LATHAM&WATKINS

Number 484 6 October 2005

Client Alert

French Data Protection and Employment Law v. Sarbanes-Oxley — Codes of Business Ethics and Whistleblower Procedures in France Under Fire

In May 2005, the French data protection authority (CNIL[1]) issued two decisions which have the effect of impeding the implementation of certain whistleblower procedures in France.

Both decisions relate to major US groups of companies present in France via large affiliates, such as McDonald's Corporation (McDonald's France)[2] and Exide Technologies (Compagnie Européenne d'Accumulateurs or CEAC)[3].

While these decisions have a binding effect on these two French companies only, CNIL's intention was clearly to give them the widest possible impact. CNIL has given them broad coverage and commented on them in an editorial on its homepage.

Therefore, groups of companies, which have implemented whistleblower procedures in France, could be in breach of French legislation, namely French data protection law[4]. Moreover, whistleblower procedures are generally set forth in Codes of Business Ethics which could also be subject to French rules, in particular those embodied in labor law. Therefore, all codes and procedures relating to business ethics in France should be reviewed.

Codes of Business Ethics and Whistleblower Procedures

In practice, many Codes of Business Ethics and whistleblower procedures have been established in recent years in the US and have converged towards a relatively standardized model. The model's core provisions reflect fundamental principles such as human and corporate values and business ethics and contain prohibitions such as insider trading, conflicts of interest, harassment and discrimination in the workplace, "off-the-books" transactions and any kind of misrepresentation in financial reporting.

These Codes of Business Ethics are generally based, among others, on the US Foreign Corrupt Practices Act and the US Sarbanes-Oxley Act of 2002 (SOX). SOX charged the US Securities and Exchange Commission (SEC) to adopt adequate rules, which require that procedures are implemented for *"the receipt, retention and treatment of complaints regarding accounting, internal controls or auditing matters, and for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters."*[5]

Based on the latter, most Codes of Business Ethics contain whistleblower procedures such as an "ethics hotline," a toll-free telephone number which employees "*may*" or "*must*" call — depending on the wording of the Code of Business Ethics — to report, anonymously or otherwise, any suspected violations of certain rules. These "ethics hotlines" are generally

> "The French data protection authority has made it clear that its decisions have been rendered in full knowledge of SOX requirements. Discussions with SEC have reportedly taken place and CNIL will start active consultations during October with employer organizations among others to find a compromise solution. Some guidance by CNIL is expected before the beginning of November 2005.[17]"

open to all employees or to certain categories of employees, not only in the US, but also in foreign jurisdictions where US groups are present, including France. They may therefore become subject to local laws and regulations, and to the scrutiny of local regulators, such as CNIL.

Characteristics of the Two Whistleblower Procedures Rejected by CNIL

The Exide Technologies whistleblower procedure allowed all employees of this global group to report, anonymously or otherwise, alleged violations of laws or internal ethics rules. Employees could either call a telephone hotline or send an e-mail to a service provider in the US. That service provider would record the complaints digitally, summarize, classify and possibly translate them, then send them to the relevant recipient(s) — General Counsel, Human Resources Manager etc. Depending on the facts, an enquiry and further follow-up could ensue. The employee targeted by an ethics report would be informed as soon as possible to allow him/her to defend himself/herself. Personal data would be stored for one year.

The McDonalds' whistleblower procedure in France was based on postal mail or fax, and applied only to approximately 1,000 mainly white-collar employees. It allowed the voluntary reporting of alleged violations of French law and internal ethics rules. Reports would be directed towards the Ethics Officer in the US who would centralize the information in a file. He would then communicate the report by password-protected e-mail to the General Counsel of McDonald's France who would dispatch it to other relevant recipients in France, such as a Human Resources Manager, Security Officer, Financial Officer, etc., for a decision to be taken concerning whether an enquiry was required. French employees suspected of violating French law or internal ethics rules would be informed "*within two days.*" If the report entailed an enquiry and disciplinary action, the relevant personal data would be kept on file for up to five years, depending on the violation in question and the employee's position in the corporate hierarchy.

Why Are Certain Whistleblower Procedures Contrary to French Law?

The McDonald's and Exide Technologies decisions are based on the same grounds.

