Privacy Rights for Employees in the Private Sector
Where the US and Europe (do not) meet

New York State Bar Association
Labor and Employment Law Section Annual Meeting
February 1, 2008

Stefan Nerinckx
Lawyer - Partner
LAGA avocats/advocaten
Brussels – Belgium – Europe

Professor Employment Law at the University-College Brussels - Belgium

Tel: +32 (0) 477 61 81 71
Fax: +32 (0)2 800 70 03

snerinckx@laga.be
www.laga.be

TABLE OF CONTENT

A. GENERAL LEGAL FRAMEWORK FROM AN EU LAW PERSPECTIVE

1. Main principles of EU data protection legislation

2. Background concerning EU data protection legislation

General introduction

Source

Aim

B. CROSS-BORDER DATA FLOWS BETWEEN THE EUROPEAN UNION AND THE UNITED STATES:

1. Main hurdles of EU data protection legislation for US companies

HR related databases: challenges

Transfer of data to the US or other non-EEA countries

Legal requirements

2. First example: Whistle-blowing

Applicable EU legislation

Situation in France and Germany

Situation in Belgium

3. Second example: Establishing a global appraisal procedure

C. INVASION OF PRIVACY BY EMPLOYERS WHO TARGET OR MONITOR EMPLOYEE BEHAVIOR - A LOCAL (BELGIAN) PERSPECTIVE

1. Data protection legislation and monitoring in HR matters

2. Privacy versus monitoring

D. CONFERENCE CONTENT

A. GENERAL LEGAL FRAMEWORK FROM AN EU LAW PERSPECTIVE

1. Main principles of EU data protection legislation

1. Applicability

EU data protection legislation applies to all processing of personal data for the activities of a company established in the European Economic Area (EEA), consisting of the 27 EU Member States as well as Norway, Iceland and Liechtenstein. The rules also apply when companies use permanent equipment in the EEA for data processing purposes.

2. Concepts

The concepts of personal data and processing are very broad. Personal data is any data reasonably allowing identification of an individual, even indirectly. Processing is defined as any use made of such data.

3. Requirements

Processing of personal data must be fair and lawful as well as for legitimate purposes. Specific requirements apply to the processing of sensitive, health and judicial data. Personal data must be accurate and data subjects must have the right to correct their data.

4. Protection

Personal data must be adequately protected against loss or theft, including through appropriate technical and organizational measures, the scope of which is determined by the sensitive nature of the personal data. Where processing activities are outsourced to third parties, adequate contractual measures must be in place.

5. Transfer to third countries

Personal data may in principle not be transferred to non-EEA countries not offering an adequate level of protection, as determined by the European Commission. Certain exceptions to this rule exist, such as adherence to the well known Safe Harbor provisions for US-based companies and the adoption of specific contractual clauses suggested by the European Commission.

2. Background concerning the EU data protection legislation

General introduction

US law is much more fragmented than EU law in respect of data protection legislation, with various federal, state and local laws targeting different categories of data (medical and credit records, minors' use of the internet, etc.), leaving most areas of "personal data"[1] processing largely unregulated. EU legislation, on the other hand, has a much more united and uniform approach to dealing with data protection legislation.

Most EU legislation has been put forward by way of directives (in principle legal instruments that are not directly binding in the individual EEA Member States and that need to be implemented in the legal systems of the states affected). As a result, the legislation resulting from this implementation process can differ slightly from one EEA State to another, but it always maintains the same basics and principles. Differences may also arise from different interpretations of local data protection legislation by national regulators.

Source

European data protection legislation is mainly based on the EU Data Protection Directive (Directive 95/46/EC[2]) (the ***DPD***), as adopted by the European Parliament in 1995 with a view to ensuring respect of "fundamental rights and freedoms, notably the right to privacy, and contributing to economic and social progress, trade expansion and the well-being of individuals".

The DPD creates a comprehensive framework for data protection regulation throughout Europe. It applies to any data processed[3] within the EEA that identifies or could identify any person, including information collected and retained by employers.

---

[1] "Personal data" means any information relating to an identified or identifiable natural person ("data subject"). Examples of personal data include the name of the person, a photo, a telephone number (even a work phone number), a code, a bank account number, an e-mail address, a fingerprint, and so forth. The concept is not limited to data traditionally considered as private or sensitive. Even data related to the professional and public life of a person can be considered to be "personal data". Only data with regard to a physical person is taken into account and not that with regard to a legal person or an association (e.g. a non-commercial firm or a trading company).

