Personal Data Breach Notification System in the European

FAYE FANGFEI WANG*

Abstract

The fast-moving technologies continually challenge present rules on data-privacy protection. The expansion of computing functions, speed of processing and storage capabilities makes personal information difficult to be controlled. In the EU, the revised EC e-Privacy Directive amended by the Directive 2009/136/EC modifies existing provisions and makes new provisions to enhance privacy protection in the electronic communications sector, which includes the further development of the system of notification of the personal data breach to minimise adverse effects. This paper aims to examine and evaluate the personal data breach notification system, interpret the requirement of "without undue delay" duty and discuss the impact of the revised Directive to business organisations. It finally proposes solutions to improve the notification system to increase the efficiency of privacy protection.

A. Introduction

In the age of the internet and globalisation, it is getting harder to keep personal details private as personal data can be automatically stored, processed, distributed or transferred by automated information systems in a split second. New technologies dramatically change one's life style. Nowadays, online shopping and social networking have become part of daily life, whilst automated transactions via high-frequency trading platforms have grown to be common in financial industries and Google mapping has turned into a daily tool. Google Street View of towns and cities for Google mapping may contain individuals' sensitive information such as images and vehicle numbers. It was reported that Google collected personal data including full emails and passwords from unsuspecting internet users via Wi-Fi networks when its Street View cars mapped the towns and cities.[1] This is considered to be a significant breach to data-privacy protection.

---

* Senior Lecturer in Law, Brunel University, UK; PhD in Law (University of Southampton), LLM in Commercial Law (University of Aberdeen) and LLB in Law (Guangdong University of Foreign Studies), email: fangfei.wang@gmail.com.

[1] J Halliday, 'Google committed 'significant breach' over Street View', *The Guardian* (3 November 2010), available at http://www.guardian.co.uk/technology/2010/nov/03/google-information-commissioner-street-view (last visited on 3 December 2010).

With the continuing development of technology, automated decision-making on behalf of individuals is also under way. That is, automated agents make decisions for individuals based on the collected data – models of individuals' preferences. Under automated systems, personal data including a long history of individuals' activities, behaviours and habits will be analysed and processed. Individuals may be more vulnerable to attack, because the system contains personal data of increased sensitivity. For instance, the German Federal Constitutional Court in the Judgment of the First Senate of 27 February 2008 (1 BvR 370, 595/07) expressed that "the use of information technology has taken on a significance for the personality and the development of the individual which could not have been predicted. Modern information technology provides the individual with new possibilities, whilst at the same time entailing new types of endangerment of personality."[2]The new technologies raise serious concerns on personal data and privacy protection for information an individual provides to a system or captured by a computing program as "data provided by individual networked systems can be evaluated and the systems made to react in a certain manner" automatically.[3] The endangerments of users' personability are also noted, that is:

> "In the context of the data processing process, information technology systems also create by themselves large quantities of further data which can be evaluated as to the user's conduct and characteristics in the same way as data stored by the user. As a consequence, a large amount of data can be accessed in the working memory and on the storage media of such systems relating to the personal circumstances, social contacts and activities of the user. If this data is collected and evaluated by third parties, this can be highly illuminating as to the personality of the user, and may even make it possible to form a profile."[4]

In response to the ever fast-growing technology, legislators have been continuously examining and revising the existing rules to be in line with the modern technology. Business organisations that process personal data are also encouraged to take action and adopt privacy-enhancing technological measures. Those data-privacy protection measures are considered to be beneficial to business as the "payoff" to organisations can be shown on the improvement of customer satisfaction and trust, enhancement of reputation and reduction of legal liabilities,[5] although the regulatory and technological measures on data and privacy protection may contribute to a reduction of transaction speed and an increase of transaction costs.

---

[2] Case C-595/07, The German Federal Constitutional Court in the Judgment of the First Senate of 27 February 2008,1 BvR 370, para 104, available at *http://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html* (last visited on 12 November 2010).

[3] 1 BvR 370, 595/07, para 109.

[4] 1 BvR 370, 595/07, para 112.

[5] A Cavoukian, & T Hamilton, *The Privacy Payoff: How Successful Businesses Build Customer Trust* (Canada: McGraw-Hill 2002).

