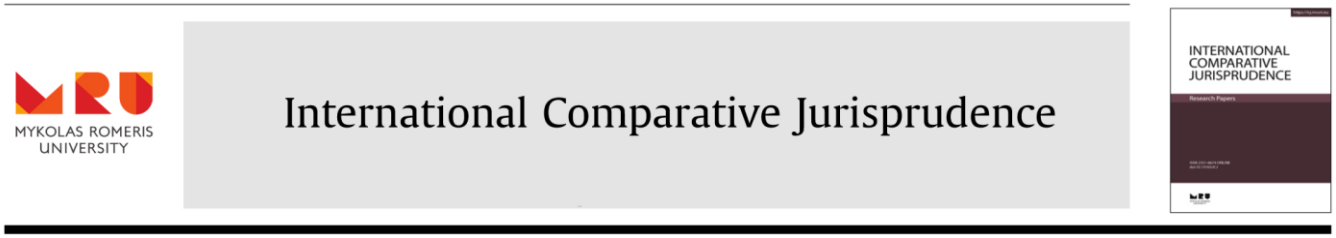
International Comparative Jurisprudence 2018 Volume 4 Issue 2
ISSN 2351-6674 (online) DOI: http://dx.doi.org/10.13165/j.icj.2018.12.003



DATA PROTECTION POST-MORTEM

Asta Tūbaitė-Stalauskienė[1]

The Court of Justice of the European Union, Luxembourg
E-mail: Asta.Tubaite-Stalauskiene@curia.europa.eu

Received: 24 September 2018; accepted: 27 November 2018
DOI: http://dx.doi.org/10.13165/j.icj.2018.12.003

Abstract. This article discusses the notion of the post-mortem privacy of the deceased Internet user and focuses on the post-mortem privacy protection aspects in common and continental law systems. It analyses the post-mortem privacy regulation by the legal framework and by contracts, provides information about existing measures to protect Internet user's data post-mortem and discusses the possibilities to improve them.

Keywords: Data protection, Regulation (EU) 2016/679, Directive 95/46/EC

Introduction

In most of the countries where data protection rights have been enacted, the concept of personal data is limited to information associated with living persons. Nevertheless, one's uniqueness, or unique personality if you like, does not vanish with death (Szekely, 2017). According to statistics provided by Internet World Stats (Internet World Stats, 2018), there are about four billion Internet users in the world. Every day, people send billions of emails and write millions of blog posts. For example, Facebook has over one billion users and more than 10 000 of them die every day (Hiscock, 2018). In the digital age, the digital data that an Internet user leaves behind after his/her demise has led to new challenges for the legal system (Buitelaar, 2017). In most countries, the issue of the extension of data privacy beyond death has remained unresolved, and at best constitutes a grey zone within the law (Szekely, 2017).

The main objectives of this article are: (1.) to define post-mortem privacy, (2.) to analyse post-mortem privacy regulation and (3.) to discuss prospects for post-mortem privacy protection. The research was carried out applying comparative, systematic and analytical methods.

1. Defining post-mortem privacy

Post-mortem privacy is an abstract notion and should be interpreted as a right of the person to preserve and control what becomes of his reputation, dignity, integrity, secrets or memory after death (Edwards & Harbinja, 2013). Privacy can be conceived as limited access to the self; privacy as secrecy; privacy as personhood or privacy as intimacy (Solove, 2002). The need to protect post-mortem privacy is necessary because of the growth of digital assets, which often have a personal and intimate nature, and also happen to be voluminous, shareable, hard to delete and categorise under current legal norms (Edwards & Harbinja, 2013). One's digital assets can be defined on a broad basis, including social network profiles (on platforms such as Facebook, Twitter, Google+, LinkedIn); emails, tweets, databases; digitized text, image, music or sound (e.g., pictures, films, e-books); passwords to accounts related to the provision of digital goods and services (e.g. eBay, Amazon, Netflix, YouTube); domain

[1] Lawyer-linguist at the Court of Justice of the European Union.

names (Edwards & Harbinja, 2013). In some cases, the material value dominates in these virtual assets (e.g. credits collected in online games, or domain names), while in other cases the values associated with the personality of the deceased are more important (e.g. the content of the deceased person's online communications); sometimes both elements are present (Szekely, 2017). The post-mortem privacy refers to different areas of law: property law, succession law, intellectual property law, etc. All these areas have a different legal attitude towards the dead, in addition to the differences between legal systems (Szekely, 2017).

