REGULATORY VIEWPOINT
W.H.J.M. NUIJS
SUPERVISION OF BEHAVIOUR AND CULTURE: AN EFFECTIVE RESPONSE TO GOVERNANCE AND RISK MANAGEMENT PROBLEMS WITHIN FINANCIAL INSTITUTIONS

GOVERNANCE
SCOTT KILLINGSWORTH
ETHICS IN THE EXECUTIVE SUITE: THE BEST, THE BRIGHTEST AND A WICKED PROBLEM PART II

EU WATCH
JEROEN TERSTEGGE
DATA PROTECTION AND THE NEW FACE OF PRIVACY COMPLIANCE

THE EFFECTIVE PRACTITIONER
EVITA SIJS
ANONYMITY, PRIVACY AND THE “INTERNAL INTEGRITY REPORTING SYSTEM”

OVER THE HORIZON
FRANÇOIS VINCKE
ETHICS AND COMPLIANCE AT THE ICC: A HISTORY OF INFLUENCE

LETTER FROM ABROAD
FABIO L.O. SEHNERT
THE FIGHT AGAINST CORRUPTION: NEWS FROM BRAZIL

THE EFFECTIVE PRACTITIONER
SYLVIE C. BLEKER-VAN EYK
THE EXTRATERRITORIAL WEB: TRACKING THE EVER EXPANDING REACH OF EXTRA-TERRITORIAL JURISDICTION PART II
## CONTENTS

### 05 REGULATORY VIEWPOINT
Supervision of Behaviour and Culture: an Effective Response to Governance and Risk Management Problems within Financial Institutions
- W.H.J.M. Nuijts

### 22 GOVERNANCE
Ethics in the Executive Suite: The Best, the Brightest and a Wicked Problem Part II: The Role of the Board in C-Suite Compliance
- S. Killingsworth

### 34 EU WATCH
Data Protection and the New Face of Privacy Compliance
- J. Terstegge

### 44 THE EFFECTIVE PRACTITIONER
Anonymity, Privacy and the “Internal Integrity Reporting System”
- E. Sips

### 54 OVER THE HORIZON
Ethics and Compliance at the ICC: A History of Influence
- F. Vincke

### 67 LETTER FROM ABROAD
The Fight Against Corruption: News from Brazil
- F.L.G. Selhorst

### 75 THE EFFECTIVE PRACTITIONER
The Extraterritorial Web: Tracking the ever Expanding Reach of Extraterritorial Jurisdiction Part II
- S.C. Bleker-van Eyk

---

### Subscription Information

**Subscription prices**

<table>
<thead>
<tr>
<th>FTEs</th>
<th>Corporate</th>
<th>Universities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal subscription</td>
<td>€ 195</td>
<td>€ 195</td>
</tr>
<tr>
<td>Institutional subscription</td>
<td>€ 450</td>
<td>€ 450</td>
</tr>
<tr>
<td>2 Online users + 1 Print copy</td>
<td>€ 650</td>
<td></td>
</tr>
<tr>
<td>5 Online users + 10 Hard copies</td>
<td>€ 750</td>
<td>€ 650</td>
</tr>
<tr>
<td>10 Online users + 50 Hard copies</td>
<td>To be negotiated</td>
<td>€ 650</td>
</tr>
</tbody>
</table>

* Online access includes the complete archive

Please go to our website for the general information regarding our journal subscriptions. [http://www.baltzersciencepublishers.com](http://www.baltzersciencepublishers.com)

**New Subscriptions**

Subscriptions start with the first announced issue of the calendar year. If subscriptions are started in the course of the calendar year the full subscription rate applies, and the subscriber will get full access to the archive of the journal.

**Change of address**

Please mail your change of address to the address mentioned on the contents page, or consult the website.

**Terminating a subscription**

Subscriptions can only be cancelled, by email or letter, until 1 December of the present subscription year. After this date subscriptions will be automatically renewed for the following year.

