การป้องกันและการจัดการข้อมูลความเป็นส่วนตัวและชื่อเสียง
The Protection and Management of Privacy and Reputation Data

พงศ์กานต์ คงศรี*
Pongkan Kongsee

บทคัดย่อ

ระบบการคุ้มครองข้อมูลหรือ EU Data Protection Directive (DPD) เป็นแนวปฏิบัติของสหภาพยุโรปที่บัญญัติขึ้นในปี พ. ศ. 2538 เพื่อปกป้องสิทธิส่วนบุคคลของพลเมืองของสหภาพยุโรปที่ได้รับการรับรองคุ้มครองสิทธิไว้ในมาตรา 8 ของอนุสัญญาของยุโรปว่าด้วยสิทธิมนุษยชน มีหลักการที่มุ่งสนับสนุนและปกป้องความเป็นส่วนตัวของผู้คนซึ่งสามารถแบ่งแยกข้อดีข้อเสียของระบบข้อมูลดังกล่าวได้ ในบทความนี้แสดงถึงเหตุผลบางประการถึงจุดประสงค์ของการปฏิรูประบบการคุ้มครองข้อมูล ที่มีแนวโน้มที่จะต้องปรับปรุงประสิทธิภาพของระบบให้สูงขึ้น ในขณะที่ยังมีข้อกังวลอยู่บ้างนอกเหนือจากความกังวลเกี่ยวกับการเปลี่ยนแปลงในระบบการปกป้องข้อมูลให้มีประสิทธิภาพดังที่ได้กล่าวมา แม้ว่าระบอบการคุ้มครองข้อมูลจะได้รับการยอมรับในแง่ของการสร้างความตระหนักถึงสิทธิในการปกป้องข้อมูล การปรับปรุงการปกป้องข้อมูลส่วนบุคคลในบางส่วน และเป็นแบบอย่างของการปฏิบัติในการปกป้องข้อมูลมาตรฐาน แต่ก็ไม่สามารถกล่าวได้ว่าได้บรรลุวัตถุประสงค์เพื่อปกป้องข้อมูลส่วนบุคคลของยุโรปได้ทั้งหมด เนื่องจากไม่ได้ผลในหลายส่วน เช่น ในแง่ของความเป็นส่วนตัวที่ลดลงและข้อมูลส่วนตัวเรื่องหนี้สิน นอกจากนี้ระบบการปกป้องข้อมูลเพื่อให้สอดคล้องกับความท้าทายใหม่ ๆ ในยุคดิจิทัลเป็นสิ่งจำเป็น ดังนั้น DPD ช่วยเพิ่มประสิทธิภาพในการปกป้องสิทธิส่วนบุคคลซึ่งเป็นสิ่งที่น่าสนใจ ดังนั้นโครงสร้างทางกฎหมายบางประการอาจมีการปรับปรุงดังที่กล่าวมาแล้วซึ่งโลกได้รับการเปลี่ยนไปสู่ยุคที่มีการรวบรวมข้อมูล การถ่ายโอนข้อมูลและอื่น ๆ ทุกนาทีทั่วโลกผ่านสื่อทางสังคมอินเทอร์เน็ต และการประมวลผลทางอินเตอร์เน็ตที่รวดเร็วนั้น ดังนั้นจึงเป็นสิ่งที่ชัดเจนว่าระบบการปกป้องข้อมูลในปัจจุบันซึ่งถูกใช้มายาวนาน 21 ปี อาจไม่ได้มีประสิทธิภาพเพียงพอที่จะจัดการกับการเปลี่ยนแปลงนี้ อย่างไรก็ตามเมื่อเทียบกับระบบการคุ้มครองข้อมูลในปัจจุบัน กับอนาคตภายหน้าซึ่งระบบการพัฒนาการคุ้มครองสิทธิที่มุ่งหวังจะนำไปสู่การปกป้องข้อมูลที่มีประสิทธิภาพยิ่งขึ้นและการปกป้องข้อมูลส่วนบุคคลที่ดียิ่งขึ้นนั้นให้กับบุคคลทั่วไปซึ่งสามารถคาดหวังและเป็นไปได้

