Bialystok Legal Studies
Białostockie Studia Prawnicze
2024 vol. 29 no. 3

sciendo

DOI: 10.15290/bsp.2024.29.03.11

Received: 30.12.2023
Accepted: 25.04.2024

Dominika Kuźnicka-Błaszkowska
University of Wroclaw, Poland
dominika.kuznicka-blaszkowska@uwr.edu.pl
ORCID ID: https://orcid.org/0000–0001-8804–569X

Mariusz Jabłoński
University of Wroclaw, Poland
mariusz.jablonski@uwr.edu.pl
ORCID ID: https://orcid.org/0000–0001-8347–1884

Information on Gender Identity as Personal Data under EU and US Data Protection Models

Abstract: One of the most important legal issues concerning gender identity is ensuring that no one is discriminated against in any type of environment and that individuals' needs are considered seriously during the legislation process. Even though this can be questioned, if one needs to process information on gender to achieve an inclusive and diverse society and law, it seems that at this point in the history of society, there are no better measures to ensure a non-discriminatory environment than processing information on gender identity. Under the current personal data protection landscape, both in the European Union and the United States, it is not clear what the conditions are for processing information on the gender of individuals. Therefore, the authors of this article analyse legal requirements from both jurisdictions, also in the light of the question of the adequacy of personal data protection in the US under article 45 of the General Data Protection Regulation.
Keywords: adequacy, gender identity, personal data protection, privacy protection, sensitive data

Introduction

The processing of personal data on gender identity is an issue that affects many data controllers. This applies to both the public sector (data processing to provide appropriate medical care, keeping civil status records, and taking actions to counteract discrimination in the public space (Agius et al., 2011, p. 59)) and the private (diversity and inclusion programmes run by employers, research on target groups and

brand perception, adapting work regulations and working conditions to the needs of non-binary or transgender people, maintaining employee documentation, and fighting discrimination). At the same time, although public and private authorities should be presumed to have good intentions when processing gender identity data, they may discriminate, unintentionally or intentionally (United Nations, 2020). Nevertheless, the question of whether processing information on gender identity helps prevent discrimination or has contradictory effects is not the subject of this article.

Performance theory explains gender as the expression of a set of assigned characteristics, designated feminine or masculine, which define 'female' or 'male' performance (Faithful, 2010, p. 456). The unity of a person's performative experience constructs our 'male' or 'female' identities (Butler, 1990, p. 22). Some individuals, however, refuse their assigned roles or go off-script, choosing instead to express themselves outside of their 'intelligible' performance (Butler, 1990, p. 23). A person's gender identity consists of both how they view themselves in terms of expression and behaviour, but also how those expressions relate to what is historically considered masculine and feminine, and ultimately male and female (Herpolsheimer, 2017, p. 47). Undoubtedly, it can also be said that gender identity is an element that can significantly affect the perception of an individual by society, and can lead to discrimination or alienation. Gender identity and its perception police interactions with gendered accommodations, such as public bathrooms, homeless shelters, medical treatment programmes, and system of confinement (D'Angelo, 2023, p. 559). By using characteristics of genders, individuals are inadvertently but inherently persecuted and stereotyped (Herpolsheimer, 2017, p. 46). There is no escape from a social perception of gender at this moment; certain characteristics which have been traditionally assigned to gender classification are active in societies, and there is a long way ahead before this perception changes.

The situation is even more complicated if one tries to rethink the concept of the necessity of including gender or sex indicators in national documents and registers (D'Angelo, 2023). If this is not the case, then valid questions arise about whether states and private sectors really *need* to process information on gender identity and whether this affects the data minimization rule. Nevertheless, it does not seem that either EU or US lawmakers are ready to admit that information on gender identity may not always be needed (the Supreme Court in Alaska, referred to below, is different), especially due to security concerns (see the example of the United Kingdom in Maier, 2020, p. 216).

In the meantime, in this article we try to focus on whether and to what extent personal data protection law in the EU and US applies to processing information on gender identity. By using comparative legal methodologies, we analyse which model of protection provides greater guarantees for individuals and how these models should be considered in light of the discussion around the adequacy of the personal data protection model in the United States. Bearing in mind the scope of this spe-

cial issue, we focus on a very specific sector of personal data protection law, while remembering that this contributes only partially to the discussion of a comparative perspective of EU and US laws. The hypothesis proven in this paper is that even though the guarantees offered in the EU and US models differ, at the end they provide a similar level of protection. Unfortunately, none of them leads to fully efficient solutions to overprocessing and discrimination based on gender identity. Considering the strong business connections between the EU and the US, and the amount of data transferred between both territories, this is crucial to understand what requirements are imposed on controllers when the laws of both jurisdictions are applied to them, and whether regulations in these jurisdictions are complementary in the light of adequacy standards (Kuźnicka-Błaszkowska, 2024, submitted).

