and does not encourage a reporting party to select a certain option. Moreover, if reporting via telephone, MSW has the capability to verbally

inform the reporting party that his/her contact information will be kept confidential. In addition, if reporting via the internet, MSW has the technical capabilities to insert a customized landing page that outlines the necessary organizational information, to include confidentiality information and CNIL regulations, if appropriate.

---

#### **Reporting is not mandatory in the E.U.**

The CNIL indicates that a whistleblower system should not be “compulsory” for employees. Contrary to this tenet, SOX regulations stipulate that employees must report violations or risk discipline if they do not report obvious or known infringements. If an organization has locations in both the U.S. and the E.U., this discrepancy between the two regulations may be a burden in regard to communication and implementation of the whistleblower services. One proposed compromise is that organizations not “require” reporting, but instead state that they “expect” violations to be reported.<sup>9</sup> In E.U. Member States, it should be communicated to the employees that there will be no adverse actions taken against employees who do not use the hotline.

---

**MSW and Organizational Compliance:** MSW does not have authority to dictate whether employees “should” or “must” report organizational violations, as it simply serves as a repository for the receipt of reports, allowing further follow-up by appropriate organizational members and the reporting party. Although MSW is able and willing to consult on implementation and communication strategies, it is ultimately the responsibility of the organization to organize a strategic method for the implementation and communication regarding the intended required usage of the system.

---

#### **Cross-Border data transfer obligations if personal data is transmitted outside of the E.U. member country to the U.S.**

SOX rules and regulations require the chairman of the audit committee to receive, handle, and

treat reported violations that are financially-related. For U.S.-based organizations, these individuals are typically located in the U.S. When non-financially related reports (e.g. sexual harassment) are submitted via the whistleblower system, CNIL regulations deem it appropriate to not necessitate the review by U.S.-based audit committee members. However, this does not always preclude them from receipt and review of the report, as even routing employment concerns could have a potential impact on financial or accounting statements.<sup>9</sup>

Data transfer outside of the E.U. is acceptable under E.U. data protection laws if appropriate cross-border data protections are utilized.<sup>9</sup> The U.S. entity receiving the information must have implemented a cross-border transfer solution. Current options include: 1) consent of the individual affected, which oftentimes is unreasonable; 2) data protection agreement; and 3) obtain certification for the U.S. Safe Harbor, which is administered by the U.S. Department of Commerce and enforced by the Federal Trade Commission. Pursuant to the CNIL, it is important to notify the reporting party if the information is transferred outside of the E.U., and also inform them of the receipts of the report.

---

***MSW and Organizational Compliance:*** *MSW complies with the E.U. data protection law in regard to cross-border transfer of information. MSW was Safe Harbor certified on January 6, 2005. Safe Harbor certification provides the following benefits: 1) All 25 Member States of the European Union will be bound by the European Commission's finding of adequacy; 2) Companies participating in Safe Harbor will be deemed adequate and data flow to those companies will continue; 3) Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted; and 4) Claims brought by European citizens against U.S. companies will be heard in the U.S. subject to*

*limited exceptions.<sup>11</sup> Furthermore, MSW has the technical capabilities to educate the professional call center agents handling hotline report intake so they can effectively educate reporting parties on the organizational report recipients. In addition, MSW facilitates online communication between the organization and the reporting party such that the organization may post information to the reporting party regarding the recipients of specified reports.*

---

### **Prompt notification to the “incriminated” person required**

CNIL purports that the “incriminated” person must be notified by the person in charge as soon as data is collected about him/her. (V-9-16). Pursuant to Article 39 of the data protection act, information provided to the “incriminated” person cannot contain the confidential information pertaining to the whistleblower, nor does it need to contain the entirety of information initially provided. There is a delay exception when protective measures need to be taken, in the case of prevention of destruction of evidence. This may include, but is not limited to, securing, copying, or performing forensic analysis on appropriate computer systems.<sup>9</sup> This delay exclusion may alleviate concerns regarding the notification to the alleged suspect prior to employing proper investigatory techniques. Nevertheless, contacting the alleged suspect is a basic principle of the data protection laws in all E.U. countries and will require, at the very least, some disclosure to the incriminated person.<sup>9</sup>

---

***MSW and Organizational Compliance:*** *Developing and implementing a sound policy for notifying “incriminated” individuals accused of wrong doing is the obligation of the organization. This policy should outline the method of contact and describe what information should typically be shared with the*

---

<sup>11</sup> Extracted from <http://www.export.gov/safeHarbor/index.html> on June 8, 2006.

