

Dutch Pro Justitia Reports as Data Processing Operations

GDPR, Wpg, Wjsg, and Article 8 ECHR Constraints on NIFP Forensic Psychiatric Reporting in the Netherlands

Dr. David Adam Braimer, PsyD

DOI: 10.5281/zenodo.19825495 **Repository:** Zenodo (CERN OpenAIRE) **Companion papers:**
- *Weaponised Forensic Psychiatry, Epistemic Risk, and Procedural Inequality: A Multilevel Analysis of Pro Justitia Reporting within European and International Human Rights Frameworks* (DOI 10.5281/zenodo.19812911), expanded edition, April 2026. - *The Weigerende Observandus and the Inversion of Winterwerp: NIFP Forensic Psychiatry, the Pieter Baan Centrum, and Article 196 Sv and Self-Incrimination Jurisprudence* (DOI 10.5281/zenodo.19817612), April 2026.

Pro Justitia Reports as Data Processing Operations: GDPR, Wpg, Wjsg, and Article 8 ECHR Constraints on NIFP Forensic Psychiatric Reporting. Zenodo.
<https://doi.org/10.5281/zenodo.19817613>

Version: First edition, April 2026

Abstract

A *pro Justitia* forensic psychiatric report is, in addition to its evidentiary status within criminal proceedings, a data processing operation in the technical sense of the General Data Protection Regulation. It involves the collection, organisation, storage, evaluation, and disclosure of personal data, including the special categories of sensitive data — health data under Article 9 GDPR and criminal-conviction-and-offence data under Article 10 GDPR — and routinely incorporates personal data concerning third parties who are not the subject of evaluation. This article argues that the data-protection dimension of NIFP-affiliated *pro Justitia* practice has been systematically under-theorised in Dutch academic literature and is, on the doctrinal analysis developed below, in significant tension with both the GDPR architecture and the European Court of Human Rights jurisprudence on Article 8 ECHR concerning the State-led processing of sensitive personal data. The argument proceeds through the GDPR's lawfulness and special-category-data architecture, the *lex specialis* operation of the *Wet politiegegevens* (Wpg) and the *Wet justitiële en strafvorderlijke gegevens* (Wjsg) as the Dutch transposition of the Law Enforcement Directive (Directive 2016/680), and the ECtHR jurisprudence developed in *Z v. Finland* (1997), *M.S. v. Sweden* (1997), *I v. Finland* (2008), *L.H. v. Latvia* (2014), *Y.Y. v. Russia* (2016), *Surikov v. Ukraine* (2017), *Avilkina v. Russia* (2013), and *S. and Marper v. United Kingdom* (Grand Chamber, 2008), supplemented by the Court of Justice of the European Union's jurisprudence on sensitive-data processing in criminal-justice contexts. Specific attention is given to four structural concerns: the routine inclusion of third-party material concerning persons other than the subject of evaluation; the operation of mandate-drift as a purpose-limitation breach under Article 5(1)(b) GDPR; the onward disclosure of forensic reports through *parket* channels and beyond; and the storage-limitation problems generated by indefinite retention of sensitive data within NIFP files. The article concludes with a structured complaint framework for the *Autoriteit Persoonsgegevens* (AP), with attention to parallel civil and criminal remedies under Dutch law. The pending criminal proceedings under *parket* nr 18-104657-25 before the *Rechtbank Noord-Nederland*, locatie Leeuwarden, in which a *pro Justitia* report by Mw. V. Rama, *forensisch psychiater* at the NIFP, dated 20 November 2025, has been deployed in proceedings that include a regiezitting of 4 December 2025 before a chamber composed of mr. S. T. Kooistra (presiding), mr. H. C. L. Vreugdenhil, and mr. A. Dijkstra, with W. van Goor as griffier, are taken as the doctrinal occasion. The disciplinary complaint against Mw. V. Rama before the *Regionaal Tuchtcollege voor de*

Gezondheidszorg te Zwolle and the international submissions to United Nations Special Procedures, the European Court of Human Rights, and the Office of the Prosecutor of the International Criminal Court remain pending; nothing in this article asserts a factual finding concerning the conduct of any individual. The defendant in the underlying proceedings is referred to throughout as “the defendant” or “the defendant/victim”; defence counsel is referred to by initials only (mr. S.N.dJ.); members of the defendant’s household are not identified.

