

**FEEDBACK ON THE PROPOSALS INCLUDED IN
THE EUROPEAN COMMISSION'S
COMMUNICATION TO THE EUROPEAN
PARLIAMENT ON A COMPREHENSIVE
APPROACH ON PERSONAL DATA PROTECTION
IN THE EUROPEAN UNION**

Contents

Introduction	3
About our feedback	3
Protecting sensitive data: Name as a special category	4
Wrongful publication of name to reveal ethnicity and race	5
Job applications	5
Making remedies and sanctions more effective - more bite.	6
Power to impose fines	8
Power to issue undertakings/request commitment letters	8
Reducing the administrative burden	8
The cumbersome notification system	8
Notification fee	9
Enhancing data controllers' responsibility	9
Mandatory appointment of a Data Protection Officer alongside the current notification duty ..	9
A stronger institutional arrangement for better enforcement of data protection rules.....	10
Increasing DPAs enforcement powers	11
Checks, Supervision and Accountability of DPAs	11
Contact Information	12

Feedback on the proposals included in the European Commission's Communication¹ to the European Parliament on a comprehensive approach on personal data protection in the European Union.

Introduction

Lee & White Consultants is a data protection law consultancy providing compliance advice and practical solutions to help our clients comply with the data protection and privacy legislations.

We audit, assist and advise.

Lee & White Consultants is dedicated to promoting the protection of personal data in organisations of all levels. We aim to help businesses see the good business sense in protecting personal data. Personal data is an asset which organisations need in order to be able to carry out their operations and deliver their undertakings. Processing personal data is inevitable – without it, business and commerce will be obsolete. The value of personal data makes it worth protecting.

About our feedback

Lee & White Consultants is very grateful to the European Commission for launching this consultation on the Commission's comprehensive approach on personal data protection in the European Union.

The feedback Lee & White Consultants has provided is based on experiences with our data protection clients which include national and multinational organisations, our continuous dialog with them and our research² on the compliance of different types of organisations with the Belgian data protection legislation, implementing the current Data Protection Directive³.

Our report in 2005 on the **compliance of Belgian websites**⁴ with regard to the processing of personal data in accordance with the Belgian Data Protection Law, implementing European Union Directive 95/46/EC revealed that **97% of the websites were non-compliant** and our second Report in 2006 on the compliance of **Belgian non-profit organizations' (NPO)** and **political parties' websites**⁵ with regard to the processing of personal data revealed that **not a single website was compliant** with the Belgian data protection legislation, implementing the current Data Protection Directive.

We have referred to some of the issues faced by many organisations we have come in touch with and the reasons for any non-compliance with the national data protection legislation, implementing the current Data Protection Directive, in sharing our thoughts on the matter with the Commission.

¹ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION, 'A comprehensive approach on personal data protection in the European Union'

http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

² Lee & White Consultants is in the midst of studying the situation in Belgium to determine whether any improvement to compliance has emerged 5 years since its first report on the compliance of Belgian websites in 2005 with regard to the Belgian data protection law.

³ Directive 95/46/EC

⁴ <http://www.leewhiteconsultants.com/Main/Publications/Reports.aspx>

⁵ <http://www.leewhiteconsultants.com/Main/Publications/Reports.aspx>

We hope that this feedback on the proposals included in the Commission's Communication reinforces the need for some obvious changes to the 1995 Data Protection Directive and supports the Commission in its process of reviewing the general EU legal framework on the protection of personal data to address the new challenges for personal data protection.

Protecting sensitive data⁶: Name as a special category

According to the Commission's Communication⁷,

The Commission will consider:

- whether other categories of data should be considered as '**sensitive data**', for example **genetic** data;
- further clarifying and **harmonising the conditions** allowing for the processing of categories of sensitive data.

It is submitted that the Commission's review of the general EU legal framework on the protection of personal data, in particular, with regard to widening the scope of the current categories of data considered as sensitive data, should take into account whether "name" demands a re-think to be adapted as a special category falling under the definition of sensitive data.