คำสำคัญ : สิทธิส่วนบุคคล การคุ้มครองข้อมูล แนวปฏิบัติ

---

* อาจารย์ประจำ คณะนิติศาสตร์ มหาวิทยาลัยนเรศวร

* Lecturer, School of Law, Naresuan University

Abstract

Data protection regime or the EU Data Protection Directive (DPD) is the EU directive created in 1995, in order to protect privacy right of the EU citizen guaranteed in the Article 8 of the European Convention on Human Rights. There are principles aiming to support and protect people's privacy that can devide pros and cons of data regime. In this article, there are some reasons demonstrate about the purposed reform of the regime likely to improve its effectiveness. Whereas, there are still some concerns, apart from the concerns about the changes in purposed data protection regime mentioned about the effectiveness of the proposed data regulation. Although the data protection regime should be given the credit in term of raising awareness of data protection right, improving privacy protection in some areas and being a model for standard data protection practice, it cannot be said that it had completed its aim to protect European's privacy right due to the ineffectiveness in many areas such as in term of decease's privacy and information obligation. The new challenges in digital age is required for the data protection regime. Thus, whether the DPD will improve the privacy right protection's effectiveness is an interesting question, then, some structure of legal areas might be met improving. As mention above, the world has been changed to the era where the data has been collected, transferred and so on, every minute around the world via the internet, social media and cloud computing. Therefore, it is clear that the current 21 years old data protection regime may not be effective enough to deal with this change. Nevertheless, by comparison with the current data protection regime, the bright future where the proposed regime brings a better effective data and privacy protection to individuals can be expected.

Keywords: Privacy Right, Data Protection, Directive

Introduction

The European Commission set out plans for data protection reform across the European Union in order to make Europe "fit for the digital age" in 2012. Almost four years later, an agreement was reached on what the involved and how it will be enforced.

Unlike the General Data Protection Regulation (GDPR), the new EU framework applies to organizations in all member-states and has implication for business and individuals across Europe and beyond, Data protection regime or the EU Data Protection Directive (DPD) is the EU directive created in 1995, aiming to protect the privacy rights of the EU citizens from the personal data processing[1] such as collection, recording and adaption.[2] Nevertheless, since it has been 21 years from the time that the directive was introduced, the effectiveness of the directive is in doubt. As a result, the data protection reform is proposed by the European Commission in order to improve and fill the gaps of the DPD directive. Thus, it is interesting whether the new EU data protection regime will be able to provide a better privacy rights protection to the EU citizens. In this essay, the effectiveness of the data protection directive (DPD) will be examined, and the potential improvement in the data protection reform's effectiveness will be predicted.

General Data Protection Regulation (GDPR) is one of the key components of the reform in 2012. The digital future of Europe can only be built on trust differ from some issues EU Data Protection Directive that occur some point to figure out by following of this content.

The aim of the data protection regime

In order to protect privacy rights of the EU citizens guaranteed in Article 8 of the European Convention on Human Rights[3] , Article 1 of the directive states that the directive aims to protect the personal data which is the information directly or indirectly relate to identified person,[4] from the various types of the personal data processing. Therefore, all EU personal data such as photographs, medical histories, bank statement or even opinions about an individual are protected from any data processing such as collecting, recording and transmission, under the directive.

[1] Data Protection Directive article 1.

[2] Data Protection Directive article 2b.

[3] "Everyone has the right to respect for his private and family life, his home and his correspondence".

[4] Data Protection Directive article 1.

How does the directive protect privacy right?

In summary, from 34 articles contained in the directive, there are six main principles aiming to protect people's privacy.[5]

1) Notice: data subject has to be informed before the collection.[6]

2) Security: personal data must be saved in appropriate methods pursuant to the risks caused by the processing and the data's characteristic.[7]

3) Correction: an individual has to be given the right to access and correct any inaccuracies of their personal data.[8]

4) Consent: the consent of the data subject is required before any data processing.[9]

5) Purpose: the personal data has to be collected for particular and lawful purposes, and cannot be additionally processed in other way, contradicting to the original purposes.[10]

6) Enforcement: legal relief has to be provided via appropriate choices to the injured person.[11]

Does the data regime achieve its aim?

In order to evaluate the effectiveness of the directive, the praises and criticisms of the directive have to be examined.

The advantages of the directive

The directive is praised in five main areas.

1) The technology utilization

[5] Rebecca Herold et al., "European Union (Eu) Data Protection Directive of 1995 Frequently Asked Questions," http://www.informationshield.com/papers/EU%20Data%20Protection%20Directive%20FAQ.pdf, (last visited 30 April 2013).

[6]Margaret Rouse, "Eu Data Protection Directive (Directive 95/46/Ec)," http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive, (last visited 30 April 2013)

[7] Data Protection Directive article 17(1).

[8] Margaret Rouse, op. cit.

[9] Ibid.

[10] Rebecca Herold et al., op. cit.

[11] Ibid.

Through Article 17 of the directive which imposes the data controller to use the appropriate technical to shield personal data, indirect technology utilization for preventing privacy right can be seen in the directive.[12]

2) A good model for data protection practice

The directive is widely accepted, as a model for good practice standard for data protection, from many jurisdictions around the world.[13] Many countries such as Hong Kong, Chile and Canada used the directive as a model for their legislative reform.[14]

3) Raising awareness of data protection right.