1.1. Particular aspects of a common law system

In common law systems, the main principle has traditionally been *actio personalis moritur cum persona*[2]. This principle means that personal causes of an action die with the person (Edwards & Harbinja, 2013). In the case of a deceased person, the legal definitions of damage to good reputation become meaningless – in contrast with the deceased's economic rights, such as copyright or the right to own property, which the legal successors will inherit and continue to practise (Szekely, 2017). Nevertheless, common law is beginning to accept the protection of personality rights. The United Kingdom, one of the countries with a common law system and a member of the European Union, incorporated the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) into its legal system. One of the consequences that resulted from this can be seen in the way the British courts have ruled in cases related to the use of pictures of celebrities and others (including deceased persons): without actually attending the protection of personality rights beyond death, they limited the commercial or trademark-type marketing of the visual representation of persons (Szekely, 2017).

1.2. Particular aspects of a continental law system

By contrast, many states with a continental law system recognise the existence of personality rights and their persistence after death, for reasons related to the historical respect for notions of liberty, dignity and reputation, and especially of creators (Edwards & Harbinja, 2013). In Germany, the right to human dignity is regarded as the cornerstone of the entire legal system, one that gives rise to all the other human and personality rights. The German courts have declared in the cases Mephisto (1971, BVefGE 30, 173) and Marlene Dietrich (1999, BGH 1 ZR 49/97) that the inviolability of human dignity does not end with death, and that the state has to guarantee continued protection in this area (Szekely, 2017). However, countries of the civilian tradition treat the transmission of personality rights differently. For example, French law distinguishes between the economic and personal aspects of personality rights (a dualistic conception, as opposed to the German monistic position) and treats the latter as non-transmissible (Edwards & Harbinja, 2013).

2. Post-mortem privacy regulation

2.1. Regulation by legal framework

2.1.1. EU legislation

According to Article 2 of Directive 95/46/EC[3] "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". That means that Directive 96/46 applies only to living individuals. That directive conferred on Member States a greater or lesser discretion in the implementation of some of its provisions. In the case C-101/01 Lindqvist, the Court of Justice of the European Union decided that "measures taken by the Member States to ensure the protection of personal data must be consistent both with the

[2] This principle was established by the King's Bench Division of England and Wales High Court in the famous case of *Baker v. Bolton* (1808) 1 Camp. 439; 170 ER 1033.
[3] No longer in force.

provisions of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it" (Lindqvist, paragraph 99). Some EU Member States have used this possibility, and, as we will see below, their data protection laws offer some post-mortem data protection (Harbinja, 2017).

The Regulation (EU) 2016/679 (GDPR) is applicable from 25 May 2018. According to its Recital 27, "this Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons". That means that the GDPR gives each Member State the choice to extend the protection to dead people. The GDPR establishes the right to be forgotten. This right was recognised and developed by the Court of Justice of the European Union in the case C‑131/12 Google. Article 17 of the GDPR introduces the right to erasure (right to be forgotten). This right enables data subjects to request data controllers (e.g. Google) to delete their data if retained without legitimate grounds. The GDPR does not introduce something fundamentally new. Directive 95/46 already included the right to be forgotten in Article 12(b) and Article 14(1)(a). Under Directive 95/46, data subjects could ask a court to order the data controller to cease data processing when it caused damage. Under the GDPR, data subjects can bypass court intervention and set the issue directly with the data controller (including any search engine) (De la Tour & Gauberti, 2017). According to Article 4 of the GDPR a data subject is defined as "an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". As the definition is broad, it is unclear whether such a definition could encompass dead persons. As mentioned before, in its Recital 27, the GDPR gives each Member State a choice to extend this definition to dead people, or not.

2.1.2. National legislation in EU Member States

Some EU Member States chose to include the deceased in the definition of natural persons and to apply provisions of the GDPR to them. Other Member States exclude the deceased.