For the purposes of this Directive⁸, Article 2 defines 'personal data' as follows:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

The Directive then provides for the processing of special categories of data under Article 8 – that:

Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Since the implementation of this Directive, there has been a general consensus amongst member states, and specifically amongst members of the public, that the 'name' of an individual undoubtedly, is personal data.

However, the manner in which, and the purpose(s) for which an individual is identified through his/her name, can potentially **reveal the individual's racial or ethnic origin and religious beliefs**. To that extent, it should be considered whether an individual's name should then fall within the definition of "sensitive personal data" which is currently already prohibited as a general rule and be accorded further safeguards.

⁶ 2.1.6. Protecting sensitive data, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION, 'A comprehensive approach on personal data protection in the European Union'

⁷ Texts in the grey textboxes are taken ad verbatim from the Commission's Communication for easy reference.

⁸ Directive 95/46/EC

Wrongful publication of name to reveal ethnicity and race

The reason for this submission finds its base from a recent development in Belgium in October 2010, when a Flemish politician of the Belgian political party VLAAMS BELANG⁹ published names of 770 inhabitants of the North Antwerp district to highlight that only 21 names were Flemish and the rest were immigrants. He later removed their last names following criticism from the Belgian Privacy Commission that data from which the **ethnic origin** of a person can be inferred should not be published and that the necessary steps would be taken.

Job applications

The name of an individual (revealing the individual's racial or ethnic origin and religious beliefs) has also often been one of the main reasons for the individual's job application to be set aside based on racial stereotyping. Many individuals with names revealing their obvious racial and ethnic origin are not given a fair chance in the job market – whether their qualifications exceed those of their peers or otherwise.

A particular racial origin, is more often than not, knowingly or otherwise, intentionally or subconsciously, black marked by other members of society owing to something done or a bad quality that a particular group of that racial origin has acquired in the past and which affects the way the general public think about them – to this day.

When this stereotyping takes place, the name of an individual of that racial origin plays a vital part in triggering an alert 'button' in the minds of the people. This exercise is undoubtedly discriminatory, and is a mistake which continues to take place until today. It is both a historical fact and a continuing societal development.

Organisations shy away from candidates whose names reveal a black marked ethnic or racial origin, and this leads to a greater number of unemployed individuals of that particular ethnicity. It also reduces well qualified and suitable white-collar candidates to jobs which they are forced to take beneath their good qualifications. The discrimination is obvious, and so is the resulting vicious cycle.

To this extent, the nature of such an exercise i.e. the processing of the name of the individual in a job application which results in this discrimination is also contrary to Article 14 of the European Convention of Human Rights (ECHR) which secures the rights under the Convention against any discrimination¹⁰.

There is certainly awareness of the problem faced in this area and in some member states such as the United Kingdom, and particularly Belgium, steps have been taken to minimise this abuse especially in the government sector. For example, Selor¹¹, the Belgian selection agency for the Belgian government makes use of anonymous curriculum vitae following the Belgian Royal Decree of April 25, 2005 in order to curb against discrimination on grounds of sex, age, race or social origin.

There are several options (including but not limited to) available to address this current issue:

⁹ A political party in the Flemish Community of Belgium that advocates the independence of Flanders and strict limits on immigration - http://en.wikipedia.org/wiki/Vlaams_Belang

¹⁰ ARTICLE 14, ECHR: The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

¹¹ <http://www.selor.be/>

- The name of an individual is scrapped out from the curriculum vitae, leaving only their experience and qualifications as the basis for an invitation to an interview,¹² or
- The name of an individual is reconsidered as being part of **sensitive data** which reveals the individual's racial or ethnic origin and subject to specific conditions, or
- The name of an individual is classified as **encoded personal data** which can only be related to an identified or identifiable individual by means of a code and subject to specific conditions.

Whichever the option taken may be, the ultimate aim is to ensure that the conditions for processing an individual's name are more specific and focussed on better protecting the name of an individual. Thus, a re-consideration of the current status is certainly necessary.