**ISSN:** 2211-8934 • E-ISSN: 2211-8942

---

**Advertising Rate Card**

2012 prices, excluding applicable VAT.

<table>
<thead>
<tr>
<th>Format</th>
<th>Rate (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full page</td>
<td>1x € 1000</td>
</tr>
<tr>
<td>5x € 750 (per page)</td>
<td></td>
</tr>
<tr>
<td>Half page</td>
<td>1x € 800</td>
</tr>
<tr>
<td>5x € 450 (per half page)</td>
<td></td>
</tr>
</tbody>
</table>

For technical instructions please contact the marketing/sales department: [info@baltzersciencepublishers.com](mailto:info@baltzersciencepublishers.com)
New European privacy law is on its way. In this article, Evita Sips tries to reconcile European scepticism towards anonymous finger-pointing and the rights of the individual. In a world recently shocked by the Snowden revelations demonstrating how ineffective privacy protection has become in a modern world of cyber communications, much debate and lobbying has taken place, and continues as we speak. Evita Sips welcomes the proposal for one of its main objectives – the reduction of bureaucratic inefficiency due to European fragmentation – however regrets its failure to reduce major bureaucratic and aimless annoyance for multinational companies. Multinationals have to deal with the challenge of making an Internal Integrity Reporting System (a.k.a. “Whistleblowing Scheme”) compliant with privacy law. This article provides insight into the origin, history and extent of the bureaucratic burden surrounding the introduction and operation of reporting systems in organisations. The organisation seeking to satisfy the increasing need to have effective Internal Integrity Reporting Systems in place, remain frustrated by European limitations on the use of anonymity, at differing degrees across member states, which in turn has resulted in creative interpretations and variation. This article asks questions of the new law, and in seeking to provide alternatives for a more balanced approach for the use of anonymity in internal reporting procedures, raises a number of concerns that organisations across the EU should be aware of. Eva Sips looks into finding a solution within the principle of accountability, but this article has been written foremost in the anticipation of generating support and better leads on how to improve on the philosophical and legal confusion that currently reins supreme. In the meantime the identification of the issues highlights the points in need of attention as companies seek to harmonise Internal Integrity Reporting Systems across borders.

* Evita Sips is Managing Consultant of People Intouch B.V. and Editor in Chief of Privacy Compliance.

THE EFFECTIVE PRACTITIONER – ANONYMITY, PRIVACY AND THE “INTERNAL INTEGRITY REPORTING SYSTEM”

Hotlines were introduced in Europe as a result of the international reach of the Sarbanes Oxley Act … Europeans (led by the French) were – to put it mildly – ‘not amused’

Legitimate Interest and Adequate Procedures
Many companies nowadays install an internal reporting procedure as part of their integrity management/compliance programs. The set-up of the procedure varies per company. Some companies use reporting systems as part of their procedure. Often these systems provide user-friendly features, which allow employees to easily file reports of ethical wrongdoing. The (automated) system and procedures around it obviously have to be compliant with privacy regulations. Because personal data might be part of a report, the automated processing of data needs to be notified to the relevant, local privacy authorities, introducing a bureaucratic hassle which organisations have to face. This annoyance could in fact be avoided, if a company does not include an easy access automated system as part of their internal reporting procedure. This is, however, not an option for many companies committing to the task of discovering fraud and other serious (criminal) offences, such as bribery, child labour, environmental pollution, sexual harassment, unsafe labour conditions or discrimination. Companies are required to set up sophisticated internal reporting procedures, which must be effective and do the job. It is widely accepted that employee reporting is a main source of fraud detection, and that anonymity is often the only way of getting the silent witness to speak up. Installing a worldwide (anonymous) misconduct reporting system would be an evident part of this. Newly enacted anti-corruption legislation even encourages companies to implement such a system as an ‘adequate procedure’ to help protect against prosecution.²

Brief History of an Unbalanced Approach
Automated systems as part of an internal reporting procedure, first arrived in Europe in the form of a “Hotline” (American call center). When these hotlines were introduced in Europe as a result of the international reach of the Sarbanes Oxley Act (2002)(SOX), Europeans (led by the French) were – to put it mildly – ‘not amused’. Immediately, it was associated with cultural sentiments and references to historic regimes whereby innocent or patriotic citizens were betrayed and sent to detention (or worse: to the guillotine).

