

Protection of personal data of individuals in insolvency proceedings

Daryna Shykeriava*

Mykolas Romeris University, Vilnius, Lithuania; ORCID: 0009-0004-3581-3578

Abstract

Insolvency proceedings have a public nature and require disclosure of massive amounts of personal information. At the same time, each individual has a right to the protection of personal information. Publicly available information about insolvency proceedings may bar the 'fresh start' that an insolvent person reasonably expects. This article analyses the protection of personal data in insolvency proceedings of individuals. It is construed of three parts, where the first part analyses the protection of personal data as a fundamental human right; the second part deals with possibilities to find a balance between publicity of insolvency proceedings and protection of the right to personal information; and the third part compares Ukraine's and European Union's legal regimes on treatment of personal data in course of debt discharge proceeding. The problem was analysed using analytical, structural-functional, synthesis and comparison methods.

Keywords

Fresh start • GDPR • insolvency proceeding • the Law of Ukraine on the Protection of Personal Data

INTRODUCTION

Business initiative has always been a cornerstone of economic relations, aimed to serve the interests of society and the person behind these initiatives (European Commission, 2008). Regardless of its type, the entrepreneurship activity as a system cannot exist without loan relationships, especially important for business growth. However, entrepreneurship activities are coupled with risks of the failure to pay debts due, resulting in insolvency. In this situation, a State has to intervene and 'give a hand' to the business in distress, providing a possibility for a discharge of debt procedure. The aim of discharge of debt procedure is to grant a full discharge of debt (Directive (EU) 2019/1023, Article 1) and mitigate the negative effects of over-indebtedness (Recital 73). On the contrary, the conduct of insolvency proceedings inevitably requires collecting and processing of personal data of an insolvent entrepreneur (Article 29(1)), which is vital for the proper exercise of the rights and functions of the participants in this procedure (Bolzanus and Jokubauskas, 2025). The Restructuring and Insolvency Directive (hereinafter – Directive) harmonises certain elements of the discharge procedure in the European Union (EU) law. Although collection of personal information during insolvency

proceedings poses reasonable questions of whether it is (in)compatible with the standards of protection of personal data in the EU, the Directive does not address this issue, warranting recourse to other legal instruments.

The General Data Protection Regulation (GDPR) establishes the rules on treatment of personal information in the EU. The GDPR has been regulating personal data circulation for almost 9 years, seeking to ensure compliance with national laws on data protection across all the EU Member States. The treatment of personal data is based on the main principles established in Article 5 of the GDPR. One of such main principles is the data minimisation principle, which allows only adequate, relevant, and limited to the purposes of processing of personal data (Article 5(1)(c)). However, the GDPR is silent as well regarding the processing of personal data in the course of discharge of debt procedure of insolvent entrepreneurs. This leads to the question of whether the overarching nature of the GDPR covers the treatment of personal data during insolvency proceedings? Are the rules on the discharge procedure (in)compatible with the requirements for the lawful processing of personal data in the GDPR?

As the insolvency proceedings have the public nature (Regulation (EU) 2015/848 on insolvency proceedings European Insolvency Regulation (EIR), Article 1(1)), the discharge procedure requires the collection and publication

* Corresponding author: dashykeriava@stud.mruni.eu

Open Access. © 2025 Daryna Shykeriava, published by Sciendo

 This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

of private information (Article 24(1)) in order to satisfy the interests of creditors and ultimate purposes of insolvency proceedings (Recital 78). While it limits the protection of private information, it also may contradict the fundamental nature of this right. Nevertheless, absolute protection of the right to private information would intervene with the interests involved in insolvency proceedings. The existing collision between fundamental human rights and public interests in insolvency proceeding justifies the relevance of the topic. Recently, the Court of Justice of the European Union (CJEU) has dealt with this problem in the *Schufa* case, where a private creditor assessment institution refused to delete personal data regarding an individual's discharge of debts, which was kept longer than in the public register (CJEU UF (C 26/22), AB (C 64/2) v Schufa, 2024). The CJEU has ruled that such practices must be precluded when they override the legitimate purposes of data storage (para. 114(3)). Nevertheless, the need to ensure personal data protection in discharge proceedings without neglecting the public interest involved creates scientific demand for further research on this topic.

