

# SUMMARY OF THE BELGIAN DATA PRIVACY COMMISSION'S RECOMMENDATION ON WHISTLEBLOWING SYSTEMS

|   |   |
|---|---|
| <p><b>INTRODUCTION</b></p>                                    | <p>In early December 2006, the Belgian Data Privacy Commission released its recommendation regarding use of whistleblowing schemes in Belgium by organizations operating in Belgium. Global Compliance summarizes that recommendation below and provides Global Compliance's perspective.</p>   |
| <p><b>Overview</b></p>  | <p>The Belgian Data Privacy Commission believes that in almost all cases the use of a whistleblowing system will automatically imply a processing of personal data so that the processing of personal data within the framework of such a whistleblowing system must comply with the applicable provisions of the Belgian data protection statute (the la loi du 8 décembre 1992 relative à la protection de la vie privée, which we will refer to here as the "LVP").</p> <p>The Commission believes that personal data must be processed in accordance with the following provisions:</p> <ul style="list-style-type: none"> <li>- <b>admissibility, fair play, legality and purpose</b></li> <li>- <b>proportionality</b></li> <li>- <b>accuracy and precision</b></li> <li>- <b>transparency</b></li> <li>- <b>security</b></li> <li>- <b>rights of access, rectification and erasure of personal data</b> concerning them for all persons whose personal data are kept within the framework of the whistleblowing system (particularly the whistleblower and the incriminated person)</li> <li>- <b>obligation of declaration</b></li> </ul> <p>The Commission considers that the whistleblowing systems are only compatible with the LVP if they minimally respect the fundamental principles disclosed above. These principles can therefore be used as a guideline for organizations planning to implement such systems or if necessary to adapt such systems already in existence.</p> |
| <p><b>Admissibility, fair play, legality, and purpose</b></p> | <p><u>Admissibility</u></p> <p>With regard to admissibility, the Commission has found two possible legal bases enabling an organization to justify its whistleblowing system:</p> <ol style="list-style-type: none"> <li>1. The existence of a legal or regulatory obligation requiring it to process personal data by means of a whistleblowing system;</li> <li>2. In the absence of such a legal obligation, a legitimate interest therein provided the fundamental freedoms and rights of the incriminated person are not taken advantage of</li> </ol> <p><u>Fair play, legality and purpose</u></p> <p>The scope and purpose of the whistleblowing system, the type of reports that can be made by the whistleblower via the internal whistleblowing system, and the scope of this system must be described with precision</p>  |

## SUMMARY OF THE BELGIAN DATA PRIVACY COMMISSION'S RECOMMENDATION ON WHISTLEBLOWING SYSTEMS

|  |   |
|--|---|
|  | <p>for the employees who might use the system or become involved in it.</p> <ul style="list-style-type: none"><li>• The organization must also take care to precisely describe the procedure for filing and processing reports (who, what, where, when, how, etc.).</li><li>• The system must clearly describe the consequences of justified and unjustified alerts.</li><li>• The person in charge of the processing, with whom employees (whether a whistleblower or an incriminated person) can exercise their rights of access, rectification, and erasure of the personal data, must be explicitly designated.</li><li>• The whistleblowing system cannot impose reporting obligations on members of the staff. The use of the whistleblowing system must therefore be optional by nature.</li><li>• The whistleblower must have reasonable grounds to have suspected the problematic situation he is reporting. Accordingly, mere rumors are not considered as sufficient grounds for filing a report.</li><li>• The information provided must be sufficiently precise. Accepting overly vague reports could lead to a “whistleblowing culture”, which naturally must be avoided.</li><li>• The Commission favors a general prohibition of anonymous reporting. The Belgian Commission expressed agreement with the argument developed by EU Article 29 Working Party that authorizes the processing of anonymous reports on a very restricted basis if they meet certain conditions. On the contrary, the Commission promotes reports in which the whistleblower is identified.</li><li>• When processing the report, the whistleblowing system must make it impossible to identify the whistleblower or include any information that could lead to his identification without his consent.</li><li>• The report must be collected and processed by a person in the organization specifically appointed to hear complaints (complaint manager), who is bound to professional confidentiality when processing the report, even with regard to executives (unless immediate precautionary measures are required), other members of the staff, labor union organizations, and third parties.</li><li>• Only after the accusations have been processed and the complaint manager has found the charges to be either well-grounded or clearly baseless can the result be communicated to the organization.</li><li>• The complaint manager must be able to work with sufficient autonomy with respect to the organization. The whistleblowing system must guarantee that this autonomy cannot be compromised. The complaint manager must act by having precisely defined responsibility and accordingly may be questioned, for example, in case of a breach in his obligation of confidentiality with regard to the</li></ul> |
|--|---|

