SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

Communication and Notification of Personal Data Breaches Pursuant to the General Data Protection Regulation[1]

Jakub Morávek

Abstract: *The paper focuses primarily on the communication and notification of personal data breaches pursuant to the General Data Protection Regulation. The author discusses the issue in the context of the nemo tenetur principle and the related constitutional aspects.*

Key Words: *Labour Law; Personal Data Protection; Data Breach; General Data Protection Regulation; nemo tenetur Principle; the Czech Republic.*

Introduction

The adoption of the General Data Protection Regulation[2] was referred to as a "revolution". Yet the reality is different. The General Data Protection Regulation does not change the basic regulatory scheme in terms of the principles and obligations governing personal data protection and the status of the entities involved (controller, processor, data subject).[3] Re-

[1] The author of the presented paper is a secretary and senior lecturer at the Department of Labour Law and Social Security Law of the Faculty of Law of the Charles University in Prague. He is a vice-chairman of the Czech Association for Labour Law and Social Security Law and an attorney at law in Prague. The paper reflects the legal status as of 10 May 2019. The paper was drafted within and under the support of the research project *"Private Law and the Challenges of Today"* (in the Czech original *"Soukromé právo a výzvy dneška"*), project ID PROGRES Q03 at the Charles University in Prague, the Czech Republic, and the University Research Centres (UNCE) project UNCE/HUM/034 *"Dependent Work in the 21st Century – Issues and Challenges"* (in the Czech original *"Závislá práce v 21. století – otázky a výzvy"*).

[2] See *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)*. OJ EU L 119, 2016-05-04, pp. 1-88.

[3] Cf. MORÁVEK, J. Obecné nařízení o ochraně osobních údajů nejen z hlediska právní úpravy pracovněprávních vztahů. In: Z. GREGOROVÁ, ed. *Pracovní právo 2017: Ochrana osobních údajů, služební zákon a sociální souvislosti zaměstnávání cizinců* [online]. 1. vyd. Brno: Masarykova univerzita v Brně, 2018, pp. 13-47 [cit. 2019-04-26]. Acta Universitatis Brunensis, Iuridica, Volume 609. ISBN 978-80-210-8930-3. Available at: https://www.law.muni.cz/sborniky/pracpravo2017/files/PracovniPravo2017.pdf.

SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

flecting on the existing case law, particularly the decisions of the Court of Justice of the European Union, and the methodical recommendations and interpretation opinions of the Article 29 Data Protection Working Party[4] (now transformed into the European Data Protection Board), the General Data Protection Regulation has deepened certain principles and broadened certain obligations. In addition, the General Data Protection Regulation has introduced some new or fairly new concepts. From the local law perspective, these include the personal data protection officers, the codes of conduct or approved consistency mechanisms, the explicitly anchored mechanism of engaging sub-processors and creating processing chains, or the explicit formulation of binding corporate rules. Another novelty is the concept of communication and notification of personal data breaches.

The term "novelty" is nevertheless relative, as the concept is not completely unknown. For quite some time, Section 88 of the Act No. 127/2005 Coll. on Electronic Communications, building on the European legislation, has contained a similar concept. Our considerations on and objections against the constitutionality of the concept presented below also apply to the Act on Electronic Communications, except that, with regards to the position of the obligated entities pursuant to the aforementioned Act and the level of risk to the protected interests of the persons concerned, the rationale behind the concept can be understood. In the context of the General Data Protection Regulation, however, the situation is much more complicated.[5]

Personal data breach

Pursuant to the Article 4(12) of the General Data Protection Regulation, a security breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed; in other words, it is a disruption of the confidentiality, integrity or availability of the personal data being processed.

[4] See Data Protection Working Party pursuant to the Article 29 of the *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*. OJ EC L 281, 1995-11-23, pp. 31-50.

[5] See *Act No. 127/2005 Coll. on Electronic Communications*.

In the context of the Article 29 Data Protection Working Party, recommendation of 3 October 2017,[6] e.g. the loss of a storage medium containing personal data, the sending of an e-mail containing personal data to an incorrect e-mail address, the destruction of personal data media, the unauthorized deletion or modification of the personal data being processed, the access to personal data by an unauthorized person or the unauthorized disclosure of personal data constitute a personal data breach.

Based on the likely level of risk to the rights and freedoms of the data subjects or third parties arising from a personal data breach, the General Data Protection Regulation requires the data controller:

- to document the data breach;[7]
- to document the data breach and to notify it to the supervisory authority;
- to document the data breach, to notify it to the supervisory authority and to communicate it to the data subject.