In the EU, the EC e-Privacy Directive has been amended by the Directive 2009/136/EC[6] to keep in line with the current social and technological development, which includes the further development of the data breach notification system to minimise adverse effects on data breach. An official recommendation document called "A comprehensive approach on personal data protection in the European Union" (known as "the EU Comprehensive Approach 2010") was also issued on 4 November 2010 to address challenging legal matters for the communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions.[7] It confirms a number of key objectives of future assessment and evaluation of data protection to ensure a fair balance and coherent application between the protection of individual privacy rights and the free circulation of personal data within the internal market. For example, the EU Comprehensive Approach 2010 introduces a general principle of transparency, data minimisation and prior consent of personal data processing and the obligations of data controllers including modalities and formalities; defines the categories of sensitive data as well as harmonises the conditions on the processing of such data; promotes awareness-raising activities on data protection; encourages the cooperation and coordination between Data Protection Authorities; and proposes remedies including court actions and sanctions as well as supports self-regulatory initiatives. It also aims to improve and streamline the current procedures for international data transfers by examining the adequacy of data transfer procedures and specifying the criteria and requirements for the assessment of the level of data protection in a third country or an international organisation.

Traditionally, the EU legislation is geared to protect individual privacy rights, whilst the US and international guidelines are designed to promote the free flow of cross-border data for the development of global economy.[8] The above measures proposed by the EU Comprehensive Approach reassures the objective of data-privacy protection – a fair balance and coherent application between data protection and the free circulation of personal data within the internal market. This vision has also been developed upon the recent case *European Commission v. Germany* (C-518/07) 09 March 2010: the European Court of Justice (Grand Chamber) confirms that the main objective of the Directive was to strike a fair balance between the protection of the

---

[6] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *Official Journal of the European Union*, L 337/11, 18 December 2009, p 0011–0036.

[7] 'A Comprehensive Approach on Personal Data Protection in the European Union' – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM(2010) 609/3 (hereafter "the EU Comprehensive Approach 2010").

[8] F Wang, *Law of Electronic Commercial Transactions: Contemporary issues in the EU, US and China* (Oxford: Cavendish-Routledge Publishing, 2010), p 121.

right to private life and the free movement of personal data.[9] Although the EC Directives have the wording of "neither restrict nor prohibit the free flow of personal data"[10] and "ensure the free flow of personal data"[11], they don't explicitly express the objective of "a fair balance" between data-privacy protection and the free flow of personal data. The main methodologies of the legislative reform addressed by the EU Comprehensive Approach 2010 lie in the introduction of new principles and modalities of obligations. The expectation of ultimate outcomes is to create a fair balance by introducing a new coherent general legal framework for consistent and adequate protection on data transfers within EU member states and from EU member states to third countries outside the EU.

This paper aims to examine and evaluate the current data breach notification system, interpret the practice of "without undue delay" duty and discuss its impact to business organisations. It finally proposes solutions to improve the notification system to enhance the efficiency of privacy protection.

B. Current EU Legal Framework for Personal Data Breach Notification

1. Definition of Personal Data and Personal Data Breach

Data protection and privacy protection have a close relationship which can be understood from a macro perspective as "data protection is to protect the rights of data ownership and balance the benefits between the protection of data ownership and the permission of data free-flow, while privacy protection is to protect fundamental human rights as stated in Article 8 of the Convention of Human Rights and Fundamental Freedoms in 1950."[12] From a micro perspective, privacy protection is mostly connected with personal data protection in particular sensitive personal data protection.

Personal data has been defined in the EC Data Protection Directive as "any information relating to an identified or identifiable natural person ('data subject'); and 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, culture or social identity".[13] The further interpretation of "personal data" in relation to privacy can be found by a UK leading

---

[9] Case C-518/07 *European Commission v. Germany*, European Court of Justice (Grand Chamber), 9 March 2010 [2010] 3 C.M.L.R. 3, para 24 and 30.

[10] Article 1(2) of the EC Data Protection Directive.

[11] Recital 1 of the EC e-Privacy Directive.

[12] F Wang, & N Griffiths, 'Protecting Privacy in Automated Transaction Systems: A Legal and Technological Perspective in the EU' (2010) 24 International Review of Law, Computers and Technology 153, p 154.

