SENTENCE ADJUSTMENT MECHANISMS IN EUROPE:

European Standards and National Patterns Across Seven European Countries

December 2025

EUROPEAN PRISON LITIGATION NETWORK

This report is part
of the project

PRISON CIVIL ACT

Activating civil society
interventions to address the
structural problems of prison
systems in Europe

In partnership with:

UNIVERSIDAD
COMPLUTENSE
MADRID

HELSINKI FOUNDATION
FOR HUMAN RIGHTS

Universidad
Francisco de Vitoria
UFV Madrid

Centre de
Recherches
en Droit Pénal

ULB

FORUM PENAL
Associação de Advogados Penalistas

Strafvollzugsarchiv

**Funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

CHAPTER 3

Data Protection and Automated Decision-Making in Sentence Adjustment: European Standards through the Lens of Prisoners' Rights

AUTHOR:
Viktoria Kasongo Akerø
European Prison Litigation Network

EUROPEAN PRISON LITIGATION NETWORK

CONTENTS

INTRODUCTION

Across Europe, considerations of data protection have become increasingly central to the determination of access to sentence adjustment mechanisms, viewed from the perspective of prisoners' rights. Access to sentence adjustment mechanisms now depends not only on judicial determinations or professional discretion, but on the collection of large datasets, inter-agency information flows, and, in many systems, algorithmically supported risk assessments. As penal policy has shifted toward risk management and actuarial governance, criminal procedure has undergone a process of progressive technologisation, culminating in the growing incursion of statistical, data-driven evaluations of risk and a corresponding expansion in the processing of prisoners' personal data, both in invasiveness and scope.[1]

While there exists a growing body of scholarship examining predictive policing,[2] algorithmic governance,[3] and data protection in criminal justice more broadly,[4] there are few, if any, focused assessments of data protection and automated processing standards across the EU and CoE in light of prisoners' rights in the context of sentence adjustment mechanisms. Yet the specific context of sentence adjustment raises distinct concerns. Data protection and standards governing automated processing are especially crucial here, as the data collected and the ways it is processed are highly sensitive, personal, and wide-reaching. The data can be deeply invasive, and decisions informed by it carry profound consequences for the individual, directly affecting their access to liberty.

This chapter provides a focused assessment of Council of Europe ('CoE') and European Union ('EU') standards on data protection and automated

1 C McKay, 'Predicting risk in criminal procedure: actuarial tools, algorithms, AI and judicial decision-making' (2020) Current Issues in Criminal Justice 32(1) 22–39.

2 See, e.g., Ferguson, Andrew Guthrie, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (NYU Press 2017); Brayne, Sarah, Predict and Surveil: Data, Discretion, and the Future of Policing (Oxford University Press 2020); Sanders, Carrie B. and Sheptycki, James, 'Policing, Crime and "Big Data"; Towards a Critique of the Moral Economy of Stochastic Governance' (2017) 8 Crime, Media, Culture 3; Meijer, Albert and Wessels, Martijn, 'Predictive Policing: Review of Benefits and Drawbacks' (2019) 38 International Journal of Public Administration 1031.

3 See, e.g., Lynskey, Orla, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 International Journal of Law in Context 319; Kaminski, Margot E., 'The Right to Explanation, Explained' (2019) 34 Berkeley Technology Law Journal 189; Selbst, Andrew D. and Powles, Julia, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233; Wachter, Sandra, Mittelstadt, Brent, and Floridi, Luciano, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.

4 Eubanks, Virginia, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St Martin's Press 2018); Yeung, Karen, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 Regulation & Governance 505.

processing as they apply to the execution of criminal sentences, examined through the lens of prisoners' rights in the context of sentence adjustment. It proceeds in two parts.

Part I situates sentence adjustment within the broader European data protection framework. It begins by outlining the definition of 'personal data' and the legal tests for distinguishing personal from non-personal information, and then provides context for the ways in which the prisoner is a complex and especially vulnerable data subject, whose personal data is extensively collected, processed, and mobilised in decisions affecting liberty. It then traces the intertwined historical development of CoE and EU data protection standards, highlighting the evolution from Convention 108 and Recommendation R(87)15 to the General Data Protection Regulation (GDPR)[5] and the later Law Enforcement Directive ('LED').[6] The chapter next examines the structural relationship between the GDPR and the LED in the context of sentence enforcement, before analysing the substantive principles governing data processing under both instruments. It also briefly addresses the limitations and critiques of these standards when applied in criminal justice settings.

Part II turns to the growing role of automated and semi-automated processing in sentence adjustment decisions. After situating risk assessment instruments within the broader shift toward actuarial penal governance, it examines the regulatory treatment of automated decision-making under Article 22 GDPR and Article 11 LED. This Part evaluates the scope of the prohibition on decisions based solely on automated processing, the meaning of 'significant effects', the adequacy of safeguards, such as human intervention, and the challenges of transparency and contestability in practice. It assesses whether the existing European framework meaningfully constrains algorithmically structured decision-making in the context of sentence adjustment mechanisms.

5 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 (General Data Protection Regulation) [2016] OJ L119/1.

6 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

1 EUROPEAN DATA PROTECTION STANDARDS IN THE CONTEXT OF SENTENCE ADJUSTMENT

1.1 CONTEXT

WHAT QUALIFIES AS 'PERSONAL DATA'?

European data protection law constructs "personal data" broadly to encompass any information relating to an identified or identifiable natural person. Under GDPR Article 4, personal data includes information that can directly or indirectly identify a person, such as names, identification numbers, location data, online identifiers, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity. The LED, Article 3, adopts an almost identical definition, reflecting the consistency of EU standards across civilian and law enforcement contexts. Both instruments further define "processing" expansively, covering operations such as collection, organisation, storage, use, dissemination, alignment, combination, restriction, and erasure, whether automated or manual.

At first glance, the concept may appear straightforward; however, "what constitutes personal data is one of the central causes of doubt" in the current data protection framework.[7] Guidance is available from the Article 29 Working Party on interpreting the four elements outlined in Article 4(1) GDPR – namely, 'any information', 'relating to', 'an identified or identifiable', and 'natural person'.[8]

Drawing a clear distinction between personal and non-personal data is essential for defining the reach of European data protection law. Personal data—including 'pseudonymous' data—falls within the Regulation's scope, whereas non-personal data does not. Determining whether a piece of information qualifies as personal data is therefore critical, and this task becomes increasingly burdensome as the data itself grows more complex.

7 Lilian Edwards, 'Data Protection I: Enter the GDPR' in Lilian Edwards (ed), Law, Policy and the Internet (Hart 2018) 84; see also Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 International Data Privacy Law 11.

8 Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data (WP 136) 01248/07/EN, 6.