The objective of the concept is to respond to a situation where a failure to notify the data breach or a delayed notification could have a significant negative impact on the rights and freedoms of natural persons. In addition, consultation with the Office for Personal Data Protection should ensure adequate resolution of the situation (selection of the appropriate technical or organizational measures, etc.) which the controller may not be able to achieve without the assistance (advice).

The rights and freedoms are not limited to merely the right to privacy or the right to the protection of personal data. In this context, the rights cover the full spectrum of fundamental rights and freedoms, including the right to the protection of life and health or the right to the protection of property – e.g. a loss of contact data, identification data, birth number and signature specimen (identity theft) may involve a risk to the data subject's property; a loss, long-term unavailability or unauthorized alteration of medical records may involve a risk to human life and health; etc.

[6] On the notification of personal data breaches pursuant to the *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)*. OJ EU L 119, 2016-05-04, pp. 1-88.

[7] For example, the destruction of a personal data medium if other copies exist of the personal data being processed.

SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

The risk to the rights and freedoms may concern not only the data subjects, but also other people (e.g. the data subject's family members, etc.; such situation may arise upon interference with the data subject's property that constitutes part of the community property of spouses).

Notification of a personal data breach

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data controller shall notify the personal data breach to the Office for Personal Data Protection. The Office for Personal Data Protection requests[8] that the notification be made via a data box or the e-mail address provided by the Office for Personal Data Protection. In addition to the preferred channels, a written submission can be made to the Office for Personal Data Protection. The written submission is subject to compliance with the notification deadline.

The obligation to notify the Office for Personal Data Protection arises when the controller becomes aware of the circumstances that imply, with adequate certainty, that there was a personal data breach and allow to assess the seriousness of the personal data breach in terms of the level of risk to the rights and freedoms of the persons concerned. The obligation must be fulfilled without undue delay after the information that has to be included in the notification pursuant to the Article 33(3) is available to the controller.

In connection with the personal data breach, the controller is expected to implement certain internal processes and, in particular, to ensure the security of processing and/or to implement measures to eliminate or to minimize the related risks. For this reason, the notification deadline was set out more specifically as follows: the controller should notify a data breach not later than 72 hours after having become aware of the breach.

Exceeding the 72-hour deadline does not necessarily constitute an infringement by the controller, since the primary obligation is to notify the personal data breach without undue delay. Depending on the circumstances, the corresponding deadline may be longer than 72 hours (see also Recital 85). Where the 72-hour deadline is not met, the reasons for

[8] See *Úřad pro ochranu osobních údajů* [online]. 2019 [cit. 2019-07-08]. Available at: https://www.uoou.cz/.

the delay (being legitimate reasons) have to be included in the notification by the controller.

The General Data Protection Regulation prefers (in order to protect the rights and freedoms of the persons concerned) the earliest possible communication between the controller and the Office for Personal Data Protection. The notification duty may, therefore, be fulfilled in phases, as separate facts that should be included in the notification (Article 33(3) of the General Data Protection Regulation) become available to the controller. Fulfilment of the notification duty in several phases may not be an exception. The controller may generally be able to assess the security incident in terms of the risks to the rights and freedoms within 72 hours; nevertheless, the controller may be unable to adequately respond by implementing measures to address the personal data breach within the same deadline. The "without undue delay" deadline shall apply to each individual piece of information that is to be included in the notification, even if the notification is made in phases.

The notification shall contain at least the information stipulated in the Article 33(3) of the General Data Protection Regulation.

Communication of a personal data breach

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall notify (Article 34 of the General Data Protection Regulation) the personal data breach to the Office for Personal Data Protection as described above. In addition, the personal data breach shall also be communicated, without undue delay, to the data subjects concerned. No framework deadline is stipulated for the communication of a data breach, as in the case of the notification to the Office for Personal Data Protection. In principle, the communication to the data subjects should precede the notification to the Office for Personal Data Protection and should be made immediately after the personal data breach has been detected. The aim is to immediately alert the data subjects to the risk and to provide them with information (and time) necessary to eliminate or at least to minimize the risk to their rights and freedoms.

An example of a personal data breach is the loss of the data subject's medical records, where the knowledge of previous therapy, medications, test results, etc. is necessary for further treatment of the data subject. Another example is the loss of the data subject's personal data which al-

SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

low to manipulate with/to dispose of the data subject's assets. In such case, the rights and freedoms of third parties may also be jeopardized (e.g. if the assets constitute part of the community property of spouses).

