

Agnieszka Grzelak*

PROTECTION OF PERSONAL DATA OF CRIME VICTIMS IN EUROPEAN UNION LAW – LATEST DEVELOPMENTS

Abstract:

In EU law a lot of attention has recently been paid to personal data protection standards. In parallel to the development of the general EU rules on data protection, the Members States also develop cooperation between law enforcement agencies and create new information exchange possibilities, including the processing of personal data of participants in criminal proceedings. The aim of this article is to analyse whether the personal data of victims of crime are safeguarded according to the standards of the Charter of Fundamental Rights. For this purpose, the author analyses two directives: 2012/29/EU, which regulates minimum standards of victims of crime; and 2016/680/EU (also known as the Law Enforcement Directive), which regulates personal data processing for the purpose of combating crime. Based on the example of the Polish legislation implementing both directives, the author comes to the conclusion that the EU legislation is not fully coherent and leaves too much margin of appreciation to the national legislator. This results in a failure to achieve the basic goals of both directives. The author expects the necessary reflection not only from the national legislator, but also from the European Commission, which should check the correctness of the implementation of the directives, as well as from national courts, which should use all possible measures to ensure that the national law is interpreted in the light of the objectives of the directives.

Keywords: personal data protection, police directive, victim of crime, Charter of Fundamental Rights

* Dr. habil., professor at the Kozminski University in Warsaw, email: agrzelak@alk.edu.pl, ORCID: <https://orcid.org/0000-0002-5867-8135>. This article was partially prepared as part of a project financed by the National Science Centre – decision DEC-2012/07/B/HS5/03908. In the framework of the research the author dealt with, *inter alia*, the emergence of the concept of the right to personal data protection within the right to privacy and the international standard of its protection. For further details, see A. Grzelak, *Ochrona danych osobowych we współpracy policyjnej i sądowej w sprawach karnych UE. W stronę standardu europejskiego* [Personal data protection in the field of police and judicial cooperation in criminal matters in the EU. Towards a European standard], SGH, Warszawa: 2015.

INTRODUCTION

The issue of personal data protection has become one of the leading topics in European Union (EU) law recently. This is undoubtedly related to the legislative reform carried out in recent years in this area. The main elements of the reform are Regulation 2016/679 (GDPR),¹ as well as Directive 2016/680/EU² (Law Enforcement Directive). At the same time, the area of freedom, security and justice (AFSJ) has become one of the most dynamic EU integration fields in recent years. Since the Treaty of Amsterdam, the mutual recognition procedure has been the main regulatory practice in this policy field. The EU institutions are adopting more and more legislation which governs the exchange of information, including exchange of personal data, between the competent authorities of the Member States involved in the fight against crime. This requires us to consider the coherence and effectiveness of the adopted provisions, as well as their consistency with the fundamental rights protection standards.

The general problem of protection of the rights of victims of crime is analysed in the literature mostly in the context of the provisions of Directive 2012/29/EU³ and the minimal standards established by this directive. These publications however omit the specific issue of data protection.⁴ In turn, the protection of personal data of crime victims has been mostly examined on the basis of the Polish law in 2014⁵ and – including the draft law enforcement directive – in 2016.⁶ While expiry of the implementation

¹ 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) [2016] OJ L 119 with corr.

² Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119.

³ Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA [2012] OJ L 315.

⁴ See generally M. Kolendowska-Matejczuk, *Ochrona praw ofiar przestępstw na gruncie przepisów Unii Europejskiej w świetle dyrektywy 2012/29/UE* [Protection of the rights of victims of crime under European Union law in the light of Directive 2012/29/EU], 2 *Krakowskie Studia Międzynarodowe* 61 (2013). Cf. European Parliament, *The Victims' Rights Directive 2012/29/EU: European Implementation Assessment: Study*, 2017; I. Gážiová, J. Kralík, *The New European Network on Victims' Rights*, 16(1) *International and Comparative Law Review* 83 (2016), S. Buczman, *An overview of legal acts on protection of victims of crime in the view of the adoption of the Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime in the European Union*, 14(2) *ERA Forum* 235 (2013).

⁵ See generally L. Mazowiecka (ed.), *Ochrona danych osobowych i wizerunku ofiary przestępstwa* [Protection of personal data and image of the victim of crime], Wolters Kluwer, Warszawa: 2014.

⁶ See A. Grzelak, *Ochrona danych osobowych ofiar przestępstw w prawie Unii Europejskiej* [Protection of personal data of victims of crime under EU law], in: D. Kornobis-Romanowska (ed.), *Unia Europejska w roli gwarantów praw podstawowych* [The European Union as guarantor of fundamental rights], Currenda, Sopot: 2016, p. 187.

deadline of the law enforcement directive is therefore the right time to formulate more precise conclusions, nevertheless this article is limited to the issue of protection of data of victims, leaving other problems related to the implementation of Directive 2016/680 for discussion in other studies, in particular the question of the compliance of Polish criminal law procedure with the Law Enforcement Directive.⁷

In 2016 the general conclusion of my article, based on my preliminary research, was that Directive 2012/29/EU (the victim's rights directive) does not pay particular attention to the privacy of a victim – rather it is a part of a general scheme of assistance to victims. Moreover, the article stated that the draft directive was vague and imprecise, so there was a strong need to strengthen guarantees in the soon-to-be adopted final version of the directive. Now, in 2019 we can see that not so much has changed, and a lot still depends on the decisions of the national legislator. The law enforcement directive (Directive 2016/680), which is deliberately imprecise to leave room for the actions on the national level, requires taking into account the special position of victims of crimes. However, the law implementing Directive 2016/680/EU in Poland does not apply to the files of court proceedings conducted on the basis of the provisions of the Code of Criminal Procedure, which is one of the basic problems of the law implementing the Law Enforcement Directive in Poland.⁸ Therefore, the preliminary conclusion from 2016 requires reconsideration due to this unexpected and controversial decision of the Polish legislator. It is thus necessary to ask whether the personal data of victims of crimes are properly protected and safeguarded in a manner consistent with the standards stemming from both directives, but most of all with the standards contained in the EU Charter of Fundamental Rights (Charter).