[2] Council and European Parliament Directive 95/46/EC, Recitals 2, 1995 O.J. (L 281) 31, available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; also Directive 2002/58 in respect of privacy and electronic communication and Directive 2006/24/EC of March 15, 2006, in respect of the storage of communication data.

[3] "Processing" is understood as meaning any treatment or ensemble of treatment processes with regard to the processing of personal data. The processing concerned is very varied and relates to the collection of data, keeping, use, modifying, communicating it, etc. Any time a person is requested to complete an answer strip, this is considered as a processing of data for the person who collects the data. A hotel that offers the facility of reserving via the internet also processes data when it registers the name of the customer, the dates of the stay and the guest's credit card number. The local authority also processes data when it transmits the names of the persons who have submitted a building application to a contractor who wishes to send them advertising.

Aim

The DPD has two main purposes: (1) to protect individual privacy, and (2) to harmonize data protection regulations, to encourage a secure and trustworthy data flow between EEA Member States and any third parties that enforce levels of data protection that conform to the DPD's standards. The EU legislation pursues these goals by establishing standards on data quality, legitimacy criteria for data processing, notice and consent requirements, and protection of the data subject's right with regard to his or her personal data, including the right to access and correct it.

The DPD requires the following:

- Personal data must only be collected for legitimate purposes such as (1) the performance of a contract to which the data subject is a party; (2) compliance with a legal obligation; or (3) any purpose to which the data subject unambiguously consents;
- The data must be processed fairly and lawfully. The entity processing personal data ("data controller") has a duty to inform the data subject of its identity, the purpose of the data processing, and other specifics relating to the data processing;
- The data must be accurate and up-to-date. Data subjects have the right to access their personal data and to change or delete incorrect information;
- Data controllers must implement security measures to ensure that personal data is adequately protected;
- Violations of data protection regulations call for judicial solutions, administrative solutions, liability, and penalties.

There is no prohibition against sending genuinely *anonymized* data out of the EEA, however. Where it is impossible to determine the identity of the data subject, the data transmission falls outside the scope of the DPD.

In addition to regulating the treatment of personal data within the EEA, the DPD also regulates the transfer of personal data from an EEA Member State to a third country. With some exceptions, the DPD requires that third countries that receive data from an EEA Member State enact similarly stringent data protection.

The EEA Member States and the European Commission have deemed current US data protection inadequate for third-party transfer purposes (see supra).

B. CROSS-BORDER DATA FLOWS BETWEEN THE EUROPEAN UNION AND THE UNITED STATES

1. Main hurdles of EU data protection legislation for US companies

HR-related databases: challenges

EU data protection legislation has posed specific challenges to US employers who conduct business in Europe, by regulating their ability to collect, retain, and transfer employee data within Europe and internationally.[4] The legal framework applies to all processing of personal data for the activities of a company established in the EEA.

Early in 2007, a French subsidiary of a US-based company became the first local branch of a US company to be fined for data protection violations. France's data protection regulator[5] (the CNIL) levied a fine of €30,000 (or about $44,000) against the company after it ignored CNIL's requests for clarification about one of its human resource databases, and then gave the regulator misleading information concerning the database.

Transfer of data to the US or other non-EEA Countries

The transfer of personal data contained in the database to a non-EEA country that lacks an adequate level of data protection as assessed and determined by the European Commission (such as the United States) is in principle forbidden by EU data protection legislation. Countries considered to offer an adequate level of protection are: Switzerland, Argentina, Canada, Guernsey, the Isle of Man and the United States of America (only in respect of flight passenger records). Any multinational that wishes to lawfully transfer personal data from Europe to other non-EEA countries should ensure that it sends the data overseas pursuant to an EU-accepted method. This highlights an important aspect of EU data protection legislation for businesses headquartered outside of Europe, such as in the US, namely the fact that the applicability of the regulatory framework is not determined by the location where the business is set up, but rather by the objective qualities of their personal data processing activities.

Significantly, due to the sector or context specific approach of its data protection regulations, which do not offer comprehensive protection, the EU has ruled that the United States does *not* possess an adequate level of data protection (some exceptions are applicable to this general rule, for example, flight passenger records). As a result, the transfer of personal data from an EEA country to the US is generally speaking not allowed, unless specific exceptions apply, such as Safe Harbor provisions or the adoption of contractual measures or binding corporate rules (see infra – legal requirements).