According to a study conducted by Rambøll Management, the Italian retailers believe that the data protection regime has increased the data protection awareness.[15] It is likely that the fact that appropriate procedures are required before disclosing personal data will become more aware.[16]

4) Deterrent effect

By imposing sanction on the non-compliances and giving any EU people right to bring the claim of data protection infringement against non-compliance companies, the deterrent consequence can be produced. The example of the suits causing deterrent effect and increased companies' awareness can be seen in Sweden where the American Airlines was lost in Swedish Appellant Court under the claim that the Airline could not retain the passenger's personal information, without explicit consent from the passengers.[17] Another example was found in 1999 where Microsoft spent $60,000 in order to settle accusations filed by Spain that Microsoft failed to clearly disclose to the Spanish purchasers about what would happen to their personal data after the Windows registration.[18] As a result, the companies will be more

[12] Neil Robinson et al., "Review of the European Data Protection Directive," http://www.rand.org/pubs/technical_reports/TR710.html, (last visited 29 April 2016)

[13] Ibid.

[14] Ibid.

[15] Rambøll Management, "Economic Evaluation of the Data Protection Directive 9 5 / 4 6 / Ec," http://ec.europa.eu/justice/policies/privacy/docs/studies/economic_evaluation_en.pdf, (last visited 1 May 2013)

[16] Ibid.

[17] Rebecca Herold et al., op. cit.

[18] Ibid.

aware when they conduct personal data processing, and be deterred from omitting data protection actions.

5) Privacy right protection improvement

Owing to the directive implemented in national legislation, the privacy right was more protected. For instance, the UK pharmacy claimed that due to the restriction of data access enacted in the new legislation, which permits only the pharmacist to access every data, the personal privacy data is better protected.[19] The customs authorities in the UK also agreed that the legislation implementing the directive provided better safety measure to the individual privacy's rights.[20]

The disadvantages of the directive

Beside the mentioned advantages, there are many criticisms about the current directive.

1) Out of date

This is one of the two main reasons why the data protection reform has to be purposed. Since the current directive was introduced 21 years ago when the internet was used by less than 1% of EU citizens[21], it is criticized for being outdated, and cannot deal with the rapid technological advances and globalization such as social network, cloud computing and smartcards which bring new challenges for data protection and privacy right to this digital age.[22] For example, business community argued that the requirement of an adequate level of protection for transferring data to third countries is no longer necessary in the globalization age.[23] The distinguishing between EU countries and others was needless and unproductive.[24]

2) Lack of consistency of implementing

---

[19] Rambøll Management, op.cit.

[20] Ibid.

[21] European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses," http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, (last visited 1 May 2013).

[22] European Commission, "Why Do We Need an Eu Data Protection Reform?," http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf, (last visited 1 May 2013).

[23] Neil Robinson et al., op.cit.

[24] Ibid.

Another main reason of the need of data protection regime reform is the inconsistency in enforcement. As a result of different implementation of the directive in 27 EU member states, the divergence in enforcement and level of personal data protection occurred.[25] An example can be seen in the notification obligation under article 18 of the directive, which imposes an obligation to notify the national supervisory authority before performing specified data processing on the data controller where each EU member states has differently implemented their own rules and exemptions of notifying data processing.[26] Consequently, the rules and exception of notifying are different in each country leading to inconsistency, and higher expenses and amount of works for data controllers.[27]

3) The absence of post-mortem privacy protection

There is no context dealing with the personal data of the deceased person in the data protection directive.[28] Indeed, according to article 29 of data protection working party, the information of deceased individual is not deemed as personal data in the meaning of the directive rules.[29] This is also emphasized in the UK data protection act 1998 section 1(1) (e) which limits the meaning of personal data only to "data which relate to a living individual". As a result, this would contribute to a gap of law dealing with deceased's personal data. Moreover, it seems that the privacy and data protection rights of a dead person are not recognized and protected under EU law.

4) The ineffectiveness of the information obligation

In order to increase transparency in data processing, the information obligation is enacted in Articles 10 and 11 of the directive.[30] Under these Articles, certain information has to be provided to the data subject. As a result, privacy notices, privacy policies or consent

---

[25] European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses." http://europa.eu/rapid/press-release_IP-12-46_en.htm, (last visited 1 May 2013).

[26] Neil Robinson et al., op. cit.

[27] Ibid.

[28] Edina Harbinja, "Does the Eu Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives," SCRIPTed Journal of law, Technology & Society 10,1 (2013): 26.

[29] Ibid.