Information about insolvency proceedings of natural persons may have a negative impact on the reputation of a person when it discloses a failure to comply with financial obligations (Bolzanus and Jokubauskas, 2025). The possibility for an individual in distress to improve their financial situation prevents the negative effects of insolvency on society as a whole, such as social exclusion, health and social problems and an expanding grey sector of the economy (European Court of Human Rights [ECHR], *Bäck v. Finland*, 2004). Therefore, an insolvent individual deserves to get a chance to start all over again with the possibility to pursue business activities and consume without the burden of pre-bankruptcy debts after the discharge is granted (Bolzanus and Jokubauskas, 2025). In this situation, information concerning the failure to perform financial obligation may be a hurdle for an insolvent entrepreneur to enjoy a fresh start (a second chance), which is granted after the discharge procedure.

Being public and collective in nature (Regulation (EU) 2015/848, Article 1(1)), insolvency proceedings require disclosure of personal information in order to allow creditors to become aware of the proceedings and to lodge their claims (Recital 12). The public character of insolvency proceedings is ensured by establishment and maintenance of one or several registers in which information concerning insolvency proceedings is published (Article 24(1)). While private agencies also collect this information to disclose it upon the request of credit institutions, the question arises: to what extent does the public character of insolvency proceedings limit the protection of personal information? Whether EU legal framework has effective regulation to balance the interests? Is it possible that some interests prevail over others in order to promote harmonisation?

To reveal problems related to the processing of personal information during and after the discharge procedure, the article consists of three parts. Namely, first, it deals with the right to protection of personal data as a fundamental human right; second, it focuses on the possible ways to ensure a balance between the publicity of the discharge procedure as the pivotal element and effectiveness of the 'fresh start' when the discharge procedure is completed and, third, it deals with the recent legislative initiatives in Ukraine related to the protection of private information in discharge proceeding and analyses whether it is compatible with the standards of the protection of personal data in EU law.

RESEARCH RESULTS AND DISCUSSION

Protection of personal data as a fundamental human right

Personal data is one of the biggest assets that any person possesses (Birch et al., 2021) since it is the key element of self-identification. Unlawful processing of personal information leads to underestimation of its true value and great impact on an individual's life. Protection of personal data has notably been connected with freedom, such as the freedom to establish individual paths in life and the power to resist interferences with this freedom as well as the protection of freedom itself (González Fuster, 2014a,b). It is an integral part of human dignity, which has become particularly fragile in the pool of global information society and therefore requires a strong level of protection (European Commission, 2017).

The needs to protect personal data are reflected in the EU law. The Charter of Fundamental Rights of the European Union (hereinafter – Charter) establishes the protection of fundamental rights of each person in order to create an area of freedom, security and justice. The right to protection of personal data is reinforced in the Charter (Article 8(1)) and secured by the principles of personal data processing (Regulation (EU) 2016/679, Article 5). Rendering the personal data protection as a fundamental right constitutes a significant enhancement of the level of protection effectively granted to individuals throughout the EU (González Fuster and Gellert, 2012).

Recognition of the protection of personal data contributes to the aims of the Charter to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible (European Union, 2012). This approach is reflected in the legislation of the EU Member States regarding the protection of personal data, which is regarded as being of constitutional or equivalent importance (González Fuster, 2014a,b).

The CJEU recognised that the right to protection of personal information is a general principle of EU law (CJEU Stauber,

Case C-29/69, 1969). Since the right to data protection is a fundamental right in the EU, it has the following characteristics: it is inherent, basic, imprescriptible, indivisible, universal and interdependent (Rubin, 2003). The inalienability of the right to protection of personal information means that it cannot be taken away, even if it is subject to violation. First, it cannot be rightfully taken away from someone, and second, it cannot be given away, transferred or forfeited (Custers and Malgieri, 2022).