---

[4] Please note there exists no exhaustive legal definition of privacy – ECHR, Niemitz v. Germany, December 16, 1992.

[5] La Commission Nationale de L'informatique et des Libertés, www.cnil.fr.

Needless to say, this causes considerable issues in practice. Depending on how EU law has been implemented into national statute, an employer's violation of that legislation can lead to a private cause of action, civil enforcement action by data protection regulators or even criminal penalties.

Legal requirements

Because of the non adequate level of data protection in the EEA/US relation, currently, the EU recognizes three cross-border data-flow vehicles with the US: a US company can self-certify with the US Department of Commerce that it adheres to a standardized set of data protection principles (known as the "safe harbor" system); it can adhere to certain "Model contracts" with its European subsidiaries, agreeing to abide by mandatory data protection provisions; or finally it can develop a set of "binding corporate rules" - company-drafted data protection regulations that apply throughout the company and which must be ratified by each EEA member state's data protection authority. Failure to implement at least one of the above three methods could result in significant liability and negative exposure for US companies having a place of business in the EEA at which personal data is processed.

Many international companies in practice draw up a Model contract (a "Data flow Charter") taking into account the model clauses proposed by the European Commission in its decisions of 2001 and 2004[6] or so-called "binding corporate rules". The United States is in most cases included in the geographic sphere of a Model contract or Data-flow Charter. Such a Charter is concluded between the different entities that represent or make up the group of companies. Such a Charter regulates the legal issues related to the exchange of information and also the use of the data, correction of data, etc. Its provisions will in practice apply to any personal data sent from an suitable country to a non-suitable country. The fact that a contract is signed between companies does not in itself preclude authorization in principle having to be given by the employee. In that respect the employee will still need to give his/her consent to how the information is processed, how data can be accessed, the identity of any recipients, how requests for information and rectification can be made, etc.

Furthermore a company operating a database (processing data) for the activities of its EEA subsidiary must comply with the general requirements of purpose (goal directed), proportionality and transparency. Besides the employees have a right to know what data are processed about them and they should in most cases agree on any exchange of data by the employer.

In addition, unless exceptions apply, the local data protection regulator must be notified of the processing activity. Depending on the exact scope and use of the personal data, this may be the case for payroll databases, appraisal forms and databases in respect of evaluations, etc. by which personal data are processed within the EEA that are capable of identifying a person.

[6] Commission Decision of June 15, 2001, on standard contractual clauses for the transfer of personal data to third countries and Commission Decision of December 27, 2004, amending such Decision as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries; Commission Decision of December 27, 2001, on standard contractual clauses for the transfer of personal data to processors established in third countries.

We demonstrate the possible impact of the EU data protection legislation on the basis of two examples.

2 First example: Whistle-blowing

The US Sarbanes Oxley Act 2002 (SOX) requires an anonymous method for employees to report their concerns regarding accounting and financial matters and the adoption of a code of ethical conduct designed to promote the reporting of code violations.[7] This obligation applies to all SEC-listed companies, including their foreign branches.[8] The measure was introduced in order to guarantee a certain level of financial oversight, accountancy controls and independent audits.

In order to comply with the SOX requirements, many international SEC-listed companies have set up worldwide "whistle-blowing hotlines", where employees (in Europe and elsewhere) can anonymously report wrongdoings by their work colleagues (infringements of company rules and policies, as well as breaches of the law). These whistle-blowing hotlines assume that back-office systems exist containing the personal data of the persons claiming the wrongdoing and those being reported.

SOX also provides protection for whistleblowers against dismissal, threats, etc.[9]

Applicable EU legislation

As mentioned, the DPD requires that, in relation to personal data:

- individuals have a right to know what data is processed about them;
- the data is processed fairly and lawfully;
- the data is kept for no longer than necessary – accurate and up to date;
- the data is kept and managed securely.

Furthermore, as noted above, the DPD provides that in principle personal data cannot be transferred to a country outside the EEA without further formality unless the country in question ensures an adequate level of data protection (of the individual).

Therefore, if personal data is transferred from an EU branch office or if an employee reports a colleague from within the EEA, the recipient US entity should have in place an appropriate cross-border transfer solution (see supra).