The general aim of this article is to analyse whether the two paths of legislative development in EU law – the stronger protection of victims of crime in criminal proceedings as well as the reform of personal data safeguards – are deliberately parallel and consistent and whether there is a cohesion between these two processes. The scope of the analysis requires concentrating both on the problem of respecting the rights of victims of crimes in general as well as in the context of protection of their personal data. This topic can be also addressed in a broader way, i.e. whether the EU guarantees and promotes the right to protection of personal data in relation to victims of crime as a separate goal, or whether the adoption of legislation in this respect by the EU is the result and side effect of other objectives, such as establishing good cooperation between law enforcement agencies and mutual recognition in criminal matters. The noticeable

⁷ For more on Directive 2016/680 see generally A. Grzelak (ed.), *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz* [Commentary on the law on the protection of personal data processed in connection with the fight against and prevention of crime], CH Beck, Warszawa: 2019; M. Kusak, *Ochrona danych osobowych w sprawach karnych – rekomendacje na tle transpozycji dyrektywy 2016/680/UE* [Protection of personal data in criminal matters – recommendations based on the transposition of Directive 2016/680/EU], 10 Europejski Przegląd Sądowy 10 (2017).

⁸ O.J. 2019, item 125. See also A. Grzelak, M. Wróblewski, *Komentarz do art. 3* [Comment on Art. 3], in: Grzelak, *supra* note 7.

differences between Directive 2012/29/EU and the law enforcement directive vis-à-vis the protection of personal data of crime victims are possibly reflected at the level of guarantees and rights granted to the data subject. Therefore, the main research question in this article concerns the level of personal data protection of victims of crime.

This article is divided into several sections. The first section discusses the definition of a victim of a crime contained in EU law and its application, which is limited to natural persons. The second section presents the general standard of data protection derived from the Charter. In the following sections the article focuses on the relevant EU legislation and presents some comments on the imprecise language of the directives and the discretionary powers of the Member States and their consequences for the level of protection of victims in the national legislation.

1. DEFINITION OF A VICTIM OF CRIME IN THE EU LEGISLATION

Any analysis of personal data protection issues should start from clarifying the definition of the notion “victim of a crime”. This is necessary in order to determine the correlation between the rights of victims of crime (under Directive 2012/29/EU) and the need to protect their personal data during criminal proceedings (under the Law Enforcement Directive) – the latter aspect being innovative in these considerations.

At present Directive 2012/29/EU is the fundamental EU act that regulates the position of the victim of a crime in any criminal proceeding and defines the concept of a “victim of crime.”⁹ For the purposes of the directive, the definition of a victim is included in its Art. 2(1). This notion encompasses two ideas: (1) a direct victim, which means “a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence”; and (2) an indirect victim, who is a “family member of a person whose death was directly caused by a criminal offence and who has suffered harm as a result of that person’s death.”

In the first place this definition clearly indicates that for the purposes of Directive 2012/29/EU only natural persons are considered to be victims of crimes.¹⁰ Apparently the directive fails to consider legal persons as victims. This is consistent with the provisions of the Law Enforcement Directive, which also does not allow legal persons to be considered as victims whose data should be protected under its provisions. Moreover, this is not only in line with the jurisprudence of the Court of Justice,¹¹ but also with the definition of a victim provided in other international acts, especially in the 1985 UN

⁹ This definition has already been described in the author’s previous research (see Grzelak, *supra*, note 6, p. 189), however without reference to the provisions of Directive 2016/680.

¹⁰ See generally S. Walklate (ed.), *Handbook of Victims and Victimology*, Routledge, London: 2018. See also S. Buczman, *An overview of the law concerning protection of victims of crime in the view of the adoption of the Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime in the European Union*, 14(2) ERA Forum 235 (2013).

¹¹ Case C-205/09, *Criminal proceedings against Emil Eredics and Mária Vassné Sápi*, ECLI:EU:C:2010:623.

Declaration on the basic principles of justice for victims of crime and abuse of power.¹² This declaration confirmed the need to adopt measures, both at the national and international levels, to secure universal and effective recognition of the rights of victims of crime. The declaration defined the concept of a “victim” as a person who, individually or collectively, has suffered harm to his or her physical or mental health, suffered emotional disorders, material damage, or serious breach of their fundamental rights as a result of acts or omissions that were in breach of the criminal law in force in the given country, including laws on the criminal misuse of powers.¹³

Secondly, Directive 2012/29/EU extends the concept of a victim of crime to family members. This – in comparison to an earlier act governing the rights of victims of crime, namely Council framework decision 2001/220/JHA – is an important development.¹⁴ The final decision whether all family members should be considered as victims for the purpose of national criminal proceedings has been left by Directive 2012/29/EU to the national legislator.¹⁵ In turn, the Law Enforcement Directive does not refer directly to the notion of a victim, which means that in this text the notion should be correlated with state law. However, the national legislator is bound by the scope of application of the directive. It should be taken into account that although in Polish criminal law a legal person may be a victim,¹⁶ it is not possible to talk about the protection of personal data of legal persons for the purposes of personal data protection. This is a right vested in natural persons. At the same time, this does not mean that the national legislator cannot grant certain rights to legal persons – only that this is not a requirement under EU law.

To sum up, both Directive 2012/29/EU and Directive 2016/680 use the term “victim of a crime” in a narrower sense than is the case in some national criminal codes.

2. CHARTER’S STANDARD OF PERSONAL DATA PROTECTION

Since the Treaty of Lisbon the right to protection of personal data is a separate fundamental right, although still directly connected with the general right to privacy.¹⁷ Art.

¹² Available at: <http://www.un.org/documents/ga/res/40/a40r034.htm> (accessed 30 May 2019).

¹³ E.g. B. Buneci, *The notion of victim in international and European judicial proceedings*, 3(1) Perspectives of Business Law Journal 48 (2014).

¹⁴ For some remarks on the position of the EU institutions with regard to the incorporating a family member into the definition, see S. Buczman, R. Kierzyńska *Protection of victims of crime in the view of the Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime in the European Union and the Directive 2011/99/EU on the European protection order*, available at: https://www.ja-sr.sk/files/Kierzyńska_Buczman_Protection%20of%20victims.pdf (accessed 30 May 2019).

¹⁵ See Art. 2(2) of Directive 2012/29/EU.