1. Protecting information on gender identity under the EU data protection model

A data controller considering processing information on the gender identity of data subjects should first reflect whether this information constitutes personal data within the meaning of the General Data Protection Regulation (GDPR). Omitting this stage may result in serious consequences, not only by violating the transparency obligations, but also by not recording the fact of processing information on gender identity in the data processing inventory or, potentially, in the data protection impact assessment. The controller's lack of awareness of what data they process may lead to a violation of the principle of minimization and proportionality or prevent proper risk analysis. But first and foremost, lack of understanding of what categories of data are being processed certainly leads to serious threats to the safety of processed personal data, and as a consequence may lead to the disclosure of information on gender identity to unknown individuals and, further, to discrimination.

According to the definition included in Art. 4 of the GDPR, any information about an identified or identifiable natural person should be considered as personal data. Factors enabling the identification of a natural person include their physical, physiological, genetic, mental, economic, cultural, or social identity. The threshold according to which the identification of an individual is determined remains low: the individual does not need to be identified, but only made identifiable (Jasserand, 2016, p. 302). Although gender identity has not been explicitly mentioned among the factors enabling the identification of a natural person, according to psychological science, it should be recognized that gender identity is part of social identities (Gulczyńska & Jankowiak, 2009, p. 30). Moreover, information about sex and gender is used to confirm the identity of an individual and, ironically, the world does not accept one's identity until that proof is presented (Herpolsheimer, 2017, p. 58). Therefore, assuming that the overriding purpose of the GDPR is to protect the rights

and freedoms of the individual, including, above all, their privacy and personal data, it seems that Art. 4 sec. 1 should be interpreted broadly, especially in the case of information in relation to which there is a high probability that its unauthorized disclosure would lead to a violation of the rights and freedoms of the individual. This is particularly important in the case of individuals who identify themselves as transgender or non-binary, who suffer from discrimination and exclusion not only in the EU or US, but around the world (Gates, 2011; Kuźnicka, 2018; Śledzińska-Simon, 2020).

It should therefore be considered that where information on gender identity is related to a specific person, it should be measured as personal data relating to that individual. Such a situation will not take place in the opposite case, i.e. when the information on gender identity does not concern a specific, already identified person or additional factors. In the vast majority of cases, information about gender identity alone will not allow the identification of the person to whom it relates. However, it may happen that information about gender identity, together with other information that is not personal data on its own, when combined can lead to the identification of an individual. Such a scenario, assuming correct identification, presupposes that information on gender identity will also be included in the catalogue of personal data.

2. Information on gender identity as sensitive data under the GDPR

Against this background, however, the question arises of whether, due to the importance of information on gender identity for an individual, it should be treated as a special category of personal data (sensitive data). However, it seems that proposal that the recognition that information on gender identity is protected under Art. 9 of the GDPR is a proposal that goes too far. Pursuant to the aforementioned provision regarding special categories of personal data subject to protection under Art. 9 of the GDPR, information about sexual orientation and sexuality is recognized, among other things. The catalogue specified in Art. 9 of the GDPR is a closed one; it should not be treated as extensive. The doctrine indicates that sensitive data should include information unequivocally stating certain properties of a natural person, as well as information from which such knowledge can be derived with a high degree of probability by an average recipient (Sakowska-Baryła, 2018). Such a situation does not occur in the case of information about gender identity – its disclosure does not lead to an unequivocal determination of an individual's sexual orientation or sexuality, or other data indicated in the provision in question.

Taking into account the existing legal status in most EU countries, in which information about whether someone is a woman or a man is not a special category of personal data, it should consequently be considered that information about someone's transgender or non-binary status will not be sensitive data either. Additionally,

gender identity does not determine a person's sexual orientation. Both women and men, as well as transgender and non-binary people, can be heterosexual, homosexual, pansexual, or asexual (taking into account only the simplest and most popular division of sexual orientations). The disclosure and processing of information on gender identity will therefore not involve the processing of data on an individual's sexual orientation.