The communication shall use clear and plain language so that the content can be understood by the addressee. Special attention should be paid to formulating the information if the recipient is a child. If the recipient's capacity is unknown, he/she will be presumed to have the intellect of an average individual (Section 4(1) of the Civil Code). In addition to the nature of the breach, the communication shall include at least the information and the description of measures pursuant to the Article 33(3) of the General Data Protection Regulation (see above).

With respect to the personal data controller's obligation to ensure security of the personal data being processed and the obligation to minimize the risks to the rights and freedoms of the data subject, the communication should also include (see Recital 86) a recommendation of effective measures whereby the person concerned can eliminate or at least minimize the risks to the rights and freedoms (e.g. immediate change of the login information upon loss of mailbox login data, etc.).

If the controller is reluctant to comply with the communication obligation toward data subjects, the Office for Personal Data Protection may, pursuant to the Article 34(4) of the General Data Protection Regulation, require fulfilment of the obligation by the controller (having considered the likelihood of the level of risk the personal data breach may result in). The Office for Personal Data Protection may also decide that the communication obligation does not have to be fulfilled on the grounds that certain requirements for exemption have been met. Given the absence of detailed provisions governing the process, the general provisions contained in the Code of Administrative Procedure should be followed.

The communication to the data subject shall not be required if any of the following conditions are met:

(a) The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.

The above-mentioned condition may relate to two situations:

1. either the controller implemented the appropriate measures before the personal data breach; the controller has encrypted or thoroughly pseudonymised the data and, under normal circumstances, it is impossible for an unauthorized person to read the data. In addition, the controller has a copy of the stolen data;

2. or a technical solution was adopted after the personal data breach, but has the same effect and, in the light of circumstances, it is impossible that a high risk to the data subject's rights and freedoms may have arisen in the meantime.

As in the first case the obligation to notify and to communicate the personal data breach does not arise at all (there is no high risk to the rights and freedoms), the exemption should, in fact, relate to the latter. In the context of the exemption stipulated under letter (b), however, which would then be deprived of any content, the exemption under letter (a) cannot but relate to the first case described. The exemption under letter (b) can, therefore, relate to the second case.

(b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

(c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The concept of disproportionate effort must be interpreted in the context of the proportionality principle (test). In measuring the interests concerned, both the potential interference with the data subjects' interests and the costs incurred by the data controller need to be considered, as well as the risk arising from possible delay if contacting the data subjects would require tracing the contact details which are currently unavailable to the data controller. Account must also be taken of the controller's position and responsibilities.

In these cases, the controller is required to inform the data subjects at least by a public statement (on the website, in the media, by the bulk e-mail messages, etc.).

Section 12 of the Act No. 110/2019 Coll. on the Processing of Personal Data (hereinafter referred to as the "Data Processing Act") derogates from the general statutory provisions. Pursuant to the above-stated Section, the data controller may fulfil the communication obligation to a lim-

SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

ited extent only or to postpone its fulfilment (i.e. to communicate the data breach, yet not without undue delay) if it is necessary and adequate in scope to secure the protected interest stipulated in the Section 6(2) of the Data Processing Act; Section 6(2) of the Data Processing Act stipulates among protected interests, inter alia, the protection of rights and freedoms of persons or the enforcement of private law claims.[9]

Such case (in relation to labour relations) may involve the destruction of media containing the data on data subjects (employees) who are deemed to have been involved in causing damage to the employer's property; if there are multiple liable employees, such situation may, subject to individual personal liability of employees, result in a potentially high risk to the rights and freedoms of at least some of the employees concerned, while communicating the incident to the employees concerned may frustrate the employer's enforcement of claims.

The controller shall report to the Office for Personal Data Protection the non-communication or limited communication of a personal data breach, pursuant to the provision of the Section 12 of the Data Processing Act, without undue delay. Section 11(2) of this Act shall apply to the reporting to the Office for Personal Data Protection accordingly.

Communication and notification of a personal data breach and documentation of the same

The obligation to notify and to communicate personal data breaches solely lies with the controller. This does not exclude that, under the authority of the personal data controller, the obligation to the Office for Personal Data Protection or to the data subjects may be fulfilled by the personal data processor or by another authorized representative on the controller's behalf. Pursuant to the General Data Protection Regulation (Article 33(2)), the processor only has the obligation to notify the controller without undue delay after becoming aware of a personal data breach.