[13] Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.

case *Durant v. the Financial Services Authority (FSA)*.[14] The English Court of Appeal held that personal data only refers to information that affects one's personal or family life, business or professional capacity. The UK Information Commissioner also published a discussion of the implications of Durant case.[15] The Information Commissioner confirms the court judgments on the measure of the scope of individual information that the individual information in question should be capable of having an adverse impact on the individual's privacy. The two notions of identification are recognised as a biographical sense and an individual focus as the Judge ruled that:

> "The first is whether the information is biographical in a significant sense, that is, going beyond the recording of [the individual's] involvement in a matter or an event which has no personal connotations; … The second concerns focus. The information should have the [individual] as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest …".[16]

The above justification provides helpful guidance and greater clarity regarding the complex meaning of "personal data" in relation to privacy. However, the EC Data Protection Directive does not define "sensitive personal data", although Recital (34) and (70) of the EC Data Protection Directive mentioned the term "sensitive" data and Article 8 of the EC Data Protection Directive refers to "the processing of sensitive data" without using the wording of "sensitive". Article 8(1) of the EC Data Protection Directive provides 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."

Those special categories of data are currently already prohibited as a general rule, with limited exceptions under certain conditions and safeguards. In this sense, privacy protection mostly refers to sensitive personal data. The personal data breach notification provision of the EC e-Privacy Directive does not implicitly refer to notification of only sensitive personal data breach to the competent national authorities, although it requires additional notice to a subscriber or individual "when the personal data breach is likely to adversely affect the personal data or privacy". [17]

The EU Comprehensive Approach 2010 has identified the importance of understanding the scope of "sensitive personal data" as it proposes that "in the light of

---

[14] *Durant v. the Financial Services Authority (FSA)* [2003] EWCA Civ 1746.

[15] 'The *Durant* Case and its Impact on the Interpretation of the Data Protection Act 1998', Information Commissioner's Office, 27 February 2006, available at <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf> (last visited on 12 November 2010).

[16] *Durant v. the Financial Services Authority (FSA)* [2003] EWCA Civ 1746.

[17] Article 4(3) of the EC e-Privacy Directive amended by the Directive 2009/136/EC.

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. This concerns, for example, genetic data which is currently not explicitly mentioned as a sensitive category of data."[18] However, the Comprehensive Approach did not mention about giving a definition of "sensitive personal data" under the EC Data Protection Directive.

As to the definition of "personal data breach", the concept has been added in the revised EC e-Privacy Directive. It means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."[19] Personal data breach may lead to serious consequences, if protection measures are not implemented in time. It was reported that the UK branch of Zurich Insurance Plc (Zurich UK) had lost 46,000 customers' personal details due to the data security failings, including identity details, and in some cases bank account and credit card information, details about insured assets and security arrangements. The UK Financial Services Authority (FSA) has fined Zurich Insurance Plc £2,275,000 for failing to have adequate systems and controls in place to prevent the loss of customers' confidential information as the loss could have led to serious financial detriment for customers and even exposed them to the risk of burglary.[20] In order to increase the possibility of promptly implementing appropriate technological measures to personal data breach, the duty of notification of personal data breach needs to be introduced to service providers and enhanced by competent national authorities.

The EU Comprehensive approach 2010 has proposed to examine the modalities of a personal data breach notification system in the general legal framework, including details such as the addressees of such notifications and the criteria for triggering the obligation to notify.[21]

2. Security of Processing: Data Breach Notification Duty

It is known that there are seven general principles set out in the old EC Directives on data-privacy protection. They are: security, confidentiality, data quality, onward transfer, choice, notice and access. There are also five sub-principles with regard to data quality has been set out in Article 6 of the EC Data Protection Directive, whilst there are six sub-principles concerning the transfer of personal data to a third country set out in Article 25 of the EC Data Protection Directive.

---

[18] The EU Comprehensive Approach 2010, p 9.

[19] Article 2(h) of the EC e-Privacy Directive amended by the Directive 2009/136/EC.

[20] 'FSA fines Zurich Insurance £2,275,000 following the Loss of 46,000 Policy Holders' Personal Details', 24 August 2010, FSA/PN/134/2010, available at *http://www.fsa.gov.uk/pages/Library/Communication/PR/2010/134.shtml* (last visited on 6 December 2010).

[21] The EU Comprehensive Approach 2010, p 7.