The relationship between information on gender identity and information on an individual's sexuality, which is also subject to special protection under Art. 9 of the GDPR, seems to be a little more complicated. Sexual identity is defined by psychologists as a construct of many aspects of human sexuality and the result of both biological and social factors (Bancrofsekt, 2011). At the same time, gender identity does not lead to the disclosure of information about sexuality per se. The latter, on the basis of the GDPR, is understood broadly; it may include information about sex life or sexual abstinence (Sakowska-Baryła, 2018). Sexuality data may include information such as frequency of sexual contact or preferences for sexual behaviour, but also sexual disorders. None of these are directly and inextricably linked to gender identity; it is impossible to assign specific sexual behaviours as a characteristic of one, given sex.

Important measures regarding the recognition of information on gender identity have been taken by the UK supervisory authority. Even though these considerations have been made after Brexit, to the best of our knowledge this is the only existing interpretation of processing information on gender identity under law which substantially incorporates the EU GDPR. Although, as a rule, the British Information Commissioner's Office (ICO) does not consider information on gender identity as sensitive data, it points out that due to the fact that it concerns people who are particularly vulnerable to exclusion and discrimination, it should be subject to increased protection. As mentioned in the explanatory memorandum to the decision about the Mermaids organization (ICO, 2021), regardless of whether information on gender identity should be classified as sensitive data or whether it may lead to the disclosure of other sensitive data, unauthorized access to and dissemination of this information entails significant damage to and suffering for data subjects.[1] Therefore, ensuring an adequate level of protection of this data is necessary, also taking into account the consequences of its disclosure for the data subject. However, one should agree with the ICO, which indicates that in some cases, information about gender reclassification may lead to the disclosure of data on the health of a given individual (ICO, 2021).[2] At the same time, information on gender identity will not always lead to the disclosure

1 Mermaids is an association of parents of transgender people actively counteracting discrimination against their children in the public space.

2 This may also happen in legal documents when an individual is in the process of gender reclassification, as various states require confirmation of the medical treatment and its type before reclassification of gender, e.g. in a birth certificate.

of information on gender reclassification. In cases where the sex recorded in the birth certificate corresponds to the actual gender identity of the individual, disclosure of information about gender identity will in no way lead to the disclosure of information about gender reclassification (because such a reclassification probably did not take place). This is similar in the case of people whose recorded sex does not agree with their sense of identity, but who have not started the reclassification process. One of the situations in which information about gender identity may lead to disclosure of information about reclassification, and thus health status, is when an individual has already made a full gender reclassification and at the same time still uses documents specifying their sex in the way it was recorded at birth.

In its decision, the ICO suggests that a risk-based approach should be followed if information on gender identity is processed by the controller. Even though this approach is strongly present in the GDPR, this leaves a lot of responsibility in the hands of the controller; it is a direct obligation put on them through Arts. 24 and 25 GDPR. However, this approach may have important consequences for individuals if the controller fails to fully comply or makes incorrect assessments. A risk-based approach requires controllers to take the risks to the rights and freedoms of data subjects into account; it considers both the extensiveness of the measures that should be taken to ensure compliance and the outcomes that should be reachable through these measures (Quelle, 2018, p. 506). The risk-based approach asks controllers to build a form of compliance that does not merely 'tick boxes', but is tailored to respect the rights and freedoms of data subjects (Quelle, 2018, p. 506). In fact, a risk-based approach requires controllers to assess whether existing norms are sufficient to ensure the protection of individuals' rights and freedoms, and if not, to implement additional measures. This surely puts more obligations on the controllers and requires them to have knowledge and experience not only in the field of processing personal data, but also to become experts on human rights (or at least be close to it). This requirement may be overkill to many businesses, and in fact seems to shift responsibility for protecting fundamental rights from the state to business.

Nevertheless, even though the existing data protection regulation in the European Union does not provide strengthened protection for processing information about gender identity, the current wording of the GDPR, especially a narrow interpretation of Art. 9, does not allow for providing sufficient guarantees for processing personal data disclosing gender status. Enhanced protection should surely be given to those who identify as transgender or non-binary (considering their vulnerable status (Malgieri & Fuster, 2020)), but such protection may also become a tool for counteracting discrimination against women and men in specific areas of their lives. To achieve this goal, there is a need to change the current interpretation of Art. 9 GDPR in a way which will allow the expansion of protection to different personal data (which may bring further uncertainties and difficulties and is not the preferred solution), will change the literal meaning of Art. 9 to include information on gender iden-

tity in the catalogue of sensitive data, or will shift the protection towards focusing on use, harm, and risk rather than on the nature of the personal data (Solove, 2024), which is clearly visible in the data protection model in the United States.