According to CNIL, whistleblower procedures can degenerate into an "*organized system of denunciation in the workplace.*"

CNIL ruled that "*the implementation by an employer of a mechanism intended to arrange for the compilation of personal data from its employees, in whatever form, concerning their work colleagues, relating to acts which are contrary to the regulations of the company or to the law*" could lead to an "*organized system of denunciation*". This analysis is reinforced by CNIL's general reservations concerning the processing of personal data that questions an "employee's or citizen's integrity" and carries the risk that employees may be "*stigmatized.*"

CNIL therefore "*expresses its reservation in principle*" concerning such a mechanism, based on fundamental rights such as "*human rights and individual liberties.*"

The reason why these whistleblower procedures, which have so profoundly irritated CNIL and which are *in fine* intended to protect the rights of shareholders and employees appear to be of historical and philosophical origin. Historical, in that the concept of "denunciation," particularly anonymous denunciation, evokes troubled memories arising from certain practices during World War II. Philosophical, insofar as a Commissioner of CNIL, Hubert Bouchet, commented in an editorial on CNIL's homepage: "*The way to hell is paved with good intentions.*"

Setting aside the underlying "moral" issue raised by CNIL, its decision appears to be questionable from a procedural standpoint: Indeed, CNIL evokes simply a "*reservation in principle*" in view of a "*risk*" that fundamental principles be breached. It fails there to *rule whether or not* the characteristics of the whistleblower

procedures — or the risk they contain according to CNIL —, as they were presented by McDonald's and Exide Technologies, *constitute* a breach of such fundamental principles. CNIL's apparent desire to make the decisions as far-reaching as possible ("*a mechanism […] in whatever form*"), combined with the historical and philosophical background that explain it, arguably make the decisions vague and imprecise.

It is noteworthy that, according to CNIL, the fact that whistleblowers can remain anonymous is only an aggravating factor. It is, therefore, the whistleblower procedure as such that is at stake.

Whistleblower Procedures Can Be *"Disproportionate"*

According to CNIL, the whistleblower procedures presented by McDonald's and Exide Technologies are disproportionate. CNIL considers that French law already includes provisions that "*guarantee that legal and internal rules be complied with,*" such as internal training, audit and control by the company's statutory auditor, the role of labor inspection and courts. It can be added that employee representatives have, by law, the mission to receive complaints concerning employees' rights and individual liberties[6].

Specific Categories of Personal Data Processing Require a Prior Authorization by CNIL

According to data protection law, certain kinds of processing of personal data are subject to a prior authorization by CNIL (in contrast to a mere declaration). Such kinds of processing comprise "*automated processing of personal data that […] could exclude persons from a right, a service or the benefit of a contract, in the absence of any legislative or regulatory basis.*"[7]

Since the personal data collected through the whistleblower procedure could lead to disciplinary action, including the termination of a contract of employment, CNIL concludes that such data processing requires prior authorization, which it denied.

CNIL's analysis on this point appears questionable.

Prior authorization of processing of personal data that could "*exclude persons from a right, a service or the benefit of a contract*" aims mainly at placing "blacklisting" of people under particular scrutiny. Such "blacklisting" had the effect mainly of depriving those with low income the right to be offered certain goods or services, without any legislation or regulation allowing such deprivation. The whistleblower procedures in the McDonald's and Exide Technologies cases can hardly be assimilated into blacklisting employees, a practice which could deprive them of their contracts of employment *without a legal basis*. Indeed, French labor law *does* provide the legal basis that allows an employer to "*exclude*" an employee, on disciplinary grounds, from his or her contract of employment[8], in particular for misconduct.This legal basis provides for the necessary protection of the employee against unjustified decisions and guarantees him/her the right to defend his/her interests.

However, CNIL interprets the relevant provision of the data protection law in a way that a "*legislative or regulatory basis*" would be required for the data processing *itself*, rather than for the "*exclusion from a right*" which could result from such data processing. Such interpretation has not yet been tested by the courts.

Note, moreover, that the transfer of personal data outside the EU may also require CNIL's prior consent: Whenever personal data is transferred outside the European Union (the EU) or certain jurisdictions which guarantee an "*adequate level of data protection,*"[9] the data subject's individual consent is required[10]. Alternatively, a data transfer agreement or binding corporate rules can be entered into under which the data importer (*e.g.* the US affiliate) commits to abide by "adequate" data protection principles, which are pre-approved by the EU Commission. Such data transfer agreement or binding corporate rules require a CNIL decision[11] granted on a case-by-case basis before they may serve as a legal basis for such a transfer of personal data.

