

INFORMED CONSENT IN BIOMETRIC MIGRATION MANAGEMENT

Helga ŠPADINA

PhD, Associate Professor, Faculty of Law, University Josip Juraj Strossmayer,
Osijek, Croatia, ORCID: <https://orcid.org/0000-0002-5826-176X>

e-mail: hspadina@pravos.hr

Abstract

Biometric data collection and automated recognition based on biological and behavioural characteristics has been widely introduced firstly for citizens and later for migrants.

While the positive effects of biometrics use in migration management are plenty and offer quick and reliable identification of a person, efficient matching and immediate alert on the sensitive data, we need to be aware of reliability, data minimization, technical difficulties, ethical issues, reversibility and consent. In the European Union, milestones were the introduction of the EU GDPR Regulation, Entry/Exit System (EES) and reformed EURODAC system for collection of biometric data.

The paper looks into the legal aspects of informed consent for the use of biometric data in digital migration management in the European Union. Focus is on the "strict proportionality assessment" established by the Court of Justice of the European Union (CJEU) which ruled that biometric processing is a limitation on privacy that must pass the test. Further, we will analyse CJEU individual assessment benchmark, systematic data collection ban, right to erase standard and indefinite data storage limits established by the Court.

The main research question of the paper is whether we can have meaningful consent in migration management, taking into the consideration situations in which migrants are forced to migrate and cannot really provide informed and free consent having in mind their situation.

Keywords: *migration management, consent, CJEU, biometric data.*

1. The concept and meaning of consent¹

1.1. The concept of consent

In order to understand legal concept and legal implications of consent, one firstly needs to look into the moral and philosophical concept of consent. Consent as a concept of law and precondition for many legal actions to be valid was firstly developed within the realm of the medicine and only later, it was developed for other areas of life, including law. McLean traces how bioethics shifted away from medical paternalism toward a model where consent serves strictly to protect and honor a patient's self-determination and bodily integrity (McLean, 2021).

Consent is widely recognized as a normative power that alters moral relationships (Kleinig??), justifying or legitimating acts, arrangements or expectations (Simons, 1998) and being “a purely subjective mental state consisting of the intention to forgo or waive one's moral or legal objection to a boundary-crossing act” (Alexander, 1996). The same author anchors consent in the autonomous choice of the individual, emphasizing that consent must be an expression of a person's voluntary will to change the normative boundaries surrounding them and considers it to have “a transformative power of the moral and legal status of an action because „it turns what would otherwise be a serious moral and legal wrong (like battery, theft, or trespass) into a perfectly permissible, non-wrongful act (like surgery, a gift, or a invited visit)” (Alexander, 1996). Similarly, Kleinig sees consent as an action that waives a right, thereby rendering permissible what would otherwise be a moral or legal wrong (Kleinig, 2010)

Kleinig emphasizes corner stones of consent being intentionality (as a conscious, intentional conveyance of permission), voluntariness (free from coercion, manipulation, or undue pressure that compromises the agent's autonomy), competence (individual must possess the cognitive capacity and maturity to understand the nature and consequences of what they are agreeing to) and information because a meaningful consent requires that the consenter is adequately informed about the parameters, risks, and implications of the act in question (Kleinig, 2010)

Overall, majority of definitions on consent include the same elements: decisional capacity (competence) by which the individual must possess the necessary

¹ AI declaration: This article was prepared with assistance from an AI language model (OpenAI GPT), used as an academic writing assistant. The assistant worked exclusively from materials, instructions, and prior theoretical notes supplied by the author. The author performed the primary conceptual and scholarly work; defined the aims and scope; developed the argument; determined the structure and style; selected, checked, and interpreted the references; reviewed and directed all drafts; made substantive revisions; and approved the final text. The assistant contributed at a later stage of the writing process and was used primarily to support drafting, exposition, restructuring, and revision. Any material generated during this process was reviewed, selected, revised, and verified by the author before inclusion. Full responsibility for the content, interpretations, references, and citations rests entirely with the human author. This disclosure is provided in the interest of transparency and in line with current journal and research integrity guidance regarding the use of generative AI.

cognitive, mental, and legal capability to understand the nature and consequences of their choice; voluntariness by which the choice must be made freely without the presence of coercion, threats, duress, or overwhelming force and information by which the individual must be sufficiently informed about the facts of the scenario, deceptive manipulation or errors of critical fact invalidate the choice.