The classification of personal data is context-dependent. A single data point may be considered personal or non-personal depending on the circumstances, and thus either fall under or escape the Regulation's application. Data is deemed to "relate to" a data subject when it is "about that individual".[9] This includes not only information held in an individual's file but also vehicle data that reveals information about the data subject.[10] A person is regarded as identified or identifiable if they can be "distinguished" from others.[11] Identification does not require the individual's name; they may be identified through alternative means such as a telephone number.[12] This underlines that the concept of personal data should be interpreted broadly, a position consistently embraced by the Court. In Nowak, the Court held that the expression 'any information' reflects "the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective".[13]

The legal test for distinguishing between personal and non-personal data is articulated in Recital 26 GDPR, which provides:

> " (p)ersonal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. "

In sum, the classification of personal data must be understood broadly and contextually. Information qualifies as personal not only when it directly identifies an individual, but also when it "relates to" a natural person who can be identified, directly or indirectly, through any reasonably available means. This expansive interpretation ensures that the wide range of data collected for parole and other sentence adjustment

9 A29WP on the concept of personal data.

10 Ibid, 7; CJEU, Case C-345/17 Sergejs Buivids (2019) EU:C:2019:122, para 31.

11 CJEU, Case C-101/01 Bodil Lindqvist (2003) EU:C:2003:596, para 27.

12 Ibid.

13 CJEU, Case C-434/16 Peter Nowak (2017) EU:C:2017:582, para 34.

mechanisms—including offence history, behavioural records, risk and psychological assessments, social and economic factors, professional reports, and reintegration plans—are construed as falling squarely within the protective scope of the GDPR,[14] influencing decisions about an individual's liberty.

THE PRISONER AS A DATA SUBJECT

Prisoners are subject to intensive data collection that extends far beyond the mere recording of offence history. Personal information is harvested to construct a "comprehensive profile" that includes social, psychological, environmental, and economic factors. Personal information is collected and processed to capture behavioural patterns, disciplinary records, social and economic indicators such as housing stability, family support, and employment readiness, as well as health and psychological information, including medical records, mental health diagnoses, and substance use history. The transition to risk-based actuarial governance has intensified the collection of diverse datasets.

The Polish context offers illustration of the vast variety, invasiveness and scope of the data collected on prisoners both leading up to and during imprisonment. Information gathered extends far beyond basic identification and conviction details, encompassing criminal history, sentence progression, and granular assessments of behaviour in custody, participation in work and educational programmes, disciplinary records, and compliance with institutional rules. Risk assessment tools such as PSORR[15] aggregate hundreds of static and dynamic variables, including family background, early socialisation patterns, financial instability, housing prospects, social networks, mental health diagnoses, substance dependence, sexual disorders and attitudinal indicators such as remorse, denial or 'demoralisation'.

The data is drawn from a wide array of sources: prison staff observations, psychological, psychiatric and sexological examinations, structured risk assessment instruments, historical criminal justice records, the prisoner's own statements, and probation officers' social inquiries involving interviews with family members and neighbours as well as home visits assessing living conditions and social environment. It is then consolidated and preserved within institutional files and expert reports and, crucially, within the Central Database of Persons Deprived of Liberty, a centralised IT system that records conduct, behavioural changes,

14 See, e.g., in the UK context LINL.

15 For further information, see the section below.

legal-status developments and leave outcomes over time. A longitudinal, digitised and predictive record that penetrates deeply into the private, psychological and social spheres of prisoners' lives is produced.

Data protection standards are especially crucial when viewed from the perspective of safeguarding the rights of prisoners. Through the collection and processing of personal data, prison and probation services exercise some of the most direct manifestations of public power, with the potential to profoundly impact human dignity, rights, and privacy.[16] The data harvested by prison and probation services directly shape classification, progression, parole and access to liberty, and thus have grave consequences for the individual concerned. Moreover, individuals in detention are in a structurally vulnerable position, characterised by dependency on the authorities that collect and process their data and by limited practical capacity to access, verify or challenge the information held about them. Within this context, data protection standards – including the core principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality (security)[17] – form part of the guarantee of a fair, transparent and rights-compliant execution of sentence. European standards, as developed by the Council of Europe and the European Union, have evolved over the years in response to these and wider challenges, and it is to those standards that the analysis now turns.

1.2 THE COE AND EU'S INTERTWINED TRAJECTORIES: THE HISTORICAL CONSTRUCTION OF EUROPEAN DATA PROTECTION STANDARDS

Over the past four decades, the development of European data protection standards has been shaped by a dynamic interplay between the Council of Europe and the European Union. The CoE pioneered early binding and soft law instruments, while the EU has emerged as the central authority in the digital era through the GDPR and Law Enforcement Directive. Over time, the two systems have influenced one another, resulting in substantial convergence of European data protection standards.

16 CM/Rec(2024)5 - Recommendation of the Committee of Ministers to member States regarding the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services (Adopted by the Committee of Ministers on 9 October 2024 at the 1509th meeting of the Ministers' Deputies)

17 See Article 5 GDPR.

Challenges to the use of data by the State and law enforcement authorities for criminal justice purposes have traditionally been anchored in Article 8 of the European Convention on Human Rights, which provides for the right to respect for private life.[18] Several factors explain this. Most notably, the EU Charter of Fundamental Rights only became legally binding in December 2009, by which time a substantial body of jurisprudence under Article 8 ECHR had already been established. Even after the Charter entered into force, its relevance in the law enforcement sphere remained constrained. Under Article 51(1) of the EU Charter, it binds Member States only when they are implementing Union law. Prior to the adoption of the Law Enforcement Directive (LED), there was no EU legislation governing the processing of personal data by law enforcement authorities for purely domestic criminal justice purposes. As a result, such data processing fell outside the scope of the Charter. With the subsequent introduction of EU legislation in this field, however, the conditions and implications of the Charter's application now warrant closer examination.

The CoE acted as a pioneer in this area in general and for standards on data protection in the context of law enforcement, particularly early on with both its flagship hard law, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'),[19] and its flagship soft law instrument, Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector (1987). The Convention 108 was the first European-wide common 'model law'. This was seminal in several respects – it inscribed in a legally binding instrument the notion of 'data protection', made the link between data protection and the 'right to privacy' protected under Article 8 ECHR.[20] Its coming into force in 1985 coincided with the milestone 1987 Leander judgement[21] of the European Court of Human Rights, when the Court first declared that the mere storage of personal data, in that case by the police, amounts to an interference with Article 8. Convention 108 laid down basic principles of data protection, which remained cornerstones of European data protection law until the present day, and their importance was reinforced by the adoption of the amending protocol to the Modernised Convention 108.[22]

18 See, e.g., ECtHR, S and Marper v United Kingdom (Applications nos. 30562/04 and 30566/04) [2008] ECHR 1581 (Grand Chamber, 4 December 2008).

19 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Treaty Series No 108, opened for signature 28 January 1981, entered into force 1 October 1985) ('Convention 108').

20 González Fuster, The Emergence of the Personal Data Protection as a Fundamental Right in the EU (Springer 2014), p. 89.