Whistleblower Procedures Can Be *"Disloyal"*

This final reason for CNIL's refusal to authorize the whistleblower procedures proposed by McDonald's and Exide Technologies is based on the principle that a whistleblower's target must be informed that facts concerning him/her have been reported. Only such information indeed allows him/her to defend himself/herself and eventually claim that such data be corrected or deleted as appropriate. The right of an employee to be informed of, and to defend himself/herself against, incorrect allegations is indeed a fundamental principle which results notably from a combination of data protection and labor law[12]. However, when data about one person (the data subject) is provided by a third party (the whistleblower) — a situation the law referred to as indirect data collection[13] — , the information of the data subject that personal data about him/her is being processed, requires in most cases that the data controller informs the data subject directly. By definition, the processing of personal data provided by the whistleblower about the data subject, and the information of the data subject, can hardly be simultaneous. The law requires that the data subject be informed "*as soon as the data is recorded*"[14] (except in certain cases, which seem inapplicable here[15]).

McDonald's proposed to inform the data subject "*within two working days,*" Exide proposed "*as soon as possible*." CNIL rejected both, considering that "*by definition, the target is not informed as soon as the data is collected, so that he is not in a position to oppose the processing of such data. The data collection […] is therefore disloyal.*" (emphasis added). Thus, finding that the data subject is "*by definition*" informed too late, CNIL appears to add a requirement to the law, which seems difficult to reconcile with the practicability of the law.

Positions of Other EU Member States

The apparent absence of reaction to date of data protection authorities in major economies (*i.e.* Germany and the UK) could partly be due to procedural factors: the German and UK data protection authorities, unlike the French CNIL, require substantially less filing of documents, agreements and data processing declarations. Therefore, they seem to concentrate on other issues. It is, however, not excluded that regulators in other EU countries could take views similar to those of CNIL.

Perspectives

CNIL's decisions place the French companies and French affiliates of companies which are subject to SOX in a delicate situation with respect to the implementation in France of whistleblower procedures similar to the ones barred by CNIL. In the current situation, subject to further guidance by CNIL or the courts, similar whistleblower procedures could be in breach of French law and entail civil or criminal sanctions.

CNIL has made it clear its decisions have been rendered in the full knowledge of SOX requirements. Therefore, CNIL contacted the French Ministry of Labor and the SEC to seek a compromise solution that would satisfy the legal principles of each jurisdiction. Discussions with SEC have reportedly[16] taken place and CNIL will start active consultations during October with employer organizations among others to find a compromise. Some guidance by CNIL is expected before the beginning of November 2005.[17] Prior to the implementation in France, companies are, therefore, advised to thoroughly review their whistleblower procedures, notably in light of the forthcoming CNIL recommendations.

Why Are Certain Codes of Business Ethics Contrary to French Law?

Beyond the recent decisions of CNIL, which call into question certain whistle-blower procedures, it must be noted also that Business Codes of Ethics with their considerably broader scope of application could be subject to French law.

French Rules Applicable to Codes of Business Ethics

Codes of Business Ethics may contain permanent provisions of a "*disciplinary nature*" and specifically prohibit harassment in the workplace. Both items, general and specific, if they are imposed on employees working habitually in France[17], are subject to mandatory rules set forth by the French Labor Code. Accordingly, such provisions must generally be laid down in a specific manner, sometimes with pre-defined wording, in an "employee compliance manual."[18] Such manuals are usually subject to prior information and consultation procedures by employee representatives, and scrutiny by the labor administration and courts. A company which simply posted Business Ethics rules on its intranet has recently been ordered in Court[19] to withdraw such rules and abide by the mandatory prior information and consultation procedures before being authorized to apply them in France. Non-compliance with such procedures could lead to criminal sanctions.

Moreover, prior to implementing any mechanism that "*allows*" the monitoring of employees' activities[20], even if such monitoring is not the primary purpose of the mechanism, the relevant employee representative bodies must first be informed and consulted[21].

Language Requirements

Business Codes of Ethics generally contain employee obligations. According to mandatory French law, all documents that impose obligations on employees must be written in French[22]. While the law allows for an exception concerning "*documents that are received from outside France*," courts have considered this exception very narrowly or have even overruled it. There is no exception to the legal requirement that "employee compliance manuals" must be written in French[23].

Courts have recently ordered affiliates of US companies in France[24] to provide French translations of certain internal documents containing employee obligations.

Beyond the CNIL Decisions — What Now?

The following are ideas which have not yet been tested by CNIL, and its forthcoming recommendation are not yet public, so what follows is our analysis, not CNIL's official position. Note that McDonald's held discussions with CNIL over several months in an attempt to adapt its whistleblower procedure to CNIL's requirements. In the current situation, the setting-up of a whistle-blower procedure in France requires thorough and careful consideration and prior consultation with CNIL.