¹⁶ See Art. 49 of the Code of Criminal Procedure, O.J. 2018, item 1987.

¹⁷ E.g. G. Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Cham: 2014, p. 198. The author observes that the coexistence of Arts. 7 and 8 of the Charter might be explained in terms of a compromise between divergent national constitutional approaches (those envisioning privacy as encompassing personal data protection vs. those conceiving of

16 of the Treaty on the Functioning of the EU (TFEU) provided the legal basis for the Commission to initiate a discussion on strengthening the safeguards for the protection of personal data in the EU. At the same time, the Lisbon Treaty not only introduced Art. 16 TFEU but also declared that the Charter is a binding legal instrument. The general standard of data protection in the EU is thus based on both Art. 8 of the Charter, which grants every citizen the right to the protection of personal data concerning him or her, and Art. 16 TFEU. Moreover, they define the minimum rules of data processing, being that the data must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or on some other legitimate basis laid down by law. The structure of Art. 8 of the Charter is typical: it sets forth the general structure and does not deal with the lawful limitations, which are addressed by Art. 52. The three paragraphs of Art. 8 of the Charter together describe the general right to the protection of personal data, formally granted to everybody in Art. 8(1); described in Art. 8(2) as requiring that personal data are processed “fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” and that “everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified”; as well as encompassing pursuant to Art. 8(3) the existence of an independent supervisory authority. Thus there are six constituent components of the right to data protection: (1) the requirement of fair processing; (2) the requirement of processing for specified purposes; (3) the requirement of a legitimate basis, which can be either a basis laid down by law or based on the consent of the person concerned; (4) the right of access to data; (5) the right to have data rectified; and (6) independent supervision.¹⁸

Two Declarations annexed to the Lisbon Treaty specifically relate to Art. 16 TFEU, one of which suggests that “specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation (...) may prove necessary because of the specific nature of these fields.”¹⁹ This decision of the Member States served as an excuse for the Commission – and later on for the EU legislator (the EU Council and the Parliament) – to prepare and adopt Directive 2016/680, which is not only a separate act (separate from the act which generally regulates data protection processing – the GDPR), but which is also different in terms of its application and the results to be achieved. This serves as an explanation behind the introduction of the possibility for Member States to derogate from the general rules on the processing of personal data, which is justified by the need to ensure efficiency

personal data protection as an autonomous fundamental right); but it can also be described, from an EU perspective, as the outcome of an unresolved friction between an established approach and a novel one. See also J. Sobczak, *Komentarz do art. 8 Karty Praw Podstawowych* [Commentary on Art. 8 of the Charter of Fundamental Rights], in: A Wróbel (ed.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz* [Charter of Fundamental Rights of the European Union. Commentary], CH Beck, Warszawa: 2013, p. 259.

¹⁸ See Gonzalez Fuster, *supra*, note 17, p. 204.

¹⁹ Declaration No. 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

in criminal proceedings and the admissibility of introducing restrictions to the right to protection of personal data if such is related to the interests of justice.

At the same time, the Treaty of Lisbon has significantly strengthened the powers of the EU in the field of police and judicial cooperation in criminal matters. Art. 82 TFEU states that the fundamental principle in the field of judicial cooperation in criminal matters is the principle of mutual recognition of judgments and judicial decisions, which requires the approximation of the laws and regulations of the Member States. To the extent necessary to facilitate the implementation of this principle, the European Parliament and the Council should be empowered to adopt directives laying down relevant minimum standards, possibly including the rights of individuals in criminal proceedings and the rights of victims of crime. This article of the TFEU was the legal basis for the adoption of Directive 2012/29/EU.

The difficulties in balancing the right to personal data protection and the right to privacy on the one hand, and the obligations of the state to guarantee public security on the other was illustrated by the Court of Justice first in the *Digital Rights Ireland*²⁰ case, then in the *Tele 2*²¹ case, and most recently also in the *Ministerio Fiscal* case.²² These cases clearly show that there is a growing need to ensure a better balance between security-focused instruments and fundamental rights, especially if there is a special treaty provision devoted to the right to data protection and also a special legal basis to address the growing need to pay attention to the rights of victims of crime. The Court of Justice explained the basic rules and emphasized that the ideas which emerged from Art. 16 TFEU and Art. 8 of the Charter should be a *leitmotiv* for the EU legislator when adopting all secondary legislative acts, as well as for the national legislator when implementing EU law.

The EU measures dedicated to the protection of victims of crime – discussed for several years and finally adopted – consist of not only a few acts regulating victims' rights and position in criminal proceedings, but also specific criminal law instruments for enforcing the protection of victims.

3. MINIMUM STANDARDS ON THE PROTECTION OF VICTIMS OF CRIME IN DIRECTIVE 2012/29/EU

The Treaty of Lisbon has introduced significant changes in the system of police and judicial cooperation in criminal matters. The main changes are related to the decision to transfer this area of cooperation from the intergovernmental level to the supranational system. This is connected not only with changes in the law-making process, but also with regard to the competences of EU institutions (especially the Commission and Court of Justice) with respect to enforcing compliance with the adopted law. The

²⁰ Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238.

²¹ Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen i Secretary of State for the Home Department v. Tom Watson and others*, ECLI:EU:C:2016:970.

²² Case C-207/16, *Proceedings brought by Ministerio Fiscal*, ECLI:EU:C:2018:788.

TFEU also regulates more precisely the EU's competence to legislate in the field of criminal law, including the mutual recognition of judgments in criminal matters. The European Parliament and the Council, on the basis of Art. 82(2)(c) TFEU, have the competence to adopt directives establishing minimum rules which concern the rights of victims of crimes in order to facilitate the mutual recognition of judgments and judicial decisions and to establish police and judicial cooperation in criminal matters having a cross-border dimension.