3. Protecting information on gender identity under US federal law

The entire system of protecting privacy and personal data in the United States is very different from the European. Law is fragmented, even though certain states have made the effort to introduce some general legislation. Mainly recognized as providing privacy standards in the country, the Fourth Amendment of the US Constitution does not apply to relations between private entities, and when it comes to relations between individuals and the state, it only applies in very limited circumstances (Judgment of the US Supreme Court, 1960; Kuźnicka-Błaszkowska, 2024 in press). Therefore, one should not look for guarantees for the safe and lawful processing of information on gender identity in the US Constitution.

Whereas the EU has acquired one definition of personal data under the GDPR, which refers to any information that identifies or allow the identification of an individual, the United States has taken a slightly different approach. Personally Identifiable Information (PII), as personal data is called under the US data protection model, does not have a single broad definition. Each state and each sector is regulated differently, which is one of the first reasons why the discussion about the adequacy of the US data protection model is so difficult (Schwartz & Solove, 2014, p. 879). Nevertheless, under state laws, the term 'personal data' as well as 'sensitive data' is used in certain legislation, and the meaning is close to EU standards.

On the federal level, the US still lacks comprehensive legislation in this field. There are a couple of examples of legal acts which aim to protect certain information on the individual. The Health Insurance Portability and Accountability Act (HIPAA) provides a broad definition of health-related information that is subject to strict standards regarding safety and disclosure. Processing of PII under HIPAA is regulated in a manner that is more closely analogous to the European model: HIPAA features enhanced notice requirements, as well as the requirement that 'Covered Entities' (generally, health care providers and insurers) obtain consent before using or disclosing protected health information for any purpose other than treatment, payment, or other health care operations. In either case, a fundamental part of the rationale for these controls is that sensitive personal information is easily subject to abuse or misuse, both by governments and by private employers, neighbours, or others. Information on gender and sex (as discussed above) will not always be related to information concerning health. Nevertheless, medical providers do collect and process information on gender identity, regardless of whether this is absolutely necessary considering the procedure a patient is subject to or whether it is justified by the fact

that 1) the medical provider is keen to use the right pronouns or 2) this information is required to ensure that the treatment provided is tailored to the patient (Ogden et al., 2020, p. 619). Considering that both purposes for processing information on gender identity may be justified under HIPAA, any wrongs shall be addressed by this Act. At the same time, the US model of personal data protection focuses rather on misuses of personal data which may lead to harm, discrimination, or exclusion. If none of this happens, an individual will not be able to build a case and therefore assert their rights in court.

Another legal instrument which aims at protecting the personal data of individuals on the federal level is the Children's Online Privacy Protection Act (COPPA). Unfortunately, COPPA mainly applies to commercial websites and online services targeting children under 13. Websites that do not target children – so-called general audience websites – that have 'actual knowledge' that they collect personal data from children also fall within the scope of COPPA. Under COPPA, personal data is defined as individually identifiable information about an individual, collected online. The definition contained in the Act is interpreted as providing guarantees for the processing of certain categories of personal data, such as age, gender, height, weight, school grade, interests, habits, hobbies, pets, friends, zip code, even first name (only), and the recording of preferences and movements online, as long as first and last names, address, phone number, or other contact information is solicited (Bartow, 2000, p. 661). COPPA does not distinguish sensitive data from 'ordinary' personal data, and therefore does not require different measures when personal data is processed. Similarly, to the GDPR, COPPA requires parental consent for processing children's data and an appropriate notification (Kuźnicka-Błaszkowska, 2022, pp. 495–497). Under COPPA, there is no enhanced protection for processing information about gender identity.

It has to be mentioned that despite the lack of comprehensive privacy laws, certain initiatives ensure that processing information on gender status does not lead to discrimination against individuals. Most of these relate to including information on gender identity in official documents such as passports and driving licences, but also birth certificates, medical files, and prison certifications. Considering the dual lawmaking system in the US, this is not only a question of having gender information included in the above-mentioned documents, but is also about introducing general, comprehensive, and unilateral classifications on requirements regarding gender identification (Spade, 2007–2008).