Contemplate Non-Automated Collection of Personal Data?

The French data protection law applies to non-automated processing of personal data, only if such processing leads to the creation of "*structured and stable*" files[25]. This means that an ethics alert by mail, re-dispatched upon reception to the relevant recipient, without ever constituting or being included in a file or computerized processing, would not fall under the scope of the French data protection law. It is, however, difficult to imagine how a SOX-compliant whistle-blower procedure in a multinational group of companies would not lead to the creation of a file of a certain structure and (though limited) stability in time and/or without using computerized files. It is worth noting here that non-automated processing does not eliminate the risk of false denunciation and the related liability exposures.

Direct French Whistleblowers Exclusively Towards a French "Ethics Committee"?

The transfer of personal whistleblower data outside France increases CNIL's level of scrutiny. It has not yet been tested whether or not SOX and French data protection law can be complied with, when personal whistleblower data is treated exclusively by a French "ethics committee". Concerning alleged violations of rules by French management, for which a local French "ethics committee" may not be the appropriate recipient, a narrow

exception could be made. The risk that such data processing is considered disproportionate could thus be reduced.

Reduce the Scope of Whistleblower Procedures?

It appears that CNIL was irritated about the very broad scope of facts that could be reported though the McDonald's and Exide whistleblower procedures. Excluding purely HR-related facts from the whistleblower procedure could reduce the risk that the procedure is considered disproportionate.

Include a "Guarantor" of Employee Rights Among the Members of the "Ethics Committee"?

CNIL's general policy concerning personal data processing in employee surveillance matters in recent years was to recommend the involvement of employee representatives[26]. This approach is in line with French labor law, which makes employee representatives the natural recipients of complaints concerning alleged violations of certain rules protecting employees[27]. Thus, rather than adding the whistleblower procedure to existing procedures, both could "merge." While the membership of employee representatives in an "ethics committee" cannot be imposed on them, they may agree that the existence of a whistleblower procedure concerning alleged violations of certain defined rules is of interest not only to the company, but also to the employees.

Alternatively, to an employee representative, a data protection officer[28] could be a member of the French "ethics committee." Such a data protection officer has specific obligations vis-à-vis CNIL, serves as a substitute for CNIL's controlling powers to some extent and has an obligation to be neutral. While it is not the data protection officer's legal missions to assume such responsibilities, his presence could be a positive element in a file presented to CNIL. A government decree about the conditions of the mission of a data protection officer is pending and should be forthcoming soon.

Remind Potential Whistleblowers that False Denunciation Made in Bad Faith is a Criminal Offence

False denunciation, made in bad faith to the employer is a criminal offence[29]. An employer who remains inactive when false denunciations have been made in bad faith, could be exposed to civil liability vis-à-vis the victim of such false denunciations[30]. It will, therefore, be necessary to make false denunciations subject to sanctions, like violations of (other) ethics rules.

In All Cases, Ensure that the Data Subject is Immediately Informed

According to French data protection law, it is generally necessary to inform the data subject immediately about whom data has been provided by a whistleblower. However, wordings such as "*within two working days*" or "*as soon as possible*" have been rejected by CNIL on questionable grounds[31].

Consider "Off-Shore" Data Processing?

A radical reaction to CNIL's decisions could be to consider processing personal data solely "off-shore." The scope of French data protection law however is far-reaching. It applies to processing personal data by a data controller[32] (i) which is "*established*" in France (in order to be considered established in France, a branch office in France of a US company, for example, could suffice), or (ii) which uses means of data processing in France. This broad definition could make off-shore data-processing subject to French data protection law, depending, however, on how exactly the processing is carried out in this second option.

It is noteworthy that in both the McDonald's and Exide Technologies decision, CNIL ruled expressly that it had jurisdiction because the French affiliates of the said US companies defined themselves (and should be defined due to the precise circumstances that appeared during the investigation of the matter by CNIL) as the "data controllers."

Conclusion

Automated processing of personal data is subject to a prior declaration at CNIL, in some cases even prior authorization. If, for instance, a whistleblower procedure — or other processing of personal data falling under the scope of French law — has been implemented in France without complying with these requirements, it is most likely that it contravenes with French law and it should, therefore, be suspended immediately and regulated for the future.