In relation to the controller's obligation to ensure security of the personal data being processed, the obligation to safeguard the interests and rights and freedoms of data subjects and the liability to duly and timely discharge the obligations pursuant to the Articles 33 and 34 of the General Data Protection Regulation, at least the following should be set in the context of regulating the relationship between the controller and the

[9] See *Act No. 110/2019 Coll. on the Processing of Personal Data*.

processor: the need to inform each other of data breaches, of the Office for Personal Data Protection notification and of measures that should be or have been adopted to minimize the risks to the rights and freedoms of the data subject following a personal data breach.

The controller's (or the processor's) obligation to ensure timely and effective protection of the personal data being processed and the obligation to ensure compliance with the communication and notification duties may also involve setting up an internal whistleblower system.[10]

Each personal data breach shall be documented by the controller.

The General Data Protection Regulation only prescribes the general structure of the record. Pursuant to the Article 33(5) of the General Data Protection Regulation, the record should contain:

- a description of the facts of the personal data breach;
- a description of the effects of the personal data breach in relation to the rights and freedoms of the data subject;
- the reason why the personal data breach does not involve a risk to the data subject's rights and freedoms;
- a description of measures envisaged and taken to eliminate the risk of recurrence;
- if the personal data breach resulted in interference with the data subject's rights and freedoms, a description of measures eliminating the risk to the data subject's rights and freedoms and, if the risk cannot be eliminated, a description of measures mitigating the risk;
- if, pursuant to the Article 34(3) of the General Data Protection Regulation or pursuant to the Section 12 of the Data Processing Act, the personal data controller has failed to discharge or postponed the discharge of the duty to communicate the personal data breach to the data subject, the record should also contain the reasons for the controller's conduct;
- it should also be clear from the documentation why the personal data controller discharged the communication or notification duty in phases or why the duty in question was not fulfilled by the statutory deadline.

[10] Concerning whistleblowing see e.g. PICHRT, J. ed. *Whistleblowing*. 1. vyd. Praha: Wolters Kluwer, 2013. 260 p. ISBN 978-80-7478-393-7.

SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

Notification of a personal data breach in light of the legal maxim *"nemo tenetur se ipsum accusare"*

The basic idea behind the regulation of communication and notification of personal data breaches is a good one. In essence, the idea grasps that which follows from the general obligation to prevent harm and from the common decency, i.e. that in the event of an incident that may affect the interests, rights and freedoms of another, the person affected should be informed of the incident and should have the time and opportunity to adopt the relevant measures to avert any negative consequences. If the situation is the informer's fault, the informer should participate in averting the negative consequences. It is also reasonable for the obligated party to have an opportunity to contact a competent institution to discuss the matter and to receive advice as to the best solution of the situation.

The stories of legal concepts, however, rarely tend to have happy endings. Legal concepts, especially the new and unrefined ones, are seldom reasonable, well-functioning and without any issues. The notification of a personal data breach is no exception to this rule.

Pursuant to the provision of the Section 62(1)(a) of the Data Processing Act, a controller has committed a non-criminal offense if he/she has infringed, inter alia, Article 33 of the General Data Protection Regulation (failed to duly notify a personal data breach to the Office for Personal Data Protection pursuant to the aforementioned provision).

The problem arises when, based on the notification of a personal data breach, the supervisory authority identifies possible infringement of the General Data Protection Regulation by the controller (scope of data, retention period, security, etc.) and proceeds with sanctions.

The core of the problem is the conflict of two legal principles: the principle of officiality, on the one hand, and the principle *nemo tenetur se ipsum accusare*, on the other hand. The solution is not an easy one. No prosecution means suppression of the effects of personal data protection legislation. Prosecution, on the other hand, means violation of a constitutional principle and one of the underlying principles of a democratic rule of law the path to which was long and painful (and sometimes blood-stained).[11]

[11] Cf. particularly HOLLÄNDER, P. *Příběhy právních pojmů*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017, p. 164. ISBN 978-80-7380-654-5.

The opinion of the Office for Personal Data Protection is not clear yet, as there were not sufficient grounds for potential sanctioning of personal data controllers in the period of absence of adaptation legislation in the form of the Data Processing Act. The Office for Personal Data Protection's statement[12] saying that some notifications of personal data breaches had been referred for inspection[13] nevertheless suggests that the Office for Personal Data Protection does not seem reluctant to sanction the controllers.

In this context, let us review the essence of the principle *nemo tenetur se ipsum accusare*.