Further, we can differ two types of consent – the first defines direct, expressed consent as “direct, unambiguous permission communicated explicitly through spoken words, written documents, or clear non-verbal physical signs.” The second type is implied consent as a “permission that is not explicitly spoken or written but is reasonably inferred by a person’s cooperative actions, the circumstances of a situation, or community social practices” (Simons, 1998).

1.2. Autonomy as a precondition for consent

One of the central pillars of consent is autonomy and respect for autonomy has become the primary justification for consent in contemporary biomedical law (McLean, 2021). Autonomy can be the key value because a person’s well-being depends heavily on their capacity to lead an autonomous life—meaning they can choose and pursue their own goals without coercion or manipulation (Raz, 1986). Rights can be derived from their role in protecting the vital interest of personal autonomy the philosophy of autonomy, instead of building political morality on rights or equality (Raz, 1986).

Scientists question validity of respect for autonomy argument related to consent because according to them, current legal framework for consent, which has its basis in the idea of autonomous authorization, does not work in practice (Schermer, Custers, van der Hof, 2014), leading to ‘consent desensitization’.

Some authors go even further and explicitly reject the standard bioethical concept of consent as a localized, individual act of "autonomous authorization" and they propose a holistic "transactional" model where the moral permissibility of an action depends on the entire interactive context, fairness of terms, and background conditions shaping the relationship (Miller, Wertheimer, 2010).

According to Miller and Wertheimer, valid individual consent is not a definitive moral golden ticket because a transaction can be morally compromised or unfair even if a person technically issues legally and philosophically valid consent. Further, they consider consent not to be necessary when for example in emergency healthcare it would be perfectly ethical to proceed without a formal act of individual consent (Miller, Wertheimer, 2010).

O'Neill argues that the true value of informed consent lies not in promoting individual autonomy, but in preventing deception and coercion. Medical ethics relies too heavily on vague and conflicting definitions of individual autonomy and uses informed consent as a blanket tool to maximize personal choice, which in itself she seems as philosophically weak because genuine autonomy varies wildly among individuals (O'Neill, 2003).

1.3. Informed consent

In addition to the autonomy to give consent, not all consents are considered as complete and legally acceptable. In order to be legally legitimate and comply with legal requirements, consent needs to be informed. Let us look into the foundation of informed consent.

The main arguments for informed consent revolve around protection, autonomy, prevention of abusive conduct, trust, self-ownership, non-domination, and personal integrity (Nir, 2019).

Consent has to be fully informed when we have a full disclosure (Nir, 2019). It needs to be voluntary, and decisionally-capacitated consent with consenters understanding completely all that has been disclosed (Nir, 2019). All of those elements form a regulatory commitment to informed consent.

Fully informed consent usually assumes freedom from controlling interference and from an inadequate understanding of the basic risks of the intervention, components of fully autonomous choice as well (Beauchamp and Childress, 2008).

1.4. European Union definition of consent

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) definition of 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (Art 4, P. 14). GDPR definition (Art 4, p.11): *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;* In services, trade and commercial relations, consent under the GDPR Regulation must be freely given. Individuals must have a genuine choice. Consent is invalid if there is a clear imbalance of power (like employer-employee) or if access to a service is bundled or conditioned on consenting to unnecessary data processing.

Consent also needs to be specific and informed. Users must understand exactly what they are agreeing to. This means privacy notices must be written in plain, clear language and must state who the data controller is and how the data will be used. Clearly defined, distinct purposes are required.