Endnotes

[1] *Commission Nationale de l'Informatique et des Libertés*. CNIL is an independent agency of the national administration. Its members comprise, among others, senators, representatives and judges. CNIL has the power to control compliance by companies with French data protection law. It can inflict monetary and other sanctions, including fines up to €150,000 in case of a first breach and up to €300,000 in case of repeat offense. CNIL may also file complaints with the Public Prosecutor. A Court could impose substantial fines and imprisonment of up to 5 years. CNIL's sanctions can be appealed before the French Administrative Supreme Court (*Conseil d'Etat*), whereas criminal sanctions imposed by a Court can be appealed before the Appellate Court and, finally, the French Supreme Court (*Chambre criminelle de la Cour de cassation*). Last but not least, a person infringing French data protection law is exposed to civil liability claims by the victim.

[2] CNIL decision no. 2005/110 of May 26, 2005 "McDonald's France".

[3] CNIL decision no. 2005/111 of May 26, 2005 "*Compagnie européenne d'accumulateurs*".

[4] It is not the purpose of this Client Alert to address more generally French data protection principles. *See however Client Alert* 405 of September 7, 2004 about the "*New Law Relating to the Protection of Individuals with Regard to the Processing of Personal Data*".

[5] Section 301 of the U.S. Sarbanes-Oxley Act of 2002.

[6] Article L422-1 of the French Labor Code.

[7] Article 25 § I 4 of the Law no. 78/17 of January 6, 1978 as amended (the "French Data Protection Law").

[8] Articles L122-9 and L122-41 of the French Labor Code.

[9] Currently: Argentina, Canada (subject to certain restrictions), Guernsey, the Ile of Man, Liechtenstein, Norway, Switzerland and Iceland. While the U.S.A. are excluded from this list, certain U.S. companies have been approved "Safe Harbor". This scheme, available to U.S. companies, has not proven to be popular as it imposes a large number of obligations and, in particular, includes filing and commitments which are available to the public. Therefore, in practice, most companies prefer to enter into data transfer agreements or binding corporate rules to satisfy EU and national data protection principles.

[10] The data subject's individual consent is practically very difficult to obtain for the purposes of a whistleblower procedure. In addition, CNIL and the working group of European data protection authorities (the "Article 29 data protection working party") expressed their reserves concerning the validity of individual consent sought collectively from employees, whose individual freedom to grant or deny their consent could be questionable. Other exceptions exist, but are outside the scope of the present Client Alert and are therefore not further referred to herein.

[11] Article 69 of the French Data Protection Law.

[12] Articles 38 *et seq.* of the French Data Protection Law and Article L122-41 of the French Labor Code.

[13] Article 32 of the French Data Protection Law.

[14] Article 32 § III of the French Data Protection Law.

[15] By exception, if such efforts are disproportionate, the data controller is not bound to inform the data subject.

[16] *Les Echos*, September 22, 2005, "la CNIL en pourparlers sur l'alerte éthique avec le régulateur américain"

[17] Lignes éthiques, whistleblowing : la CNIL prépare des recommandations à l'usage des entreprises (September 28, 2005 CNIL Website).

[18] Note that the mandatory provisions of French labor law apply to employees whose habitual workplace is France, irrespective of the nationality of the employee, the nationality of the employer company or the choice-of-law-clause that may be inserted in contracts of employment (Rome Convention on the Law Applicable to Contractual Obligations, opened for signature on June 19, 1980 (80/934/EEC), Article 6 § 1).

[19] First instance tribunal of Nanterre, October 6, 2004, "Novartis Pharma".

[20] Article L432-2-1 of the French Labor Code.

[21] *E.g.* log journals of Internet and e-mail applications could be considered a mechanism that allows the monitoring of employee activity. Therefore, the implementation of restrictions to private use of Internet and e-mail on the workplace, which are sometimes

contained in Codes of Business Ethics, is subject to certain rules protecting employee data and privacy.

[22] Article L122-39-1 of the French Labor Code.

[23] Article L122-35 of the French Labor Code.

[24] First instance tribunal of Versailles, January 11, 2005 "GE Medical"; appeal pending.

[25] Article 2 of the French Data Protection Law, subject to certain transitional provisions.

[26] In particular CNIL's report about employee surveillance in the workplace.

[27] The staff delegate (*délégué du personnel*) is designed by law to be the recipient of information, among others, about harassment (Article L422-1-1 of the French Labor Code). He is also typically designed to assist employees during dismissal procedures, including on disciplinary grounds, whatever the reason that disciplinary action is being taken (Article L122-14 of the French Labor Code).

[28] *Correspondant à la protection de données*, Article 22 § 3 of the French Data Protection Law.