Keywords: GDPR Article 9; Article 10 GDPR; Law Enforcement Directive; *Wet politiegegevens*; *Wet justitiële en strafvorderlijke gegevens*; Article 8 ECHR; *Z v. Finland*; *S. and Marper v. UK*; sensitive personal data; *pro Justitia*; NIFP; *Autoriteit Persoonsgegevens*; third-party data; purpose limitation; storage limitation.

1. Introduction: The Data-Protection Lens on Forensic Psychiatric Reporting

The doctrinal centre of gravity in academic discussion of forensic psychiatric reporting is criminal-procedural. The relevant frameworks are those of the *Wetboek van Strafvordering*, the case law of the *Hoge Raad* on the use of expert evidence in Dutch criminal proceedings, and the European Convention on Human Rights as articulated by the European Court of Human Rights. The companion papers to which this article is the third instalment in a sequence — *Weaponised Forensic Psychiatry, Epistemic Risk, and Procedural Inequality* (DOI 10.5281/zenodo.19812911) and *The Weigerende Observandus and the Inversion of Winterwerp* (DOI 10.5281/zenodo.19817612) — develop those frameworks at length.

A second analytic lens, however, is largely absent from the existing literature: that of data-protection law. A *pro Justitia* report is, in addition to its evidentiary character, a data processing operation. It involves the systematic collection, organisation, storage, evaluation, and disclosure of personal data within the meaning of Article 4(1) of the General Data Protection Regulation (GDPR). The personal data processed includes special categories of sensitive data — data concerning health under Article 9 GDPR — that engage enhanced protection under both the Regulation and the parallel framework of the Law Enforcement Directive (Directive (EU) 2016/680) as transposed into Dutch law through the *Wet politiegegevens* (Wpg) and the *Wet justitiële en strafvorderlijke gegevens* (Wjsg). The processing is conducted by State actors — the *Nederlands Instituut voor Forensische Psychiatrie en Psychologie* (NIFP), the *Openbaar Ministerie* (OM), the *Dienst Justitiële Inrichtingen* (DJI), and ultimately the trial court — each of whose roles is itself a controllership or processorship under the Regulation.

The data-protection lens reveals a set of structural concerns that the criminal-procedural lens does not surface. *First*, *pro Justitia* reports routinely include personal data concerning third parties — partners, children, family members, professional contacts, prior healthcare providers — who have not consented to forensic evaluation and who are not the subject of the proceedings. *Second*, the materials relied upon by the evaluator may extend beyond the strict mandate of the forensic question and into adjacent topics — political views, religious identification, geopolitical concerns, separate legal proceedings — that engage the principle of purpose limitation under Article 5(1)(b) GDPR. *Third*, the onward disclosure of the report — from the NIFP to the OM, from the OM to the trial court, from the trial court to the defence and the public, and (after conviction) to

subsequent recipients including reclassering, prison medical services, and TBS-klinieken — occurs through institutional channels whose data-protection foundations have not been systematically tested. Fourth, the long-term retention of forensic reports and underlying materials within NIFP files raises storage-limitation problems addressed in ECtHR jurisprudence on indefinite retention of sensitive data.