Consent also needs to be revocable without detriment and withdrawing consent must be just as easy as giving it. Crucially, a user cannot be penalized, charged extra, or denied the core service just because they decide to opt-out later

The EU Charter on Fundamental Rights in Article 8 provides protection of personal data, stipulating that "everyone has the right to the protection of personal

data...such data must be 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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”

2. The Entry/Exit System (EES), the EU GDPR Regulation and reformed EURODAC system for collection of biometric data

Data access across the EU GDPR, the Entry/Exit System (EES), and the reformed EURODAC system is regulated through a multi-tiered architecture. This framework balances strict data protection rights with migration management. Instead of operating as open-access databases, these systems utilize a strict "need-to-know" access model.

The EU general data protection regulation framework establishes the core rules for processing biometric data (classified as Special Category Data under Article 9), classified as high-risk. Data access is strictly limited by the purpose limitation: data collected for border control or asylum verification cannot be repurposed for unrelated administrative tasks. Another safeguard is data minimization by which access logs must limit visible fields and only data points relevant to the specific official making the query are exposed.

2.1. The Entry/Exit System/EES Regulation (EU) 2017/2226

The Entry/Exit System/EES Regulation (EU) 2017/2226 regulates an automated IT system for registering non-EU nationals travelling for a short stay, each time they cross the external borders of EU Member States using the system. The system registers the person's name, travel document data, biometric data (fingerprints and captured facial images) and the date and place of entry and exit and refusals of entry, allowing the automatic detection of overstayers (travellers who have exceeded the maximum duration of their authorized stay). The Entry/Exit System/EES Regulation (EU) 2017/2226 dictates exactly which entities can access short-stay traveler biometrics (four fingerprints and a live facial image (EC web site, 2026). If a third-country national refuses to provide their biometric data to border authorities, they will be formally denied entry at the border crossing point.

While Article 9 of the GDPR requires explicit consent to process special category data (like biometrics), it provides exceptions. The EES utilizes specific legal overrides like legal obligation and public interest superseding individual choice and stipulated by the GDPR Article 6(1)(c) and Article 9(2)(g) by which biometric data can be processed without consent if it is necessary for reasons of substantial public interest based on Union or Member State law.

Under the EES Regulation, personal data can be shared with the whole range of authorities within the EU – such as border, visa, immigration and law enforcement,

but also it can be shared with international organisations or third countries' authorities, and to the limited extent transport carriers. Refusal to provide biometric data, results in denied entry into the territory of the European countries using the EES system.

Under the EU EES, individual consent is completely irrelevant and is not used as the legal basis for collecting biometric data. The EES represents, in sophisticated legal form, a model for the mass biometric registration of mobile population. It bypasses the standard GDPR requirement for explicit consent by operating under a strict statutory mandate (Jain, 2026). The same author emphasizes a basic consent flaw of the system as follows: *"once biometric data is captured at the border for one stated purpose, it becomes permanently available and shared across linked systems for purposes that were neither the original basis for collection nor ever subjected to an independent necessity assessment. The design is not incidental to the system's operation but constitutive of it, and it puts the system in direct tension with Article 8 of the EU Charter of Fundamental Rights and the proportionality doctrine developed by the Court of Justice in Digital Rights Ireland (Joined Cases C-293/12 and C-594/12) and the Schrems II line of jurisprudence."* (Jain, 2026).

Biometric template captured under the EES is retained centrally for up to five years, integrated across law enforcement-accessible databases, and cannot be revoked or replaced if a system breach occurs.

In recent months, employment of the EES at the EU border crossings caused the whole range of problems for passengers and staff working with the system. Biometric data capturing caused severe delays in flights and many passengers complained for not being able to travel at all due to EES rules. This demonstrated that the introduction of the system was not properly conducted and showed a significant legal gap between the regulations and reality in which passengers are unable to contest decisions of the immigration officers, frequently are not provided with translation services and immigration proceedings in implementing EES were missing the procedural transparency protections mandated by the CJEU. Once again, in EU migration law we had situation in which a new measure – taking of biometrics – was introduced in the summer period when the airports are overcrowded and for the sake of the management of arrivals, taking of biometric data was insufficiently explained and data subject i.e. passengers coming from outside of the EU, had very limited options for procedural transparency and rights protection, including inability to refuse to give biometric data.