[29] Article 226-10 of the French Criminal Code.

[30] It results from case-law that the employer is under the obligation to use his disciplinary authority to guarantee normal working conditions, in particular when an employee faces an aggressive attitude (*e.g.* CA Bordeaux, March 30, 2000 "Marbot et Cie / Durepaire"

[31] Article 32 § III of the French Data Protection Law. See our analysis of CNIL's interpretation of this provision under Section 1.

[32] The "data controller" *is defined as the "entity that determines the purpose and the means of data processing"* (Article 3 § 1 of the French Data Protection Law).

Decision No. 2005-111 dated May 26, 2005 concerning the authorization request by *Compagnie européenne d'accumulateurs* to implement an ethics line process.

May 26, 2005 — Theme(s): Employment (authorization request No. 1045938)

The *Commission nationale de l'informatique et des libertés*,

With regard to the declaration concerning the implementation of an "ethics line" process within the *Compagnie européenne d'accumulateurs*, referred on July 29, 2004,

In view of Convention No. 108 of the Council of Europe for the protection of persons with regard to automated processing of personal data,

In view of Directive 95/46/EC of the European Parliament and Council dated October 24, 1995 concerning the protection of individuals with regard to the processing of personal data and the free movement of such data,

In view of French law No. 78-17 dated January 6, 1978 relating to computerized data, files and civil liberties, amended by French law No. 2004-801 dated August 6, 2004 concerning the protection of individuals with regard to personal data processing,

In light of the report from Commissioner Hubert Bouchet and of the observations by Government Commissioner Charlotte Marie Pitrat,

Hereby makes the following observations:

With regard to the submitted process:

The *Compagnie européenne d'accumulateurs* (CEAC) submitted to CNIL a declaration relating to the implementation of a "hotline" (a dedicated telephone line) for its 1,500 employees.

This "ethic hotline" process, designed by its parent company Exide Technologies in order to comply with the provisions of the "Sarbanes-Oxley" Act, allows all employees of the group to communicate with the audit committee of Exide's board of directors on matters such as potential accounting inaccuracies or irregularities.

The "hotline" also allows employees to notify management of possible infringements relating to the company's regulations (ethical or commercial rules) or laws, as in force.

The process will make use of both a toll-free number and electronic mail.

In both cases the alerts, as well as the information requests, shall be sent to an American sub-contractor acting on behalf of Exide Technologies. When calls are made in French, a second American sub-contractor shall intervene.

The person originating the call may remain anonymous should he/she desire this.

The sub-contractors shall register on a digital media the contents of all requests and alerts in accordance with the following classification: "(1) human resources and issues in the workplace, (2) fraud or theft, (3) accounting error, (4) issues relating to ethic and behavior principles".

According to such classification, a written summary relating to the calls and electronic messages shall then be submitted, by encrypted e-mail, to the persons entitled to this effect by the parent company (legal department, accounting department, international committee, committee of the board of directors in charge of verification of the accounts).

The recipient of the information within Exide Technologies shall carry out, where necessary, an internal investigation, to be completed in connection with the General Counsel France (CEAC) who should receive the necessary data by e-mail.

A "follow-up" shall also be sent, by e-mail, from the parent company to the General Counsel France, who shall forward it to the Human Resources manager.

"Any employee involved in a report shall be informed as soon as possible of any allegation made against him so that he can explain himself."

Finally, data shall be stored for no more than one year.

With regard to the determination of the data controller and enforcement of the law of January 6, 1978

Article 3 of the law dated January 6, 1978 as amended provides that the data controller of a personal data processing is, unless otherwise designated by a legislative or regulatory provision applicable to this processing, the person, the public authority, the department or the entity which determines the purposes and means of such processing.

According to the notification filed by the company CEAC, it appears that the latter acts before CNIL as the data controller of the "ethic hotline" process it wishes to implement, in particular with regard to data processing carried out during investigations concerning determined employees after an alert was notified within the framework of the process.

As a consequence, the Commission considers that the law dated January 6, 1978 is applicable to the submitted "ethic hotline" process and that itself is competent to rule on the compliance of the project with the law.

With regard to the applicable declaration procedure

The Commission notes that the contemplated process may lead CEAC to decide, on the grounds of the corrective measures it must take following an alert, to exclude the employees who are deemed to have committed a wrongful act from the benefit of their employment contracts, in the absence of any legislative or regulatory provision applicable to this type of processing.

As a consequence, the authorization procedure provided under Article 25§I-4 of the law dated January 6, 1978 as amended must apply to the submitted personal data processing.