21 Leander v Sweden (1987) 9 EHRR 433 (ECtHR).

22 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), opened for signature 10 October 2018.

Prior to the Treaty of Lisbon,[23] the European Communities lacked competence in the law enforcement field. Under the three-pillar structure established by the Treaty on European Union, cooperation in criminal matters remained largely intergovernmental, and EU regulatory powers in this sector were limited. During this period, the principal reference framework for data protection in law enforcement was provided by the Council of Europe. The Convention 108 and Recommendation R(87)15 shaped data protection standards in law enforcement from the Schengen negotiations of 1985 and the 1990 Implementing Convention, through to the adoption of the 2008 Framework Decision on data protection in police and judicial cooperation.

Convention 108 thus exercised sustained influence over EU law enforcement data protection rules, including indirectly over the later Law Enforcement Directive ('LED').[24] However, the balance of normative leadership shifted following the entry into force of the Lisbon Treaty, which introduced a clear and comprehensive legal basis for EU data protection legislation in Article 16 TFEU. With strengthened competence in the Area of Freedom, Security and Justice, the EU adopted the General Data Protection Regulation ('GDPR')[25] and the Law Enforcement Directive in 2016. These instruments have become the central instruments in the field.

The final text of the Law Enforcement Directive reflects this transitional moment: it is the product of combined influences stemming from Convention 108 and R(87)15 on the one hand, and the GDPR on the other. Yet once the GDPR proposal was tabled in 2012, the direction of influence increasingly ran from the EU to the Council of Europe. The Council of Europe consequently undertook the modernisation of Convention 108 in order to maintain alignment with evolving EU standards, culminating in the adoption of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised Convention 108, 'Convention 108+') in 2018,[26] two years after the GDPR. The subsequent Practical Guide to the Modernised Convention,[27] adopted shortly after the Law Enforcement Directive, demonstrates substantial convergence between the Council of Europe and EU frameworks, particularly in the alignment between Convention 108+ and the GDPR.

23 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C 306/1 (13 December 2007, entered into force 1 December 2009).

24 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

26 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

27 The Modernised Convention 108: A Practical Guide.

1.3 NAVIGATING THE OVERLAP: THE LED AND GDPR

The relationship between the LED and the GDPR is defined by both complementary and distinct scopes, yet in practice, the boundaries between them can be blurred, particularly in the context of criminal justice and the execution of sentences. Broadly, the GDPR establishes a harmonised framework for general data processing across the EU, applying to private actors, administrative bodies, and public authorities outside the law enforcement sphere. Its material scope expressly excludes processing carried out by competent authorities for the prevention, investigation, detection, or prosecution of criminal offences, as well as for the execution of criminal penalties or safeguarding public security.[28] Conversely, the LED operates as lex specialis for such law enforcement activities, establishing a tailored regime for personal data processing by competent authorities, including prison administrations, probation services, and judicial bodies.[29]

In order to fall within the scope of the LED, the data processing must be undertaken by a 'competent authority'. A competent authority is defined as:

> " any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security; or any other body or entity entrusted by Member State law to exercise public authority and public powers for these purposes.[30] "

Where a private entity processes personal data for law enforcement objectives, it must first be formally authorised under Member State law in order to fall outside the material scope of the GDPR and instead come within the relevant provisions of the LED. In the absence of such a legal designation, the GDPR remains applicable to private actors engaging in processing for law enforcement purposes.

28 Article 2, GDPR.

29 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

30 Article 3(7)(a) and (b) LED.

This interpretation finds implicit support in Article 23 GDPR, which permits Union or Member State legislation to limit certain GDPR obligations where this is necessary for law enforcement aims. The very existence of this provision suggests that, without such legislative restriction, the GDPR would continue to govern processing undertaken in this context. Consequently, much depends on how a 'competent authority' is defined for the purposes of the LED, and under what conditions a private body may be considered to have been legally entrusted with that role. It remains open to question, however, whether such entrustment must take the form of a specific legislative measure.[31]

Secondly, even where processing is carried out by a "competent authority", the applicable legal regime depends on the objective pursued. The decisive factor is therefore the purpose of the processing. In the context of data sharing, if a competent authority transfers personal data to a body that is not itself a competent authority for law enforcement purposes, for example, providing data to a private company, the transfer falls within the scope of the LED. By contrast, where the transmission serves a non-law enforcement aim, such as sharing information with medical or social services, the GDPR governs the processing.[32]

Similarly, if personal data are initially collected by a competent authority for law enforcement purposes but are subsequently processed for different, non-law enforcement objectives, the GDPR becomes applicable.[33] Garstka describes this movement from the LED framework to that of the GDPR as a "downgrade".[34] However, it is not self-evident that the LED always offers stronger safeguards than the GDPR, particularly in relation to automated decision-making.[35]

This practical overlap between the LED and GDPR creates a zone of uncertainty. When it is unclear which legal regime governs the processing of their personal data, prisoners may face reduced safeguards, inconsistent access to information, and limited remedies. Decisions about temporary release, parole, or other sentence adjustments may be influenced by data processed under different standards, with varying procedural guarantees.

31 Kamil Garstka, 'Between Security and Data Protection: Searching for a Model Big Data Surveillance Scheme within the European Union Data Protection Framework' (2018) PDF accessed 17 February 2026.

32 Recital 34 LED.

33 Article 9(1) and Recital 11 LED.

34 Garstka (n 17).

35 See, e.g., Orla Lynskey, (2019) Criminal justice profiling and EU data protection law: precarious protection from predictive policing. International Journal of Law in Context, 15(2), 162-176. LINK.

1.4 PRECARIOUS PROTECTIONS? SUBSTANTIVE SAFEGUARDS UNDER LED AND GDPR

Having clarified the boundary between the LED and the GDPR, the substantive standards each instrument establishes in relation to the processing of personal data in the context of the execution of criminal sentences will now be outlined. Both instruments share dual objectives of protecting personal data and facilitating its free movement within the EU. The LED adapts these objectives to the law enforcement context, imposing a positive duty on Member States to safeguard the fundamental rights of data subjects and a negative duty to avoid unnecessary restrictions on cross-border data exchange by competent authorities.

The LED defines personal data broadly, encompassing any information relating to an identified or identifiable individual, including identifiers such as names, identification numbers, location data, or factors relating to physical, physiological, genetic, mental, economic, cultural, or social identity. In addition, it identifies specific "special categories of data" or sensitive data, including information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation, and biometric data when used to uniquely identify an individual.[36][37] Recital 37 LED emphasises that heightened protection may be required not only because of the intrinsic sensitivity of the data but also because of the context in which it is processed, such as during monitoring of an individual's movements in the course of sentence enforcement. The LED combines both the nature of the data and the context of processing to determine which personal data merit stricter safeguards.