Acting on the basis of this treaty provision, the European Commission adopted in 2011 the Communication on strengthening victims' rights in the EU²³ and presented a proposal for a directive establishing minimum standards on the rights, support, and protection of victims of crime,²⁴ which was adopted in 2012 as Directive 2012/29/EU.²⁵ The Commission identified five areas of victims' needs. They include: respectful treatment and recognition as victims; protection from intimidation, retaliation and further harm by the accused or suspect(s) and from harm during criminal investigations and court proceedings; support, including immediate assistance following a crime; longer-term physical and psychological assistance and practical assistance; and access to justice to ensure that victims are aware of their rights and understand them and are able to participate in proceedings and receive compensation and restoration, whether through financial damages paid by the state or by the offender or through mediation or other form of restorative justice. The directive establishes minimum standards on the rights, support and protection of victims of crime and ensures that persons who have fallen victim to a crime are recognised and treated with respect. They must also receive proper protection, support, and access to justice.

The directive considerably strengthens the rights of victims and their family members to information, support and protection. It further strengthens the victims' procedural rights in criminal proceedings. The directive also requires that EU countries ensure appropriate training on victims' needs for those officials who are likely to come into contact with them. As a result, it is now the most important act of law setting out the basic standards that regulate the situation of victims of crime in the EU. The general opinion is that the directive – even though the text has been weakened during the negotiations in comparison to the original draft – protects the rights of victims of crime better than the replaced Framework Decision 2001/220/JHA.²⁶ The standard rights,

²³ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Strengthening victims' rights in the EU, COM(2011) 274 final.

²⁴ Proposal for a Directive of the European Parliament and of the Council establishing minimum standards on the rights, support and protection of victims of crime, COM(2011) 275 final.

²⁵ Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, 2012 OJ L 315. The Directive entered into force on 15 November 2012 and had to be implemented by 16 November 2015.

²⁶ See C. Rasquete, A. Ferreira, F.M. Marques, *Why do we need concrete measures for victims at EU level? A view from the coalface*, 15 ERA Forum 119 (2014).

such as respect and recognition in criminal proceedings, safeguarding the possibility for victims to be heard during proceedings and to supply evidence, should be extended to recognize and safeguard the right to receive information, the right to compensation, mediation, and many other remedies, as well as the right to privacy, including personal data protection.

One of the objectives of the directive is to guarantee the right to respect for private and family life, while observing the right to a fair trial, guaranteed by Art. 47 of the Charter.²⁷ The right to privacy refers to protections involving access to the victims' personal information. Control over the release of personal information protects victims from being re-victimized during criminal proceedings. Protecting the privacy of a victim should be considered as one of the most important means of preventing secondary victimisation, intimidation, and retaliation. Victims' needs should be considered and addressed in a comprehensive, coordinated manner, avoiding partial or inconsistent solutions likely to give rise to secondary victimisation.²⁸ As is correctly stated in the preamble of Directive 2012/29/EU, the victim's privacy can be safeguarded through a range of measures, including non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of the victim. However, there might be cases where, exceptionally, the victim can benefit from such disclosure or even the widespread publication of information. Measures to protect the privacy and images of victims and of their family members should always be consistent with the right to a fair trial and freedom of expression, as recognised in Arts. 47 and 11 of the Charter, the meaning and scope of which should – in accordance with Art. 52(3) of the Charter – be the same as those laid down by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

Accordingly, Art. 21 of Directive 2012/29/EU requires

Member States to ensure that competent authorities may take during the criminal proceedings appropriate measures to protect the privacy, including personal characteristics^[29] of the victim taken into account in the individual assessment provided for under Article 22, and images of victims and of their family members. Furthermore, Member States shall

²⁷ See para. 66 of the preamble of Directive 2012/29/EU. For general critical remarks on the directive, especially on Art. 22, which addresses the rights of vulnerable victims, cf. R. Lang, E. Schenkel, *Directive UE no 2012/29 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité: aperçu et critique*, 583 *Revue de l'Union Européenne* 626 (2014). The authors give an overview of the directive and focus on criticism of Art. 22, which provides for specific rights for victims with special protection needs.

²⁸ For further information on the situation of victims of crime in the EU, see the following report by the Fundamental Rights Agency: *Victims of crime in the EU: the extent and nature of support for victims*, FRA 2015, available at: http://fra.europa.eu/sites/default/files/fra-2015-victims-crime-eu-support_en_0.pdf (accessed on 30 May 2019).

²⁹ According to para. 56 of the preamble to the Directive, individual assessments should take into account the personal characteristics of the victim such as his or her age, gender and gender identity or expression, ethnicity, race, religion, sexual orientation, health, disability, residence status, communication difficulties, relationship to or dependence on the offender and previous experience with crime.

ensure that competent authorities may take all lawful measures to prevent public dissemination of any information that could lead to the identification of a child victim.

The purpose of this provision was obviously to ensure that when victims have been identified as being vulnerable to further victimisation or intimidation, appropriate measures are taken to help prevent such harm. Such measures should be available throughout the criminal proceedings, whether during the initial investigative or prosecutorial phase or during the trial itself. The necessary measures will vary depending on the stage of proceedings.

As compared to the previously binding Art. 8 of framework decision 2001/220/JHA, the new provisions introduced by Directive 2012/29/EU are not significantly wider. Framework Decision 2001/220/JHA provided in Art. 8³⁰ that

each Member State shall ensure a suitable level of protection for victims and, where appropriate, their families or persons in a similar position, particularly as regards their safety and protection of their privacy, where the competent authorities consider that there is a serious risk of reprisals or firm evidence of serious intent to intrude upon their privacy.

Member States were obliged to guarantee that “it is possible to adopt, if necessary, as part of the court proceedings, appropriate measures to protect the privacy and photographic image of victims and their families or persons in a similar position.” Art. 21 of Directive 2012/29/EU is thus slightly more concrete than the replaced Art. 8 of framework decision 2001/220/JHA, which means that the EU legislation in this area has taken a step forward in comparison to the previously binding general obligation to provide “adequate protection” only.

The draft directive contained in document COM(2011)275 final was the subject of an opinion by the European Data Protection Supervisor (EDPS),³¹ who criticized the proposal and specifically the wording of Art. 23 of the draft directive (finally adopted as Art. 21).³² It stated that the only area regulated by this provision were the powers of judicial authorities at the stage of judicial proceedings, whereas privacy should be guaranteed not only in the course of judicial proceedings but also during the investigation and pre-trial stages. These comments were taken into account, and consequently the guaranteed protection is extended beyond the phase of judicial proceedings. Other comments from the EDPS however were not taken into consideration, including remarks regarding the

³⁰ This provision has been interpreted by the Court of Justice, however in different respects. In joined cases C- 483/09 *Magatte Gueye* and C-1/10 *Valentín Salmerón Sanchez* (ECR 2011, I-08263, para. 69), the Court decided that Art. 8 of the Framework Decision cannot be interpreted in such a way that it restricts the choice by Member States of the criminal penalties they establish in their domestic legal systems.