Several states in the US have made an effort to try to fill a gap in the model of personal data protection in their territory by passing their own rules and regulations in this area. The majority of them are modelled on the GDPR; however, certain differences have been introduced. Considering their powers, no states have been able to implement comprehensive, pan-sectoral regulation, but they have surely made important steps in ensuring the highest possible level of personal data protection there.

4. Protecting information on gender identity under US state law: The examples of Delaware, Oregon, and Alaska

Law implemented on the state level is applicable only to processing and controllers connected with the territory of the given state. One must be very careful when analysing the rules about the processing of personal information in specific states and when considering the changing landscape of privacy protection there. Among multiple states which have introduced several pieces of data protection legislation in recent years, only a couple distinguish between 'usual' and special categories of personal data (sensitive data). The scope of this article does not allow us to describe and explain each and every one of the state laws, but considering the theme of this analysis, it is crucial to explain how Oregon and Delaware protect information on gender identity, as these are the only states which directly refer to gender identity in their data protection laws.

Under the Delaware Personal Data Privacy Act (DPDPA), 'personal data' means any information that is linked or reasonably linkable to an identified or identifiable individual, and does not include de-identified data or publicly available information.[3] The DPDPA also defines the term sensitive data as 'personal data that includes any of the following: a. Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis (including pregnancy), sex life, sexual orientation, *status as transgender or nonbinary*, national origin, citizenship status, or immigration status; b. Genetic or biometric data; c. Personal data of a known child; d. Precise geolocation data' (emphasis added). It is important to mention that 'sensitive data' under the DPDPA protects only information on whether the individual is transgender or non-binary, but not information if someone is man or woman. This seems to be reasonable, up to a point. Indeed, over the last few years, it has been transgender and non-binary individuals suffering the most from discrimination and exclusion.

The DPDPA requires the controller who processes sensitive data (including information on transgender or non-binary status) to obtain prior consent from the individual (the consumer) or, if this consumer is known to be a child, from its parent or lawful guardian. Additionally, processing of sensitive data should also be included in the data processing assessment. However, this requirement applies only to controllers who process personal data of more than 100,000 consumers. Data processing

3 'De-identified data' means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses such data does all of the following: a) takes reasonable measures to ensure that such data cannot be associated with an individual; b) publicly commits to processing such data only in a de-identified fashion and does not attempt to re-identify such data; c) contractually obligates any recipients of such data to comply with all of the provisions of the law applicable to the controller with respect to such data.

assessment in Delaware (similar to the EU) must be conducted in the case of processing activities that present a heightened risk of harm to a consumer. This surely enhances the need for stronger protection of information on transgender or non-binary status. Another measure which should ensure the safety of the processing of sensitive data, including information on transgender or non-binary status, is the necessity for the controller to conduct enhanced control over recipients to whom de-identified or pseudonymous data is provided. In such a scenario, the controller must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous or de-identified data is subject, and must take appropriate steps to address any breaches of those commitments.

Even though the DPDPA provides reasonable guarantees for processing information on transgender or non-binary status, one must keep in mind that protection under this Act does not 'apply to individual(s) acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit organization, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, non-profit organization, or government agency" (DPDPA). Moreover, the protection applies only to residents of Delaware. This means that any consumer who is not a resident of this state must rely in this regard on the protection provided by federal law (which, as has been already stated, does not provide comprehensive measures).

Another state which has introduced a law aiming to strengthen measures around the processing of information on gender is Oregon. Senate Bill 619 (Oregon Consumer Privacy Act, OCPA) defines personal data as data, derived data, or any unique identifier that is linked to or can be reasonably linkable to a consumer or to a device that identifies, is linked to, or is reasonably linkable to one or more consumers in a household. However, the term 'personal data' under OCPA does not include de-identified data or data that (a) is lawfully available through federal, state, or local government records or through widely distributed media, or (b) a controller has reasonably understood to have been lawfully made available to the public by a consumer. This means that if a consumer made certain information publicly available (i.e. on an Instagram account, Facebook, etc.), the protection under OCPA does not apply. It is also crucial to understand that if the interpretation of 'publicly available' is understood as broadly as under the Fourth Amendment, any attempt to protect this information will be extremely difficult. This is because, so far, the Supreme Court has recognized that an individual who discloses certain information to a third party (regardless of whether this is an individual or a company) or abandons it in a public space should not have a reasonable expectation of privacy (Solove, 2011, pp. 93–114, and the case law referred to therein).