One of the axioms of a materially perceived democratic rule of law is the right to a fair trial. The right to a fair trial consists of a group of subrights (the right to a legal judge, foreseeable decision and convincing justification, etc.). One of the rights that make up the group is a person's right not to testify if the testimony could involve the person or his/her close person in a criminal prosecution or a danger thereof. At the constitutional level, this right is stipulated in the Article 37(1) of the Charter of Fundamental Rights and Freedoms and, specifically in relation to a prosecuted person, in the Article 40(4) of the same Charter. The right not to testify is also guaranteed by the international law, e.g. in the Article 14(3)(g) of the International Covenant on Civil and Political Rights or, in the context of the case law of the European Court of Human Rights, in the Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

The right to deny testimony means that a person must not be forced to self-incrimination by the public power. The right not to testify or the privilege against compelled self-incrimination necessitates extensive interpretation, involving not just the testimony per se, but active collaboration in general.[14]

The right not to testify or the privilege against compelled self-incrimination is widely addressed in the case law of the high courts. The

[12] See Tiskové zprávy. In: *Úřad pro ochranu osobních údajů* [online]. 2019 [cit. 2019-07-08]. Available at: https://www.uoou.cz/tiskove-zpravy/ds-1017/p1=1017.
[13] The Office for Personal Data Protection may be deemed to act upon Recitals 87 and 88 of the General Data Protection Regulation.
[14] See e.g. *Finding of the Constitutional Court of the Czech Republic Ref. No. I. ÚS 402/05* [2005-11-08].

SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

Constitutional Court of the Czech Republic gave detailed comments on the concept and its genesis in the case file no. III. ÚS 528/06.[15]

In the context of understanding of the concept as contained in the Czech Constitutional Court case law, two types of acts may be distinguished from the point of view of the principle *nemo tenetur*. One is the act of a person exposing oneself (or a close person) to the risk of a criminal prosecution. The person cannot be compelled to such act. The second group comprises acts of which the person is merely a passive object and which he/she may be compelled by lawful means to sustain.

Despite its key importance for a fair trial, the *nemo tenetur* rule is not unlimited. For example, sustaining the collection of a control sample during an inspection carried out by the Czech Trade Inspection Authority cannot be described as compelling self-incrimination or self-accusation. The person concerned is obliged to tolerate the act and may be compelled, by permissible means, to collaborate.

If, on the other hand, a person is asked to take active steps, e.g. to execute certain deeds (under the threat of an administrative fine for failure to cooperate), etc., the borderline has been crossed between an act where the person is merely a passive object and a situation where the person is forced to an act of self-incrimination (of oneself or a close person). Forcing a person *"to speak"* under the threat of an administrative fine would violate the privilege against compelled self-incrimination (subjecting him/her or a close person to an incrimination).[16]

The person concerned must always be advised of the right not to testify (or to deny active cooperation) well in advance. Insufficient instructions that may (even without the use of a threat or actual coercive instrument, e.g. administrative fine) result in incriminating evidence against the cooperating person who had the right not to testify (or to de-

[15] Similarly cf. e.g. *Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 118/01* [2003-01-28]; *Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 255/05* [2005-06-23]; and *Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 552/05* [2006-01-12].

[16] Cf. e.g. *Finding of the Constitutional Court of the Czech Republic Ref. No. I. ÚS 671/05* [2006-02-22].

ny active cooperation) constitute a serious procedural defect.[17] Forced evidence cannot be used.[18, 19]

The prohibition against compelling active collaboration pursuant to the principle *nemo tenetur* applies to the public power as a whole. Both the compelling of active collaboration using legal instruments (civil fines, etc.) and the statutory duty to notify the relevant public authority (non-compliance with which constitutes an infringement) where the prescribed content of the notification may result in facts directly leading to sanctions imposed upon the notifier are outside the above-mentioned constitutional limit.

Closing conclusions

As the popular saying goes, even good intentions may lead to unintended consequences. It is too early to jump to any conclusions. The Office for Personal Data Protection's approach and the application practice will be of the key importance. If not correctly grasped, however, the legislation governing the notification of personal data breaches may prove the saying to be true.

Application of the principle of officiality will mean violation of the principle *nemo tenetur* against the personal data controller. Another option in the context of *nemo tenetur* is to exclude from criminal liability the acts that are the subject of notification; this option would rely on the identity (consistency) of an act, with the exclusion of any conduct consistent with the notified conduct or the notified consequences. Such approach could, however, lead to major interference with the public liability for violations of the data protection legislation. Preserving liability for violations of the data protection legislation if there is evidence that the controller notified the relevant conduct in order to eliminate his/her own liability could have a somewhat mitigating effect.