2.2. EU GDPR Regulation

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) is crucial legal instrument for data protection in the EU. The Article 42 of the GDPR regulates that the consent cannot

be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

Recital 43 of that regulation states that, in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data where there is a clear imbalance between the data subject and the controller. That recital also clarifies that consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.

In the third place, Article 7(4) of the GDPR provides that when assessing whether consent is freely given, utmost account must be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Purpose limitation under Article 5(1)(b) GDPR prohibits data collected for one purpose from being reprocessed in an incompatible way. The EES Regulation circumvents this not by openly violating it, but by building the secondary purposes through regulation that law enforcement has access to data, ETIAS cross-referencing is possible, and allows matching.

2.3. EURODAC

The EURODAC Regulation (EU) 2024/1358, which governs the biometric tracking of irregular migrants and asylum seekers across the EU. Migrants over the age of 14 are legally required to submit fingerprints and facial images. There is no mechanism to request or record consent. Coerced physical compliance is authorized by EU law rather than validated by individual agreement. Biometric tracking of irregular migrants and asylum seekers is based on the same principles as the EU EES, so that individual consent is superseded by the public interest and statutory requirements.

3. Judiciary interpretation of consent to provision of biometric data

3.1. Public interest v. consent

The Court of Justice of the European Union has examined consent in the light of migration law in case *Schwarz v. Stadt Bochum* (Case C-291/12) when the applicant applied for passport, refusing to consent to fingerprinting. The applicant revoked application of the Article 8(2) of the EU Charter on Fundamental Rights, according to which personal data cannot be processed except on the basis of the consent of the person concerned or some other legitimate basis laid down by law. The Court emphasised that “citizens of the Union wishing to travel are not free to object to the processing of their fingerprints... because that document must contain fingerprints pursuant to Article 1(2) of Regulation No 2252/2004...and cannot be deemed to have consented to that processing” (p.32).

The Court further noted that “rights recognised by Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, Volker und Markus Schecke and Eifert, and Case C-543/09 *Deutsche Telekom*).”

The Court continued that “as long as those limitations are provided for by law, respect the essence of those rights and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others” the general interests of the Union prevail over consent to collection of biometric data. The Court concluded that this violation is legally permissible only because it is prescribed by law, pursues an objective of general public interest (preventing illegal entry/falsification), and is strictly proportionate.

The position of the Court of Justice of the European Union clearly demonstrates that data collection and processing in migration management is treated as a mandatory, statutorily enforced limitation on fundamental rights. This restriction must bypass consent entirely and find its justification under alternative legal grounds, such as public interest or compliance with legal obligations.

3.2. Inherent power imbalance v. consent

In all situations where there are relationships of authority (such as relationship between employer and employee) or inherent power imbalance which makes it unlikely that a person can refuse consent to the processing of personal or biometric data without fear of adverse consequences, consent cannot be freely given. This was re-affirmed by the Court of Justice of the European Union that has established that the inherent power imbalance between state authorities and third-country nationals rules out the possibility of consent to collecting and processing of biometric data can be “freely given.” The CJEU codified this institutional imbalance in *Meta Platforms v. Bundeskartellamt* (Case C-252/21). The Court explicitly ruled that a “dominant position may create a clear imbalance...and must be taken into consideration in assessing whether the user of that network has validly and, in particular, freely given consent, since that circumstance is liable to affect the freedom of choice of that user, who might be unable to refuse or withdraw consent without detriment, as stated in recital 42 of the GDPR”.

3.3. Transparency of processing v. consent

Migrants do not have the right to withhold consent collection and processing of their biometric data, but the CJEU shifted a focus from choice to comprehensive procedural transparency. Thus, migrants retain a strict right to be informed about how their data is handled. The CJEU reinforced that transparency obligations must be strictly executed at the point of data collection, meaning that even if data collection is mandatory, border authorities must proactively issue clear, multilingual, and accessible notices explaining who will see the data, how long it will be stored (e.g. in the Eurodac database), and how individuals can access or correct it (case *EDPS v. Single Resolution Board* (Case C-413/23)).