² For example: UK Bribery Act (2010).
The fact that it was an American practice being forced upon the Europeans did not help either. Furthermore, when it comes to (anonymously) reporting on other persons, the Americans do not appear to have any inhibitions. European privacy authorities finally responded when the European Working Party Article 29 drafted an Opinion on Whistleblowing Schemes in 2006. Reacting to the American model of reporting systems that was only aimed at protecting the identity and privacy of the ‘whistleblower’, the European privacy authorities rightfully also aimed at protecting the privacy of the (wrongfully) accused persons (something which is irrelevant in the American environment). It has unfortunately been a feature of the European authorities only to focus on the possible negative effect on the accused persons ever since; unfortunate because it ignores the fact that systems exist that allow communication with the anonymous reporter. This is important, because this ability enables continuous fact-finding and verification. This way, ungrounded or even purposely false reports can be filtered out. These reports can be ignored and all (personal) data can be deleted immediately. This technique thus greatly reduces the risk, feared by the Working Party, of encouraging false accusations, and would therefore rather see anonymous reporting abolished. Forced to allow anonymity because of the international reach of SOX, a weak compromise was reached and a limited Whistleblowing Scheme was eventually published. Hence, the Opinion is aimed at limiting anonymous reports as much as possible. To date the Opinion is the only legal guideline on Whistleblowing Schemes at European level.

**Bureaucratic Burden**

The aforementioned Opinion of the Working Party Article 29 was an advice, which national privacy authorities could use in the formulation of their national laws. Although the advice was not always followed through, it did set the tone. Today some privacy authorities have published their own (additional) recommendations.
Due to the lack of harmonisation, the process of notifying the system to European privacy authorities is complex, uncertain, expensive, time consuming, diverse and therefore extremely inefficient.

on this topic, others have not. Unfortunately, it varies per authority on how the Opinion is interpreted. This has resulted in a situation whereby different requirements per country exist. In some countries there are limitations as to what you may report (France), in other countries there are limitations about to whom, who may report (Sweden, Austria) and in other countries limitations to the use of anonymity apply (Spain, Portugal). This patchwork of requirements makes it virtually impossible for an international operating company to have one single procedure in place worldwide. Even more so, because this topic is not a top priority with the privacy authorities, the requirements are not clearly set out and it is therefore very difficult for the corporate centre, especially multinationals operating in various countries, to gain certainty about how to comply with the various privacy laws in Europe.

In order to be on the safe side in respect to this matter, incredible time and money is spent on legal advice. Understandably, privacy lawyers take a strict legal approach to the topic. Sometimes resulting in procedural or system requirements, which completely undermine the working of an effective internal reporting system. Nonetheless, when seeking to set in place adequate procedures to combat corruption, companies obviously want to comply with privacy legislation as well. Unfortunately, the current variations in European privacy legislation makes such compliance very hard, if not impossible. Due to the lack of harmonisation, the process of notifying the system to European privacy authorities is complex, uncertain, expensive, time consuming, diverse and therefore extremely inefficient.

A Balanced Use of Anonymity
It is widely acknowledged that guaranteed anonymity is the only way of encouraging silent witnesses to come forward with their concerns about possible breaches of ethics. Offering anonymity takes away the fear of

---

retaliation and encourages silent witnesses to come forward with what they know – allowing companies to respond and cause change. Furthermore, anonymity is the only way to truly protect the ‘whistleblower’; it is the only way his privacy can be guaranteed and how he can be protected and ‘left alone’. Therefore, companies have implemented sophisticated internal reporting systems, which allow employees to anonymously report violations they witness. Unfortunately, as described earlier, European privacy authorities have reservations about the use of anonymity. It is a sensitive topic, a topic non grata, which upholds the strong European black-and-white thinking about anonymity: whereby anonymous reports equate to false reports.