With regard to the compliance of the process with the law of January 6, 1978

In light of the law of January 6, 1978 as amended, and Article 1 of this law, the Commission expresses its reservation in principle on the implementation by an employer of a mechanism intended to arrange for the compilation of personal data from its employees, in whatever form, concerning their work colleagues, relating to acts which are in breach of the regulations of the company or the law, given the fact that it could lead to an organized system of denunciation in the workplace.

In this sense, the Commission notes that the possibility of carrying out an anonymous "ethic alert" would increase the risk of false denunciation.

In addition, the Commission considers that the mechanism presented is disproportionate considering the objectives pursued and the risks of false denunciation and stigmatization of employees who are the target of an "ethic alert". In this regard, it notes that other methods are already provided for by law to ensure that the legal provisions and internal regulations set forth by companies, are complied with (actions to raise awareness through information and training, role of auditing and alerting statutory auditors on financial and accounting matters, bringing actions before the labor inspection and competent courts).

The Commission finally notes that employees who have been the target of an alert, by definition, would not be informed as soon as the data questioning their professional integrity or integrity as a citizen, is recorded, so that they are not in a position to oppose to the processing of such data concerning them. The means of

collection and processing of such data, some of which may concern acts which could constitute a criminal offence, are therefore disloyal within the meaning of Article 6 of the law of January 6, 1978 as amended.

In light of the above observations, the Commission does not authorize the implementation of the professional integrity mechanism as submitted by the *Compagnie européenne d'accumulateurs*.

The Chairman, Alex Türk

Decision No. 2005-110 dated May 26, 2005 concerning the authorization request by McDonald's France to implement a professional integrity plan.

May 26, 2005 – Theme(s): Employment (authorization request No. 1065767)

The *Commission nationale de l'informatique et des libertés*,

With regard to the declaration concerning the implementation of a professional integrity plan within the McDonald's France group, referred on January 7, 2005,

In view of Convention No. 108 of the Council of Europe for the protection of persons with regard to automated processing of personal data,

In view of Directive 95/46/EC of the European Parliament and Council dated October 24, 1995 concerning the protection of individuals with regard to the processing of personal data and the free movement of such data,

In view of French law No. 78-17 dated January 6, 1978 relating to computerized data, files and civil liberties, amended by French law No. 2004-801 dated August 6, 2004 concerning the protection of individuals with regard to personal data processing,

In light of the report from Commissioner Hubert Bouchet and of the observations by Government Commissioner Charlotte Marie Pitrat,

Hereby makes the following observations:

With regard to the submitted plan:

The McDonald's France company referred the matter to CNIL to implement a "professional integrity plan".

The plan falls within the framework of the "code of ethics" of the McDonald's international group and allow staff members of the group's French subsidiaries to inform the American parent company (McDonald's Corporation) by mail or fax of behavior by colleagues "deemed contrary to French law and to the code of ethics".

The proposed plan would only apply to certain McDonald's France employees, *i.e.*, all staff members at the head office and white-collar employees in the 175 group restaurants, *i.e.*, approximately one thousand persons.

The application of this plan, although set forth in the group's code of ethics, would not be a binding obligation for staff members. Staff members would be clearly informed thereof.

The content of the alerts sent to the ethics department at McDonald's Corporation in the USA in the form of mail or faxes would be stored in a central system under the responsibility of the company's ethics manager. Each file stored in this system would be identified by an alert number to ensure the confidentiality of such information.

The ethics manager at the McDonald's Corporation would inform the General Counsel at McDonald's France by password-protected e-mail of the content of the mail or fax received. The data would then be directed, depending on the type of

alerts, to the appropriate department manager as per the following organization defined by McDonald's: human resources manager (for alerts concerning labor law: alleged harassment, consumption of alcohol at the workplace, discrimination, inconsistent statements of hours worked, other subjects of concern relating to behavior at the place of work), the security officer (claims of behavior which might be deemed embezzlement, claims of theft of company assets, espionage or sabotage, corruption, transmission or disclosure of confidential information), the accounting and finance officer (internal control audits, financial irregularities, debatable practice in accounting) or other recipients (depending on the type of alleged infringement).

The department manager would decide whether or not to open an investigation and would forward the alert where applicable only to the persons who should take part in the investigation. The manager would also inform the General Counsel at McDonald's France and consult him to carry out the investigation.

In the event that a member of McDonald's France general management is targeted, the investigation would be conducted directly by the American parent company.