The LED establishes fundamental principles for processing personal data by competent authorities in the criminal justice system, including lawfulness, purpose limitation, data minimisation, and storage limitation, requiring that data be collected for specified, explicit, and legitimate purposes, be adequate and relevant, and not be excessive relative to the objectives of law enforcement or sentence execution. It obliges authorities to set time limits for the retention of data or conduct periodic reviews, ensuring that personal data are not retained longer than necessary. The Directive also guarantees data subjects rights of access, rectification, erasure, and restriction of processing, although Member

36 Art. 10 LED.

37 Catherine Jasserand, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data' (2016) 2 European Data Protection Law Review 297.

States may legislate specific limitations where necessary for operational reasons. Authorities are required to provide information about data processing in an intelligible and accessible form. These principles guide prison administrations, probation services, and judicial bodies in the management of conviction-related data during incarceration, probation, or electronic monitoring.

In addition to these core principles, the LED sets standards for governance, oversight, and accountability. Competent authorities must designate a data protection officer to support compliance, implement appropriate technical and organisational security measures, and carry out data protection impact assessments where processing is likely to result in high risks to the rights and freedoms of data subjects. Supervisory authorities are responsible for oversight and may be the same bodies designated under the GDPR. They are expected to cooperate with supervisory authorities in other Member States to ensure a harmonised approach across the EU. The LED also establishes rules for transfers of personal data outside the EU, which are only permissible where necessary for law enforcement or sentence enforcement purposes and subject to adequate safeguards.

A central focus of the LED is the processing of personal data in the execution of criminal penalties. Recital 35 clarifies that Member States may allow individuals to consent to specific data processing, such as location monitoring via electronic tagging. By contrast, the GDPR governs processing that falls outside the law enforcement scope, such as the use of conviction-related data by administrative bodies or private actors for employment, regulatory, or other non-criminal justice purposes. Article 10 GDPR requires that any comprehensive register of criminal convictions be maintained exclusively under official authority, ensuring safeguards outside the LED framework.

Despite the comprehensive principles articulated in both the GDPR and the LED, scholars have raised concerns that the protective effect of these data protection standards in criminal justice settings is precarious.[38] It is often uncertain whether even highly intrusive profiling technologies fall clearly within the scope of existing data protection rules, as is discussed further below.[39] Determining applicability often hinges on complex, context-specific legal assessments that individuals – including

38 See, e.g., Lynskey (n 21); Stergios Aidinlis, David Barnard-Wills, Leanne Cochrane, Krzysztof Garstka, Agata Gurzawska and Joshua Hughes, 'Between GDPR and Law Enforcement Directive in Security Research: The Use of Personal Data by Law Enforcement Authorities' (2024) European Journal of Law and Technology Vol 15 No 3 LINK accessed 17 February 2026; Maria Grazia Porcedda, Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis (Hart Publishing, 1st edn 2023) Hart Studies in Information Law and Regulation.

39 Lynskey (n 21).

prisoners affected by such systems – are ill-positioned to perform themselves. This ambiguity weakens the substantive safeguards that the legal framework nominally provides.

Furthermore, data protection law in the law enforcement field remains under-developed, particularly in relation to profiling and the substantive rights available to data subjects. Provisions that are intended to guarantee rights, such as access, rectification, erasure, and restriction, can be limited or qualified by Member State law where operational needs are invoked. This flexibility can pose a significant dilution of the robustness of data protection standards.[40]

Finally, even fundamental principles such as data minimisation and purpose limitation, which are intended to constrain excessive or unrelated uses of personal information, can be difficult to enforce in practice within the sentence enforcement field. Without clear and enforceable operational standards, and with limited empirical evidence on how these principles are applied in law enforcement and sentence adjustment activities, there is a risk that broad collections of conviction-related data are reused for ancillary purposes or retained beyond what is necessary. Academic literature underscores that, in practice, these principles may be frustrated by procedural and technological realities, leading to outcomes that fall short of the normative aims of the GDPR and LED.[41]

40 Aidinlis et al (n 24).

41 Porcedda (n 24).

2 EUROPEAN STANDARDS ON AUTOMATED DECISION-MAKING (ADM) AND ARTIFICIAL INTELLIGENCE (AI)

2.1 CONTEXT

The second component increasingly relevant in the context of sentence adjustment mechanisms is the impact on prisoners' rights arising from the automated analysis of data for predictive criminal justice purposes. The progressive technologisation of criminal procedure has brought statistical, data-driven evaluations of risk into the judicial sphere. Human evaluative functions are increasingly supplemented by a variety of actuarial, algorithmic, machine learning, and Artificial Intelligence (AI) tools, which claim to provide accurate predictive capabilities and objective, consistent assessments of risk.[42] Yet these developments have generated significant ethical and human rights concerns worldwide, particularly regarding proprietary algorithms that may embed statistical bias and diminish the role of human judicial assessment.[43] A recent report from England and Wales noted a "lack of explicit standards, best practice, and openness or transparency about the use of algorithmic systems in criminal justice".[44] It is against this backdrop that the establishment and enforcement of human rights standards has become increasingly urgent.

This development must further be situated within the broader shift in penal policy in Europe, characterised by a growing emphasis on risk management and actuarial governance.[45] Indeed, the emergence of

42 Barabas, C., Dinakar, K., Ito, J., Virza, M., & Zittrain, J. (2017). Interventions over predictions: Reframing the ethical debate for actuarial risk assessment. arXiv preprint arXiv: 1712.08238.

43 Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. ProPublica. Retrieved from LINK; Barabas, C., Dinakar, K., Ito, J., Virza, M., & Zittrain, J. (2017). Interventions over predictions: Reframing the ethical debate for actuarial risk assessment. arXiv preprint arXiv: 1712.08238; Dawson, D., Schleiger, E., Horton, J., McLaughlin, J., Robinson, C., Quezada, G., ... Hajkowicz, S. (2019). Artificial intelligence: Australia's ethics framework. Data61 CSIRO, Australia. Retrieved from LINK European Commission High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. Retrieved from LINK; Wexler, R. (2017). Code of Silence. How private companies hide flaws in the software that governments use to decide who goes to prison and who gets out. Washington Monthly. Retrieved from LINK.

44 Law Society Commission on the Use of Algorithms in the Justice System and The Law Society of England and Wales. (2019, June). Algorithms in the criminal justice system. The Law Society of England and Wales. Retrieved from LINK, page 4.

45 Paula Maurutto and Kelly Hannah-Moffat, 'Assembling Risk and the Restructuring of Penal Control' (2006) 46(3) British Journal of Criminology 438; Sonja Snacken, An Bauwens, Dirk van Zyl Smit, Hanne Tournel and Ria Machiels, 'Prisons and Punishment in Europe' in Sophie Body-Gendrot, Mike Hough, Katalin Kerezsi, René Lévy and Sonja Snacken (eds), The Routledge Handbook of European Criminology (Routledge 2013) 422.

structured and increasingly technologised risk assessment instruments reflects what penal sociology has described as the "new penology": a reconfiguration of penal power away from individualised moral judgement and towards the management of aggregated risk.