Recently, the principle of enforceability has been added under Article 15(a) of the new EC e-Privacy Directive. However, one of the most common principles specified by the Organisation for Economic Co-operation and Development (OECD) in 1980 and the Asia-Pacific Economic Co-operation (APEC) in 2004 still has not been highlighted in the EU data-privacy legislation. That is accountability. Accountability mechanisms fall into two categories: one is structure and the other is transparency.[22] The issue of transparency in data-privacy protection has been raised by the EU Comprehensive Approach 2010. The Approach has proposed the introduction of "a general principle of transparent processing of personal data in the legal framework" accordingly.[23]

Among the general principles, security and confidentiality are particularly enhanced by the new EC e-Privacy Directive. "Security" is one of the most essential principles for personal data and privacy protection. The original Article 4 of the e-Privacy Directive provides the provision of "Security" that:

> 1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
>
> 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

As shown above, the provision of "security" under the EC e-Privacy Directive introduces "taking appropriate technical and organisational measures" and "informing duty" to safeguard security in a descriptively conceptual way. The Directive 2009/136/EC makes efforts to increase the legal certainty of security by providing more detailed explanations and procedures. The Directive 2009/136/EC changes the title/provision heading of Article 4 of the e-Privacy Directive from "Security" to "Security of Processing" and inserts one sub-section in Article 4(1) and three additional sections as Article 4(3)–(5) targeting at mandatory personal data breach notification measures etc to the previous provision. The EC e-Privacy Directive and the Directive 2009/136/EC particularise and complement the Data Protection Directive by translating the principle of the security set out in the EC Data Protection Directive into specific rules.

---

[22] F Wang, *Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective* (Oxford: Chandos Publishing 2009), p 73.

[23] The EU Comprehensive Approach 2010, p 6.

The change of title of Article 4 demonstrates the importance of the "processing" stage for the protection of personal data and privacy. The Article 4 (1a) of the Directive 2009/136/EC further emphasises the processing part of ensuring security which makes sure that "personal data can be accessed only by authorised personnel for legally authorised purposes". It requires the protection of "personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure" and ensures "the implementation of a security policy with respect to the processing of personal data". It also suggests that "relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve." The wording of the insertion (Article 4(1a) of the Directive 2009/136/EC) brings to consistency to the data protection principles outlined in Articles 6, 7 and 17 of the EC Data Protection Directive. That is personal data must be processed fairly and lawfully.

Moreover, the European Data Protection Supervisor (EDPS) welcomes the adoption of a security breach notification system as it will encourage business organisations to improve data security and enhance the accountability of the personal data.[24] That is, network operators and Internet Service Providers ("ISPs") should notify the National Regulatory Authorities ("NRAs") and also their customers of security breach. This recommendation has been adopted in the amendment of the EC e-Privacy Directive under the Directive 2009/136/EC and set up under the provision of "security of processing". There are three additional sub-sections: "notification obligations from service providers" (Article 4(3)), "duty from competent national authorities" (Article 4(4)) and "adoption of measures resulting from consultation" (Article 4(5)).

The added Article 4(3) from the Directive 2009/136/EC provides the key requirements of "notification of personal data breach" from the service provider that:

> "[I]n the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and indi-

[24] Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. C-128/33, 6.6.2009.

> viduals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so."

The above sub-section continues with the specification of requirements on to whom the notification shall be made. There are twofold: one is to the competent national authority and the other is to the subscriber or individual. For the purposes of this Article, as for much of this Directive, the competent national authority refers to the Information Commissioner's Office (ICO).[25]

The service provider should notify the competent national authority of the personal data breach in the first instance. There is no requirement of notification of a personal data breach to a subscriber or individual concerned if the provider had demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach.[26]

With regard to the notification content to the subscriber or individual, the service provider is required to describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. With regard to the notification content to the competent national authority, the service provider is required to provide additional information describing the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

The further insertion of "duty from competent national authorities" (Article 4(4) of the EC e-Privacy Directive) particularises specific requirements of competent national authorises to give support and guidance and enhance the implementation certainty. According to these two inserted sections, the competent national authorities are encouraged to adopt guidelines and issue instructions to the notification of personal data breaches for service providers as well as impose appropriate sanctions in the event of a failure to comply with notification obligations. Another insertion of "the Commission's adoption of measures resulting from consultation" (Article 4(5) of the EC e-Privacy Directive) specify the role of the Commission as a guardian to adopt appropriate technical implementing measures following consultation with agents, working parties and supervisors.