For example, under Article 3(2) of the UK Data Protection Act 2018 personal data "means any information relating to an identified or identifiable living individual". The Estonian Personal Data Protection Act gives the data subject the freedom to decide the fate of their personal data in advance of death. In Article 12(6) it states, that "the consent of a data subject shall remain valid during the lifetime of the data subject and for thirty years after the death of the data subject unless the data subject has decided otherwise". According to Article 13(1) "after the death of a data subject, processing personal data relating to the data subject is permitted only with the written consent of the successor, spouse, descendant or ascendant, brother or sister of the data subject, except if consent is not required for the processing of the personal data or if thirty years have passed from the death of the data subject". Under Article 28(3)(3) of the Bulgarian Law for the Protection of Personal Data "in event of death of the natural person his/her rights shall be exercised by his/her heirs". That means that the subject's rights of access to personal data are extended to the heirs of the data subject.

One section of French Law n°78-17 of 16 January 1978 relating to IT, databases and freedoms (*Loi informatique et libertés*) is dedicated to deceased people. This Law was amended by the Digital Republic Act (*Loi n°2016-1321 pour une République numérique*) of 7 October 2016 and the Law for Protection of Personal Data (*Loi n° 2018-493 relative à la protection des données personnelles*) of 20 June 2018, to conform to the new rules resulting from the new GDPR.

The amended *Loi informatique et libertés* allows natural persons to control their data on the internet. Under Article 40 of this law, natural persons have the right to request the data controller to rectify, complete, update, lock or delete his/her personal data if this data is incomplete, outdated, or if there are no legal grounds to collect, use or communicate such data. Article 40-1 of the *Loi informatique et libertés* states that any person can set some guidelines relating to the preservation, withdrawal and communication of his/her personal data after his/her death. This law allows people to give instructions as to what should be done with his/her online data after his/her death. People can choose in advance to delete, conserve or communicate their data after death. It also gives rights to the heirs to act even when the deceased person has left no instructions. Under Part III of Article 40-1 the heirs of a deceased person can ask to stop processing the deceased person's data, to remove, modify or update such data (De la Tour & Gauberti, 2017). Under Article 79(2) of the GDPR, a data controller or processor can be sued in the EU Member State where the data controller or processor has an establishment. If the data controller or processor has an establishment in France (e.g. Google France), not only citizens of France, but also citizens of other EU Member States can sue such a data controller or processor in France in order to enforce their right to be forgotten, or that of their close deceased. This is an excellent opportunity for all data subjects because they can be protected by French law, which is favourable to data protection, in particular in relation to the right of dead people to be forgotten.

2.1.3. US legislation

In the US there is an evident universal principle according to which freedom of speech is more important than a person's right to control their own personal data. However, US states have been pioneers in legislating the transmission of digital assets on death and post-mortem privacy. As the rules and procedures in this area were non-consistent from state to state, it was necessary to harmonise the legislation within the US. In July 2012 the US Uniform Law Commission (ULC), also known as the National Conference of Commissioners on Uniform State Laws (NCCUSL), which proposes to states a well-drafted legislation that brings clarity and stability to critical areas of state statutory law, appointed the Committee to draft the Uniform Fiduciary Access to Digital Assets Act (UFADAA). The final draft was adopted in December 2015. The UFADAA enables Internet users to plan the management of their digital assets so that they can plan the management of their tangible property. The UFADAA makes users' online instructions legally enforceable. It grants priority to service providers' terms and conditions and users' choices over any other provisions, including wills (Harbinja, 2017).

2.2. Regulation by contracts

The fate of virtual legacies is basically in the hands of the service providers. This is so because the price users pay for the seemingly free services is the sale and marketing of their data and personality, which service providers determine from the position of unilateral power (formally through a contract to which users agreed to by signing it) (Szekely, 2017). Many digital assets are controlled, both practically and legally, by digital intermediaries – companies such as Google, Facebook, eBay, Twitter, etc. Access to social network profiles is restricted to those who signed the contract with a social network platform. Before setting up a profile or an account, a user has to sign an agreement known as terms and conditions. This agreement is a legal contract. A user signs this contract by clicking an "I accept" button. Usually, he/she should do it after he/she has read the terms and conditions set out by the platform. Research shows that most users either do not read or do not understand the privacy policies and do not have any effective ability either to renegotiate the terms or, in many cases, to go to a competitor platform due to the operation of network effect within an oligopolistic market (Edwards & Harbinja, 2013). What happens to digital assets when a user dies and the subscriber contract terminates? Intermediary contracts often do not contain any explicit rules on what happens to assets stored or created on their platforms upon death. Even if rules exist, there is a potential conflict on death between the rules of contract and the rules of succession, as well as between the wishes of the deceased and the wishes of the survivors (Edwards & Harbinja, 2013).