Finally, in the *Opinion 1/15 (EU-Canada PNR Agreement)*, the CJEU reviewed the systematic transfer of Passenger Name Record (PNR) data of all international flight passengers entering or leaving the EU. The Court ruled that bulk data transfers cannot be covered by a blanket assumption of user consent via purchasing a plane ticket. Because travelers cannot realistically opt out of air travel surveillance, the collection must be bound by clear international agreements, heavily restricted automated filters, and immediate notification pathways for travelers.

3.4. Proportionality v. consent

The Court of Justice of the European Union has been clear on the point that generalized retention of sensitive personal data must satisfy a proportionality test. As confirmed in *La Quadrature du Net and Others* (Case C-511/18), even in national security contexts, proportionality requires that access to retained data be limited to serious crime, subject to prior review by an independent authority, and accompanied by notification to affected individuals where possible.

In the judgment in *Ligue des droits humains* (Case C-817/19) the Court held that the indiscriminate processing of all passengers' travel data under the PNR Directive, applied without any risk-based differentiation, fails to meet the necessity requirement laid down in Article 52(1) of the Charter.

The Court's judgment in *Prokuratuur* (Case C-746/18) reinforced that even targeted access by Europol and national police authorities to communications metadata requires prior judicial or independent administrative authorization under the Article 87 TFEU.

3.5. Systematic collection of data interpreted by the CJEU

Collection of personal data, including collection of biometric data by national authorities presents particularly sensitive area and as such, the Court of Justice of the European Union took a position that blanket or systematic collection of biometric data violates EU law. Under its individual assessment benchmark, authorities cannot rely on a presumed premise of "consent" and they must prove the "absolute necessity" of the collection on a strict case-by-case basis. This strict necessity test is the CJEU's benchmark for evaluating individual assessments of biometric processing by which the Court does not recognize so called blanket approvals. Legal threshold for collecting biometrics like fingerprints or facial photos goes beyond a reasonable suspicion of a criminal offense and Authorities must explicitly demonstrate that less intrusive alternative measures could not achieve the same investigative purpose.

Every biometric request requires explicit reasoning, so the individual can exercise their right to a judicial appeal. National frameworks must explicitly restrict processing to highly specific, concrete legal purposes instead of generic profiling. National laws that render biometric collection automatic—without giving authorities the power to assess the specific risk of the individual—would be considered illegal. Fining or penalizing an individual for refusing to give biometric data is only legal if

the underlying collection strictly passes the proportionality and absolute necessity checks first.

Two benchmark rulings that define the CJEU's framework on biometric collection are *Comdribus* (Case C-371/24) and *JH v Policejní prezidium* (Case C-57/23). Both rulings restrict the police's ability to automate the collection of sensitive bodily data, but *Comdribus* limits collection during initial police custody, while in *JH v Policejní prezidium* the Court limits indefinite database retention.

This case firmly established the CJEU's individual assessment benchmark regarding the initial collection of fingerprints and photographs under threat of criminal penalties. A climate justice activist ("HW") was detained in Paris for organizing an unauthorized demonstration. While in custody, he refused to provide fingerprints or photographs. Even though he was ultimately acquitted of the underlying demonstration offense, French courts still fined and convicted him solely for refusing the biometric collection. The Court ruled that France's broad police profiling practices violated EU law. Biometric data collection cannot be a systematic, automatic procedure for anyone placed in custody. According to the individual assessment benchmark, the police must demonstrate "absolute necessity" on a case-by-case basis. The fact that someone is a suspect does not automatically justify taking biometrics; authorities must explicitly state specific reasons why the data is required for *that specific* investigation. Penalizing an individual for refusing collection is illegal unless the underlying collection request first passes this strict proportionality test.