In this respect, the EU Data Protection Working Group ("Working Group article 29"), an independent EU advisory body set up to provide expert opinion to the EU Commission on queries regarding data protection recognizes on the one hand the usefulness of whistle-blowing schemes and on the other emphasizes the necessity of compliance with the principles underlying the protection of personal data.

---

[7] US Sarbanes-Oxley Act 2002 (Sox) requires audit committees to establish procedures for "confidential, anonymous submission by employees (…) of concerns regarding questionable accounting or auditing matters" (section 301).

[8] Scope: SEC listed Companies and their foreign affiliates (although employee protection seems to be limited to the US … – see Carnero v. Boston Scientific Corporation, US Court of App., 5 Jan. 06)

[9] section 806.

The report underlined the necessity of whistle-blowing systems being legitimate (having a legal basis or a legitimate purpose), respecting proportionality, being transparent, protecting the interests of the incriminated person, preserving security and confidentiality of the data treated, notifying the local authorities of the system and respecting the regulations in respect of the transfer of data outside the EEA.

Situation in France and Germany

In both France and Germany, the data protection regulators and courts have ruled against certain existing company whistle-blowing procedures. These rulings were based both on infringement of the protection of privacy principles (transparency, proportionality) and infringement of local labor legislation (mandatory procedures on the introduction of monitoring and disciplinary measures – works council consultation,). They made also useful suggestions for implementing legally whistle-blowing line.

Situation in Belgium

The Belgian data protection regulator (Regulator)[10] has recently taken an official position on the legality of whistle-blowing hotlines.[11]

The Regulator underlines that the sphere of application of whistle-blowing schemes and their purpose need to be clearly determined. Furthermore, the Regulator is not in favor of anonymous reporting and considers the system as complementary to other control systems within the company. The whistle-blowing system may only be applicable to major infringements and may not include an obligation to report information. Notifications must be accurate and very precise.

To set up a whistle-blowing procedure in Belgium, it is important that the hotline is established in agreement with the works council (workers' representatives – in most EEA countries this will be the case). Furthermore, a monitoring and reporting procedure should be put in place for complaints together with potential disciplinary sanctions. Additionally, protection should be put in place against the employee making the complaint.

Only the Belgian Act on the prevention of harassment in the workplace offers protection against dismissal for employees who file a complaint with a competent manager (person of trust); the manager has to examine the complaint and subsequently contact the person accused of harassment. False complaints within the whistle-blowing procedure should also be sanctioned.

A proper defense system (instant notification, possibility of receiving details about the complaint) should be put in place for the employee complained of. Employees fired as a consequence of a complaint reported on the whistle-blowing hotline without having had a serious chance to defend themselves and without knowing how the company found out about their wrongdoing can claim abusive dismissal before the labor court.

---

[10] Commissie voor de bescherming van de persoonlijke levenssfeer/Commission pour la protection de la vie privée, www.privacycommission.be.

[11] Advice of 29 November 2006 http://www.privacycommission.be/nl/decisions/commission/recommendations.

As a consequence, US companies establishing a branch office in Belgium and wishing to implement a whistle-blowing hotline should at least acknowledge the following possible issues requiring to be resolved (together with the elements mentioned above):

- violation of the rules concerning the implementation of internal regulations or amendments thereof (e.g. if the hotline procedure has been introduced unilaterally);
- the language formalizing the hotline procedure;
- the issue of the data subject's rights to information and defense (transparency and unfair means of collecting personal information);
- the goals of the hotline possibly being achievable by tools that have less of an impact on employee privacy (disproportionate character);
- personal data possibly being transferred outside the EEA without proper cross-border guarantees for data protection.

3. Second example: Establishing a global appraisal procedure

A Belgian office/branch of a US headquarter implements an appraisal procedure that also covers its overseas employees established in the EEA.

The appraisal will inevitably increase the exchange of information such as the name of the employee, basic information concerning employment (date of hiring, title, department) and evaluation data (key competences, achievements, review of strength and areas that require improvement/development).

Since the employer determines the purposes and means of processing the personal data concerned, the local data protection legislation where the employees work in the EEA applies once processing of the data relates to the activities of that employer's place of business in an EEA state.

Duties of the employer

The US headquarter (the employer) can legally process the data mentioned above as part of its appraisal procedure, since the Data Protection Act provides that data can be processed for the purposes of personnel administration.