Additionally, OCPA defines sensitive data in a way that also protects information on an individual's status as transgender or non-binary. Unfortunately, the strength-

ened protection does not include the content of communications or any data generated by or connected to an advanced two way communication systems or equipment for use by a utility. What is also important, similar to the DPDPA, is that OCPA provides limited protection for individuals that does not include either employment relations or relations between the state and the individual.

As the US law system is broadly based on case law, to further understand the nuances of protecting information on gender identity by states, it is crucial to look into specific decisions of states' supreme courts. In *K.L. v. State Dept of Admin*, the Superior Court of Alaska found that the routine disclosure of an individual's state-issued driving licence would expose their transgender status, would at least implicate non-fundamental aspects of the right to privacy, and that any procedure for changing the gender-identity marker on an individual's licence 'indirectly threatens the disclosure of this sensitive personal information' (Judgement of the Superior Court of Alaska, 2012). The court sympathized with the plaintiff, stating that one's transgender status is 'private, sensitive personal information'.

Summary

The above analysis shows that the overall goal of both the US and the EU is the protection of the individual against discrimination, harm, and misuse of personal data. However, the United States does not regulate this in either a comprehensive or a detailed way. Thus, the United States and the EU share a similar goal in regulating this type of information, but the means they employ to reach that end are quite different (Hemnes, 2012, p. 11). Additionally, the protection guaranteed to individuals either at state or at federal level does not apply to data subjects in all areas of their lives and does not oblige all controllers (in public or private entities) to ensure that personal data is protected during processing.

Current interpretation of the GDPR does not provide sufficient guarantees for processing information on gender identity. This type of personal data cannot be considered as sensitive data (a special category of personal data) under Art. 9 GDPR. Enhanced protection can be foreseen; however, it is not certain whether the risk-based approach required by the GDPR is sufficient, considering the greater threat, and the serious societal implications, if information on gender identity is disclosed to certain actors. The approach taken by Oregon and Delaware provides a higher level of protection of personal data in the form of information on gender identity. However, as mentioned above, it has limited applicability. In terms of the subject matter, protection is definitely more useful to individuals, but the narrow scope of regulation means that in most situations, this protection is illusory or even non-existent. The ideal solution should aim at combining broad subjective protection with broadening the scope of regulation towards entities obliged to protect personal data.

Even if one considers the risk-based approach which is strongly promoted in the US and under Art. 24 and 25 of the GDPR, it may be impossible to introduce a unified and comprehensive course in international companies based only on this factor. Neither the EU nor the US are monoliths – the level of discrimination and exclusion based on gender identity varies in each state of the US and in each Member State of the EU. This is not only the consequence of different levels of social openness and respect for fundamental human rights, but also a matter of legislation, which may or may not allow for gender affirmations and the procedures required to legally adjust gender in official documents. In such a scenario, it seems that controllers should take the most restrictive approach possible to processing information on gender identity, which may have enormous financial implications and create a poor user experience.

Funding

Research conducted by Dominika Kuźnicka-Błaszkowska for this article was funded in whole by National Science Centre PRELUDIUM 20, NO. 0209/0037/22, registration no: 2021/41/N/HS5/03225, contract no: UMO-2021/41/N/HS5/03225. For the purpose of Open Access, the author has applied a CC-BY public copyright licence to any Author Accepted Manuscript (AAM) version arising from this submission.

REFERENCES

Agius, S., Kohler, R., Aujean, S., & Ehrt, J. (2011). *Human rights and gender identity: Best practice catalogue*. ILGA-Europe. https://www.ilga-europe.org/files/uploads/2022/04/Human-Rights-Gender-Identity-Best-Practice-Catalogue.pdf

Bancrofsekt, J. (2011). *Seksualność człowieka*. Wydawnictwo Medyczne Urban & Partner.

Bartow, A. (2000). Our data ourselves: Privacy, propertization, and gender. *University of San Francisco Law Review*, *34*(4), 633–704.

Butler, J. (1990). *Gender trouble: Feminism and the subversion of identity*. Routledge.

D'Angelo, M. (2023). Gender registration and international law: Are gender markers necessary? *Cardozo International & Comparative Law Review*, *6*(2), 559–584.

Faithful, R. (2010). (Law) breaking gender: In search of transformative gender law. *American University Journal of Gender, Social Policy & the Law*, *18*(3), 455–470

Hemnes, T. (2012). The ownership and exploitation of personal identity in the new media age. *John Marshall Review of Intellectual Property Law*, *12*(1), 1–39.