2.2.1. Facebook code solutions for post-mortem privacy

For example, Facebook gives a user the possibility to inform in advance whether they would like to have their account memorialised or permanently deleted from Facebook. Memorialised accounts are a place where friends and family can share memories after a person has passed away. Memorialised accounts have the following key features: "the word *Remembering* is shown next to the person's name on their profile, depending on the privacy settings of the account; friends can share memories on the memorialised timeline; content the person shared (e.g. photos, posts) stays on Facebook, and is visible to the audience it was shared with; memorialised profiles do not appear in public spaces such as in suggestions for People You May Know, ads or birthday reminders; no one can log into a memorialised account; memorialised accounts that do not have a legacy contact cannot be changed. A legacy contact is someone a user chooses to look after his/her account if it is memorialised. Once the account is memorialised, a legacy contact will have the option to write a post for a deceased person profile (e.g. to share a final message on your behalf). The legacy contact can also respond to new friend requests, update profile picture and cover photo, and request the removal of the deceased person account. A user has the option to allow a legacy contact to download a copy of what he/she has shared on Facebook. However, a legacy contact is not allowed to log into an account, remove or change past posts, photos and other things shared on the timeline, read private messages or remove friends. A user must be 18 or older to select a legacy contact.

However, this could lead to conflicts between the interests of heirs and those of a friend designated as a legal contact, enabled to download the deceased's digital content. For instance, if the legacy contact acquires this content with the permission of the user, this content will be exempt from the provisions of the intestacy laws. In that way, Facebook protects the deceased's choice made before death. However, all this needs to be clarified (Harbinja, 2017).

2.2.2. Google code solutions for the post-mortem privacy

Google has recently proposed a new solution for post-mortem transmission of emails and other assets. Inactive Account Manager is a possibility for users to share parts of their account data or inform someone if they have been inactive for a certain period. The service provider looks at several signals to determine whether a user is still using his/her Google Account. These include last sign-ins, recent activity in My Activity, usage of Gmail (e.g. the Gmail app on your phone), and Android check-ins. The user can nominate up to 10 trusted contacts. If a user does not sign into any Google service for the time chosen by him/her (3-18 months), the trusted contacts will receive a pre-written email with the user's wishes for his/her account. The trusted contacts have to prove their identity to be entitled to download data the user left them. A user can choose to give his/her trusted persons full access to his/her Google account, including email and chat histories, and can allow downloading specific data. Google also allows the deletion of an account and all its data.

A fundamental problem with Inactive Account Manager is verification of trusted contacts. According to the mandatory procedure, a text message is sent to trusted contacts. The user can also choose to notify his/her timeout by email. A phone number is not an official way to prove identity. Furthermore, people change their mobile phone providers and numbers, and some of them may never be notified (Harbinja, 2017).

Very often people have firmer ties with friends online than with their heirs offline. Their decision to transfer the content to trusted contacts (friends) could lead to conflicts between the interests of the deceased person, which he/she expressed in his/her digital will, family (as his/her heirs) and friends (Harbinja, 2017).

2.2.3. Code solutions for post-mortem privacy of other service providers

Twitter has no equivalent to a legacy contact or a way to plan for your online data after your death. If the Twitter user dies, the service provider deletes an account if a person acting on behalf of the estate or an immediate family member of the deceased can provide a copy of his/her ID, and a copy of the death certificate.

LinkedIn, Snapchat, Tumblr offer no type of death planning, though all offer some form of account management for the deceased. LinkedIn will let a verified family member have an account removed. Snapchat deletes the account of a deceased person at the request of a family member (with a death certificate). Tumblr also lets a family member request to delete an account. In some sites (e.g. Yahoo) immediate family members can use standard protocols to request the deletion of a deceased person's account.