But, the employer has to adhere by following main duties:

(a) informing the personnel;
(b) guaranteeing the right to access/rectification/erasure/blocking;
(c) guaranteeing data quality;
(d) notification to the data protection regulator in the case of automatic processing;
(e) general obligations if personal data is communicated to the US; the US headquarters will also have to respect local EEA-state data protection law when processing personal data. However, several obligations must be fulfilled by the employer when sending employees' personal data to the US, i.e. the necessary framework must be set to exchange data with a country without an adequate level of protection in respect of personal data processing, possible consent by the employee, …

C. INVASION OF PRIVACY BY EMPLOYERS WHO TARGET OR MONITOR EMPLOYEE BEHAVIOR - A LOCAL (BELGIAN) PERSPECTIVE

As mentioned earlier, much of the exchange and processing of personal data is organized by EU law. Furthermore, local legislation protecting the data regarding the employee's private life is also heavily regulated by EU law. However, most of the EU legislation needs to be implemented into local rules. If we take Belgium as an example, we note that the legislation is fairly scattered in nature.

1. Data protection legislation and monitoring in HR matters[12]

The employment relationship is in principle (and in most EEA jurisdictions) characterized by a link of subordination between the parties. The employer can give orders to his employees and take steps to verify that they are followed. As the employer owns the material used by the employees to work with (e.g. to communicate by e-mail or internet), he has the right to control use of his property. On the other hand, this right of control is limited by the general principle that parties have to execute their contracts in good faith and that both parties to an employment contract have to show mutual respect.

Furthermore, as human beings, both employees and employers are protected by fundamental laws, and more specifically, in the present regard, by article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.[13]

In Belgium, this provision is supplemented by article 22 of the Belgian Constitution, which enshrines everyone's right "*to respect for their private and family life, their home and their correspondence*". As a general principle, one should say that employees and employees do not fully lose the protection of privacy when they enter a working environment. However, it does mean that the employer will have to exercise his control in a reasonable fashion.

Furthermore <u>other</u> local legislation will regulate different aspects of the protection of private life in an employer/employee relationship. For instance, in Belgium legislation is enacted at different levels (i.e. national level, by the social partners - employers' and employees' representatives - by the data protection regulator and, of course, it is interpreted by the courts):

- Section 124(3°) of the Electronic Communications Act of June 13, 2005, prohibits the intentional cognizance of telecommunication data concerning other persons;
- Section 314 *bis* of the Criminal Code concerns the protection of 'private communication' during its transmission;
- The Belgian Telecoms Acts of June 13, 2005, (sec. 124) and June 30, 1994, (sec. 314 of the Criminal Code) thus, in principle, prohibit employers from monitoring any data or content of the employee communications without the

[12] We are not elaborating here on any measures to be taken in respect of exchange of personal data between entities, neither are we going to comment here on any registration formalities; I will limit myself to give the general principles in monitoring of personal data by the employer.
[13] Article 8 of the Treaty of Rome of November 4, 1950, to protect Human Rights and Fundamental Freedoms.

consent of the parties involved (i.e. senders and addressees). Non-compliance is subject to criminal penalties;
- The Act of December 8, 1992, on the protection of the privacy with regard to the processing of personal data;
- Collective Labor Agreement no. 38 of December 6, 1983;
- Collective Labour Agreement no. 39 of December 13, 1983;
- Collective Labor Agreement no. 81 of April 26, 2002, clarifies the rules and conditions under which an employer can monitor the e-mail and internet behavior of his employees;
- Collective Labor Agreement no. 68 of June 16, 1998: camera surveillance at the workplace is prohibited (except as set out in accordance with the rules of CLA 68) and Act of March 21, 2007, on camera surveillance applicable to the workplace if the workplace is also a public place (e.g. a shop);[14]
- Proposal of Act of February 18, 2005, on GPS monitoring, i.e. regulation with regard to GPS monitoring in company cars. The principle holds that monitoring in company vehicles is only allowed after an agreement with "employee representation organs"; furthermore it is only allowed to preserve the safety of the employee, safety of the company car, for professional needs (e.g. logistics) and for monitoring of the activity of the employee;
- CLA no. 89 of January 30, 2007, on body searches;
- Recommendations of the data protection regulator, for instance in respect of whistle-blowing (see supra –November 29, 2006) and for instance in respect of GPS monitoring (September 7, 2005);
- etc.