[30] Neil Robinson et al., op. cit.

notice is used as a main method to provide these information to the data subject.[31] However, in practice, this aim of the directive seems to be unsuccessful. The consumers found that data policies are not useful for them because the policies are written in legal terminology which is complicated and difficult to understand.[32] This is because the detailed descriptions of data processing activities, which are difficult to express in ordinary words, are required in some national laws.[33] Consequently, the data policies are usually ignored or were not read by the data subject.[34] As a result, it is likely that the privacy policies are used to meet the legal requirement imposed by the directive rather than increasing the transparency which is the main purpose of the provisions.[35]

5) The ineffectiveness of the notification obligation

Beside the lack of consistency in implementation of this obligation in each EU countries, the notification obligation is criticized in its purpose.[36] The notification as a register process was perceived as a tool for indirectly collecting tax to fund the government in some states.[37] In addition, the benefit of the register of data controller to the consumer is not clear.[38] Thus, it seems that the register is only helpful no more than as a criteria to determine due diligence conducting for lawyers.[39]

6) The ineffectiveness of the remedies and sanctions

Although imposing sanctions on the non-compliance companies is a good step to deter data protection infringement, this method is still criticized about its effectiveness in reality. Firstly, it is difficult for the injured person to ask for compensation because the damages may not immediately occur when the data is leaked although such privacy and security risk are caused by the data controller's negligence.[40] For instance, in term of confidential data such

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] Ibid.

[40] Neil Robinson et al., op. cit.

as credit card information, as long as that information is not used, the damages will not occur.[41] As a result, it is very hard for the data subject to get any compensation even the privacy risk of the data subject has already occurred because any damage has not been existed. Furthermore, some damages such as the loss of time for obtaining a new safety data, such as a new credit card, are difficult to quantify.[42] Finally, many damages and compensations are too small and not worthy for an individual to spend time and effort to bother it.[43]As a result, it is unlikely that the sanction can effectively deter the personal data infringements.

7) Conflict between other non- EU membership national law and EU law

In practice, data controllers may face the situation where there are differences between two legal frameworks without any clear answer whether which rule prevails.[44] An example is in SWIFT case, where the data is not allowed to be revealed under EU law whereas it is mandatory to reveal such data under the US law.[45] As a result, the data controller would be end up in liability whatever they decided.[46] Consequently, this may lead to serious confusions and deter foreign investment.

Although the data protection regime should be given the credit in term of raising awareness of data protection rights, improving privacy protection in some areas and being a model for standard data protection practice, it cannot be said that it had completed its aim to protect European's privacy right due to the ineffectiveness in many areas such as in term of decease's privacy and personal data right, and information obligation. Moreover, if consider the fact that the ways of data processing have been dramatically changed from last 21 years due to the technological development and globalization as well as the lack of harmonization between each EU member countries, it is undoubted that a new rule which can deal with these new challenges better than this directive is needed.[47]

---

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses." http://europa.eu/rapid/press-release_IP-12-46_en.htm, (last visited 1 May 2013).

2. EU , Information Commissioner's Office and UK legal's view.

Is the proposed reform of the regime likely to improve its effectiveness?

As mentioned before that the reform of the data protection regime in order to meet with the new challenges in digital age is required, thus, whether the new rule will improve the privacy right protection's effectiveness is an interesting question. To answer this question, the prediction about the changes existing in the purposed data protection reform will be discussed below.

1) Increased consistency

According to the research conducted in June 2011, 9 of 10 of EU citizens want the data protection rights to be the same in every member states.[48] In order to achieve this requirement, the EU commission proposed to change type of instrument of the regime from a Directive to a Regulation.[49] Unlike the directive which provides flexibility to each member state to implement the directive on their national law, the regulation will be directly enforceable in each member states without any implementation.[50] As a result, the discrepancies caused by room for interpretation of each country's legislator in the directive would be avoided, and the inconsistency among the EU states will be increased.[51]

Nevertheless, there is a concern about this change. The UK government and the Information Commissioner's Office (ICO) argued that creating an inflexible rule without concern about culture and legal system differences of each state may cause serious risks.[52] The ICO

[48] Special Eurobarometer 359 'Attitudes on Data Protection and Electronic Identity in the European Union, June 2011' cited in European Commission, "Why Do We Need an Eu Data Protection Reform?" https://publications.europa.eu/en/publication-detail/-/publication/de4 9 b2 7 8 - bd0 a-4 6 c7 - 9 a3 5 - 95a8ddb83f5e, (last visited 1 May 2013)

[49] Slaughter and May, "The New Eu Data Protection Regulation Revolution or Evolution?," http://www.slaughterandmay.com/media/1844766/the-new-eu-data-protection-regulation-revolution-or-evolution.pdf, (last visited 1 May 2013)

[50] EURORDIS, "Questions & Answers on the Revision of the Personal Data Protection Directive: Processing and Free Movement of Data," http://www.eurordis.org/sites/default/files/personal-data-protection-directive-qa.pdf, (last visited 2 May 2013)

[51] EURORDIS, op. cit.