Personal data are elements of self-identification, which are indispensable to human nature and have the status of a fundamental human right, formalised in the Charter and upheld by the CJEU. The right to protection of personal data is granted absolute protection as the right of constitutional or equivalent significance. Its inalienable nature justifies a strong level of protection from any sort of violation. The debt discharge procedure requires disclosure of the information, which identifies a debtor, such as full name, registration number and address, with the aim of determining the existence of the grounds for opening the discharge procedure (Bolzas and Jokubauskas, 2025). Personal data that are sensitive in relation to fundamental rights and freedoms merit specific protection since the context of their processing could create significant risks to fundamental rights and freedoms (Regulation (EU) 2016/679, Recital 51). When sensitive information about a debtor or even their family members becomes publicly available, it creates a direct clash between fundamental human rights and discharge proceedings, threatening the security of the right to protection of personal information.

BALANCE BETWEEN PUBLICITY OF DISCHARGE PROCEDURE AND PROTECTION OF PERSONAL INFORMATION OF A DEBTOR

Processing of personal data in the discharge procedure involves different interests. On the one hand, the public nature of the proceeding requires that information regarding insolvency proceedings to be openly accessible (Regulation (EU) 2015/848, Recital 76). On the other hand, this information consists of personal data, access to which may be restricted. At the same time, during and after the discharge procedure, the potential creditors need to assess the creditworthiness of an individual before entering into a contract, while a person, discharged from debts, reasonably expects to start economic activity again. When creditors are granted unlimited access to personal information, they intervene with the right to protection of personal information and *vice versa* – when protection of personal information restricts any incentives to verify the creditworthiness of a client – it contradicts the principle of transparency of insolvency proceedings. It is impossible to

satisfy to the maximum extent the interests of one side without violating the rights of the other side. Therefore, there is a need to find a balance between transparency and sufficient security of personal information.

The GDPR imposes obligations towards States regarding the lawful processing of personal data. The main elements of the lawful processing of personal data are the consent of the data subject, the necessity for compliance with the legal obligation to which the controller is subject (Regulation (EU) 2016/679, Recital 40), including the entities to, the purposes for which the personal data may be disclosed, the purpose limitation as well as storage periods (Article 6(3)). Derogations from the general prohibition for processing the special categories of personal data are possible when the data subject gives explicit consent or in respect of processing carried out in the course of legitimate activities with the purpose of permitting the exercise of fundamental freedoms (Recital 51).

To ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, two points shall be taken into account: any link between legitimate purposes and the purposes of the intended further processing as well as the reasonable expectations of data subjects based on their relationship with the controller (Recital 50). The interests and fundamental rights of the data subject override the interest of the data controller when data subjects do not reasonably expect further processing (Recital 47).

The risk to the rights and freedoms of natural persons may result from personal data processing, which could lead to physical, material or non-material damage (Recital 75). To mitigate these risks, GDPR establishes exceptions to the processing when lawful interests are overridden by the fundamental rights and freedoms of the data subject, which require the protection of personal data (Article 6(1)(f)). This provision is secured by the right to rectification, according to which the controller of the information shall rectify the personal data, which is inaccurate (Article 16) or has been unlawfully processed (Article 17(1)(d)).

While GDPR lays down general rules relating to the processing of personal data (Regulation (EU) 2015/848, Article 1(1)) establishes rules governing public collective cross-border proceedings for the purpose of rescue, adjustment of debt, reorganisation or liquidation (Article 1(1)). The EIR also applies to the discharge procedure provided it falls under the list of national insolvency proceedings under Annex A of the EIR. It is not to mention that the EIR and the Directive should be compatible (Recital 11, 12).