These structural concerns engage the GDPR architecture; the Wpg and Wjsg as the *lex specialis* for criminal-justice processing; the ECtHR’s Article 8 jurisprudence on sensitive-data processing by State actors; and the parallel CJEU framework on the proportionality of sensitive-data processing in criminal-justice contexts. The argument of this article is that the structural concerns are not minor or technical but engage substantive normative requirements; that the present operation of NIFP-affiliated *pro Justitia* practice is in significant tension with those requirements; and that the data-protection track offers a parallel forum — the *Autoriteit Persoonsgegevens* (AP) — that is filable now, that operates on shorter timescales than the criminal court, that has no exhaustion-of-domestic-remedies barrier, and that generates evidence and findings deployable across the criminal, civil, and international proceedings.

The article proceeds in twelve sections. Section 2 develops the phenomenology of the *pro Justitia* report as a data processing operation. Section 3 sets out the relevant GDPR architecture. Section 4 examines the *lex specialis* operation of the Wpg and Wjsg. Section 5 analyses the ECtHR jurisprudence on Article 8 sensitive-data processing. Section 6 examines the parallel CJEU jurisprudence. Section 7 develops the third-party-data problem. Section 8 develops the purpose-limitation and mandate-drift analysis. Section 9 develops the storage-limitation and onward-disclosure analysis. Section 10 sets out the available remedies, with primary attention to the AP complaint procedure. Section 11 articulates a reform agenda. Section 12 concludes.

A methodological note: the analysis is doctrinal, not adjudicative. The *pro Justitia* report by Mw. V. Rama dated 20 November 2025 in parket nr 18-104657-25 is taken as the illustrative case for the structural analysis, but no factual finding is asserted concerning the conduct of any individual. The disciplinary complaint pending before the *Regionaal Tuchtcollege voor de Gezondheidszorg te Zwolle*, the criminal proceedings, and the international submissions to UN Special Procedures, the ECtHR, and the ICC OTP remain at various stages of pendency. The naming convention adopted in the companion papers is preserved: the defendant is referred to as “the defendant” or

“the defendant/victim”; defence counsel is referred to by initials only (mr. S.N.dJ.); members of the defendant’s household are not identified; public actors are named in respect of conduct undertaken in their public functions, on the basis of public-record material, and only to the extent that such conduct is documented in those public-record sources.

2. The *Pro Justitia* Report as Data Processing Operation

2.1 The Phenomenology

A *pro Justitia* report is the textual product of a sequence of data-processing activities. Reconstructing those activities makes the data-protection analysis tractable.

The sequence typically begins with the *trajectconsult*, in which a NIFP psychologist or psychiatrist receives the case dossier transmitted by the *Officier van Justitie*, examines its contents, and produces a recommendation about the form of *pro Justitia* evaluation appropriate to the case. The dossier transmission is a data processing operation: personal data concerning the defendant — including criminal-investigation data, prior justice-system contacts, and any prior mental-health information available to the prosecuting authority — is transferred from the OM to the NIFP. The *trajectconsult* itself involves further processing: the NIFP professional reads, evaluates, and forms judgments about the data; produces a written recommendation incorporating those judgments; and stores the recommendation in NIFP files.

The next stage is the ambulatory *pro Justitia* evaluation itself. The evaluator receives the dossier; conducts interviews with the defendant; collects collateral information from members of the defendant’s environment, prior healthcare providers, and other sources; structures observations; conducts psychometric testing where appropriate; consults the relevant clinical literature; and produces the report. Each of these activities involves processing of personal data: the defendant’s data, third-party data, sensitive health data, and criminal-conviction data.

The report itself is an integration of these inputs. It records the materials reviewed, the evaluator’s observations, the diagnostic formulation (where reached) or the methodological self-limitation (where not reached), and the answers to the research questions. The report is then stored within NIFP files and transmitted to the commissioning authority — typically the OM — and subsequently to the trial court, the defence, and any other recipients in the proceedings.

Each step in this sequence is a data processing operation. Each processing operation is subject to the relevant data-protection regime. The regulatory question is which regime applies, and on what terms.

2.2 Data Subjects and Data Categories

The data subjects engaged by the *pro Justitia* sequence include, at minimum: the defendant; partners, family members, and other persons in the defendant's household environment; prior healthcare providers; professional and personal contacts identified during the evaluation; persons identified in the defendant's account during interview; and any further persons whose information enters the dossier or the evaluation by other routes.