The EU Comprehensive Approach 2010 has raised discussion on possible solutions to ensure consistency in implementation of technological protection measures, for instance, it suggests introducing modalities and using one or more EU standard forms ('privacy information notices') by data controllers.[27]

---

[25] 'Implementing the Revised EU Electronic Communications Framework: Overall Approaches and Consultation on Specific Issues', Department for Business, Innovation and Skills (BIS), September 2010, available at http://www.bis.gov.uk/Consultations/revised-eu-electronic-communications-framework (last visited on 6 December 2010).

[26] Article 4(3) of the EC e-Privacy Directive.

[27] The EU Comprehensive Approach 2010, p 6.

C. Future Legislative Reform for Data Breach Notification System

There is no doubt that the new EC e-Privacy Directive has been modernised to be compatible with the current technology in order to protect the users' data-privacy rights and enhance the public safety. However, technologies have been continually fast-growing which leave legislators with no choice but to re-examine existing rules continually.

For example, drivers who wish to park their cars on the streets of London but have no coins or cash at hand can phone and pay the car parking service by quoting a specific street parking location number, vehicle registration number, parking period, name and credit card number according to the parking instruction post on the side of the streets. Some months later, if he/she wants to use this service again, he/she only needs to call, quoting their name, the specific street parking location number and the last four digits of his/her credit card. The transaction can be done automatically using the stored information/data. With the further development of automated information systems, it is not hard to imagine, in a few years' time, when we park our cars, our credit cards will be automatically charged for the parking fee without any human interaction as the automated system will immediately identify where we are and what we are doing.

Such automated decisions-making systems can equally apply to other industries such as travel agencies. The automated travel agent can design and offer a most favourable travel package to an individual based on the information that the individual gives and other data sources that the agent collect such as passenger records, vehicle traffic records, health conditions and annual incomes etc. This is also known as "service-oriented computing". Apart from the functional development of computing technology, the growth of the capacity of computing facilities is also astonishing. It is suggested that the capacity of a computer is doubled every 18 months which means that after a period of 15 years, the processing and storage capabilities of our computers are increased by a factor of 1,000.[28] It implies that personal data will be more largely captured, widely used, heavily stored and broadly analysed in the future automated computing service systems. Personal data protection, therefore, will be greatly challenged due to the large-scale development in computing functions, speed of processing and storage capabilities. There is an increasing need of further considerations on matters such as the time limit of notification obligations and remedies on data-privacy infringements.

1. Timeframe of Notification

The new EC e-Privacy Directive requires that in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. The provider of publicly available electronic communications services refers to

[28] R Wacks, *Privacy: A Very Short Introduction* (New York: Oxford University Press 2010), p 127.

public and private electronic communications sectors and horizontally to all business organizations that process certain types of information.

As discussed earlier, the update of Article 4 of the EC e-Privacy Directive introduces the concepts and requirements of "notification of data breach" and "duty from competent national authorities". It well reflects on the principles set out in Article 12(c) and 28 of the EC Data Protection Directive. However, it does not specify a timeframe for the notification of data breach except for the requirement of "without undue delay". Moreover, it does not introduce modalities of the notification of data breach except for the recommendation of guidelines and instructions that may be adopted by competent national authorities. The EU Comprehensive Approach 2010 has identified the necessity of introducing modalities for providing information and drawing up one or more EU standard forms ('privacy information notices') to be used by data controllers, but it is silent on the necessity of interpreting "without undue delay" for the notification of data breach.

In the author's opinion, the interpretation of "without undue delay" is vital as the timing affects the certainty of data-privacy protection. The determination of the appropriation of time limit on notification and remedial action shall be taken into account of the speed, scope and capabilities of spreading personal data under the current and future development of technologies in particular automated information systems. In addition, the consideration of the time-limit issue for notification and remedial action can be learned from the interpretation of the time-limit requirement on the exercise of the right to access in Article 12(a) of the EC Data Protection Directive regarding information storage and disclosure in the case of *College van burgemeester en wethouders van Rotterdam v. MEE Rijkeboer Netherlands* (judgement of 7 May 2009).[29] The judgement provides that:

> "Article 12(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to ***fix a time-limit*** for storage of that information and to provide for access to that information which constitutes ***a fair balance*** between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.
>
> Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of ***one year*** and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the

[29] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. MEE Rijkeboer, European Court of Justice* (Judgement of 7 May 2009).

> interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary."[30]

Accordingly, it shall be for Member States to fix a time-limit for notification of the personal data breach and remedial action. Where the length of time for which a personal data breach is to be informed to the competent national authority or remedial action is to be taken is very long, the adverse effects of the breach of the personal data or privacy of a subscriber or individual may be higher as the implementation of appropriate technological protection measures may be delayed. The issue of a fixed time limit for notification and remedial action shall be further assessed when the Commission examines the modalities for the introduction in the general legal framework of a general personal data breach notification, including the addressees of such notifications and the criteria for triggering the obligation to notify according to the EU Comprehensive Approach 2010. The obligation of a time-limit for notification of data breach shall also be contained in EU standard forms of privacy information notices in the future.

To avoid the undue delay for notification of data breach, the adoption of regulatory and technological measures of enhancing data controllers' responsibility shall be encouraged. According to the EU Comprehensive Approach 2010, the Commission considers measures of enhancing data controller's responsibility including making the appointment of an independent Data Protection Officer mandatory and harmonising the rules related to their tasks and competences, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises; inserting an obligation for data controllers to carry out a data protection impact assessment in specific cases and further promoting the use of Privacy Enhancing Technologies (PETs) and the possibilities for the concrete implementation of the concept of 'Privacy by Design'.[31]

With regard to the issue of the necessity of reporting data breach to a subscriber or individual in addition to the competent national authority, in the author's opinion, specific conditions shall be considered:

– Whether it is necessary to report data breach to a subscriber or individual shall depend on the breach recovery status, for example, it shall not be required if the provider has demonstrated the satisfaction of remedial action to the security breach to the competent authority according to Article 4(3) of the revised EC e-Privacy Directive;
– Whether it is necessary to report data breach to a subscriber or individual shall depend on the harmful effects of notification, for example panic and social threat;

---

[30] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. MEE Rijkeboer*, European Court of Justice (Judgement of 7 May 2009), para 71.

[31] The EU Comprehensive Approach 2010, p 12.

– Whether it is necessary to report data breach to a subscriber or individual shall depend on the size of the breach effects, such as the threshold for the direct cost of personal data breach and the potential incremental cost resulted from notification, the number of affected individuals and the scale of harm.

If notification of a personal data breach to a subscriber or individual is necessary, the time limit of such notification shall be concerned in particular regarding the time period between notification to the competent national authority and notification to a subscriber or individual, because the provider is required to notify the personal data breach to the competent national authority in the first instance according to Article 4(3) of the revised EC e-Privacy Directive. Therefore, there shall be two different time periods for notification of data breach without undue delay: the first time period should be considered that the provider shall notify the competent national authority of a personal data breach as soon as the provider has noticed the breach and no later than 24 hours of having learned of such breach; and the second time period should be considered that the provider shall notify a personal data breach to a subscriber or individual when necessary within 24 hours after the notification of the personal data breach to the competent national authority. In other words, the competent national authority shall assess the satisfaction of the provider's implementing appropriate technological protection measures and inform the decision of notification to a subscriber or individual within 24 hours of the receipt of the case.

The time limit of notification of a personal data breach shall be considered, proposed and included in the guidelines and instructions issued by competent national authorities. As discussed in Section B, the update of Article 4 of the EC E-Privacy Directive recommends competent national authorities adopting guidelines and issuing instructions on notification for the personal data breach. The EU Comprehensive Approach 2010 proposes that Data Protection Authorities should strengthen their cooperation and better coordinate their activities, [32] because the consistent measures rely on the cooperation between competent national data protection authorities especially when data breach issues have a cross-border dimension. For example, when multinational enterprises are based in several Member States and are carrying out their activities in each of these countries, they might need the guidance from different national authorities and coordinated supervision from the European Data Protection Supervisor (EDPS). An unambiguous procedure for the cooperation between data protection authorities will help dealing with the notification of data breach from multinational business organisations/service providers more efficiently and better implement the "undue delay notification" duty.