The EIR integrates insolvency proceedings and requirements for its publicity under Article 1(1), providing requirements for the disclosure of personal information in the course of discharge proceedings. Accordingly, each State must

establish one or several registers for publication of information in a timely manner (Article 24) and must be the exclusive securer of personal data processed (Article 79(2)) in order to ensure a degree of transparency and foreseeability in financial transactions (Opinion of Advocate General Pikamäe, C-26/22 and C-64/22, 2023, para. 31) as well as to improve the provision of information to relevant creditors and courts, preventing the opening of parallel insolvency proceedings (Regulation (EU) 2015/848, Recital 76). Individual's name, registration number and postal address, as well as the place and date of birth, shall be published (Article 24(2)(f)) alongside the obligation to inform the data subjects about the accessibility period of the personal data stored in insolvency registers in order to ensure their rights to the erasure of data (Article 79(5)).

The activity of registers shall comply with the principle of proportionality, as a general principle of EU law, which requires that measures implemented by acts of the EU are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it (CJEU, Joined Cases C-92/09 and C-93/09, 2009, para. 74). The way in which the data are managed and recorded must respect data subject's interests since the information concerning an individual's economic situation is sensitive and requires respect for the right to protection of personal data and for private life (Opinion of Advocate General Pikamäe, C-26/22 and C-64/22, 2023, para. 32).

The CJEU has recently dealt with this issue during the proceeding between two individuals, who were granted early discharge from debts on the one side, and a private credit information agency 'Schufa' on the other side (CJEU, UF (C 26/22), AB (C 64/2) v Schufa, 2024). UF and AB were German citizens who were granted early discharge from debts by judicial decision, which should be discontinued from the registers after 6 months as established by German legislation (para. 25). At the same time, private credit information agency 'Schufa', which collects information from public registers in its own databases, stores this information for 3 years as approved by the competent supervisory authority (para. 26). This period significantly exceeds the period, established by German law, raising problematic questions of the lawfulness of the storage of personal data from public registers by credit information agencies for a longer period of time as well as priority of interests in case of the clash between the right to protection of personal information and the requirement of transparency.

When UF and AB requested the erasure of the information, the credit agency refused to do so, arguing compliance with the GDPR (para. 27). Further complaints to the competent supervisory authority were also declined and the judicial proceeding had started, as a result of which the court referred

to the CJEU the question of lawfulness of storage of personal data by private agencies (paras. 28-38).

The CJEU set out three cumulative conditions for the processing of personal data to be lawful. Namely, the court found that in such cases, processing of personal data is lawful if (i) it pursues a legitimate interest by the data controller or by a third party, (ii) personal data is processed for the legitimate interests and (iii) the interests or freedoms and fundamental rights of the person concerned by the data protection do not take precedence (para. 75).

While the processing of personal data serves credit agencies' economic interests, that processing also serves the legitimate interest of their contractual partners in assessing credit worthiness of the individuals (para. 83) as well as ensuring the proper functioning of the credit system as a whole (para. 86). However, the achievement of their legitimate interests must commensurate with fundamental rights and freedoms of the data subject, particularly in the light of the reasonable expectations, the scale of the processing and its impact on a person (para. 87).

The CJEU highlighted that the purpose for the collecting of information in public insolvency registers is to improve the provision of information to creditors, and the time limit for the retention of such data must be set in compliance with the GDPR (para. 96). Therefore, the 6-month period established by German legislature is compatible with this requirement, and after its expiry, the rights and interests of the data subject take precedence over those of the public to have access to that information (para. 97).

Moreover, parallel storage of personal data in the databases of the credit agencies during the 6-month period constitutes interference with fundamental human rights since it reinforces the violation of the individual's right to privacy (para. 100). The CJEU reinforced the individuals' right to erasure of personal data kept in the registers for the period longer than it is kept in the public registers, justified by the credit agencies' failure to provide proofs of lawful processing of personal data (paras. 107-113).