As the Commission stated in its Communication, "*in the light of technological and other societal developments, there is a need to reconsider the existing provisions on sensitive data, to examine whether other categories of data should be added and to further clarify the conditions for their processing.*"

Making remedies and sanctions more effective¹³ - more bite.

The Commission will therefore:

- consider the possibility of **extending the power to bring an action before the national courts** to data protection authorities and to civil society associations, as well as to other associations representing data subjects' interests;
- assess the need for **strengthening the existing provisions on sanctions**, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective.

Undoubtedly, the implementation and enforcement of the data protection legislation is a vital aspect in guaranteeing that individuals' rights are firmly upheld. For the fulfilment of this necessary action, the Data Protection Authorities (DPAs) must have sufficient enforcement powers.

The current Directive¹⁴ gives the DPAs investigative and intervention powers, as well as the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated. The DPAs are also endowed with the power to hear complaints, and have a valuable advisory role.

Whilst these powers are essential, it is submitted that the DPAs should be endowed with more **active enforcement powers**. There is a strong need for the DPAs to have more bite for some obvious reasons which have resulted in non-compliance of national data protection laws. For example, in

¹² <http://inarimedia.wordpress.com/2010/01/02/could-anonymous-recruiting-cut-discrimination/>

¹³ 2.1.7. Making remedies and sanctions more effective, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, 'A comprehensive approach on personal data protection in the European Union'

¹⁴ Article 28

Belgium, the Belgian DPA's powers are mainly to advise, recommend and handle complaints. Coupled with the public's lack of awareness on data protection – which results in lesser complaints than the reality of the breach situation, many organisations abuse this fact and operate without fear or respect for the data protection legislation and dismiss their legal obligation to protect personal data. Some of the common arguments by the data controllers concerning compliance include:

- Low risk of being caught

There is a misconception that since enforcement in this area appears to be low-key, the low risk of being caught is a justifiable excuse not to use the organisation's budget to meet the legal obligations of the data protection legislations.

Although some organisations suspected of non-compliance with the privacy laws are being given warnings to clean up their act and those misusing customers' information are being reprimanded, nevertheless it seems to be undertaken very slowly by the authorities and there are very few examples of these reprimands and warnings being publicised.

Also, only a minute number of organisations have been exposed and to that extent, at an underrated scale. This shortcoming waters down the urgency, importance and necessity for the protection of personal data.

- No one reads the Privacy Policy

Section IV of the current Directive¹⁵ prescribes that certain necessary information must be provided to the data subject. This is typically laid out in a privacy policy on an organisation's website.

However, a research undertaken on the websites of a random selection of Belgian organisations¹⁶ found that whilst a minority of organisations seek to strictly abide by this legal requirement, the majority of organisations either "Copy and Paste" another's privacy policy with clear shortcomings such as not providing all the required information on the privacy statement, having similar typos or failing to replace the other organisation's name, or make no effort to have any privacy policy with the requisite information on the grounds that "no one reads the privacy policy anyway."

As the Directive stands, the current powers of the DPAs are soft and this has resulted in a similar soft approach in national legislations. It does not have the necessary teeth to tackle the misconducts persisting. As the UK's DPA puts it:

¹⁵ The Article 29 Working Party has also given comprehensive guidance in this area as per RECOMMENDATION 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union. However, the recommendations prescribed are sadly rarely utilised by many organisations on their websites.

¹⁶ A research undertaken by Lee & White Consultants from September 2004-June 2005 found that only 3.29% of the researched Belgian websites collecting personal data were compliant in terms of having a privacy statement stating all the necessary information prescribed by the Belgian data protection law. (Report on the compliance of Belgian websites with regard to the processing of personal data in accordance with the Belgian Law on Privacy Protection in relation to the Processing of Personal Data, implementing European Union Directive 95/46/EC).

“The ICO's experience of exercising the enforcement powers in the Act has led the Information Commissioner to conclude that they are cumbersome and ineffective in addressing the most serious cases of deliberate and persistent misconduct...”¹⁷

Power to impose fines

It is therefore submitted that for strengthening the existing provisions on sanctions, in addition to explicitly including criminal sanctions in case of serious data protection violations, the Directive should explicitly prescribe that the DPAs be given the power to impose substantial fines on organisations that intentionally or negligently commit serious breaches under the data protection legislation and is likely to cause damage or distress to the individuals involved. One DPA already having such power is the UK DPA.