[32] The EU Comprehensive Approach 2010, p 12.

2. Effective Enforcement Mechanisms for Notification

The modernisation of existing legislation is of practical necessity, whilst enforcement is of fundamental importance, because any legislative and technological measures to protect consumers' privacy can only be effective if they are properly implemented and enforced. The implementation of the "without undue delay" requirement to notification of the personal data breach is fundamentally important to enhance the quality control of data protection, reduce the risk of potential personal harm and financial loss as well as increase consumers' confidence and trust in using automated information systems. According to the Article 4(4) of the revised EC e-Privacy Directive, the service providers should be liable for breach of the "without undue delay" obligation.

The mechanisms of enforcement are threefold: the first is by national enforcement authorities; the second is by court litigation; and the third is by out-of-court resolutions or self-regulatory enforcement initiatives.

With regard to the exercise of the power of national enforcement authorities, the competent national authority shall impose appropriate sanctions on service providers in breach of notification obligation according to Article 4(4) of the revised EC e-Privacy Directive. Article 15(a) of the revised EC e-Privacy Directive further particularises the implementation and enforcement of the provisions of the Directive ensuring Member States to lay down the rules on penalties including criminal sanctions and enhance the power of competent national authorities in terms of order, investigation and cross-border cooperation. It was reported that "the lack of a legal obligation for service providers to report data breaches in some member states may aggravate the weakness of the enforcement system,"[33] thus, Member States shall amend national laws including the introduction of the data breach notification system in order to comply with the revised EC e-Privacy Directive. National laws shall ensure that competent national authorities have access to effective sanctions on the breach of the "without undue delay" notification duty of the service provider. Competent national authorities may also be allowed to impose a civil monetary penalty for breach of the "without undue delay" notification depending to the nature and effects of individual cases according to national laws.

As to court litigation, the EU Comprehensive Approach 2010 considers that it is essential to have effective provisions on remedies and sanctions that the Commission will 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; and 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

[33] 'Data Protection in the European Union: the Role of National Data Protection Authorities', European Union Agency for Fundamental Rights (FRA) (Luxembourg: Publications Office of the European Union, 2010), p 43.

them more effective".[34] However, it is time-consuming and complicated to enforce privacy protection in courts and it is even more complex when the dispute concerns the transfer of data between EU member states or from the EU to a third country outside the EU member states due to the challenges of ascertaining jurisdiction and applicable law. Currently there is only one main article concerning conflict-of-law rules in the EC Data Protection Directive – Article 4.

The adoption of self-regulatory enforcement initiatives may avoid the complication of the determination of jurisdiction and choice of law. The initiatives have been strongly encouraged by the FTC Fair Information Practices Report in 2000, OECD Privacy Online: Policy and Practice Guidance in 2003, and the EU Comprehensive Approach in 2010. Due to the fact that the current provisions on self-regulation (code of conduct) – Article 27 of the EC Data Protection Directive – have rarely been used so far and are not considered satisfactory by private stakeholders, the European Commission continues to encourage data controllers to employ self-regulatory initiatives so as to establish a better enforcement system. It is known that a trustmark or privacy seal program is one of the most common recommended self-regulatory initiatives on data-privacy protection.

A "mark" or "seal" should be deemed as "a readily recognizable emblem, voluntarily displayed on a Web site, which signifies that a site has met recognized industry privacy requirements".[35] A trustmark or privacy seal program can be beneficial for promoting effective enforcement on data-privacy protection compliance including the assessment of the compliance of the "without undue delay" data breach notification duty. Currently, the best known providers for online privacy seals are the American companies such as TRUSTe, BBBOnline and VeriSign. Those seal programs have been designed to meet the conditions of the international regulations and US-EU Safe Harbor Agreement. They have procedures in common: users can file a complaint to a seal program provider and the seal program provider will respond to a complaint by imposing sanctions on accredited websites. However, those privacy seal programs cannot require a licensee to pay monetary damages or take further steps to exempt from legal violation. In the EU, the European Commission has proposed to explore the possible creation of EU certification schemes (e.g. 'privacy seals'). The idea is to provide standardisation for 'privacy-compliant' processes, technologies, products and services and used by both individuals and data controllers.[36] The Commission will examine how privacy seals fit in with the legal obligation and international technical standards, and propose measures to ensure the trustworthiness of such privacy seals. In the author's opinion, a regulation or guideline of privacy seals might be necessary to introduce consistent conduct of privacy seal providers that opt for certified technologies, products or services in member states. Such regulation shall provide a stronger institutional arrangement for the effective enforcement of data protection

---

[34] The EU Comprehensive Approach 2010, p 9.