This concern runs deep. Therefore, the ‘model of confidentiality’ is preferred over the ‘model of anonymity’. Confidentiality means that the identity of the reporting person is known to authorised people, and will be protected against other people. This model of confidentiality has often been proven to be unsatisfactory. The main argument being that it cannot be guaranteed that the identity of the reporting employee will always remain shielded. Often, in the guidelines of these confidentiality counsellors, an article is included which states that as soon as the interest of the organisation outweighs the interests of the employee, confidentiality cannot always be guaranteed. Indeed, guaranteed anonymity may under certain circumstances be impossible to assure, even if not divulged by those authorised to know. People are not naïve, and this uncertainty immediately results in witnesses remaining silent and the wrongdoing continuing. In the ‘whistleblowing’ debate, the two mentioned models are often portrayed as opposites (either one or the other). This is not the right approach; the strength of both models should be combined in the entire chain of facilitating safe and effective internal reporting. There are several ways to use anonymity in a reporting procedure in addition to confidentiality:

- Anonymity as Last Resort;
- Anonymity as Temporary Step in the Process;
- Internal Intake Point as Key Factor;
- Anonymous Communication Tool.

5 In the Netherlands ‘vertrouwenspersoon’.
Anonymity as a Last Resort

Within the American model, all suspicions of wrongdoing should immediately be reported through an (anonymous) hotline, bypassing conventional channels of reporting. In European culture, this is not the right approach. Anonymity should be used as an instrument of last resort: only those suspicions that otherwise would not be reported, should come in through an anonymous reporting system. In the first instance, the conventional reporting lines (including confronting the accused directly) should be the first options to be considered. The last resort criterion is also the only right one on how to limit anonymous reports. Other limitations that have been set out by privacy authorities, such as limiting about whom reports can be made, or what can be reported, do not make sense. Anonymity should be available for those witnesses of wrongdoing who fear retaliation and therefore would otherwise choose to remain silent or walk away.

Anonymity as Temporary Step in the Process

The barriers to report a witnessed wrongdoing or crime are high. One element that is often mentioned is the bystander effect: bystanders rather look the other way, especially when they think they can become (negatively) involved when speaking up. These witnesses need to be enabled and encouraged to make a first step in the most secure way possible. Once he trusts the listening party, the witness may then decide to continue the conversation in a confidential rather than an anonymous manner. A good internal reporting system should make this possible.

Internal Intake Point as Key Factor

Key in setting up an efficient internal reporting procedure is setting up a central point of intake at corporate level. This allows for the analysis of the content of the (anonymous) reports by the best-equipped people. Also, these people are trained to judge the validity of the report and are able to manage the responsible use of anonymity. As discussed earlier, vague and ungrounded reports should be disregarded. More and more large organisations create such an intake point within a dedicated corporate compliance department. Organisations which do not have the size and resources to set up their own intake center, may choose
to outsource this function to an external central point of intake.

*Anonymous Communication Tool*

One of the underlying reasons for the current inefficient approach to ‘whistleblowing’ lines appears to be the deep-rooted fear of anonymity. The privacy authorities’ fear of false reports is outdated. Nowadays, systems exist which make it possible to communicate with the anonymous reporter. This makes it possible to ask follow-up questions, verify information given, thereby filtering false reports and preventing damage to someone who may be falsely accused. Under these circumstances, there is no legitimate reason to resist the use of anonymity. Even more so: people knowing how such systems work, will realise that making false accusations is useless and even risky. This will give these systems a preventive meaning.