Though in the judgement, the CJEU did not focus on the impact of the processing of personal data for a fresh start (a second chance), and the Advocate General, in this case, highlighted the importance of the attainment of this goal. He mentioned that the discharge from remaining debts is intended to allow the person who benefits from it to re-enter economic life, which may be jeopardised by retaining the data after they have been deleted from the public insolvency register, given its negative impact on the data subject's creditworthiness (Opinion of Advocate General Pikamäe, C-26/22 and C-64/22, 2023, para. 75).

Information about personal insolvency proceedings is processed by private institutions in order to minimise risks

for business partners when engaging in relationships with former debtors. While disclosure of the information ensures transparency, it prevents individuals from making a fresh start, accomplishing it with the shadow of prior financial failures. Each State processes personal data in public registers for a defined period of time. This period serves the need for transparency and suffices to satisfy the interests involved. To protect fundamental human rights and to provide indeed a fresh start, it is crucial to comply with data protection provisions and require private institutions to remove information about personal insolvency proceedings when processing exceeds the time limits established by the GDPR. This solution contradicts the absolute protection of personal information and restricts total transparency seeking to find a proper balance and satisfy both interests without advantage to either of them.

ANALYSIS OF UKRAINE'S APPROACH ON PROCESSING OF PERSONAL DATA IN THE COURSE OF INSOLVENCY PROCEEDINGS

Ukraine has embarked on the path of bringing its legislation in line with European standards (Ukraine, 1996). Association Agreement between the EU and Ukraine establishes the basis for cooperation in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards (European Union & Ukraine, 2014). This includes alignment of processing of personal data in the course of the discharge procedure.

For the purposes of harmonisation of national legislation with European standards, Ukrainian parliament adopted the new Draft Law on Protection of Personal Data, purporting to strengthen the personal data protection (Ukraine, 2022). It provides alignment of the personal data protection terminology with international standards; details formulation of the principles of personal data processing; clears formulation of the grounds for data processing; details requirements for consent to personal data processing as well as extends the rights of data subjects and mechanisms for their exercise, along with increased fines for violations of protection of personal data (Ukraine, 2022).

However, currently, the processing of personal data is regulated by the Law of Ukraine on the Protection of Personal Data (LUPPD), which governs the protection and processing of personal data and is aimed at protecting fundamental human and civil rights and freedoms (Ukraine, 2010, Article 1). The LUPPD establishes requirements for personal data processing; rights of personal data subjects; grounds for personal data processing; procedure for the main processes of personal data processing (collection, use, accumulation

and storage, distribution, and deletion) and procedure for processing personal data, the processing of which poses a particular risk to the rights and freedoms of personal data subjects, etc (Bratasyuk, 2023). The LUPPD grants the right to access, modify or erase personal data as well as to get information about the processing of personal data given its inalienable and inviolable nature (Ukraine, 2010, Article 8). Consent is the requirement for processing of personal data along with the provision of the best interests of the data subject (Article 11).

State Bankruptcy Authority is a national body which forms and maintains the Unified Register of Debtors in respect of which bankruptcy proceedings have been opened (Ukraine, 2019, Article 3). In addition, the information regarding the initiation of the bankruptcy proceedings is published on the official web portal of the Register of Court Decisions of Ukraine, the official website of the State Bankruptcy Authority as well as in any other way not prohibited by law (Article 39(9)).

Information about the debtor shall be excluded from the Unified Register of Debtors upon the fact of the absence of debts and termination of the enforcement proceeding (Ukraine, 2016, Article 9(7)). Nevertheless, this provision does not regulate the storage period for other registers of private information. Data from the registers can be deleted upon the expiry of the data storage period determined by the consent of the data subject, termination of legal relations between the data subject and the processor of personal data, or upon the court decision (Ukraine, 2010, Article 15(2)).

The Constitution of Ukraine establishes that consent is the primary basis for the collection, storage, use and distribution of personal information (Ukraine, 1996, Article 32). Ukraine's legal framework recognises the right to protection of personal information as a fundamental human right and establishes similar provisions regarding the protection of personal data as in the EU. Similarly, Ukraine's and EU's legislation on data protection establishes consent of the data subject as the main ground for the processing of personal data. Nevertheless, further processing in the course of insolvency proceedings varies. While in Ukraine, the information regarding personal insolvency proceedings is deleted from the register immediately upon the release from debts, the EU provides different storage periods in different Member States.