*accused person. Due to the support provided by the investigative professionals of MSW's parent organization, Business Controls, Inc., MSW has the capability to consult with organizations and provide suggested sample procedures, if deemed appropriate. Furthermore, MSW is the central repository for obtaining and retaining all information submitted from the initial report (to include name of suspected individuals) and subsequent updates. The organization may also utilize MSW's message board capabilities to document and retain communication with the "incriminated" individual.*

---

### **Accused individuals have the right to respond, contest, or rectify (change) information**

A fundamental right of E.U. data protection laws is to allow the suspected person identified in a report alleging a violation to access the data, request rectification, or potential deletion of the information.<sup>9</sup> CNIL posits that such access rights do not include access to information about other individuals, such as the whistleblower's name. Under certain "blatantly abusive" conditions, subject access rights can be denied.<sup>9</sup>

---

***MSW and Organizational Compliance:*** *Accused individuals, unless they are Enterprise Portal Users on the MSW Database, do not have access to the secure database in which all reports are stored. The organization should, therefore, generate a policy outlining appropriate procedural steps regarding how to gather this information from the accused and how to effectively insert the information into the original report submitted. MSW allows for additions, responses, or requested changes to be submitted via the message boards. Additionally, MSW retains all initial information and additional information in its original form.*

---

### **Limiting whistleblowing reporting to mail, drop-box, or "non-automated" means**

There appears to be some discrepancy in the CNIL literature describing what reporting methods, if any, are excepted from CNIL regulations regarding whistleblower reporting.

Although the CNIL states that its regulations only apply to whistleblower mechanisms that are "automated," a succinct definition of what defines "automated" is difficult to find. Some documents speculate that exclusion of mail, drop-boxes, or even individual email makes appropriate sense.<sup>9</sup> Nevertheless, one cannot deny the all-encompassing presence of electronic means for the receipt, retention, dissemination, and response of such inquiries, regardless of the original submission method. In light of the implications found within the CNIL research and regulations, it is safe to presume that implementation of any whistleblower service, regardless of the available report intake mechanisms is subject to CNIL regulations.

---

***MSW and Organizational Compliance:*** *MSW is considered an "automated" service and therefore the use of such service is governed by CNIL regulations. MSW encourages organizations to err on the side of caution and assume that any implemented whistleblower service will, ultimately, be considered "automated" and, therefore, necessitates compliance with CNIL regulations and E.U. data protection laws.*

---

### **Data Retention Regulations**

The CNIL regulates the length of time organizations are allowed to retain reports, archive reports, and eventually destroy reports. The regulation states that unsubstantiated reports should be deleted "immediately." Furthermore, CNIL requires deletion of reports within two months of closure, unless there is ongoing disciplinary or court action. If there is no further action on the report, the organization must delete the file or archive the data. (Frequently Asked Questions, #17<sup>9</sup>). Archiving of information is permitted for relevant data unrelated to or beyond the required whistleblower program, especially if it affects the physical safety of others or the vital interests of the organization.<sup>9</sup> This data may be retained for up to 30 years (Frequently Asked Questions, #17<sup>9</sup>).

---

---

***MSW and Organizational Compliance:** Internal procedural documents should be generated that outline the organization's definition of "unsubstantiated" and all parties responsible for labeling and responding to reports as such should be accurately educated on the protocols.<sup>9</sup> Furthermore, effective policies regarding investigative and closure procedures must be implemented by the organization. MSW is able to delete reports from the database at the organization's request. MSW requests that the organization designate one (or at the most two) contact names of individuals who are responsible for the communication of requests relating to deletion or archiving of reports. Ultimately, it is the responsibility of the organization to establish protocols for monitoring its database, determination of closure rates, and establishment of appropriate communication triage to MSW personnel to the deletion or archival of records.*

---

---

## **THE FINAL WORD**

While E.U. data protection regulations and best compliance practices are quite perplexing, there are clearly methods organizations can employ to ensure their whistleblowing programs are compliant across all of their locations, domestic or international. It may be appealing to select a strategy and apply it universally throughout the organization. However, multinational organizations do not usually have this option. Therefore, organizations must assess their overall needs and choose responsible implementation techniques. Furthermore, multinational organizations who are considering the option of outsourcing their whistleblower program should be careful to select a vendor who understands these seemingly conflicting regulations and can articulate how they can assist organizations in compliance, both domestically and abroad.

As new guidelines and best practices continue to emerge, the organization's responsibilities are becoming clearer. However, such guidelines are continuing to evolve and we have likely not yet heard the final word regarding E.U. data protection regulation compliance requirements.