3. Prospects for post-mortem privacy protection

Because of ongoing globalisation, it would be entirely natural to expect electronic communications service providers to be carrying out very similar policies in managing deceased persons' data (Szekely, 2017). For the moment we see the opposite: the digital assets and the post-mortem privacy of the deceased are controlled by different contracts with different electronic communications service providers, most of which are based in the United States (Edwards & Harbinja, 2013). Even if the US-based companies that dominate the various parts of the Web 2.0 markets in Europe have different policies in managing deceased persons' data, their recent technical solutions for the protection of post-mortem privacy (Google Inactive Account Manager, Facebook Legacy Contact) practically recognise and promote post-mortem privacy, giving further support to the concepts. These technical solutions respect autonomy and allow users much more control over what happens to their data on death. The developments in technology demonstrate that post-mortem privacy is becoming recognised more widely in the online environment. In the US, which has traditionally been more opposed to the concept of post-mortem privacy, post-mortem privacy has been recognised through the Uniform Fiduciary Access to Digital Assets Act. For the moment not all US states have introduced this act into their own legislation. This act is vital for the digital age and should be introduced by every state as soon as possible. The harmonised legal recognition of post-mortem privacy would oblige electronic communications service providers to set up similar tools, which allow users to choose what happens to their data upon death.

The effective legal framework of post-mortem privacy is needed in Europe. The new EU data protection legislation, the GDPR, does not apply to the data of deceased people, and only provides an option for Member States to recognise post-mortem privacy. As we have seen above, France has used this possibility, and now its data protection regulation is one of the most protective for the personal data of dead people. Even if for the moment different countries across Europe have different policies concerning data protection for the deceased, there is a hope that the larger part of them will follow in France's footsteps. In any case, a resident or national of an EU Member State can now take a look at the personal data protection rules in force in other Member States. Article 79(2) of the GDPR sets out that a data controller or processor can be sued in the EU Member State where the data controller or processor has an establishment. For example, Google France has an establishment in France. That means that citizens of other EU Member States can sue Google France in France in order to enforce the right to be forgotten of their close deceased (De la Tour & Gauberti, 2017). A person who wants to enforce the right to be forgotten can start legal proceedings in France. French law will apply because under the Article 82(6) of the GDPR the applicable law is that of the EU Member State whose courts the action was brought before. This is good news for data subjects since French law is favourable to data protection, especially concerning the right of deceased people to be forgotten (De la Tour & Gauberti, 2017).

As was mentioned before, most EU Member States have not extended the definitions of personal data and data subjects in their own laws. The European legislation in this field is not harmonised. The protection of post-mortem privacy is very sporadic and non-consistent. The best option and a real improvement would be the introduction of a harmonised legal mechanism in the European law. Digital assets are counterparts of offline assets and wealth. Therefore, it is time for EU legislators to give individuals the right to choose what happens to their digital assets and privacy upon death (Harbinja, 2017).

Conclusions

This article demonstrates that the concept of personal data is usually limited to information associated with living persons and that in most countries the issue of the extension of data privacy beyond death has remained unresolved or unclear. The post-mortem privacy is an abstract notion and should be interpreted as a right of the person to preserve and control what becomes of his/her reputation, dignity, integrity, secrets or memory after death (Edwards & Harbinja, 2013). Privacy is often perceived as a group of rights, which are personal. According to the common law legal system, personality rights die with the person. By contrast, according to the continental law legal system, these rights persist after death. The Regulation (EU) 2016/679 does not apply to the personal data of deceased persons, but gives each Member State the possibility to extend the protection of personal data to dead people. France used this possibility and now its data protection law, *Loi informatique et libertés*, is one of the most protective for the personal data of dead people. But most EU Member States have not used this possibility and have not extended the protection of personal data to dead people in their own laws. In the EU, legislation in this field is not harmonized and the protection of post-mortem privacy is non-consistent.
In the US, the final draft of the Uniform Fiduciary Access to Digital Assets Act was adopted in December 2015. It enables Internet users to plan the management of their digital assets. For the moment not all US states have introduced this act into their legislation.

As there is no harmonised regime, the digital assets and the post-mortem privacy of the deceased are regulated by different contracts with different electronic communications service providers. Some of them provide technical solutions for the protection of post-mortem privacy (e.g. Google Inactive Account Manager, Facebook Legacy Contact), but most of them do not have any explicit rules on what happens to assets stored or created on their platforms upon death. Even if rules exist, there is a potential conflict upon death between the rules of contract and the rules of succession, as well as between the wishes of the deceased and the wishes of the survivor.