In the second case, C-57/23: *JH v Policejní prezidium*, a Czech public official was convicted of a misconduct in public office. The Czech police collected his photographs, fingerprints, and a DNA sample. Under Czech law, this data could be stored indefinitely for "future identification" of any intentional offense. The official challenged the permanent retention as a violation of his right to privacy. The court held that while the initial collection of data for severe crimes may be justified under strict necessity, indefinite, un-categorized database storage is a grave violation of the applicable Law Enforcement Directive. This case restricted the "store and forget" policies of police databases, adding strict rules for genetic and biometric retention. Authorities must implement periodic review cycles and clear deletion timelines. "Blanket" or indiscriminate lifelong storage is banned; databases must utilize mandatory periodic reviews to assess if keeping the data remains strictly necessary. Individuals must have an effective legal remedy to demand data erasure once they are rehabilitated.

In case C-118/22, *NG v Bulgaria*, the CJEU ruled on the ban on lifelong retention that storing a convicted individual's biometric data until their death is contrary to EU law. Even if an individual was lawfully convicted, once they are legally rehabilitated or their sentence is served, the data must be eligible for erasure unless specific, heightened risks are actively proven.

3.6. Obligation of periodic review of stored biometric data

In case C-57/23, *JH v Policejní prezidium*, the Court required from the EU national laws to set a clear timeframe for periodic reviews of stored data. During periodic reviews, the data controller (the police) bears the burden to prove that retaining the biometrics is still *strictly necessary* to prevent or investigate severe crimes; if they cannot, the data must be automatically erased.

3.7. Right to erasure of biometric data

The Court of Justice of the European Union (CJEU) rules that individuals have a strict "right to erasure" (right to be forgotten) for biometric data if its continued storage is no longer strictly necessary. Under Article 16 of the Law Enforcement Directive (LED), the CJEU has completely outlawed "store-and-forget" policies, meaning police databases cannot indefinitely retain fingerprints, facial images, or DNA profiles. The CJEU enforces the right to immediate erasure upon acquittal (standard set in *Comdribus* case).

Further, the Court deciding in the Case C-371/24, for biometric data collected during custody, but the accused was subsequently acquitted or the charges were dropped, the baseline justification for keeping disappears.

If a court finds that the initial collection lacked an individualized assessment of "absolute necessity," the data is deemed unlawfully processed and must be erased immediately without waiting for database retention cycles.

4. Meaningful consent in processing of biometrical data in migration management

Consent in the EU migration management is highly contested topic. Similarly to labour relations, where due to the severe power imbalance between the employer and employee, the voluntary nature of the agreement legally invalidates consent, it is not realistic to expect that a migrant could freely consent to the use of his/her biometric data. For the reasons of regulatory compliance, an illusion of choice was created. Thus, in the EU migration management today we have a pro forma administrative requirement devoid of substantive user agency and pure liability-mitigation formality in a form of a take-it-or-leave-it ultimatum. Non-voluntary compliance clause directly states that the person wishing to move to the EU Members States has no real choice but to agree to collection and processing of his or her biometric data.

In migration management, this imbalance is absolute: a migrant cannot refuse data collection without risking the rejection of their asylum claim, detention, or immediate deportation. Because true autonomy is missing, Member States cannot legally use consent to justify processing asylum or border data.

McLean argues that while the law claims to prioritize patient autonomy, its actual application in medical contexts often dilutes or misinterprets the concept, reducing it

to a mere bureaucratic box-checking exercise. Courts and medical institutions frequently prioritize risk management, professional standards, and institutional efficiency over genuine patient choice (McLean, 2021).

Under the Regulation (EU) 2017/2226, the collection of biometrics (a facial image and fingerprints) constitutes a mandatory element of the entry procedure for short-stay third-country nationals (Articles 16 and 17). That obligation operates in conjunction with the Schengen Borders Code (Regulation (EU) 2016/399), which requires third-country nationals to submit to border checks in order to fulfil the conditions of entry (Articles 6 and 8). A refusal to provide the required biometric data prevents the completion of those legally required checks and therefore entails a refusal of entry under Article 14 of the Schengen Borders Code, which is subsequently recorded in the EES. The GDPR recognises that consent is invalid where a significant power imbalance means the data subject has no genuine free choice (Recital 43 and Art 7(4), GDPR) (Jain, 2026).