## SUMMARY OF THE BELGIAN DATA PRIVACY COMMISSION'S RECOMMENDATION ON WHISTLEBLOWING SYSTEMS

|                               |   |
|-------------------------------|---|
|                               | <p>whistleblower, the incriminated person, or third parties during the processing of the report.</p> <ul style="list-style-type: none"> <li>• The complaint manager must be protected from any pressure exerted by executive management or labor unions, particularly if the person incriminated is an executive or officer with a labor union.</li> <li>• The complaint manager must process the report with the utmost discretion.</li> <li>• The complaint manager shall cease processing the report within the whistleblowing procedure in the event of intentional violation of confidentiality by the whistleblower himself.</li> </ul>   |
| <p><b>Proportionality</b></p> | <p><u>A limitation in the scope of application</u></p> <p>Normal control procedures with regard to executive officers, accounting, etc., conducted by persons who represent the management of the organization - whose task is precisely that of detecting and processing wrongdoing in the company – should suffice to dissipate concerns related to conduct that violates the company's standard by the personnel.</p> <p>The internal whistleblowing system can only be used as a specific and subsidiary channel whereby all or certain members of the staff (precisely designated in the whistleblowing system) can report serious irregularities within the company.</p> <p>The Commission stressed the strictly supplemental nature of the whistleblowing system. It can only involve reports concerning problems that clearly would not be processed by the normal line of command and for which there is no specific procedure or body legally regulated to handle them.</p> <p>A whistleblowing system can only involve reports pertaining to serious acts such as violation of regulations applicable to the organization in question or internal written company rules (particularly in the departments of finance and accounting), or if a crime is involved. It therefore must involve serious wrongdoing or sufficiently serious facts or situations that must be reported in the general interests of the company or for the proper governance of the organization and for which the whistleblower considers it not or no longer possible to report or complain through normal channels.</p> <p>The complaint manager must ensure that personal data:</p> <ul style="list-style-type: none"> <li>– are adequate, pertinent, and not excessive for the processing of the report alert;</li> <li>– remain limited to the designation of the facts and do not contain judgments of worth;</li> <li>– are explicitly disclosed as such if they concern unproven facts;</li> <li>– are kept for a period of time not exceeding that necessary to process the report, including any legal or disciplinary procedures with regard to the person incriminated for a justified report, or with regard to the whistleblower in case of an unjustified report or libelous accusation.</li> </ul> |

## SUMMARY OF THE BELGIAN DATA PRIVACY COMMISSION'S RECOMMENDATION ON WHISTLEBLOWING SYSTEMS

|                                      |   |
|--------------------------------------|---|
| <p><b>Precision and Accuracy</b></p> | <p>The complaint manager is responsible for monitoring that the personal data intended for processing reports are accurate and precise.</p>   |
| <p><b>Transparency</b></p>           | <p><u>Collective level</u></p> <p>The organization that wishes to set up a whistleblowing system must respect the laws on collective labor rights and notify its staff, the company council, the committee for the protection and prevention of work, the labor union delegation, or the negotiation or bargaining committees.</p> <p><u>Individual level</u></p> <p>All co-workers of the organization who are conceivably involved in the whistleblowing system must be notified of:</p> <ul style="list-style-type: none"> <li>– the scope and the purposes of the whistleblowing system;</li> <li>– the procedure for filing and processing reports;</li> <li>– the consequences of justified and unjustified reports;</li> <li>– how to exercise rights for accessing, correcting and erasing information and the procedure by which to do so;</li> <li>– third parties to which personal data concerning the whistleblower and the incriminated person may be transmitted within the framework of the processing of the report</li> </ul> <p>It is important for the whistleblower to be notified of the obligation of confidentiality when filing the report and during the processing of the report.</p> <p>The incriminated person must be informed as quickly as possible by the complaint manager of the existence of a report and the facts he/she is charged with in order to enable him to exercise his rights.</p> <p>The information of the incriminated person can be reported in exceptional circumstances (e.g., if there is the possibility of evidence being destroyed).</p> |
| <p><b>Security</b></p>               | <p>The whistleblowing system must provide guarantees so that personal data processed within the reporting procedure are not processed for other purposes. It must:</p> <ul style="list-style-type: none"> <li>– involve an operation that is differentiated from other processing operations;</li> <li>– provide guarantees of integrity, authenticity, availability, and confidentiality of the personal data;</li> <li>– ensure that personal data cannot be illegally destroyed during the processing of the report;</li> <li>– make it possible to conduct the audit so the way in which the personal data are processed can be easily tracked (control to determine who did what, with what personal data, and at what time).</li> </ul> <p>The guarantee of anonymity of the whistleblower and any parties involved is also important at the security level.</p>  |