³¹ Opinion of 17 October 2011 on the legislative package on the victims of crime, including a proposal for a Directive establishing minimum standards on the rights, support and protection of the victims of crime and a proposal for a Regulation on mutual recognition of protection measures in civil matters.

³² According to draft Art. 23(1): Member States shall ensure that judicial authorities may adopt during the court proceedings, appropriate measures to protect the privacy and photographic images of victims and their family members. Art. 23(2): Member States shall encourage the media to pursue self-regulatory measures in order to protect victims’ privacy, personal integrity and personal data.

absence of any indication as to the nature of the specific measures that may be adopted by judicial authorities to enforce the victim's right to data protection.³³

There are also other acts adopted within the framework of the police and judicial cooperation in criminal matters which also, albeit indirectly, refer to the question of protection of personal data of victims of crime. For example, Directive 2011/99/EU on the European protection order³⁴ should be mentioned. This act establishes an instrument for mutual recognition of specific restrictions and prohibitions imposed upon individuals in criminal proceedings as a means of protection for other persons. These protection measures are listed in Art. 5 of the directive. If such a measure is applied while the victim already resides or intends to go to a Member State other than that in which the court issued such a protection measure, the victim can apply for a European protection order, resulting in the ability to recognize and enforce it in the Member States where the victim resides. A mutual recognition instrument, such as the European protection order, can potentially impact the fundamental rights of both the victims and the offender. These rights include the right to liberty and security, respect for private and family life, protection of personal data, freedom of movement, the right to an effective remedy and to a fair trial, and the principle of legality and proportionality of criminal offences. The impact on these rights and the proportionality of their limitation would depend on the particular type of protection measure to be defined in the legal act which would be subject to mutual recognition. For instance, Member States can impose national protection measures that can result in anything from restrictions on making phone calls to an individual to being barred from a family home. A mutual recognition instrument would result in parallel measures being applied in another Member State to which the victim moves or travels. In such a case, respect for private and family life will be particularly affected. Recognition of the protection order would also require that information on the offender was exchanged between relevant Member States' authorities, which could impact the right to protection of personal data. Such a procedure would also be connected with the flow and processing of personal data of victims of crime.

The specific legislation regulating the standing of victims of particular categories of crime, such as terrorism or organized crime, tackles the problem of the protection of victims in a very general manner. For example, Directive (EU) 2017/541 on combating terrorism³⁵ requires that Member States should adopt measures of protection, support and

³³ The example quoted by the EDPS was the recommendation of the Committee of Ministers of the Council of Europe Rec(2006)8, which states that the State shall require all agencies who have contact with victims to adopt clear standards by which they may disclose to third parties the information received from the victim or concerning them only if the victim clearly consented to its disclosure or there is a legal requirement or authorization to disclose it (*see* section 10.8).

³⁴ Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order [2011] OJ L 338.

³⁵ Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2005] OJ L 88.

assistance responding to the specific needs of victims of terrorism, in accordance with Directive 2012/29/EU. That means that privacy of victims should be addressed in the same way as in the case of Directive 2012/29/EU, which has become the main reference point. There are also two other directives which, as regards the protection of the right to privacy of victims of crime, refer directly to the standards set out in the general act on the rights of victims of crime: Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims;³⁶ and Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography.³⁷

The guarantees relating to personal data protection provided for in these acts do not exceed those established by Directive 2012/29/EU itself, and thus it can be concluded that it sets a minimum standard in this area. Despite it being a not particularly high one, the very fact of introducing a standard as such should be assessed positively.

Thus the main responsibility lies with the Member States, which must adopt measures implementing the general directions indicated in Directive 2012/29/EU. However, they must do so in accordance with the ECHR and the Charter. One should also keep in mind that – according to Art. 82(2) TFEU – each Member State can at any time adopt measures that go beyond the minimum standards as set out in Directive 2012/29/EU and guarantee a higher standard of protection for victims of crime.

4. PERSONAL DATA PROTECTION OF VICTIMS OF CRIME IN THE LAW ENFORCEMENT DIRECTIVE

The system of protection of personal data in the EU has recently undergone major changes. In 2016, two legal acts were adopted: the GDPR and the Law Enforcement Directive. The latter, i.e. Directive 2016/680/EU, lays down the rules relating to the protection of natural persons with regard to the processing of their personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security. It obliges Member States on one hand to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and on the other hand to ensure that the exchange of personal data by competent authorities within the Union – where such exchange is required by the Union or Member State law – is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. The Law Enforcement Directive replaces

³⁶ Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA [2011] OJ L101.

³⁷ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2004] OJ L 335 with corr.

the framework decision 2008/977/JHA,³⁸ which – as the act adopted before the Treaty of Lisbon within the framework of intergovernmental cooperation – was not fully successful. Its weakness was first of all the limited scope of its application, restricted to the transborder transfer of data, and secondly the lack of an enforcement procedure and sanctions for improper implementation.

The adoption of legal acts for the purpose of data protection in instances where data are processed by competent authorities in situations connected with combating crime creates the possibility of re-thinking the framework for the protection of crime victims, particularly in the sphere of their right to privacy. The necessity to give due consideration to the rights of victims of crime was recognized as early as in 2010,³⁹ when the Commission issued its Communication on a comprehensive approach on personal data protection in the EU⁴⁰ and started the intensive process of the general reform of the data protection system in the EU. In para. 2.3 of the Communication, which was dedicated to the revision of data protection rules in the area of police and judicial cooperation in criminal matters, the Commission found that one of the shortcomings of framework decision 2008/977/JHA was the lack of a provision that would permit making a distinction between different categories of various data subjects, such as perpetrators, victims, witnesses, experts and others. Furthermore, the framework decision failed to establish separate safeguards dedicated to the protection of persons other than the perpetrator.