Herpolsheimer, A. (2017). A third option: Identity documents, gender non-conformity, & the law. *Women's Rights Law Reporter*, *39*(1), 46–84.

Gates, G. (2011, April). *How many people are lesbian, gay, bisexual, and transgender?* The Williams Institute. https://williamsinstitute.law.ucla.edu/wp-content/uploads/How-Many-People-LGBT-Apr-2011.pdf

Gulczyńska J., & Jankowiak, B. (2009). Tożsamość płciowa w rozwoju psychoseksualnym człowieka. *Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa*, *2*, 30–39.

Information Commissioner's Office (ICO). (n.d.). *What is special category data?* Retrieved 6 November 2023, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

Information Commissioner's Office (ICO). (2021, 5 July). *Data Protection Act 2018 (Part 6, Section 155), Supervisory powers of the Information Commissioner: Monetary penalty notice*. https://ico.org.uk/media/action-weve-taken/mpns/2620171/mermaids-mpn-20210705.pdf

Jasserand, C. (2016). Legal nature of biometric data: From generic personal data to sensitive data. *European Data Protection Law Review*, *2*(3), 297–311.

Judgment of the Superior Court of Alaska on the case of *K.L. v. State Dept of Admin*, K.L., 2012 WL 2685183.

Judgment of the US Supreme Court of 27 June 1960 on the case of *Elkins v. United States*, 364 U.S., 206 (1960).

Kuźnicka, D. (2018). Pozycja prawna i społeczna shemale w Indiach. *Wrocławskie Studia Erazmiańskie*, *12*, 261–280.

Kuźnicka-Błaszkowska, D. (2022). Protecting children's personal data under General Data Protection Regulation and California Consumer Privacy Act in relation to information society services – European perspective. *Przegląd Prawa Konstytucyjnego*, *70*(6), 487–408.

Kuźnicka-Blaszkowska, D. (in press). The Fourth Amendment to the US Constitution in light of EU data protection model. *Przegląd Prawa Konstytucyjnego*.

Kuźnicka-Błaszkowska, D. (2024). The meaning of 'adequate' under GDPR – lesson learnt from EU bodies. Manuscript submitted for publication.

Maier, M. (2020). Altering gender markers on government identity documents: Unpredictable, burdensome, and oppressive. *University of Pennsylvania Journal of Law and Social Change*, *23*(3), 203–250.

Malgieri, G., & Fuster, G. (2020). The vulnerable data subject: A gendered data subject? *European Journal of Law and Technology*, *13*(2), Available at SSRN: https://ssrn.com/abstract=3913249 or http://dx.doi.org/10.2139/ssrn.3913249

Mottet, L., & Ohle, J.M. (2003). *Transitioning our shelters: A guide to making homeless shelters safe for transgender people*. National Gay and Lesbian Task Force Policy Institute / National Coalition for the Homeless. https://srlp.org/wp-content/uploads/2012/08/TransitioningOurShelters.pdf

Ogden, S.N., Scheffey, K.L., Blosnich, J.R., & Dichter, M.E. (2020). 'Do I feel safe revealing this information to you?' Patient perspectives on disclosing sexual orientation and gender identity in healthcare. *Journal of American College Health*, *68*(6), 617–623.

Quelle, C. (2018). Enhancing compliance under the General Data Protection Regulation: The risky upshot of the accountability – and risk-based approach. *European Journal of Risk Regulation*, *9*(3), 502–526.

Sakowska-Baryła, M. (2018). *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. C.H. Beck.

Schwartz, P.M., & Solove, D.J. (2014). Reconciling personal information in the United States and European Union. *California Law Review*, *102*(4), 877–916.

Solove, D. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

Solove, D. (2024). Data is what data does: Regulating based on harm and risk instead of sensitive data. *Northwestern University Law Review*, *118*(4), 1081–1137. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198

Śledzińska-Simon, A. (2020). Populists, gender, and national identity. *International Journal of Constitutional Law*, *18*(2), 447–454.

Spade, D. (2007–2008). Documenting gender. *Hastings Law Journal*, *59*(4), 731–842.

United Nations. (2020, 24 March). *Report of the Special Rapporteur on the right to privacy*, A/HRC/43/52. https://www.ohchr.org/en/documents/thematic-reports/ahrc4352-report-special-rapporteur-right-privacy