It is submitted that DPAs of *all* member states be given a similar power laid down in the Directive so that the DPAs will be better empowered to deal with these violations and to order organisations to pay up to a maximum fine as a penalty for serious breaches under the national data protection legislation. Undoubtedly, this financial penalty will set an example for wayward organisations and act as a deterrent and promote compliance¹⁸.

Power to issue undertakings/request commitment letters

This power will make it obligatory for an organisation to perform certain actions in order to improve its compliance within a specified period of time.

The strengthening of the DPAs powers in terms of the ability to impose a financial penalty for serious breaches and to issue undertakings will certainly result in a stronger institutional arrangement for better enforcement of data protection rules as proposed by the European Commission¹⁹.

Reducing the administrative burden²⁰

The Commission will explore different possibilities for the **simplification and harmonisation of the current notification system**, including the possible drawing up of a **uniform EU-wide registration form**.

The cumbersome notification system

The current notification system, such as in Belgium, is highly cumbersome and tedious. The number of pages contained in a notification form to be filled in entails areas following the data protection rules which are highly difficult for the layman to understand. Even those with a legal background are not always sure of the content to be put down.

¹⁷

http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf

¹⁸ http://www.ico.gov.uk/~media/documents/pressreleases/2010/penalties_guidance_120110.ashx

¹⁹ 2.5. A stronger institutional arrangement for better enforcement of data protection rules, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION, 'A comprehensive approach on personal data protection in the European Union'.

²⁰ 2.2.2. Reducing the administrative burden, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION, 'A comprehensive approach on personal data protection in the European Union'

In addition, certain sections in the notification form may be skipped and filled in at a later time and the question is, how many organisations ever return to fill in those sections? As such, how transparent is a data controller under the current notification system?

Notification fee

The fact that in order to notify the DPA, a data controller (including an individual independent contractor with his own company) is required to pay a notification fee puts off the business world and acts as a deterrent. Data controllers come mainly from the world of commerce and their priority is to minimize cost and expenditure and maximise profit. The notification fee is seen as another extra expense to companies and coupled with the fact that there is no real risk of being caught for non-compliance, notification is the last on the agenda, if at all.

Enhancing data controllers' responsibility²¹

The Commission will examine the following elements to enhance data controllers' responsibility:

- making the appointment of an independent **Data Protection Officer** mandatory and harmonising the rules related to their tasks and competences³¹, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;
- including in the legal framework an obligation for data controllers to carry out a **data protection impact assessment** in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;
- further promoting the use of PETs and the possibilities for the concrete implementation of the concept of '**Privacy by Design**'.

Mandatory appointment of a Data Protection Officer alongside the current notification duty

Presently, just as any other European institution, the European Commission must appoint at least one person as a Data Protection Officer ("DPO")²². This appointment is however, optional under the Directive for member states – depending on the choice they make in the implementation of the Directive. As such, national data protection legislations which do not make the appointment of a DPO necessary rely on the notification duty of the data controller.

It is high time that the Directive provides for this mandatory appointment of an independent Data Protection Officer within *all* organisations in all member states to ensure the proper execution of the

²¹ 2.2.4 Enhancing data controller's responsibility, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION, 'A comprehensive approach on personal data protection in the European Union'

²² Regulation (EC) 45/2001

data controller's duties to protect personal data and to notify the national DPA of the organisation's data processing activities.

The current situation is such that many organisations – especially those in the private sector, do not notify their respective DPAs. In most cases, there is no one available to handle and oversee the data protection matters of an organisation. In other instances, organisations combine several roles within and the responsibility of protecting personal data is lost – either with the overload of differing responsibilities or because of conflicting interests.