In other words, the Commission's message was that detailed provisions addressing the specific nature of law enforcement measures should be laid down, including the distinction between different categories of data subjects, such as victims, witnesses or suspects. The rights of these different groups may vary in order to ensure on the one hand a high level of data protection and, on the other hand, to facilitate the exchange of data between the relevant authorities. This means that the right balance must be attained between protecting fundamental rights and ensuring security. It should be borne in mind that both the ECHR and the Charter allow for limits on the right to privacy – including the right to protection of personal data – if certain conditions are fulfilled.

The outcome of these considerations of the Commission was reflected in the proposed Art. 5 of the draft directive on data protection for law enforcement purposes,⁴¹ subsequently adopted as Art. 6 of the Law Enforcement Directive. This provision requires distinguishing between different categories of data subjects. According to Art. 6 of the Law Enforcement Directive, Member States shall require the controller – where

³⁸ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350.

³⁹ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union, COM(2010)609. For further information on this Communication, see also R. Jay, *Data protection. Law and practice*, Sweet & Maxwell, London: 2012, pp. 48-50.

⁴⁰ COM(2012)9 final.

⁴¹ COM (2012)10 final.

applicable and as far as possible – to make a clear distinction between personal data of different categories of data subjects, such as: (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; (b) persons convicted of a criminal offence; (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and (d) other parties to a criminal offence. The EU legislation has not, however, set forth the particular method for enforcing this distinction. Moreover, the enforceability of the provision is restricted by the additional condition, expressed as “where applicable and as far as possible”, which definitely softens the obligation imposed on the Member States. According to Art. 29 of the Working Party, “the obligatory distinctions must lead to a gradual regime of different time frames to be envisaged in relation to the different categories of data subjects.”⁴² This can be seen as establishing an overall framework for how to differentiate and how to provide a special position to crime victims.

Interestingly enough, according to the Commission this is a novelty – such an approach has not been taken in any of the provisions of Directive 95/46/EC or Framework Decision 2008/977/JHA, even though it is endorsed in Recommendation R(87)15 of the Committee of Ministers of the Council of Europe concerning the use of personal data in the police sector.⁴³ The Commission’s assessment in this regard is, however, only partially true, as the same Recommendation R(87)15 does not provide for such an obligation. It only states, in section 3.2, that as far as possible the different categories of data stored should be distinguished in accordance with their degree of accuracy and reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments. Therefore, it requires the differentiation of data only with respect to their reliability.

The key problem relating to this provision is its implementation. It raises doubts, in particular because of its lack of precision in the description of the method and consequences of the proposed distinction. Another issue that may be considered problematic is the use of the phrase “as far as possible”, which leaves a large margin of discretion to the Member States. It is worth noting that a similar distinction with regard to the scope and collection and processing of personal data depending on the category of data subjects is also the subject of a Europol regulation⁴⁴ as well as of regulation 1725/2018.⁴⁵ In the case of Europol, not only is it necessary to distinguish the data, but

⁴² Art. 29 of the Working Party, WP 258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680).

⁴³ Recommendation R(87)15 regulating the use of personal data in the police sector; available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf (accessed 30 May 2019), p. 68.

⁴⁴ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L 135.

⁴⁵ Cf. Art. 73 of the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by

also – according to Art. 30 – there are limitations on the legal processing of personal data of victims. Processing of personal data with respect to victims of a criminal offence, witnesses, or other persons who can provide information concerning criminal offences, or with respect to persons under the age of 18, shall be allowed only if it is strictly necessary and proportionate for preventing or combating a crime that falls within Europol's objectives. Moreover, if personal data of victims are stored for a period exceeding five years, the European Data Protection Supervisor shall be informed accordingly. These rules can serve as an example for the national legislator on how to implement the very imprecise Art. 6 of the Law Enforcement Directive.

Data recognition and the separate treatment of personal details of crime victims from the data of perpetrators of crimes is not the only way to guarantee the rights of victims of crime. In addition to the special provision that requires differentiation in the treatment of personal data of victims of crime, the Law Enforcement Directive also contains general provisions governing the processing of personal data for the purpose of combating crime. These provisions also form the basis for taking into account the special position of victims of crimes when implementing the provisions of the directive into national law. According to the preamble (recital 20), the directive does not preclude Member States from specifying processing operations and procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in the records relating to criminal proceedings. Recital 80 confirms that the directive applies also to the activities of national courts and other judicial authorities. This means that the general rules on the processing of personal data set out in the Law Enforcement Directive must also be applied to court proceedings. Member States may set the rules for data processing in national court proceedings, but these rules have to comply with the provisions of the directive.

In connection with the above, when developing a harmonised approach for identifying victims and the subsequent processing their data, it is necessary to recognise the wide variety of possible situations. The Law Enforcement Directive must regulate the principles in a general way – it is the role of the Member States to clarify them so as to safeguard on one hand the rights of victims of crimes in accordance with Directive 2016/680/EU and 2012/29/EU, but also to ensure effective preparatory and judicial proceedings. The basic principles are defined in Art. 4 of the law enforcement directive (Directive 2016/680/EU). The Member States shall provide for personal data to be processed not only lawfully and fairly, but above all the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed, as well as accurate and, where necessary, kept up to date.

The term “adequate” indicates that data to be processed should be sufficient to fulfil the purpose of its processing.⁴⁶ The detection of victims is a crucial element in

the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295.