*The New European Privacy Regulation*

Unfortunately, the new privacy Regulation will not solve the problem described above. Rather, it might impose further restrictions and it will therefore become even more problematic to implement an effective internal reporting system. The data protection complications that European multinationals run into when implementing a misconduct reporting system throughout Europe, are disproportionate and should therefore be addressed. A new legal framework, which is aimed at harmonising privacy legislation and abolishing unnecessary bureaucratic requirements, would be the ideal moment to address this issue. When the new legal framework is implemented, the content will instantly become binding across Europe. This means that the general principles, rights and obligations (proposed in articles 5, 11-20 and 32) will become the law in every individual member state. Some of these articles would not be compatible with operating an effective internal misconduct reporting system. This would result in a situation open for interpretation and uncertainty. In the European Commission’s proposal⁶ the only way this can be overcome, is if the member state restricts the privacy

Since it is proposed in the Regulation that the obligation to notify the privacy authorities will disappear and instead the controllers will have to document their compliance and have it available for the responsible authority, the bureaucratic burden would be drastically reduced.

rights and obligations by a legislative measure (see article 21). Member states are, however, not very likely to do so, at least not very soon. If they would decide to do so, this would result in separate legislation per member state. Whichever way, there will be separate privacy rules per members state. An undesirable development.

A few amendments which have been proposed by VNO-NCW/MKB Nederland would contribute to the effective implementation of ethics programs and reporting systems in organizations. It is an alternative to the Commission’s proposed article 21: To give the controller (in this situation, the company) the authority to restrict some of the rights and obligations as stated in art. 5, 11-20 and 32 as necessary in a limited number of circumstances, including internal investigations (see also article 43 of the current Dutch Data Protection Act). This is a small textual change, but with huge consequences: the data controller can (temporarily) restrict rights and obligations and thereby set up an effective internal reporting system, resulting in the company not having to deal with all the separate privacy authorities in every member state.

Unfortunately, the chance of these proposed amendments being passed, are small to zero: it is a radical change and other fundamental issues in a European privacy law are more important to lawmakers in Brussels. Furthermore, the outcome would still be uncertain, as is the case with many elements of the new legal framework. Therefore, we have to think about another solution.

The Principle of Accountability

In July 2010, the (data privacy) Working Party Article 29 wrote an Opinion about the principle of accountability, which ‘would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out [...] are complied with and to demonstrate so to the supervisory authorities upon request.’ This self-
regulation principle is also included in the new Regulation (article 22). The rules around an internal ‘whistleblowing’ policy should become part of the self-regulation of data controllers. An adequate framework with minimum requirements should be put in place by the European Data Protection Board (the successor of the Working Group Article 29), but part of this framework should be a certain amount of discretionary power for the controller to balance the different interests. Also, a self-assessment checklist can be provided. As said, the Opinion of Article 29 Working Group on Whistleblowing Schemes is outdated and needs to be revised. Furthermore, it is an Opinion, which still gives the member state the opportunity to deviate. The new framework should be binding, so that a harmonised set of rules concerning internal misconduct reporting procedures comes into place. Since it is proposed in the Regulation that the obligation to notify the privacy authorities will disappear and instead the controllers will have to document their compliance and have it available for the responsible authority, the bureaucratic burden would be drastically reduced.

Discussion
The bureaucratic burden that multinational companies have to overcome in order to make their internal integrity reporting system compliant to privacy regulations is disproportionate and out of place. As we speak, fundamental developments are taking place in the field of European privacy law, but unfortunately, the described problem will not be solved. Part of the problem is that privacy authorities are the only European regulators on this topic; no countervailing entity, like e.g., a national corporate governance authority, is in place to provide a different view. As long as this situation persists, the challenge to find a more balanced approach lies in the hands of privacy regulators. It is in all our interest that companies do not have to spend their money, time and efforts on lengthy uncertain bureaucratic processes whereby the baby is thrown out with the bath water. Also, whereby the key objective of fighting corruption, sexual harassment and other serious forms of misconduct, is seriously undermined. The principle of accountability and self-regulation clearly is part of the new European privacy law (high fines, duty of documentation). This should also
THE EFFECTIVE PRACTITIONER – ANONYMITY, PRIVACY AND THE “INTERNAL INTENSITY REPORTING SYSTEM”