[35] 'Online Privacy Seal Program', US Chamber of Commerce, available at http://www.uschamber.com/issues/technology/online-privacy-seal-programs (last visited on 8 December 2010).

[36] The EU Comprehensive Approach 2010, p 12.

rules including the obligations and liabilities of service providers and the role of competent national data protection authorities.

D. Conclusion: Impacts on Business Organisations

The modernisation of existing rules will be an ongoing process due to continuous changes of technology that impact the way we live and do business. The use of electronic services requires adequate levels of privacy, security and protection of personal data, otherwise, users may suffer financial loss and distress because they are at risk of their personal information being used other than in ways that they have given specific permission for.[37] The recent updated EU legal framework on data-privacy protection intends to bring a positive impact on the security conduct of data processing for both consumers and business organisations. The introduction of a duty on providers of electronic communications services to notify personal data breaches will be beneficial to improve consumer welfare as a result of potential reduced incidences of breaches of personal data. Such a notification system will be also beneficial to business organisations as a result of potential enhanced reputation by implementing appropriate data breach notification measures, although there may be costs to adopt such measures. The "Study on the economic benefits of privacy- technologies (PETs): Final Report to The European Commission" in July 2010 indicated that although there may be short-term costs with few tangible benefits, the longer-term impact on the business as a result of reputational gains would be significant.[38]

In response to the revised EC e-Privacy Directive, national competent authorities shall provide guidelines and instructions of data-privacy protection to business organisations that collect and process personal data. Business organisations shall develop technological approaches and tools that are compatible with the requirements of the new legislation, such as complying with the required standard of privacy-enhancing technologies (PETs), performing the duty of notification of personal data breaches without undue delay and taking possible measures and remedies to reduce or remove the risks according to the guidance of competent national authorities.

The success of the implementation of the data breach notification system requires the effects from both business organisations and competent national authorities. On one hand, business organisations shall learn the procedures of "notification of the personal data breach" system; notify competent national authorities of data breach without undue delay; and maintain a detailed list of personal data breach information,

---

[37] 'Implementing the Revised EU Electronic Communications Framework: Impact Assessment', Department for Business, Innovation and Skills (BIS), September 2010, available at http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10–1133-implementing-revised-electronic-communications-framework-impact.pdf (last visited on 6 December 2010), p 6.

[38] London Economics, *Study on the Economic Benefits of Privacy-Technologies (PETs): Final Report to The European Commission* (DG Justice, Freedom and Security), July 2010, p 74.

effects and remedial actions taken for the verification of compliance by the competent national authorities. On the other hand, competent national authorities shall provide sufficient guidelines and instructions, which, in the author's view, should include standard forms and modalities of the notification system as well as interpret "without undue delay" and provide a clear rule on the time-limit of personal data breach notification. The time limit of such notification shall be concerned not only the time limit that the provider is required to notify the personal data breach to the competent national authority in the first instance, but also the time period between notification to the competent national authority and notification to a subscriber or individual.

With regard to the enforcement of the personal data breach notification system within member states, it would be helpful that the strategy of the EU Comprehensive Approach 2010 could successfully build a common approach across the EU to remove the obstacle of the uncertainty of the timeframe of the personal data breach notification in the near future, so multinational business organisations would only have to deal with one set of rules. Business organisations shall be encouraged to adopt the self-regulatory enforcement initiatives such as the trustmarks and privacy seal programs to increase the efficiency of the enforcement of data-privacy protection.

After all, data-privacy protection legislative and technological measures shall strike a fair balance between the protection of the right to private life and the free movement of personal data.[39] For the consistent implementation of data-privacy protection within member states, the timeframe of the personal data breach notification is of great necessity to be clarified.

[39] Case C-518/07 *European Commission v. Germany*, European Court of Justice (Grand Chamber) 09 March 2010 [2010] 3 CMLR 3, paras 24 and 30.