[52] Slaughter and May, op.cit.

also recommended that some flexibility depend on different legal tradition in each country should be allowed.[53]

2) More protection measures

The proposed data protection will contain many protecting provisions imposing on data controllers as well as data processor to safeguard European privacy rights In fact, this is the first time that the data processor has direct obligations to comply with the regime.[54]

(a) Notification obligation

Under the new regime, the data controllers such as companies and organization would have an obligation to inform the national supervisory authority of any serious personal data infringements, without any delay, within 24 hours if possible.[55] Statistics revealed that the number of data breaches is lower in the states which require fast notification.[56] Therefore, according to this measure, by providing fast action to tackle the infringement, it is expected that the number of data breaches will be decreased.[57] As a result, the trust and confidence of consumers in online business will also increase.[58]

However, the 24 hours which is the deadline in this provision is criticized that it is too short and unrealistic.[59] As a result, it would be very hard to comply in practice.[60] Nonetheless,

---

[53] Information Commissioner's Office, "Data Protection Reform Latest Views from the ICO," http://www.ico.org.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/data_protection_reform_latest_views_from_the_ico.ashx, (last visited 2 May 2013)

[54] TaylorWessing, "Fundamental Overhaul of Eu Data Protection Regime Unveiled," http://www.taylorwessing.com/globaldatahub/article_eu_dp_regulation.html, (last visited 2 May 2013)

[55] European Commission, op.cit.

[56] European Commission, "The Data Protection Reform - One Year On," http://europa.eu/rapid/press-release_MEMO-13-39_en.htm, (last visited 30 April 2013)

[57] Ibid.

[58] Ibid.

[59] B.J.A. Schellekens, "The European Data Protection Reform in the Light of Cloud Computing" (Master of Laws, School of Law, Tilburg University, 2013).

[60] Ibid.

in response to this criticism, Jan-Philipp Albreacht, a rapporteur for the European Parliament's Civil Liberties has proposed to extend this deadline from 24 hours to 72 hours.[61]

(b) Penalty increasing

Unlike the current regime where the monetary penalties are different across the EU, for example the non-compliance can be fined up to 500,000 for serious violation of the DPA in the UK, the regulation would provide more consistency of the level of punishment among the EU, regarding to the seriousness of the violation.[62]

For example, the amount of fine can be varied depend on the seriousness of breach from up to 250,000 Euros or up to 0.5% of yearly worldwide turnover for minor offence to up to 1million Euros or up to 2% of yearly worldwide turnover for serious offence.[63] Moreover, the proposed penalty could be enforced to both data controllers and data processors.[64] As a result, the high amount of fine may contribute to a deterrent effect for big companies.

Nonetheless, the ICO criticized this sanction regulation that firstly, the calculating the amount of fine from the percentage of turnover would be almost impossible in reality.[65] Secondly, the word "up to" may lead to modest fines instead of punitive fines.[66]

(c) Border scope of implication

On the contrary to the directive which only applies to the non-EU institutions which use equipment in the European nations for their data processing, the purposed data protection rule will wider apply to the institutions that offer goods and services to people in the EU or

[61] Out-Law, "Consent from 'Pre-Ticked Boxes' Should Generally Not Be Valid under New Eu Data Protection Regime, Says Mep," http://www.out-law.com/en/articles/2013/january/consent-from-pre-ticked-boxes-should-generally-not-be-valid-under-new-eu-data-protection-regime-says-mep/, (last visited 2 May 2013)

[62] McClure Naismith, "Proposed Changes to the Eu Data Protection Regime: What You Need to Know,"http://www.mcclurenaismith.com/assets/publications/ebulletins/DP%20Regulation%20Article%20template.pdf, (last visited 2 May 2013)

[63] Ibid.

[64] Ibid.

[65] Information Commissioner's Office, op.cit.

[66] Slaughter and May, op.cit.

monitor the European manners although the bases of such institutions are outside the EU.[67] As a result, the big companies like Google, Microsoft and Facebook would be in the implication scope of this new regime.[68] Thus, it can be seen that the scope of implication in the purposed regulation is wider than in the directive. Consequently, this would bring benefit to the EU consumers in term of wider protection.