A harmonised legal framework appears as the only way to enable individuals to control their digital assets online and decide what happens to their privacy upon death.

References

About Inactive Account Manager. (n.d). Retrieved from: https://support.google.com/accounts/answer/3036546?hl=en.
Buitelaar, J.C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology, 19*(129), 129–142. Retrieved from: https://doi.org/10.1007/s10676-017-9421-9.
Bundesgerichtshof 1 December 1999, case Marlene Dietrich, I ZR 49/97.
Bundesverfassungsgericht 24 February 1971, case Mephisto, BVerfGE 30, 173.
Court of Justice of the European Union 6 November 2003, case C-101/01 Lindqvist, ECLI:EU:C:2003:596.
Court of Justice of the European Union 13 May 2014, case C-131/12 Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Google), ECLI:EU:C:2014:317.
Data Protection Act 2018, UK. Retrieved from: https://www.legislation.gov.uk/ukpga/2018/12/section/3.
De la Tour A., and Gauberti A. (2017). How to remove links about dead people from Google. The right to be forgotten and the deceased. Crefovi. Retrieved from: http://crefovi.com/articles/remove-links-dead-people-google-right-forgotten-deceased/.
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 (Directive 95/46/EC), OJ L 281, 23 November 1995, p. 31–50.
Edwards, L., and Harbinja, E. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment Law Journal, 32*(1), 101–147.
European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (ECHR), 4 November 1950. Retrieved from: http://www.echr.coe.int/Documents/Convention_ENG.pdf.
Harbinja, E. (2017). Post-mortem privacy 2.0: theory, law, and technology. *International Review of Law, Computers & Technology, 31*(1), 26-42. Retrieved from: http://dx.doi.org/10.1080/13600869.2017.1275116.
Hiscock, M. (2018). Dead Facebook users will soon outnumber the living. The loop. Retrieved from: http://www.theloop.ca/dead-facebook-users-will-soon-outnumber-the-living/.
How to contact Twitter about a deceased family member's account. (n.d.). Retrieved from: https://help.twitter.com/en/rules-and-policies/contact-twitter-about-a-deceased-family-members-account.
Internet World Stats. (2018). Retrieved from: http://www.internetworldstats.com/stats.htm.

King's Bench Division of England and Wales High Court 8 December 1808, case Baker v. Bolton, (1808) 1 Camp. 439; 170 ER 1033.
Law for Protection of Personal Data of Bulgaria, Prom. SG. 1/4 Jan 2002, amend. SG. 70/10 Aug 2004, amend. SG. 93/19 Oct 2004, amend. SG. 43/20 May 2005, amend. SG. 103/23 Dec 2005, amend. SG. 30/11 Apr 2006, amend. SG. 91/10 Nov 2006, amend. SG. 57/13 Jul 2007, amend. SG. 42/5 Jun 2009, amend. SG. 94/30 Nov 2010, amend. SG. 97/10 Dec 2010, amend. SG. 39/20 May 2011, amend. SG. 81/18 Oct 2011, amend. SG. 105/29 Dec 2011, amend. SG. 15/15 Feb 2013, suppl. SG. 81/14 Oct 2016, amend. SG. 85/24 Oct 2017, suppl. SG. 103/28 Dec 2017, amend. SG. 7/19 Jan 2018. Retrieved from: https://www.cpdp.bg/en/index.php?p=element&aid=373.
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Loi informatique et libertés). Retrieved from: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460.
Personal Data Protection Act of Estonia, RT I 2007, 24, 127. Retrieved from: https://www.riigiteataja.ee/en/eli/ee/529012015008/consolide/current.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), OJ L 119, 4 May 2016, p. 1–88.
Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087-1156. Retrieved from: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview.
Szekely, I. (2017). Does It Matter Where You Die? Chances of Post-Mortem Privacy in Europe and in the United States. *European Integration and Democracy Series*, (4), 313-320.
Uniform Fiduciary Access to Digital Assets Act (2015). Retrieved from: http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2015_RUFADAA_Final%20Act_2016mar8.pdf.
What will happen to my Facebook account if I pass away? (n.d.). Retrieved from: https://www.facebook.com/help/103897939701143?helpref=faq_content.
What is a legacy contact and what can they do? (n.d.). Retrieved from: https://www.facebook.com/help/1568013990080948.