4. Conclusion

The EU's, EES, and EURODAC systems employ a multi-tiered architecture that mandates mass biometric registration, utilizing strict legal overrides of GDPR consent requirements in favour of statutory obligations and public interest. This framework enables widespread data sharing, creating a structural tension with fundamental rights regarding proportionality and purpose limitation, particularly concerning the five-year retention and secondary use of biometric templates.

The Court of Justice of the European Union (CJEU) holds that in migration and administrative contexts, public interest and statutory requirements override individual consent regarding the collection of biometric data, treating it as a mandated, proportionate limitation on rights. Due to inherent power imbalances between individuals and authorities, such consent cannot be considered freely given, invalidating it as a legal basis in situations of structural asymmetry, such as in *Meta Platforms v. Bundeskartellamt*. The court mandated strict procedural transparency, including proactive notifications at the point of collection, even when data processing is mandatory, per *EDPS v. Single Resolution Board*.

Furthermore, the CJEU prohibited blanket or indiscriminate biometric collection, enforcing an "individual assessment benchmark" requiring absolute necessity and proportionality, as established in cases such as *La Quadrature du Net*, *Ligue des droits humains*, *Comdribus*, and *JH v Policejní prezidium*.

The severe power imbalance between EU authorities and migrants renders voluntary consent for biometric data processing an illusion, as refusal results in penalties like denied entry or detention. Consequently, mandatory data collection under the Schengen Borders Code and Regulation (EU) 2017/2226 acts as a pro forma requirement that violates the GDPR's requirement for genuine, free choice, as noted in analyses of the system.

Taking into consideration that we cannot consider migration related consent to collect and process biometric data genuine and freely given, we should still employ CJEU legal safeguards such as strict proportionality assessment, obligation of period review, right to erase personal data and ban on systematic collection of biometric data because those legal safeguards at least minimize possibility of data abuse and provide additional layer of legal protection to migrants.

Literature

- Alexander, L. (1996) “The Moral Magic of Consent (II),” *Legal Theory* 2: 165–274.
- Jain, S. (2026), The EU Entry/Exit System and the Interoperability Trap: How Structural Function Creep Hollows Out Proportionality, <https://www.europeanlawblog.eu/pub/iwfwun2b/release/1>
- Kleinig, J. (2010). The nature of consent. In *The ethics of consent: Theory and practice* (Miller & Wertheim, ed.), New York: Oxford University Press.
- McLean, S.A.M. (2010) *Autonomy, Consent and the Law*. Oxon: Routledge.
- Miller Franklin G. Wertheimer Alan (2010) *The Ethics of Consent: Theory and Practice* Preface to a Theory of Consent Transactions: Beyond Valid Consent” Schermer, B.W., Custers, B. & van der Hof, S. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics Inf Technol* 16, 171–182 (2014). <https://doi.org/10.1007/s10676-014-9343-8>
- Nir, E. (2019) Informed Consent, *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/spr2019/entries/informed-consent/>
- O'Neill, O. (2003) Some Limits of Informed Consent, *Journal of Medical Ethics*
- Raz, J. (1986) *The Morality of Freedom*. Oxford, New York: Clarendon Press.
- Simmons, A. John. (1998) *Consent* Routledge Encyclopedia of Philosophy, Taylor and Francis, <https://www.rep.routledge.com/articles/thematic/consent/v-1>

Legal instruments

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)

The EU Charter on Fundamental Rights

The Entry/Exit System/EES Regulation (EU) 2017/2226

Schengen Borders Code (Regulation (EU) 2016/399)

The EURODAC Regulation (EU) 2024/1358

Case-Law of the CJEU

Case C-291/12 Schwarz v. Stadt Bochum

Case C-543/09 Deutsche Telekom

Case C-252/21 Meta Platforms v. Bundeskartellamt

Case C-413/23 EDPS v. Single Resolution Board

Case C-817/19 Ligue des droits humains

Case C-746/18 Prokuratuur

Case C-371/24 Comdribus

Case C-57/23, JH v Policejní prezidium