Nevertheless, there is a concern that this measure would create a big obstacle for global business to run their business in the EU.[69] Moreover, it is doubted that how, in reality, the regulation can be enforced on the companies outside of Europe.[70]

(d) Data processors' obligations

As previously mentioned, while the current rule impose obligations only on data controllers, the purposed regime will be applied to both data controllers and data processors.[71] For instance, under the proposed rule, the data processors will have obligations on documentation keeping, data officer appointment and monetary penalty where there has been a violation.[72]

(e) Convenience on inform breaches

Under the new regime, EU citizen can inform their cases to the national data protection authority in their home country despite the fact that their personal data processing is performed outside their home country or even outside the EU.[73] As a result, this would

---

[67] McClure Naismith, " European Union: Proposed Changes to the Eu Data Protection Regime: What You Need to Know." http://www.mondaq.com/uk/x/178122/Privacy/Proposed+Changes+To+The+EU+Data+Protection+Regime+What+You+Need, (last visited 1 May 2013).

[68] Ibid.

[69] Simply Security, "Eu Proposes Data Protection Overhaul; Criticism Ensues," http://www.simplysecurity.com/2012/02/03/eu-proposes-data-protection-overhaul-criticism-ensues/, (last visited 29 April 2013)

[70] Slaughter and May, op.cit.

[71] Ibid.

[72] Ibid.

[73] EURORDIS, "Questions & Answers on the Revision of the Personal Data Protection Directive: Processing and Free Movement of Data."

encourage people to inform cases more than in the current regime because of the convenience of breaches notification.

3) Increase data subject's control and manage power on their personal data

In order to give an individual more control power on their personal data, the change in consent giving and new inventions, such as the right to data portability and the right to be forgotten are provided in the purposed data protection regulation.

(a) Explicit consent

Under the purposed regulation, the consent to data collection has to be explicitly given.[74] Thus, by this rule, the data controllers will not be able to assume that the consent has been given via implied consent techniques such as pre-ticked boxes or other default tools, which require the individuals to modify the content for objecting the data processing.[75] In addition, under this regulation, the consent would be invalid if there is a substantial imbalance power between the data controllers and the individuals, such as between employers and employees, and between data controllers and children who are under 13 years old unless parental consent is obtained.[76] Therefore, according to the purposed regulation, it can be predicted that people will be more confident that their personal data will not be processed, without their express permission.

(b) Right to data portability

The right to data portability is a new invention of data protection right created by the new regime. Under this new right, people will be able to obtain a duplication of their data from their current service provider for transferring it to another service provider if the data is collected in a commonly used format.[77] For example, the user can ask for their data from Facebook to transfer to Google Plus.[78] Consequently, it will prevent the data subjects from being locked in to one unsatisfied service provider as well as increase competition among the

[74] Slaughter and May, op. cit.

[75] Out-Law, op. cit.

[76] Slaughter and May, op.cit.

[77]Simply Security, "Eu Proposes Data Protection Overhaul; Criticism Ensues." https://blog.trendmicro.com/eu-proposes-data-protection-overhaul-criticism-ensues-2/, (last visited 1 May 2013)

[78] B.J.A. Schellekens, op. cit.

service providers.[79] In conclusion, by this new right, the data subject will be empowered to control and manage their personal data since they can freely change their service provider for better service and security.[80]

However, there are three main criticisms about this right. Firstly, it is concerned that this right would not be effective in practice because there is no requirement under the proposed regime that the data has to be processed in commonly used format.[81] As a result, the data controller may attempt to avoid this obligation by not using commonly formats.[82] Furthermore, some argued that this right would help identity theft to be easy to commit because the personal data will be easily obtained by a few click downloading.[83] Consequently, it would lead to an adverse effect of the aim of the regime, which is the privacy and data protection. Finally, the service providers have to spend a high cost for creating a system to import and export data.[84] As a result, it is likely that this cost will be passed on to the ultimate consumers.[85]

(c) Right to be forgotten

This is another new right introduced in the purposed data protection regime. The new right will oblige the data subjects to manage and control their personal data risk by providing individuals the right to ask the organization to delete their data if there is no legitimate reasons to keep it[86].Moreover, if the data controller had published that information to third parties, the data controllers also have a duty to inform the third parties to delete any links or replication of that personal data.[87] Hence, this right would be useful to the EU citizens who find that their information on the online world would lead to privacy risks, for instance, people would not recognize that there could be a risk caused by revealing their personal data when

[79] Slaughter and May, op. cit.

[80] Edina Harbinja, op.cit.

[81] Slaughter and May, op.cit.

[82] Ibid.

[83] B.J.A. Schellekens, op. cit.

[84] Ibid.

[85] Ibid.

[86] EURORDIS, op. cit.