In contrast, Ukraine imposes no limits as regards the storage of personal data by private agencies, while in the EU, the storage period is determined by domestic law. This difference is justified by the absence of the supervisory authority in Ukraine, which establishes time frames for the storage of personal data by private agencies in the EU. Both legal regimes provide the possibility to delete personal data upon the request of the data subject. Overall, Ukraine's approach mirrors the EU legal regime towards the treatment of personal

data in the course of insolvency proceedings; however, both seek to establish the balance by different means.

CONCLUSIONS

1. Personal information is a unique element of self-identification, which is inalienable from human dignity. Protection of personal information is a fundamental human right and is granted strong protection under EU law. At the same time, the self-identification of the debtor is crucial for the effectiveness of insolvency proceedings, requiring disclosure of personal information. While it serves the interests involved in the proceeding, it also poses a threat to the security and protection of the right to personal information.
2. The GDPR establishes general obligations regarding the treatment of personal data, while the EIR deals specifically with the obligation of the States to process personal data in the course of the proceedings. To answer the question regarding the balance between the public nature of the discharge procedure and the protection of personal information, the emphasis shall be given to the primary objective of the processing. To draw the line between publicity and adequate protection of personal data, priority shall be given to basic freedoms. In this regard, it is crucial to allow the publication of the information strictly for the period of time defined in the law in order to achieve the transparency criterion.
3. The CJEU has dealt with the clash between the publicity of the discharge procedure and the protection of personal information of a debtor in the *Schufa* case and established three cumulative conditions for the lawful processing of personal data, namely (i) legitimate interests, (ii) legitimate processing and (iii) fundamental human rights do not take precedence. When personal data are kept in insolvency registers established by domestic legislation period of time, it serves the interests of the creditors and ensures publicity of insolvency proceedings. Meanwhile, the collection of personal data by private credit assessment agencies violates the right to protection of personal information when it stores personal data without legitimate bases for the period exceeding the time established by domestic law. To find a balance between transparency and protection of personal information, personal data shall be kept in the public registers for the time, established by the domestic law, without further processing by private registers.
4. A general approximation of Ukraine's legal framework with the EU's legal regime is justified by the

requirement for accession to the European Union as well as the standards for processing the personal data of European data subjects. Ukraine's approach towards the treatment of personal data in the discharge procedure reflects the EU legal regime since it also provides storage of personal data in the Unified Register of Debtors for the purposes of transparency and the option of rectification of the information upon the request of the data subject. Therefore, Ukraine and the EU, both base the processing of personal data on the consent of the data subject, but the duration of storage is different, making Ukraine's approach more publicly oriented, while the EU's approach is more privacy-oriented.

REFERENCES

- Birch, K., Cochrane, D.T., Ward, C. (2021). Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech. *Big Data & Society*, 8 (1), 1-15. <https://doi.org/10.1177/20539517211017308> (date of access: 04.04.2025)
- Bolzanis, D., Jokubauskas, R. (2025, January 22). *Reconciling a Fresh Start with Personal Data: The Challenge of EU Insolvency Discharge*, *Baltic Journal of Law & Politics* 17:2 (2024): 1–18.
- Bratasyuk, O. (2023). Legal Basis of Personal Data Protection in Ukraine and Germany: Organizational and Managerial Aspect. *Visegrad Journal on Human Rights*, 42-49, <https://doi.org/10.61345/1339-7915.2023.1.5> (date of access: 04.04.2025)
- Court of Justice of the European Union (CJEU). (1969). Case C-29/69, Stauber. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61969CJ0029> (date of access: 04.04.2025)
- Court of Justice of the European Union (CJEU). (2009). Joined Cases C-92/09 and C-93/09. <https://curia.europa.eu/juris/liste.jsf?num=C-92/09&language=en> (date of access: 04.04.2025)
- Court of Justice of the European Union (CJEU). (2024). UF (C-26/22), AB (C-64/2) v Schufa. <https://curia.europa.eu/juris/liste.jsf?num=C-26/22> (date of access: 04.04.2025)
- Custers, B., Maltieri, G. (2022). Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data. *Computer Law & Security Review*, 45. articlenumber105683. <https://doi.org/10.1016/j.clsr.2022.105683> (date of access: 04.04.2025)
- European Commission. (2008). Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: "Think Small First" A "Small Business Act" for Europe (COM(2008) 394 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52008DC0394> (date of access: 04.04.2025)
- European Commission. (2017). Communication from the Commission to the European Parliament and the Council:

- Exchanging and Protecting Personal Data in a Globalised World (COM(2017) 7 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0007> (date of access: 04.04.2025)
- European Court of Human Rights. (2004). Case of Bäck v. Finland. <https://hudoc.echr.coe.int> (date of access: 04.04.2025)
- European Parliament & Council of the European Union. (2015). Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on Insolvency Proceedings (Recast). *Official Journal of the European Union*, L, 141. 19–72. <https://eur-lex.europa.eu/eli/reg/2015/848/oj/eng> (date of access: 04.04.2025)
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 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). *Official Journal of the European Union*, L, 119. 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (date of access: 04.04.2025)
- European Parliament & Council of the European Union. (2019). Directive (EU) 2019/1023 of 20 June 2019 on Preventive Restructuring Frameworks, on Discharge of Debt and Disqualifications, and on Measures to Increase the Efficiency of Procedures Concerning Restructuring, Insolvency and Discharge of Debt, and Amending Directive (EU) 2017/1132 (Directive on Restructuring and Insolvency). *Official Journal of the European Union*, L, 172. <https://eur-lex.europa.eu/eli/dir/2019/1023/oj/eng> (date of access: 04.04.2025)
- European Union & Ukraine. (2014). Association agreement. https://eur-lex.europa.eu/eli/agree_internation/2014/295/oj/eng (date of access: 04.04.2025)
- European Union. (2012). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*, C, 326. 391–404. https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng (date of access: 04.04.2025)
- González Fuster, G. (2014a). EU Fundamental Rights and Personal Data Protection. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 16. 174, DOI:10.1007/978-3-319-05023-2.
- González Fuster, G. (2014b). The Emergence of Personal Data Protection as a Fundamental Right of the EU. *Privacy and the Protection of Personal Data Avant la Lettre*, 16, DOI:10.1007/978-3-319-05023-2.
- González Fuster, G., Gellert, R. (2012). The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right. *International Review of Law, Computers & Technology*, 26 (1). 73–82, DOI:10.1080/13600869.2012.646798.
- Pikamäe, Advocate General. (2023, March 16). Opinion of Advocate General Pikamäe in case C-26/22 and C-64/22, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=271345&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=327676> (date of access: 04.04.2025)
- Rubin, E.L. (2003). Rethinking Human Rights. *International Legal Theory*, 9 (1), 135–165, <https://ssrn.com/abstract=1132250> (date of access: 04.04.2025)
- Ukraine. (1996). Constitution of Ukraine. <https://zakon.rada.gov.ua> (date of access: 04.04.2025)
- Ukraine. (2010). On Protection of Personal Data. <https://zakon.rada.gov.ua/laws/show/en/2297-17#Text> (date of access: 04.04.2025)
- Ukraine. (2016). Law of Ukraine on Enforcement Proceeding. <https://zakon.rada.gov.ua/laws/show/1404-19#top> (date of access: 04.04.2025)
- Ukraine. (2019). Code of Ukraine on Bankruptcy Procedures. <https://zakon.rada.gov.ua/laws/show/en/2597-2519> (date of access: 04.04.2025)
- Ukraine. (2022). Draft Law on Protection of Personal Data. <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=8153&conv=9> (date of access: 04.04.2025)