⁴⁶ See also The Europol Joint Supervisory Body Report, *Victims of trafficking in human beings – a data protection perspective*, available at: <https://bit.ly/2JmPF9b> (accessed 30 May 2019).

the fight against crime. Identifying victims and the processing of their personal data must be regarded as adequate, not only for operational purposes, but also for ensuring that the victims may profit from the safeguards they are entitled to. For example, the right to information (Art. 13 of the law enforcement directive) may be restricted in order to protect the rights and freedoms of others. This means that the participants' right to be informed during the criminal proceedings may be restricted if necessary to protect the victim. As is correctly identified in the reports, the principle of adequacy should lead to an analysis of what personal data is truly needed to investigate specific cases. The principle of adequacy is also an essential element of the lawful, effective, and accountable activities of law enforcement authorities.⁴⁷

It seems to be quite obvious that investigations by police and judicial authorities are generally focussed on the suspects of crime and finding evidence. When a victim's data are assessed as necessary for detecting and investigating crimes, these data will also be processed and used in the further proceeding. The accuracy principle should be applied taking into account the nature and purpose of the processing concerned; however the specificity of the proceedings does not always allow for processing fully accurate data. In some cases, a victim-centred approach should be introduced, which could be necessary to assess whether the data processing and investigation activities should be further conditioned. To make such an assessment it would be necessary to distinguish between the different phases in a law enforcement proceeding, such as detection, investigation, and prosecution. Application of the principle of accuracy should be directly linked to the data processed in these different phases of an enforcement proceeding. Whether something is accurate depends on the stage of the proceeding – what seems to be accurate at a certain moment might be inconsistent with the findings in the further stages of an investigation. Inaccurate data – even if necessary to be processed in the first phase – might create serious problems in the later phases of an investigation and prosecution. All activities aimed at combating crime, ranging from specific legislation to policies and guidelines, will lead to data processing. Without the processing of personal data of victims, fighting crime cannot be done effectively, which in turn would prevent victims from receiving the necessary protection and assistance.

At this point, it should be emphasized that the Law Enforcement Directive – although general in its content – clearly offers possibilities to ensure the special position of victims of crime. Meanwhile, the new law in Poland – the Act adopted on 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime⁴⁸ – does not address the issue correctly. First of all, Art. 19 of the Act repeats the wording of Art. 6 of the directive. The Polish legislator did not manage to adapt this provision to the national situation and did not propose anything concrete, leaving the decision to the competent authorities applying the law. Secondly, according to the final provisions (Art. 102(4)), adaptation of the principles of

⁴⁷ *Ibidem*, p. 13.

⁴⁸ O.J. 2019, item 125.

processing information and personal data in data files created before the date of entry into force of the law to the requirements referred to in Art. 19 shall take place no later than on 6 May 2023.⁴⁹ It should be added that this problem has also not been solved properly in either the British law nor in the German legislation.⁵⁰ However, this is not an excuse for a lack of effort on the part of the national legislator to properly implement the requirements contained in the directive. Thirdly, a significant problem concerns the exemption introduced in Art. 3(1). Pursuant to this provision, the Act does not apply to personal data processed in files kept on the basis of, among others, the provisions of the Code of Penal Procedure. This means that, in principle, no procedural provisions will be amended, or even analysed, for their compliance with the requirements of the directive. It should be noted that the directive itself did not provide for such an exemption.⁵¹ Therefore, the Law Enforcement Directive, by failing to make it fully clear and precise what are the consequences of differentiation between the personal data of suspects and other persons (in particular victims of crime), can still be wrongly implemented by the Member States by excluding the application of the Act to court procedures. As regards the rights of victims of crimes in the context of the processing of their personal data in Polish law, nothing has changed with the entry into force of the new provisions. This does not mean that the rights of victims of crime are not properly guaranteed in the Polish criminal process in the context of protection of their personal data. This does mean, however, that the Polish legislator made no effort to analyse this situation.

This is clearly illustrated also by the fact that there are no direct provisions which would raise the standard of protection of victims' data in the Act of 28 November 2014 on protection and assistance for the victim and the witness.⁵² These provisions not only do not really concern the protection of victims' personal data, but additionally create some threats. There are no regulations that would solve the seemingly trivial issue of the location of documentation regarding the application of aid and protection measures. For obvious reasons, such documentation cannot be an integral part of the case file, neither in the preparatory nor in the judicial proceedings. If that were the case, the parties and other persons⁵³ could easily read such documentation, which in turn it would not only completely disregard the *ratio legis* of the solution, but also the reasonableness of using such measures at all. Therefore, it is *de facto* the prosecutor and the court that take the decision, where it is registered and where such documentation regarding the application of protection measures is located.. This is only an example of provisions that should be subject to a broader analysis in the context of the implementation of the

⁴⁹ This is contrary to Art. 63 of Directive 2016/680.

⁵⁰ Cf. Part 3, chapter 2, rule 38 of the British Data Protection Act 2018 and Section 72 of the German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June 2017.

⁵¹ See the opinion of the Ministry of Foreign Affairs of 5 October 2018, attached to the Sejm's paper no. 2989, available at: <https://bit.ly/30JmM3W> (accessed on 30 May 2019).

⁵² O.J. 2015, item 21.

⁵³ Only using the powers specified in Art. 156 of the Code of Criminal Procedure, but also pursuant to Art. 321 of the Code of Criminal Procedure.

Law Enforcement Directive into the Polish legal order. It is only meant to illustrate the complexity and multiplicity of the problems.

Nevertheless, the introduction of new provisions in the Law Enforcement Directive is a significant step forward, since it is generally meant to apply to police and judicial cooperation in criminal matters and cover domestic processes and all data transfers, introducing harmonised criteria for necessary limitations to an individual's rights. It should be expected that it is very soon the task of the Court of Justice to interpret the provisions of the directives, not only by answering preliminary questions from the national courts, but also by ruling on the basis of the infringement procedure in cases of improper implementation.

5. ARE THE PERSONAL DATA OF VICTIMS OF CRIME PROPERLY PROTECTED? SOME ILLUSTRATIONS

In order to illustrate the necessity to protect personal data of victims of crime, reference should be made to several specific examples of practices which have been discussed in Poland and reflected in the decisions of the courts or the data protection supervisory organ – the General Inspector for Personal Data Protection.⁵⁴ The reason for these discussions was the need to balance certain values, especially the right to data protection versus the right to information as well as the transparency of judicial proceedings and access to public information.

One example of a situation in which these rights should be weighed is the issue of disclosing victims' names on the daily case lists on the doors of courtrooms. The question of court case lists was previously governed by the Order of the Minister of Justice of 12 December 2003.⁵⁵ Under paras. 23.1 and 2 of the Order, in essence the Secretariat of a Court was required to draw up a list of court hearings and meetings containing the names of the judges, the case reference number, the names of the parties and other persons summoned as well as other information. Such a list was intended for the information of the parties and third parties wishing to take part in the hearing. Although the principle of transparency stems from Art. 45(1) of the Constitution of the Republic of Poland, it is not an absolute right and can be limited for reasons of morality, State security and public order, or for the protection of the private life of the parties or other important personal interests. The above-mentioned regulation on court case lists gave rise to objections from some NGOs, including the Helsinki Foundation for Human Rights, which emphasized the need for change, stressing the problem of stigmatisation of the parties.⁵⁶ After a thorough analysis, taking into account the various interests the

⁵⁴ From 25 May 2018 the supervisory organ in Poland is called Prezes Urzędu Ochrony Danych Osobych – The President of the Personal Data Protection Office.