Within this configuration, recommendations concerning sentence implementation modalities, such as temporary leave, open prison placement, conditional release, or early release, have progressively shifted from uniformed prison staff to psychological and psychiatric experts. Psychosocial risk assessments have thus become a central element in decision-making concerning social reintegration. Negative assessments, often grounded in diagnostic categories or offence types, can have profound consequences for prisoners' future prospects and their ability to benefit from sentence adjustment mechanisms.[46] In many systems, risk is no longer one consideration among several; it has become the decisive criterion for determining access to sentence adjustment.

While risk assessment has traditionally relied on clinical evaluation and unstructured professional judgement, the past decade has witnessed the rapid expansion of formalised and increasingly data-driven instruments across European States, supported and promoted by European and international bodies.[47] Among the most widely used tools in Europe[48] are the VERA-2R,[49] the ERG22+,[50] the RRAP,[51] the IR46,[52] and the RADAR-iTE.[53]

As covered in our research, stark examples include the PSORR system in Poland and Catalonia's RisCanvi. In Poland, the PSORR system exemplifies a rule-based, automated decision-making tool: it calculates risk scores according to predefined criteria, producing consistent outputs for a given set of inputs, without adapting or learning from new data. In contrast, Catalonia's RisCanvi is generally regarded as an AI-supported instrument: it combines multiple risk factors—including static characteristics, dynamic behaviours, and socio-family indicators—through algorithmic weighting, generating risk predictions that can evolve as new information is incorporated.

46 Ben Crewe, 'Depth, Weight, Tightness: Revisiting the Pains of Imprisonment' (2011) 13(5) Punishment & Society 509; Jason Warr, Forensic Psychologists (Emerald Publishing 2018).

47 UNODC, the Radicalisation Awareness Network, and more recently the UN Special Rapporteur on SUMEX.

48 European Commission, Risk Assessment in Prison (Radicalisation Awareness Network, 2021) PDF accessed 17 February 2026.

49 Violent Extremist Risk Assessment 2 Revised.

50 Extremism Risk Guidelines 22+-

51 Radicalisation Risk Assessment in Prisons.

52 Islamic Radicalisation Model 46.

53 Rule-based Analysis of Potentially Destructive Perpetrators to Assess Acute Risk – Islamist Terrorism.

These instruments generally adopt a Structured Professional Judgement (SPJ) approach: they provide structured criteria and scoring frameworks, yet retain a formal role for professional discretion. At the same time, they rely on the systematic collection and processing of personal data. Risk assessment instruments operate as statistical models designed to predict the likelihood of future outcomes by correlating individual characteristics – such as demographic data, criminal history, behavioural indicators, or responses to questionnaires – with predefined risk categories. Numerical representations of these features are combined into a risk score, typically generated through statistical techniques or heuristic weighting, and used to classify individuals into risk brackets that directly influence decision-making.

European standards govern both the use of automated data analysis for predictive ends and the deployment of AI in risk assessment. These areas will be addressed and analysed in turn below.

2.2 EUROPEAN STANDARDS ON AUTOMATED DECISION-MAKING (ADM): LED ARTICLE 11 VS GDPR ARTICLE 22 – PROHIBITIONS, PROTECTIONS, AND GAPS

The use of automated data analysis for predictive ends has long been a central preoccupation of EU data protection law. This concern was already evident in the 1995 Data Protection Directive, which notably introduced a right for individuals not to be subject to decisions based solely on automated processing.[54]

Scholars have in parallel with the growth of these standards explored the implications of the growing reliance on automated decision-making, highlighting the risks and structural shifts it entails. This has given rise to a substantial interdisciplinary body of work focused on ensuring that machine-learning systems operate in ways that are fair, accountable and transparent; an agenda often encapsulated in the idea of "algorithmic due process". [55]

54 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/23.

55 Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1.

The GDPR can be understood as a legislative attempt to respond to these normative concerns, prompting extensive academic debate about how its provisions regulate automated decision-making.[56] Yet, in the specific sphere of law enforcement it is typically the less widely examined legislative counterpart to the GDPR, namely the Law Enforcement Directive (LED), that provides the governing framework.

Article 11(1) of the LED establishes a prohibition on decisions that are based exclusively on automated processing in specified situations. The wording of this provision closely mirrors that of Article 22 GDPR. As a result, the Article 29 Working Party has observed that its interpretative guidance on Article 22 GDPR is also pertinent to Article 11 LED, though it emphasised that this parallel applies subject to significant qualifications and contextual adjustments.[57]

It is helpful to recite Article 11 LED in full:

"Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller".

A notable feature of this provision is its formulation. Whereas Article 22 GDPR is expressed as an individual entitlement – stating that the data subject "shall have the right not to be subject to a decision based solely on automated processing" – Article 11 LED is cast in prohibitive terms.

In textual terms, Article 11 LED therefore appears more stringent and protective than its GDPR equivalent. This distinction prompted the Article 29 Working Party to suggest that Article 22 GDPR should likewise be understood and applied as a prohibition rather than merely as an optional right.[58] As Kaminski has observed, construing Article 22 solely as an individual right could, somewhat paradoxically, weaken its protective effect: it would enable controllers to rely routinely on algorithmic decision-making in consequential contexts, modifying their practices only when individuals actively assert their rights.[59]

56 See, e.g., Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 2 International Data Privacy Law 76.

57 Article 29 Working Party, 2017.

58 Article 29 Working Party, 2018.

59 Michael Kaminski, 'The Right to Explanation, Explained' (2018) https://ssrn.com/abstract=3196985 accessed 17 February 2026.

However, notwithstanding its seemingly stricter formulation, the prohibition in Article 11 LED is qualified in several important respects. In particular, as with Article 22 GDPR, fully automated decision-making remains permissible where it is authorised by Union or Member State law. This means that national legislatures may provide a legal basis for law enforcement authorities to rely on entirely automated systems, including for broad or individualised assessments of the risk of future criminal behaviour.

That said, the LED does introduce an absolute ban on profiling that results in discrimination on the basis of sensitive characteristics, reflecting EU anti-discrimination principles and the requirements of the EU Charter.[60] In this regard, it establishes a clear substantive limit.

Furthermore, the LED does not replicate the GDPR's additional grounds permitting automated decision-making; namely necessity for the performance of a contract or reliance on the data subject's explicit consent. Such bases are absent from Article 11 LED. The most straightforward rationale is the structural imbalance of power between individuals and law enforcement authorities in this setting.[61] The Court of Justice of the European Union has likewise acknowledged the constraints of consent where individuals lack a genuine possibility to refuse processing. [62]

Although the GDPR permits automated decision-making on a broader set of grounds, it simultaneously establishes a more detailed framework of safeguards. Under the LED, automated decisions are allowed where authorised by Union or Member State law, provided that such legislation includes "appropriate safeguards" for the rights and freedoms of data subjects, including, at a minimum, the right to obtain human intervention from the controller. Recital 38 further clarifies, albeit in non-binding terms, that meaningful human intervention requires involvement by a person with both the authority and the competence to alter the outcome.