## SUMMARY OF THE BELGIAN DATA PRIVACY COMMISSION'S RECOMMENDATION ON WHISTLEBLOWING SYSTEMS

|   |  |
|---|--|
|   | <p>Personal data cannot be exported to countries outside the European Union except under the provisions of the LVP concerning data transfers.</p> <p>Data transfers to a parent company in a country outside the European Union can only be justified if a report:</p> <ol style="list-style-type: none"> <li>1) involves particularly serious issues for which it has become obvious that the processing of the report cannot or no longer can be properly done exclusively at the European organization level</li> <li>2) the processing may have repercussions beyond the company located in Belgium or in the European Union.</li> </ol>   |
| <p><b>Rights of the Incriminated Person, The Whistleblower, Third Parties</b></p> | <p>All those involved in the whistleblowing system have rights regarding their personal data.</p> <ol style="list-style-type: none"> <li>1) They are entitled to correct any of their personal data that may be incorrect and have the right to erase: <ol style="list-style-type: none"> <li>a) data that might be incomplete;</li> <li>b) data that is not pertinent;</li> <li>c) data for which the processing is prohibited</li> <li>d) data that are kept after the report has been processed.</li> </ol> </li> <li>2) They are <u>not</u> entitled to access personal data of others unless consent has been explicitly provided.</li> </ol> <p>The incriminated person cannot access the identity of the whistleblower or that of third parties (or information that could lead to their identification) unless consent of the party in question has been provided or in the case of an unjustified report or libelous accusation of the whistleblower or false testimony from a third party.</p> <p>The whistleblower is also not entitled to access the personal data of the incriminated person or third parties. This access prohibition can however be lifted if, after an inquiry, it appears that the incriminated person mistakenly suspected the whistleblower (by affirming for example that the whistleblower was himself implied in the wrongdoing that he reported or if third parties acted in bad faith)</p> <p>The whistleblower is entitled to know the result from his report and any follow-ups.</p> |
| <p><b>Statement</b></p>   | <p>Prior to implementation, a statement or declaration of a whistleblowing system that provides for the automatic pre-processing of personal data is mandatory according to the Commission.</p>  |
| <p><b>GLOBAL COMPLIANCE'S SUMMARY</b></p>   | <p>Like its counterparts in France, Belgium's Commission believes that it is important to prevent the environment within an organization from deteriorating into a "whistleblowing culture" with the associated tensions. However, the Commission recognized the interests of an organization in having its internal rules and regulations respected, and in safeguarding its image by means of an effective internal control. In essence, the Commission explained its mission as one to find a delicate balance</p>  |

## SUMMARY OF THE BELGIAN DATA PRIVACY COMMISSION'S RECOMMENDATION ON WHISTLEBLOWING SYSTEMS

|   |  |
|---|--|
|   | <p>among the legitimate interests of all involved (the organization, the complaining party, and the individual who is the object of a complaint).</p> <p>While many parts of the Belgian Privacy Commission's recommendation are quite similar to that of the French CNIL, the few areas in which there appears to be a bit more leniency are:</p> <ol style="list-style-type: none"> <li>1) Anonymity. While the Belgian Commission encourages confidentiality versus anonymity, they are not as adamant about avoiding anonymous reports.</li> <li>2) Scope of what can be reported. The French CNIL requires reports to be limited to accounting, financial matters, banking, or anti-bribery to obtain immediate whistleblowing system authorization; however the Belgian Commission does not define the scope quite as narrowly. They only mandate that reports should pertain to serious acts such as violation of regulations applicable to the organization in question or violation of internal written company rules (particularly in the departments of finance and accounting), or if a crime is involved.</li> <li>3) While the Belgian Commission indicates that the implementation of whistleblowing systems in Belgium should be proactively communicated to notify its staff; the company council; the committee for the protection and prevention of work; the labor union delegation, or the negotiation or bargaining committees, it does not require an official authorization or certification with the Belgian Commission.</li> </ol> <p>There are clear-cut similarities between the Belgian Commission's recommendation and the French CNIL's Guidelines surrounding the handling of personal data and the rights of the accused.</p> |
| <p><b>GLOBAL COMPLIANCE'S PERSPECTIVE</b></p> | <p>At the present time, Global Compliance is conducting further analysis on the Belgian recommendation to determine if we believe a separate or altered hotline/web reporting system is required to fully comply with the Belgian Commission's recommendation, and will communicate with clients accordingly.</p> <p>Global Compliance believes it is important for all multinational organizations currently operating a whistleblowing scheme in Belgium to proactively communicate such scheme to all of the parties outlined by the recommendation if such has not been done.</p> <p>Lastly, Global Compliance believes that organizations operating in Belgium are well served to conduct an ongoing awareness and education campaign, covering at least the specific information identified by the Belgian Commission, to ensure all staff fully understands the whistleblowing system, the scope and purpose of the system and the procedures for use of the system.</p>  |