DOCUMENTATION SELF-ASSESSMENT FILE CONCERNING MISCONDUCT REPORTING. TO INCLUDE, BUT NOT BE LIMITED TO:

- A data retention policy
- The right to information policy
- The right to appeal policy
- Notifying policy
- A message intake and handling policy
- A policy to balance interest on a case-by-case basis
- Message intake and handling data flow on a need-to-know basis
- An independent message intake office(r) responsible for all anonymisation of the message content, protecting the identities and distributing messages for handling on a need-to-know basis.
- An entity (e.g. ‘Ethics Committee’) with expertise to balance the different interests
- A reporting policy (to the Board, to the Data Protection Officer, etc.)
- Anonymity as part of the process, only if the technique allows direct communication with the complainant/messenger.
- Anonymity is included in the procedure as an instrument of last resort: first, normal reporting lines should be tried/considered. Only those suspicions which otherwise would not be reported, should come in via an anonymous communication line.
- Any automated system or third party provider systems will have to be carefully selected and audited on their secure information security policies and practice.
- An internal reporting procedure which is written for all involved persons explaining the process for leaving a complaint, including privacy rights.
- Approval of applicable labour representatives

be the direction for internal reporting procedures. It is a good time to team up and set clear, reasonable and balanced demands concerning the rules about setting up an effective and safe internal reporting procedure. Until such time, the best policy would appear to have a clear vision as to the expected outcome of an Internal Integrity Reporting System, and then to ensure that local solutions are found for global objectives.

Evita Sips is Managing Consultant of People Intouch B.V., with a background in Criminology/Cultural Anthropology and with six years of experience supporting (international) organizations with implementing an effective internal reporting procedure as part of the organization’s integrity policy. www.speakup.eu
CONTENTS

05 REGULATORY VIEWPOINT
Supervision of Behaviour and Culture: an Effective Response to Governance and Risk Management Problems within Financial Institutions
– W.H.J.M. Nuijts

22 GOVERNANCE
Ethics in the Executive Suite. The Best, the Brightest and a Wicked Problem Part II: The Role of the Board in C-Suite Compliance
– S. Killingsworth

34 EU WATCH
Data Protection and the New Face of Privacy Compliance
– J. Terstegge

44 THE EFFECTIVE PRACTITIONER
Anonymity, Privacy and the “Internal Integrity Reporting System”
– E. Sips

54 OVER THE HORIZON
Ethics and Compliance at the ICC: A History of Influence
– F. Vincke

67 LETTER FROM ABROAD
The Fight Against Corruption: News from Brazil
– F.L.G. Selhorst

75 THE EFFECTIVE PRACTITIONER
The Extraterritorial Web: Tracking the ever Expanding Reach of Extraterritorial Jurisdiction Part II
– S.C. Bleker-van Eyk

Subscription prices

<table>
<thead>
<tr>
<th>Units</th>
<th>Corporate</th>
<th>Universities</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTEs</td>
<td>€ 195</td>
<td>€ 195</td>
</tr>
<tr>
<td>Institutional subscription</td>
<td>€ 450</td>
<td>€ 450</td>
</tr>
<tr>
<td>Online users + 10 Hard copies</td>
<td>€ 600</td>
<td>€ 600</td>
</tr>
<tr>
<td>10 Online users + 10 Hard copies</td>
<td>€ 750</td>
<td>€ 750</td>
</tr>
</tbody>
</table>

Please go to our website for the general information regarding our journal subscriptions.
http://www.baltzersciencepublishers.com

New Subscriptions
Subscriptions start with the first announced issue of the calendar year. If subscriptions are started in the course of the calendar year the full subscription rate applies, and the subscriber will get full access to the archive of the journal.

Change of address
Please mail your change of address to the address mentioned on the contents page, or consult the website.

Terminating a subscription
Subscriptions can only be cancelled, by email or letter, until 1 December of the present subscription year. After this date subscriptions will be automatically renewed for the following year.

ISSN: 2211-8934 • E-ISSN: 2211-8942