By comparison, Article 22(3) GDPR goes further. In addition to guaranteeing human intervention, it expressly grants individuals the right to present their views and to challenge the decision. The absence of equivalent wording in the LED suggests that these additional procedural guarantees, namely the opportunity to be heard and to contest the outcome, are not explicitly mandated in the law enforcement context.

60 Recital 38 LED; Article 11(3) LED.

61 Article 29 Working Party, 2017

62 Case C-291/12, Michael Schwarz v Stadt Bochum EU:C:2013:670.

At the same time, the LED does not establish a regime of maximum harmonisation. It makes clear that Member States may adopt provisions affording a higher level of protection.[63] Consequently, the manner in which Article 11 is implemented at national level will be crucial in determining the practical scope of individual safeguards. Furthermore, where automated decision-making involves sensitive data, Article 11(2) LED requires that such processing take place only if appropriate measures are in place to protect the data subject's rights, freedoms and legitimate interests. Considerable responsibility and discretion therefore rest with Member States, subject always to the overarching requirement that domestic implementing measures comply with the EU Charter.

Aside from the considerable potential to bypass the ban on automated decision-making through legislative means, Article 11 of the LED has other important limitations. Chief among these is that it covers only decisions that are made entirely through automated processing. Consequently, it is unclear whether outputs such as the recommendations generated by a risk assessment tool for parole eligibility qualify as decisions made 'solely' by automated processes. The answer depends on how the decision-making unfolds in practice. One must consider the degree to which the actor's own judgment and discretion shape the final decision. For example, if the actor consciously, or unconsciously, rely on the algorithm to make difficult or high-risk choices, then beyond the potential deskilling and erosion of evaluative skills this may cause, such decisions could effectively be treated as automated.[64] Conversely, if the final recommendation reflects the actor's independent judgment and oversight, then the decision is not purely automated, and Article 11 LED would not be applicable.

The next question is whether a given decision produces sufficient impact to fall within the scope of Article 11 LED. For this to occur, an automated decision must either have an 'adverse legal effect' on the individual or 'significantly affect' them. Article 11 LED differs slightly from the GDPR in its terminology: whereas the GDPR refers to decisions producing 'legal effects' or similarly significant impacts on the data subject, the LED specifies that the legal effect must be adverse. A decision is considered to 'significantly affect' a person where, for instance, they are denied access to services due to being on a blacklist.[65] In both Article 11 LED and Article 22 GDPR, decisions with only minimal or trivial effects do not meet the threshold for the prohibition.

63 Recital 15; Article 1(3) LED.

64 Michael Oswald et al, 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality' (2018) Information & Communications Technology Law 223.

65 Article 29 Working Party, 2017.

There remain open questions when applying this standard to automated systems in sentence adjustment. For instance, consider a risk assessment tool that produces recommendations on parole eligibility or early release. Article 11 LED would only be engaged if the resulting decision has a significant effect on the individual. The argument could be made within this frame that the automated recommendation itself, an advisory score or classification, does not directly impact the prisoner; it is the final decision made by the parole board or relevant authority, which incorporates the officer's judgment alongside the recommendation, that produces the tangible legal or practical effect. This is a potential gap in the protection the framework can afford for prisoners in this context.

A further question concerns broader, systemic effects. For example, if a risk assessment algorithm categorises certain groups of prisoners as high-risk or certain facilities as problematic, could the collective consequences, such as stricter conditions or increased barriers to access to sentence adjustment, trigger Article 11 LED, or must adverse effects be shown on an individual basis?

Moreover, it is uncertain how transparent automated decision-making is required to be vis-à-vis the prisoner. Article 24 LED obliges data controllers to maintain records of all categories of processing activities under their responsibility, including profiling where relevant. This is a broader requirement than what the GDPR generally prescribes, and the Article 29 Working Party has stressed that Member States should enforce it carefully. At the same time, Article 13 LED does not explicitly require that prisoners be informed about the existence of automated decision-making, unlike the GDPR. Nevertheless, as the Article 29 Working Party has noted, such information could be provided under Article 13(2)(d) LED, which allows Member States to require controllers to furnish additional details enabling individuals to exercise their rights. Providing prisoners with meaningful explanations about automated processing, including profiling and the logic underlying decisions, is particularly important to ensure fairness in line with Article 4(1) LED, which mandates lawful and fair data processing. Ultimately, the transparency and fairness of these systems will largely depend on how Member States implement and interpret the Directive.

In conclusion, while Article 11 LED appears to offer a clear prohibition on fully automated decision-making, its practical protective effect in the context of sentence adjustment is limited. National legislatures can authorise the use of automated risk assessment tools, potentially circumventing the restriction. Even where the law applies, uncertainties remain regarding the extent of human involvement required and the threshold

of impact needed to engage the prohibition. Moreover, the complexity of data flows across multiple actors in sentence adjustment, ranging from prison officers to psychologists and parole boards, further complicates the identification of applicable safeguards. Questions of transparency and access to information also persist, as prisoners may have limited awareness of how automated outputs influence decisions affecting them. Navigating the LED's protections in practice can be challenging for individuals, underscoring the critical role of national supervisory authorities and representative bodies in ensuring that prisoners' rights are effectively upheld.

2.3 EUROPEAN STANDARDS FOR AI IN RISK ASSESSMENT FOR SENTENCE DECISIONS

Artificial intelligence (AI) systems are increasingly used in European criminal justice to assess the risk of reoffending and support decisions regarding sentencing, probation, parole, and other forms of sentence adjustment.[66] These tools analyse personal, behavioural, and socio-environmental data to generate risk predictions that can influence or determine access to temporary leave, open prison regimes, or early release. An example is Catalonia's RisCanvi, included in our study on the Spanish context, which combines multiple static and dynamic risk factors through algorithmic weighting, producing risk scores that can evolve as new information is added. Technically, RisCanvi occupies a space between traditional automated decision-making (ADM) and AI: unlike fully rule-based ADM tools that deliver fixed outputs for given inputs, it incorporates adaptive, data-driven processing capable of identifying correlations not explicitly programmed, while still embedding structured professional judgement.

Offenders continue to enjoy their fundamental rights and freedoms, including the right to respect for private life and the right to data protection, when AI and related digital technologies are used. Limitations to these rights and freedoms should only be allowed when they are in accordance with law, respect the essence of fundamental rights and freedoms, pursue a legitimate aim, are necessary in a democratic society and are proportionate.[67]

66 LINK.

67 Recommendation CM/Rec(2024)5 of the Committee of Ministers to member States on the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services.