[87] Edina Harbinja, op. cit.

they were young, and then they are concerned about it later when they grow up.[88] This right will help them to manage their data risks by erasing their mistakes.[89]

3. Information Commissioner's Office legal's view and other concerns.

Nevertheless, there are two main controversies about this right. The first criticism is the right to be forgotten will conflict with the freedom of expression.[90] There are concerns that by allowing people to delete information about them even it is true and legitimate, the freedom of expression would be interfered.[91] Moreover, this would be exacerbated because the right can also be enforced to the intermediaries such as search engines like Google, who merely provide the link to that information, to delete that link.[92] However, this criticism might be overestimated since there are some exceptions provided in the purposed regulation that the data controllers are allowed to retain the data for exercising freedom of expression, for interest of public health and for the reasons of historical, statistical and scientific study.[93] Nevertheless, this exemption is still being criticized that it is not appropriate to allow data controllers to decide whether the data in dispute is subject to freedom of expression right since it is concerned that the data controller would not be able to produce the right decisions.[94]

Another criticism supported by the ICO is the right to be forgotten would not be enforceable in reality.[95] Marisa Jimenez, a Google representative, also criticized that the enforcement of this right is difficult in practice, especially when third parties are related.[96] It would be impossible to completely delete any information on the internet where the data is

[88] European Commission, "The Data Protection Reform - One Year On." http://europa.eu/rapid/press-release_MEMO-13-39_en.htm, (last visited 1 May 2013)

[89] Ibid.

[90] Slaughter and May, op. cit.

[91] Peter Fleischer, "The Right to Be Forgotten, or How to Edit Your History," http://peterfleischer.blogspot.co.uk/2012/01/right-to-be-forgotten-or-how-to-edit.html, (last visited 3 May 2013)

[92] Ibid.

[93] B.J.A. Schellekens, op. cit.

[94] Ibid.

[95] Information Commissioner's Office, op. cit.

[96] Simply Security, op.cit.

spread rapidly nowadays, especially where the data controllers does not locate in the EU countries.[97]

Other concerns

Apart from the concerns about the changes in purposed data protection regime mentioned above, there are other two concerns about the effectiveness of the purposed data regulation.

(1) Unclear draft

There are many complainings about the unclear meaning of words in the drafted regulation draft. For example, Marisa Jimenez said that the draft is very ambiguous, and could lead to misunderstanding and discrepancies in interpretation among the readers.[98] Furthermore, the ICO pointed out that the definition of personal data needs to be clarified in order to make the scope of law be clearer.[99] Moreover, a clarification of the compatible processing definition relating to sensitive personal data is asked by EURORDIS.[100] Thus, it can be seen that some area of the purposed regime needed to be more clarified in order to avoid the misunderstanding and discrepancies which will affect the effectiveness of the purposed regulation in the future.

(2) The absence of post-mortem privacy protection

Similar with the directive, the deceased data protection is still ignored by the EU Commission in the regulation. The definition of personal data in the proposed regulation is limited to living person only.[101] Moreover, dead people are excluded from the meaning of data subject in the revised version of the regulation prepared by the Council of European Union.[102] As a result of this absence, if people want to exercise the right to be forgotten under the purposed regime, they have to do it while they are still alive because this new data protection regime would not protect the deceased personal data, and it would not recognize

---

[97] Mike Masnick, "Europeans Continue to Push for 'Right to Be Forgotten'; Claim Americans 'Fetishize' Free Speech," http://www.techdirt.com/articles/20110204/00145312961/europeans-continue-to-push-right-to-be-forgotten-claim-americans-fetishize-free-speech.shtml, (last visited 3 May 2013)

[98] Simply Security, op.cit.

[99] Information Commissioner's Office, op. cit.

[100] EURORDIS, op. cit.

[101] Edina Harbinja, op. cit.

[102] Edina Harbinja, op. cit.

their wish to be forgotten in the testament.[103] However, it is still in question whether the absence of the deceased personal data protection will lead to a serious consequence, since the value of departed personal data for businesses is suspected.[104] Hence, further research in this area is needed.[105]

4. Conclusion

Due to technological development and globalization, the world has been changed to the era where the data has been collected, transferred and so on, every minute around the world via the internet, social media and cloud computing. Therefore, it is clear that the current 21 years old data protection regime may not be effective enough to deal with this changes. As a result, there is no doubt that the purposed data protection reform is welcomed in order to meet this need. Although, as of May, GDPR has now come into force. Organizations of all sizes have found themselves it to some extent, by users who did not provide consent for their data to be used when offered the chance to opt in. Analysts at Forrester say many companies have reported a decrease of between 25 percent and 40 percent of their addressable market for emails and other forms of contact. As a result, many companies find themselves having to think about new methods of attracting consumers and generating revenue. Analyst Gartner has suggested that some companies may have to rethink their data center strategy as a result of legislation such as GDPR that is different from DPD, all mentioned above have pros and cons to analyst.