⁵⁵ Order of the Minister of Justice on the organization and scope of activities of courts and other departments of the administration of justice (OJ of Minister of Justice No. 5, item 22, as amended).

⁵⁶ See Letter from the Helsinki Foundation for Human Rights to the General Inspector for Personal Data of 22 October 2012, available at: <https://bit.ly/3048Lgz> (accessed 30 May 2019).

Minister of Justice undertook legislative work aimed at amending this regulation, the final outcome of which is that sensitive data are no longer available on the daily court lists.⁵⁷ Rules of procedure of courts had to be adjusted appropriately and, according to para. 67a(2) it is prescribed that while the parties to the proceedings, as well as witnesses and experts can, in principle, be identified on the daily court list, it is possible that in certain categories of cases some data will be anonymized in order to prevent further victimisation. It seems that these new rules – although still not regulated by an act adopted by the parliament – are generally in accordance with both above-mentioned directives and do not require any further change.

Another interesting example of problems concerning the personal data of victims of crime would be the issue of publishing judgments on websites or in various electronic databases. Such judgments include the personal data of victims as well as of witnesses and other people involved in the proceeding. Similarly to the case of court lists, this context requires the balancing of various interests, such as the right to personal data protection versus free access to public information, and can give rise to the need to anonymise certain data.⁵⁸ The names of the parties and other participants in the proceedings, as well as their nicknames, should be removed from the judgment, leaving only the first letter of each name.

The problem of the protection of victims of crime in connection with personal data is also present in cases related to the publication of data on sexual offenders in a register maintained pursuant to the Act of 13 May 2016 on counteracting threats of sexual offenses.⁵⁹ The full and unambiguous identification of a person covered by the register of sexual offenders, which is publicly accessible, leads to a situation whereby the name (or names), dates of birth, and also photographs of the perpetrators can eventually lead to identification of a perpetrator's victims, especially when the victim is a family member of the perpetrator. This may result in their unacceptable victimisation.⁶⁰ According to the facts of a case reported to the Ombudsman, the inhabitants of one of small villages in Poland published on a social network a photo and data downloaded from the public

⁵⁷ For more information on this issue, *see* generally the answer of the Undersecretary of State for the Ministry of Justice to the interpellation no. 26750 on the protection of victims of sexual offences; available at: <http://sejm.gov.pl/Sejm7.nsf/InterpelacjaTresc.xsp?key=79D4F51A>. *See* also information on the webpage of the General Inspector for Data Protection at: http://www.giodo.gov.pl/347/id_art/1341/j/pl/ (both accessed 30 May 2019).

⁵⁸ In 2012 the President of the Supreme Court of Poland issued an ordinance that regulated the issue of the anonymisation of data in decisions published by the Supreme Court. *Cf.* Decree No. 11/2012 of 10 April 2012, available at: http://www.sn.pl/Aktualnosci/SiteAssets/Lists/Aktualnosci/NewForm/Zarz_PP_SN_11_2012.pdf. In 2018 the Court of Justice also decided, in all requests for preliminary rulings brought after 1 July 2018, to replace, in all its public documents, the name of natural persons involved in the case by initials. Similarly, any additional element likely to permit the identification of the persons concerned will be removed, *see* <https://bit.ly/2KwoyWE> (both accessed 30 May 2019).

⁵⁹ Ustawa z 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym [Act on combatting threats of sexually motivated crimes], O.J. 2016, item 862 as amended.

⁶⁰ *See* the position of the Polish Commissioner for Human Rights (available at: <https://bit.ly/2Lx42PT>, accessed 30 May 2019) and the case which is described therein.

register of sexual offenders. The offender was well known to the inhabitants of the village. Due to the data from the register it became clear to everybody that his children were his victims. Their data was also indirectly revealed. The Minister of Justice unfortunately has not yet responded to any document presented by the Ombudsman in this matter. The question is whether this should be understood as expressing no inclination or will to make any changes in this act. This situation is obviously contrary to the obligations imposed on the Member States by both Directives 2012/29/EU and 2016/680/EU.

CONCLUSIONS

The EU's legal obligation to ensure that victims of crime are guaranteed the right to protection of their personal data is now an obligation stemming from primary EU law. However, the right to personal data protection in the case of criminal proceedings, which encompasses the victims of crime, can be legally limited. The question is whether Member States, when implementing the required secondary legislation, will fully obey the instructions coming from the jurisprudence of the Court of Justice in this respect. Some examples clearly demonstrate that this might be problematic.

Secondly, the basic standard for the protection of personal data of victims of crime in the EU Member States is currently provided by Directives 2016/680/EU and 2012/29/EU, which correspond with each other. This standard is not satisfactory taking into account that the implementation of one directive was processed independently from the implementation of the other. However, it should be noted that both acts allow for the incorporation of general EU standards into domestic legislation. Member States are also allowed to consider the possibility of strengthening guarantees beyond the strict requirements of the directives. At the moment it seems, however, that some Member States are more interested in limiting the scope of application of these provisions than in their proper implementation, particularly with reference to the standards of human rights protection.

Thirdly, it should be stressed that the necessity to ensure the protection of victims' privacy, especially of those who belong to the category of vulnerable victims, remains insufficiently appreciated. The right to privacy of a victim is regulated in a very general manner, leaving too much space for the national legislator and thus creating the possibility of skewing the balance by giving more weight to security as a legal justification, to the detriment of fundamental rights. Also in the Law Enforcement Directive the needs of victims of crime are too vaguely recognized. There are insufficient means for ensuring a more stringent protection of data in their processing for persons who are not suspects, accused, or convicted. The directive does not specify when such data should be protected, or what the consequences of the introduced distinction should be.