AI is defined under Article 2 of the CoE Framework Convention on AI as "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments". It further sets out that "different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment". This formulation mirrors the definition set out in Article 3(1) of the EU AI Act.[68] Among AI techniques, machine learning in particular has come to be extensively deployed to detect correlations between data points, enabling systems to generate predictions and recommendations, as well as to score, classify, or rank items or individuals.[69]

In recent years, standards governing the use of artificial intelligence ('AI') have developed across the EU and CoE.[70] While early regulatory efforts focused primarily on ethical guidance and policy coordination, 2024 marked a turning point with the adoption of several binding instruments. These standards apply across criminal justice contexts, including prison and probation services, with more targeted guidance now in place, as represented by the Council of Europe 2024 Recommendation on the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services.[71]

This Recommendation seeks to guide member states as AI becomes increasingly embedded in criminal justice systems.[72] It recognises that the execution of penal sanctions constitutes one of the most intrusive exercises of public power, profoundly affecting human dignity, privacy and liberty.[73] It establishes general principles intended to ensure that AI is used legitimately, proportionately and only where it contributes to rehabilitation.[74] It emphasises that AI should assist, rather than

68 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, Article 3(1) defines an AI system as "a machinebased system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"

69 According to Binns, "[m]ost uses of machine learning in the public sector are of the supervised variety. Supervision refers to the fact that the learning algorithm has to be shown what a decisionmaker wants to predict or classify, unlike unsupervised methods that are designed to discover latent structure in a dataset". See Binns R. (2020), "Algorithmic decision-making: a guide for lawyers", Judicial Review, Vol. 25, No. 2, pp. 3-4.

70 For a recent analysis of these standards in the context of criminal justice, see Marina Matic Boskovic, 'Implications of EU AI Regulation for Criminal Justice' (2024) Regional Law Review 111–120 LINK.

71 Recommendation CM/Rec(2024)5 of the Committee of Ministers to member States on the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services.

72 Appendix I(a)

73 Preamble

74 Appendix I(d); Appendix III(4)

replace, prison and probation staff, and that decision-making must remain human-centred or "a key element".[75]

Despite its safeguards, the Recommendation amounts to a clear normative endorsement of AI in the execution of sentences,[76] including in areas such as risk assessment and offender management that directly shape decisions on progression, conditional release and other sentence adjustment mechanisms. In its specific guidance, it endorses the proposition that AI can increase the "accuracy and objectivity" of risk assessment.[77] The insistence that decisions must not be automated but instead taken by designated professionals offers limited reassurance. As our research demonstrates, in practice the outputs of such tools often carry significant—if not determinative—weight in human decision-making. This is particularly evident in contexts where sentence adjustment judges function, de facto, as 'rubber-stamping' authorities, a pattern observed in several jurisdictions.

A targeted policy and ethical framework addressing AI has emerged at EU level, with the European Union responding to rapid technological developments by moving from non-binding ethical guidance towards binding legal rules. The European Commission's Strategy on Artificial Intelligence for Europe, adopted in April 2018, stressed the strategic importance of AI for Europe's economic and social development while identifying the need to address ethical and fundamental rights concerns.[78] This was followed by the Coordinated Plan on Artificial Intelligence in December 2018, which sought to align Member State efforts, encourage public-private cooperation, develop a European data space, and improve understanding of AI-related security risks.[79] Further emphasis on data-driven innovation was set out in the Commission's Communication on Towards a Common European Data Space.[80] The 2019–2023 e-Justice Action Plan subsequently identified AI as a significant development in information and communication technologies and underlined the need to assess its implications for justice systems.[81]

75 Appendix I(d); Appendix III(8); Paragraph 18.

76 Appendix I(d) – AI should "help the criminal justice system [and] the execution of penal sanctions." Section V.B (paras 18–23) – explicit endorsement for offender management, risk assessment, rehabilitation, reintegration.

77 Para. 19.

78 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, 25 April 2018, COM (2018) 237 final.

79 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence, 7 December 2018, COM (2018) 795 final.

80 Ibid.

81 2019-2023 Action Plan European e-Justice, OJ 2019/C 96/05.

This regulatory trajectory culminated in the entry into force of the EU Artificial Intelligence Act (EUAIA) on 1 August 2024, which applies alongside the EU's horizontal legal framework on data protection. The AI Act is among the first major regulatory attempts regarding AI in the world and will enter into effect in stages, with full application expected this year.

THE EU AI ACT: A PROTECTIVE NET WITH WIDE GAPS

The AI Act establishes binding obligations for organisations that develop, deploy, or use AI systems within the EU, including those that import AI systems into the EU market. It introduces a risk-based regulatory framework under which obligations are calibrated according to the level of risk posed by the AI system, with the stated aim of addressing risks to fundamental rights, safety, and security.

The framework combines a list of prohibited practices with a category of high-risk systems subject to heightened compliance obligations, reflecting the legislature's concern that, "[a]side from the many beneficial uses of AI, it can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices [...] Such practices are particularly harmful and abusive and should be prohibited because they contradict Union".[82] In determining whether a system falls within the high-risk category, particular weight is given to the severity of its potential effects, since, "[t]he extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high risk".[83]

Individual criminal offence risk assessment and prediction "based solely on the profiling of a natural person or on assessing their personality traits and characteristics" is prohibited under Article 5(1)(d) of the Act.[84] The rationale underpinning this prohibition is to limit the harms to the right to human dignity, non-discrimination, the right to fair trial, the right to be presumed innocent, the right to defence, effective remedy, privacy and data protection.[85]

On paper, it would appear clear-cut that AI risk assessment tools used for sentence adjustment mechanisms would all fall under this category inherently. However, it is not so clear cut. Assessing whether an AI system

82 Recital 28.

83 Recital 48.

84 AI Act, Art. 5 (1) (d).

85 AI Act, Recital 48.

fits into Art 5 (1) (d) requires a three-step assessment fulfilling all of the following steps: 1. Has the AI system been placed in the market, put into service, or is it being used? 2. Is the intended purpose of the AI system "making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence"? 3. Is the assessment or prediction based solely on a. profiling,[86] and/or assessing their personality traits and characteristics such as nationality, place of birth, place of residence, number of children, level of debt, type of car, etc.[87] For instance, an AI system used by a law enforcement authority to predict criminal behaviour for crimes such as terrorism solely based on individuals' age, nationality, address, type of car and marital status, would be prohibited.[88]

At first sight, AI-based risk assessment tools used in sentencing and early release decisions might appear to fall squarely within the scope of Article 5(1)(d). However, the classification is more nuanced. Determining whether a system is prohibited under Article 5(1)(d) requires a cumulative three-step assessment. First, the AI system must have been placed on the market, put into service, or be in use. Secondly, its intended purpose must be the "making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence". Thirdly, the assessment or prediction must be based solely on (a) profiling[89] and/or (b) the evaluation of personality traits or characteristics such as nationality, place of birth, place of residence, number of children, level of debt, or similar attributes.[90] An AI system deployed by a law enforcement authority to predict terrorist offending exclusively on the basis of variables such as age, nationality, address, marital status, and vehicle ownership would therefore meet these criteria and fall within the prohibition.[91]

In practice, most risk assessment instruments currently used in European prison and sentence adjustment contexts would not automatically satisfy this definition. Algorithmic or machine learning-based systems such as HART or OxRec could potentially fall within scope, but only where they are used to predict criminal offending and where their outputs are

86 Profiling that results in indirect or direct discrimination is already prohibited under LED, Art. 11 (3). See also Article 29 Working Party, Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6.2.2018, p. 7; EU Fundamental Rights Agency, Preventing unlawful profiling today and in the future: a guide, Handbook, 2018, p. 138.