The data categories engaged include: general personal data (name, contact details, relational status, employment, residence); financial data (where relevant to alleged offences or to background context); communications data (where extracted from criminal-investigation materials); special-category data under Article 9 GDPR including data concerning health, racial or ethnic origin, religious or philosophical beliefs, sex life or sexual orientation, and political opinions; criminal-conviction-and-offence data under Article 10 GDPR; and any further categories the evaluation engages.

The breadth of these categories, and the comprehensiveness of their integration in a single forensic report, is itself doctrinally significant. The *pro Justitia* report is one of the most data-intensive documents the Dutch criminal-justice system produces. Its comprehensive scope is a function of the forensic task; its data-protection consequences flow from that scope.

2.3 Controllers, Processors, and Joint Controllership

The data-controllership analysis under Article 4(7) GDPR — the natural or legal person who, alone or jointly with others, determines the purposes and means of processing — is itself unsettled in the *pro Justitia* context. Multiple actors plausibly satisfy the controllership criterion at different stages: the OM as the commissioning authority that determines the purpose of the evaluation; the NIFP as the institutional locus of the processing operation; the individual evaluator who determines the means of processing within the evaluation; the trial court as the recipient and adjudicator. The question of whether the configuration constitutes joint controllership under Article 26 GDPR, or

successive separate controllerships, has not been the subject of authoritative determination by the AP or the courts.

The practical consequence of this regulatory uncertainty is that data-subject rights — access, rectification, erasure, restriction — operate against an unclear addressee structure. The AP has not, to date, issued comprehensive guidance on the controllership architecture of *pro Justitia* processing. The structural recommendation developed in §11 below is that the AP undertake such guidance; in the interim, the analytic framework treats each plausible controller as separately and jointly responsible for compliance with the applicable regime.

3. The GDPR Architecture: Lawfulness, Special-Category Data, Criminal-Conviction Data

3.1 The Article 5 Principles

Article 5 GDPR articulates the foundational principles that govern all processing of personal data. Each of the seven principles bears on *pro Justitia* practice. *Lawfulness, fairness, and transparency* (Article 5(1)(a)) requires processing to be conducted on a lawful basis, in a manner that is fair to the data subject, and with appropriate transparency. *Purpose limitation* (Article 5(1)(b)) requires that data be collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes. *Data minimisation* (Article 5(1)(c)) requires that data be adequate, relevant, and limited to what is necessary. *Accuracy* (Article 5(1)(d)) requires that data be kept accurate and up to date. *Storage limitation* (Article 5(1)(e)) requires that data be kept in a form permitting identification of data subjects for no longer than necessary. *Integrity and confidentiality* (Article 5(1)(f)) requires appropriate technical and organisational measures. The controller bears the *accountability* obligation (Article 5(2)) of demonstrating compliance.

Each of these principles is engaged at multiple points in the *pro Justitia* sequence. The structural concerns identified in §1 above — third-party-data inclusion, mandate drift, onward disclosure, indefinite retention — translate respectively into concerns under data minimisation, purpose limitation, lawfulness/transparency, and storage limitation.

3.2 Article 6: Lawful Basis

Article 6 GDPR specifies the six possible lawful bases for processing of personal data: consent (6(1)(a)); contract (6(1)(b)); legal obligation (6(1)(c)); vital interests (6(1)(d)); public interest or

official authority (6(1)(e)); legitimate interests (6(1)(f)). For State-led criminal-justice processing, Article 6(1)(e) — the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller — is the standard basis. The basis must, however, be “laid down by Union or Member State law” (Article 6(3)) and that law must “meet an objective of public interest and be proportionate to the legitimate aim pursued”.