With the mandatory appointment of an independent DPO, the DPO will then be responsible for ensuring that the notification duty is fulfilled by the data controller – in addition to taking care that the organisation's day to day business activities are in compliance with the data protection principles.

Also, it is submitted that whilst self-governance is welcomed, many organisations are not at the stage of implementing and abiding by the data protection principles effectively themselves. Therefore, the current notification duty to the DPA *should* continue (albeit a simplified notification system) in addition to the appointment of the DPO within an organisation both in the public and private sector, so that the national DPAs will be able to have a register of every organisation's processing activities and to verify that the notification of the purposes and main features of any processing operation is in accordance with the national measures taken under the Directive and to carry out their role as the guardians of data protection effectively.

A stronger institutional arrangement for better enforcement of data protection rules²³

The Commission's proposal for a stronger institutional arrangement for better enforcement of data protection rules is certainly welcomed.

The points below address several issues which the Commission may wish to take into account as the Commission examines:

- how to strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities in the new legal framework, including the full implementation of the concept of 'complete independence'⁵¹;
- ways to improve the cooperation and coordination between Data Protection Authorities;
- how to ensure a more consistent application of EU data protection rules across the internal market. This may include strengthening the role of national data protection supervisors, better coordinating their work via the Article 29 Working Party (which should become a more transparent body), and/or creating a mechanism for ensuring consistency in the internal market under the authority of the European Commission.

²³ 2.5. A stronger institutional arrangement for better enforcement of data protection rules, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION, 'A comprehensive approach on personal data protection in the European Union'.

Increasing DPAs enforcement powers

As already stated earlier, many organisations, especially business organisations, are under the impression that there is a low risk of being caught²⁴ for non-compliance – making the protection of personal data a low priority, in fact, no priority within the organisation's business endeavour.

Once again, reiterating the need for strengthening and granting more enforcement powers to the DPAs will inevitably lead to the building of a stronger institutional arrangement for better enforcement of data protection rules.

Checks, Supervision and Accountability of DPAs

In common with all other organisations, the DPAs are subject to the legal obligations concerning the protection of personal data.

DPAs are Data Controllers too

It has been observed that whilst the DPAs of some member states, in their capacity as data controllers themselves, seem to fare better in conforming with the data protection rules at national level in relation to the manner in which they visibly process personal data i.e. online, there remain others who need to pay more attention in their online processing of personal data, especially on their websites.

- DPAs should ensure that their privacy statement on their websites contain all the required information to be provided to the public, just as any and all other organisations should.
- DPAs should ensure their privacy statement link is visible and the privacy statement is easily readable.
- DPAs should also follow the Article 29 Working Party's recommendations²⁵ and the Commission should look into ensuring the strict monitoring of DPAs in their compliance with the general principles of data protection as set out by the Directive, and implemented in national legislations.²⁶

Whilst DPAs must remain independent in pursuing their roles as guardians of the fundamental rights and freedoms in relation to the protection of personal data, they themselves must comply with the legal obligations set out in the national data protection legislations.

As such, there should be a check and accountability mechanism to ensure that DPAs themselves are exemplary in the protection of personal data both in the virtual and real world.

To that extent, in addition to the calls for a strengthening of the Article 29 Working Party's role in coordinating DPAs' positions, and ensuring a more uniform application at national level, it is submitted that a supervisory function be given to the Working Party to supervise the DPAs in their conformity to the data protection rules they themselves are subject to - and thus an equivalent level of data protection.

²⁴ Pg. 4, Low risk of being caught.

²⁵ For example, the Article 29 Working Party's RECOMMENDATION 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp43en.pdf>

In any case, if the supervisory role is unsuited for the Article 29 Working Party, there is surely a need for some supervisory mechanism to check the DPAs and maintain conformity with the data protection rules.

At the end of the day, the better implementation and enforcement of the data protection rules begin with itself.

Contact Information

Irina Nock Krishnan
Lee & White Consultants bvba
40, de Meeûs Square,
1000 Brussels, Belgium
Phone: +32 2 401.61.26
info@leewhiteconsultants.com
<http://www.leewhiteconsultants.com>