The alert file used in the investigation would include the following data: surname, first name and town of residence of the sender of the mail (if the person has divulged his identity), name of the restaurant or office, position held by the sender, surname and first name of the person who is the target of the alleged infringement of the code of ethics, or the surname and name of another staff member who may be aware of the facts where applicable, the nature of the allegations and the conclusions of the investigation (case closed, type of sanctions taken, other corrective actions).

Staff members presumed to have infringed the code would be informed of their rights for access, rectification and opposition within two working days by the human resources manager, even if no investigation was carried out.

The result of the investigation and "corrective measures" taken (modification of internal controls or other rules in effect within the French group, disciplinary action, legal action) would be forwarded without the identity of the employee concerned by the General Counsel of McDonald's France to the ethics manager at McDonald's Corporation.

The data in the computerized alert files would be retained by McDonald's France in the event that the investigation upholds wrongful behavior for between one and five years depending on the nature of the wrongful act. The General Counsel, human resources manager, supervisor of the staff member concerned and a member of the general management team could access the data.

Alert files not resulting in an investigation or those in which the investigation was fruitless would be destroyed within two working days following the decision to close the file.

Finally, alert files held by the ethics department at McDonald's Corporation would not be kept for more than three months after the conclusions of the investigation and for five years for those concerning members of the general management team at McDonald's France.

A cross-border data-flow contract concerning personal data exchanges between France and the USA was signed by the parent company and its French subsidiary.

With regard to the determination of the data controller and enforcement of the law of January 6, 1978

Article 3 of the law dated January 6, 1978 as amended provides that the data controller of a personal data processing is, unless otherwise designated by a

legislative or regulatory provision applicable to this processing, the public authority, the department or the entity which determines the purposes and means of such processing.

According to the notification filed by the company McDonald's France, it appears that the latter acts before CNIL as the data controller of the professional integrity plan which it wishes to implement, in particular with regard to data processing carried out during investigations concerning determined employees after an alert was notified within the framework of the measure.

In addition, the motivation to implement this process, as stated in the "code of ethics" drawn up by the company McDonald's France and as substantially modified by the company during the instruction by the Commission (plans for a telephone line and e-mail address specifically for the professional integrity plan were cancelled) emphasizes the company's responsibility with regard to intended personal data processing in light of Article 3 of the above-mentioned law.

The existence of a contract governing a trans-border flow of personal data (from data controller to data controller) with the McDonald's Corporation is a further factor in favor of this analysis.

As a consequence, the Commission considers that the law dated January 6, 1978 is applicable to the submitted professional integrity plan and that itself is competent to rule on the compliance of the project with the law.

With regard to the applicable declaration procedure

The Commission notes that the proposed process may lead McDonald's France, on the grounds of the corrective measures it must take following an alert, to exclude the employees who are deemed to have committed a wrongful act, from the benefit of their employment contracts, in the absence of any legislative or regulatory provisions applicable to this type of processing.

As a consequence, the authorization procedure provided under Article 25§I-4 of the law dated January 6, 1978 as amended must apply to the submitted personal data processing.

With regard to the compliance of the process with the law of January 6, 1978

In light of the law of January 6, 1978 as amended, and Article 1 of this law, the Commission expresses its reservation in principle on the implementation by an employer of a mechanism intended to arrange for the compilation of personal data from its employees, in whatever form, concerning their work colleagues, relating to acts which are contrary to the regulations of the company or to the law, given the fact that it could lead to an organized system of denunciation in the workplace.

In this sense, the Commission notes that the possibility of an anonymous "ethic alert" would increase the risk of false denunciation.

In addition, the Commission considers the mechanism presented is disproportionate considering the objectives pursued and the risks of false denunciation and stigmatization of employees who are the target of an "ethic alert". It notes that other methods are already provided for by law to ensure that the legal provisions and internal regulations set forth by companies are complied with (actions to raise awareness through information and training, role of auditing and alerting statutory auditors on financial and accounting matters, bringing actions before the labor inspection and competent courts).

Finally, the Commission notes that employees who have been the target of an alert, by definition, would not be informed as soon as the data questioning their professional integrity or integrity as a citizen, is recorded, so that they are not in a

position to oppose to the processing of such data concerning them. The means of collection and processing of such data, some of which may concern acts which could constitute a criminal offence, are therefore disloyal within the meaning of Article 6 of the law of January 6, 1978 as amended.

In light of the above observations, the Commission does not authorize the implementation of the professional integrity plan submitted by McDonald's France.

The Chairman, Alex Türk