However, the promising attempts to provide better privacy right protection to the Europeans can be seen in the purposed regime via the changes and innovation of new rights. For instance, the responsibility and accountability of the data controller as well as the data processors will be increased by many obligations and liability imposed in the purposed regulation. The new right such as the right to data portability and the right to be forgotten have been introduced in order to provide controlling data power to the data subjects. Moreover, the harmonization of the rules has been reinforced through the change from directive to regulation. However, there is a fatal point which should not be ignored. Many

[103] Ibid.

[104] Ibid.

[105] Ibid.

provisions in the purposed regime are seriously suspected about how they can be effectively enforced in practice, especially in term of the right to be forgotten. As a result, it is still a big question for the EU Commission to answer.

Nevertheless, by comparison with the current data protection regime, the bright future where the purposed regime brings a better effective data and privacy protection to individuals can be expected.

Bibliography

European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses." http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, (last visited 1 May 2013).

European Commission, "The Data Protection Reform - One Year On." http://europa.eu/rapid/press-release_MEMO-13-39_en.htm, (last visited 30 April 2013).

European Commission, "Why Do We Need an Eu Data Protection Reform?" http://ec.europa.eu/justice/dataprotection/document/review2012/factsheets/1_en.pdf, (last visited 1 May 2013).

EURORDIS, "Questions & Answers on the Revision of the Personal Data Protection Directive: Processing and Free Movement of Data." http://www.eurordis.org/sites/default/files/personal-data-protection-directive-qa.pdf, (last visited 2 May 2013).

Fleischer, Peter. "The Right to Be Forgotten, or How to Edit Your History." http://peterfleischer.blogspot.co.uk/2012/01/right-to-be-forgotten-or-how-to-edit.html, (last visited 3 May 2013).

Harbinja, Edina, "Does the Eu Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives." SCRIPTed Journal of law, Technology & Society 10,1 (2013).

Herold, Rebecca, CISSP, CISM, CISA, and FLMI. "European Union (Eu) Data Protection Directive of 1995 Frequently Asked Questions." http://www.informationshield.com/papers/EU%20Data%20Protection%20Directive%20FAQ.pdf, (last visited 30 April 2013).

Information Commissioner's Office, "Data Protection Reform Latest Views from the Ico." http://www.ico.org.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/data_protection_reform_latest_views_from_the_ico.ashx, (last visited 2 May 2013).

Margaret Rouse, "Eu Data Protection Directive (Directive 95/46/Ec)." http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive, (last visited 30 April 2013).

Masnick, Mike, "Europeans Continue to Push for 'Right to Be Forgotten'; Claim Americans 'Fetishize' Free Speech." http://www.techdirt.com/articles/20110204/00145312961/

europeans-continue-to-push-right-to-be-forgotten-claim-americans-fetishize-free-speech.shtml, (last visited 2 May 2013).

Naismith, McClure, "Proposed Changes to the Eu Data Protection Regime: What You Need to Know." http://www.mcclurenaismith.com/assets/publications/ebulletins/DP%20Regulation%20Article%20template.pdf, (last visited 2 May 2013).

Out-Law, "Consent from 'Pre-Ticked Boxes' Should Generally Not Be Valid under New Eu Data Protection Regime, Says Mep." http://www.out-law.com/en/articles/2013/january/consent-from-pre-ticked-boxes-should-generally-not-be-valid-under-new-eu-data-protection-regime-says-mep/, (last visited 2 May 2013).

Rambøll Management, "Economic Evaluation of the Data Protection Directive 95/46/Ec." http://ec.europa.eu/justice/policies/privacy/docs/studies/economic_evaluation_en.pdf, (last visited 1 May 2013).

Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri, "Review of the European Data Protection Directive."http://www.rand.org/pubs/technical_reports/TR710.html, (last visited 29 April 2016).

Schellekens, B.J.A, The European Data Protection Reform in the Light of Cloud Computing (Master of Laws, School of Law,Tilburg University, 2013).

Simply Security, "Eu Proposes Data Protection Overhaul; Criticism Ensues." http://www.simplysecurity.com/2012/02/03/eu-proposes-data-protection-overhaul-criticism-ensues/, (last visited 29 April 2013).

Slaughter and May, "The New Eu Data Protection Regulation Revolution or Evolution?" http://www.slaughterandmay.com/media/1844766/the-new-eu-data-protection-regulation-revolution-or-evolution.pdf, (last visited 2 May 2013).

TaylorWessing, "Fundamental Overhaul of Eu Data Protection Regime Unveiled." http://www.taylorwessing.com/, (last visited 2 May 2013).