87 AI Act, Recital 42

88 AI Act Prohibition guidelines, Paragraph 202.

89 Profiling that results in indirect or direct discrimination is already prohibited under LED, Art. 11 (3). See also Article 29 Working Party, Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6.2.2018, p. 7; EU Fundamental Rights Agency, Preventing unlawful profiling today and in the future: a guide, Handbook, 2018, p. 138.

90 AI Act, Recital 42

91 AI Act Prohibition guidelines, Paragraph 202.

based solely on profiling or static personal characteristics. Where such systems incorporate broader behavioural, contextual, or dynamically assessed factors, or operate alongside meaningful human assessment, they may instead fall outside the prohibition and be subject to the high-risk regime rather than an outright ban. (This is a problem and the first place they could slip through the protective net of the Act).

Moreover, a range of exceptions to the Article 5(1)(d) prohibition apply, the most notable being where AI systems are used to support human assessment based on objective and verifiable facts directly linked to a criminal activity. Article 5(1)(d) itself provides that the prohibition "shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity."[92]

The European Commission's Guidelines on Prohibited AI Practices clarifies that where an AI system supports a human assessment that is already based on objective, verifiable facts rather than solely on profiling or personality traits, the system falls outside the scope of the prohibition and will instead be treated as a high-risk AI system under Annex III, point 6(d) of the Act. Examples include tools that aid human evaluation of behaviour already substantiated by verifiable evidence relevant to criminal activity, or where additional substantive elements beyond profiling are incorporated into the assessment.[93] In the context of risk assessment tools for sentence adjustment mechanisms, this means that where an AI system's outputs are directly linked to objective evidence of past criminal behaviour, rehabilitation indicators, or other verifiable factual bases that meaningfully inform a human decision-maker's assessment, the prohibition will not apply. Instead, such tools would be subject to the high-risk regime. Conversely, systems that produce risk predictions for individual offending solely on the basis of profiling characteristics would not qualify for this exception and remain prohibited.

It is apparent that providers of AI-based risk assessment tools for sentence adjustment purposes could relatively easily circumvent the protective net established by the prohibition. While the high-risk regime constitutes a second layer of safeguards, it contains notable gaps and may, in practice, prove insubstantial, particularly in the area of sentence adjustment.

92 AI Act Prohibition guidelines, Paragraph 214

93 PDF

Annex III of the AI Act lists so-called high-risk AI, which includes AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups.[94] Most AI-supported risk assessment tools used in parole and other sentence adjustment mechanisms can plausibly be argued to fall within the Article 6(3) exception, on the basis that they do not "materially influence" decisions but merely perform preparatory or supportive functions. This is because such tools are typically framed as providing advisory input that informs, rather than determines, the final outcome, which formally remains with a human decision-maker within the sentence adjustment structure. Thus, there is a possibility of providers self-excluding from the high-risk regime pursuant to Article 6(3) of the AI Act.

This creates a pathway for self-classification outside the high-risk regime, despite the the fact that, in practice, these tools' outputs often carry substantial weight in the decisions of human decision-makers—particularly in contexts where sentence adjustment judges effectively act as 'rubber-stamping' authorities, a pattern observed in several jurisdictions during our research, due to factors such as political pressure, resource constraints, and high case volumes.

This concern has been emphasised by a range of civil society organisations[95] and human rights actors.[96] Drawing on years of engagement in the negotiations leading to the Act's adoption, a coalition of digital rights organisations has criticised the EU AI Act for falling short of establishing a 'gold standard for human rights'.[97] This critique stems largely from the significant loopholes identified above, which create opportunities for the private sector and security agencies to circumvent safeguards. While the Act does partially prohibit the use of risk assessment tools for certain law enforcement purposes – a clear signal that the EU is willing to draw red lines against unacceptably harmful AI applications – civil society actors note that these prohibitions contain substantial gaps. In some instances, these loopholes may inadvertently legitimise certain uses, potentially undermining the intended protective effect and setting a concerning global precedent.

94 Annex III, para. 6(d).

95 CoE PDF.

96 LINK.

97 LINK.

As these actors stress, the coming years will be decisive for the AI Act's effectiveness. Implementation will be shaped by EU institutions, national lawmakers, and industry stakeholders through standard-setting, interpretive guidance, and practical deployment across member states. Ensuring that civil society groups have a meaningful seat at the table and that this process remains transparent is crucial to safeguarding the Act's human rights objectives, including, crucially, the rights of prisoners in the context of decisions affecting their liberty.

CONCLUSION

This chapter has examined the interplay between European data protection standards and the execution of criminal sentences, with particular focus on sentence adjustment mechanisms. While the Council of Europe and EU frameworks articulate important principles for the protection of personal data, their practical effect in the context of sentence adjustment remains uncertain. The sensitivity and breadth of the data involved, combined with the profound consequences for individual prisoners, means that even minor gaps in safeguards can have significant impacts.

It is apparent that the protective capacity of the GDPR and the LED depends heavily on interpretation, national implementation, and effective oversight. Article 11 LED and Article 22 GDPR articulate a prohibition on fully automated decisions, yet their scope is qualified, thresholds for applicability are uncertain, and national authorisations can effectively circumvent protections. In practice, the multi-layered flow of personal information – from prison administrations to probation services, psychologists, and parole boards – creates complexity that may obscure both transparency and accountability.

Safeguarding prisoners' rights in this context is not merely a technical or regulatory question. As access to liberty becomes increasingly mediated by data and automated processes, the adequacy of European standards becomes central to the fairness and legitimacy of contemporary penal systems. The current patchwork of GDPR and LED provisions is insufficient when viewed from the standpoint of the prisoner whose personal data are being harvested and processed for decision-making that gravely impacts their lives. Indeed, from this perspective, the matrix of standards is complex, difficult to navigate, and often of limited practical meaning to those affected. This underscores the importance of clarifying and harmonising data protection and automated processing standards with a

specific focus on prisoners' rights, alongside rigorous national oversight, clear procedural guarantees, and continuous scrutiny of how algorithmically structured decision-making shapes outcomes. Without such measures, European data protection law risks providing the appearance of protection without truly securing the substantive rights of those whose freedom and reintegration depend on its proper application.