2. Privacy versus monitoring

Whenever an employer manages (monitors) employees on the workshop floor and thus impacts their privacy, the control the employer exercises must take into account a number of criteria to ensure its legitimacy.[15]

In principle, any monitoring activities must be:

- ***goal-directed:*** the employer's action should be directed towards one or several lawful goals such as
  - preventing illegal and libelous acts, and acts in conflict with good manners and dignity (e.g. the employer's legal obligations concerning sexual harassment and racism);
  - protecting the economic, trade and confidential financial interests of the company and preventing infringements (e.g. infringement of trade secrets);
  - securing and preserving the proper technical operation of IT systems (e.g. anti-virus action);
  - enforcing compliance, in good faith, with implemented policies relating to online technologies;

[14] Camera surveillance is only permitted for health and safety reasons, the protection of company property, monitoring the production process and monitoring the activity of the employee (measurement to determine the salary).

[15] The same principles are used in respect of e-mail controls, video camera controls, GPS controls, etc.; most EU countries use the same criteria.

- ***proportional:*** the means of control has to be proportional to the stated goals. Control has to be relevant. It may only interfere with the individual's private life to a limited and reasonable extent;
- ***transparent:*** the employer is required to communicate the manner in which the controls are carried out, the relevant conditions, etc. Implementing controls requires informing the works council (or the health and safety at work committee, trade unions or individual employees). Additionally, it is essential to draw up a policy in accordance with the existing statutory provisions;
- ***the interference of privacy must be provided for by law*** (to be interpreted in the broad sense of the word,[16] i.e. the interference needs to be provided for in a contract or some other document enforceable against the employee.

The question of whether control and monitoring of the employee has been done correctly and within the bounds of the law, resulting in information that has been gathered and collected lawfully, will be very important. If the information is not gathered in accordance with the legal provisions, the evidence may be rejected in court. As such, proving a grave misdemeanor of the employee has committed by sending private emails during working hours or visiting pornographic sites during working time will be very difficult. Besides, the employer can even be liable to criminal penalties for not complying with the law.

Furthermore, please note that, in most EEA states, when a general framework is set up for monitoring the working place, the workers' representative organs need to be informed, or in some cases even consulted.

D. CONFERENCE CONTENT

In the presentation on February 1, 2008, I will develop and comment on the various cases (case law) from a Belgian and EU law perspective. Furthermore, I will develop practical tips in respect of the exchange of information flow between the US and the EEA:

- How to optimize the data flow between the US and the EEA
- Guidelines to bear in mind when setting up an HR Data Flow Chart
- Whistle-blow recommendations in major EEA jurisdictions
- etc…

Stefan Nerinckx
January 2008

[16] ECHR, Kopp v. Switzerland, March 25, 1998.

Stefan Nerinckx

A respected expert on employment, social security and immigration matters, Stefan has breadth of knowledge and experience in advising companies and individuals regarding employment law, social security and immigration law, at both a national and an international level. Besides day-to-day assistance to clients in labor-law matters and litigation and the representation of companies, he assists companies and foreign executives in international employment, social security and business migration law matters; he guides companies in structuring a flexible approach to working conditions and reward; he assists clients with the termination of employment and restructuring of companies and with forensic investigations; he negotiates on behalf of clients in individual and collective labor issues.

He holds a Masters degree in Law from the University of Brussels (Belgium) and three separate second Masters in (i) labor law (University of Brussels), (ii) human resources management (European Institute of Higher Education, Brussels, Belgium) and (iii) comparative industrial relations (Sinea/University of Bologna, Italy).

Outside his legal practice, Stefan is a professor employment/labor law at the UNIVERSITY-COLLEGE of BRUSSELS and a regular guest lecturer on labor law issues at the VLERICK SCHOOL OF MANAGEMENT in Ghent/Leuven. As a foremost practitioner in his field, Stefan is also a prolific writer and public orator, regularly contributing articles focusing on national and international employment issues and frequently speaking at conferences and seminars on pertinent issues in employment law. He is a member of the editorial team of a variety of legal journals.

He is recommended by a number of International Law Directories such as *"Europe's Legal 500"* and *"Who's Who of Business Employment Lawyers"*.

He is furthermore Co-Chair of the Human Resources Committee of the American Chamber of Commerce in Brussels – Belgium (AMCHAM) and President of the Board of Directors of the non-profit organization LABOR X ASBL/VZW (a joint venture between Vedior Interim and T-Interim (VDAB), helping deprived individuals in searching for work and improving their employability).