Two more concluding comments:

[17] Cf. e.g. *Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 89/04* [2006-02-02].

[18] Cf. e.g. *Decision of the Supreme Court of the Czechoslovak Republic Ref. No. 7 Tz 85/65* [1966-02-03].

[19] Cf. e.g. F. Púry in ŠÁMAL, P. et al. *Trestní řád: Komentář: I. díl*. 5. vyd. Praha: C. H. Beck, 2005, p. 814 and following. ISBN 80-7179-405-8.

SOCIETAS ET IURISPRUDENTIA
2019, ročník VII., číslo 3, s. 77-91
http://sei.iuridica.truni.sk
ISSN 1339-5467

Remedial measures imposed upon the notifier by the administrative authority do not contradict the principle *nemo tenetur*, since remedial measures are not a sanction.

The aforementioned conflict with the principle *nemo tenetur* does not arise if the notification implies liability on the part of the processor and the processor is subject to the Office for Personal Data Protection's sanctions. But even in this case, an important question arises, involving major ethical aspect:[20] Is legislation stipulating a general obligation to become an informant a sign of a healthy society?

References

Act No. 110/2019 Coll. on the Processing of Personal Data.

Act No. 127/2005 Coll. on Electronic Communications.

Decision of the Supreme Court of the Czechoslovak Republic Ref. No. 7 Tz 85/65 [1966-02-03].

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. OJ EC L 281, 1995-11-23, pp. 31-50.

Finding of the Constitutional Court of the Czech Republic Ref. No. I. ÚS 402/05 [2005-11-08].

Finding of the Constitutional Court of the Czech Republic Ref. No. I. ÚS 671/05 [2006-02-22].

Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 89/04 [2006-02-02].

Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 118/01 [2003-01-28].

Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 255/05 [2005-06-23].

Finding of the Constitutional Court of the Czech Republic Ref. No. II. ÚS 552/05 [2006-01-12].

[20] Cf. e.g. MORÁVEK, J. O whistleblowingu, jeho legitimitě a problémech mezinárodních přenosů osobních údajů. In: J. PICHRT, ed. *Whistleblowing*. 1. vyd. Praha: Wolters Kluwer, 2013, pp. 187-202. ISBN 978-80-7478-393-7.

HOLLÄNDER, P. *Příběhy právních pojmů*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. 285 p. ISBN 978-80-7380-654-5.

MORÁVEK, J. O whistleblowingu, jeho legitimitě a problémech mezinárodních přenosů osobních údajů. In: J. PICHRT, ed. *Whistleblowing*. 1. vyd. Praha: Wolters Kluwer, 2013, pp. 187-202. ISBN 978-80-7478-393-7.

MORÁVEK, J. Obecné nařízení o ochraně osobních údajů nejen z hlediska právní úpravy pracovněprávních vztahů. In: Z. GREGOROVÁ, ed. *Pracovní právo 2017: Ochrana osobních údajů, služební zákon a sociální souvislosti zaměstnávání cizinců* [online]. 1. vyd. Brno: Masarykova univerzita v Brně, 2018, pp. 13-47 [cit. 2019-04-26]. Acta Universitatis Brunensis, Iuridica, Volume 609. ISBN 978-80-210-8930-3. Available at: https://www.law.muni.cz/sborniky/pracpravo2017/files/PracovniPravo2017.pdf.

PICHRT, J. ed. *Whistleblowing*. 1. vyd. Praha: Wolters Kluwer, 2013. 260 p. ISBN 978-80-7478-393-7.

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). OJ EU L 119, 2016-05-04, pp. 1-88.

ŠÁMAL, P. et al. *Trestní řád: Komentář: I. díl*. 5. vyd. Praha: C. H. Beck, 2005, pp. 1-1432. ISBN 80-7179-405-8.

Tiskové zprávy. In: *Úřad pro ochranu osobních údajů* [online]. 2019 [cit. 2019-07-08]. Available at: https://www.uoou.cz/tiskove-zpravy/ds-1017/p1=1017.

Úřad pro ochranu osobních údajů [online]. 2019 [cit. 2019-07-08]. Available at: https://www.uoou.cz/.

JUDr. Jakub Morávek, Ph.D.

Faculty of Law
Charles University in Prague
Náměstí Curieových 901/7
116 40 Prague 1
Czech Republic
moravek@prf.cuni.cz