For *pro Justitia* processing, the Dutch legal basis is found in the *Wetboek van Strafvordering* provisions on expert evidence (Articles 227 et seq.) and on PBC observation (Article 196), together with the Wet BIG provisions on professional practice and the institutional foundations of the NIFP. The Dutch legal basis exists; the substantive question is whether the practice as conducted satisfies the proportionality requirement in Article 6(3).

3.3 Article 9: Special-Category Data

Article 9(1) GDPR establishes a general prohibition on processing of special categories of personal data, including data concerning health and data revealing racial or ethnic origin, religious or philosophical beliefs, political opinions, and sex life or sexual orientation. Article 9(2) lists the exceptions under which such processing may nonetheless be lawful.

For *pro Justitia* processing, the relevant Article 9(2) exceptions are: 9(2)(g) — substantial public interest, on the basis of Union or Member State law that is proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard fundamental rights and interests; 9(2)(h) — health-purposes processing, but only where carried out by professionals subject to professional secrecy; and (less plausibly) 9(2)(f) — establishment, exercise, or defence of legal claims.

The doctrinal question is how these exceptions interact in the forensic-psychiatric context. 9(2)(h) appears *prima facie* applicable, since the evaluator is a registered medical professional subject to professional secrecy under the Wet BIG. But 9(2)(h) is structured around therapeutic and preventive purposes — “preventive or occupational medicine, ... medical diagnosis, the provision of health or social care or treatment” — which sit awkwardly with forensic evaluation, the purpose of which is not therapeutic. 9(2)(g) is the more secure foundation, but it requires proportionate Member State law providing safeguards. The Wpg and Wjsg, examined in §4 below, are the candidate instruments; their adequacy as the substantive Article 9(2)(g) foundation is testable.

3.4 Article 10: Criminal-Conviction-and-Offence Data

Article 10 GDPR addresses the processing of personal data relating to criminal convictions and offences. Such processing may be carried out only under the control of official authority or when authorised by Union or Member State law providing for appropriate safeguards. The provision is structurally distinct from Article 9 — criminal-conviction data is not “special-category” in the Article 9 sense — but the regime is closely parallel.

Pro Justitia processing engages Article 10 directly, since the dossier and the evaluation routinely include criminal-investigation data, prior justice-system contacts, and detail about the alleged offence under investigation. The Wpg and Wjsg again function as the candidate Article 10 foundations.

3.5 The Interaction with the Law Enforcement Directive

A jurisdictional question that materially affects the analysis is whether *pro Justitia* processing falls within the GDPR or within Directive (EU) 2016/680 (the Law Enforcement Directive, LED). The LED applies to processing by competent authorities for purposes of prevention, investigation, detection, or prosecution of criminal offences (Article 1(1)). The GDPR explicitly excludes such processing from its scope (Article 2(2)(d)). The categorisation matters: the substantive regimes are different in significant respects, particularly on lawful bases, data-subject rights, and onward transfers.

The categorisation of *pro Justitia* processing is itself a doctrinal question. The processing serves the prosecution (LED scope) but is conducted by a healthcare-affiliated institution (NIFP) whose general practice falls within the GDPR. The processing produces evidence used in criminal proceedings (LED scope) but engages medical-professional standards that are not specific to law enforcement (GDPR-coloured). The Dutch transposition of the LED through the Wjsg suggests that the Dutch legislator regards prosecution-purpose processing as falling within the LED regime; the Wpg further provides for police-purpose processing. Whether NIFP-conducted *pro Justitia* processing falls within the Wjsg, the Wpg, both, or the residual GDPR regime is the subject of §4 below.

4. The Wpg and Wjsg as *Lex Specialis*

4.1 The Architecture of the Two Acts

The *Wet politiegegevens* (Wpg) governs the processing of personal data by the police and certain other law-enforcement bodies. The *Wet justitiële en strafvorderlijke gegevens* (Wjsg) governs the processing of personal data by the *Openbaar Ministerie*, the courts, and certain associated bodies in the context of criminal justice. Both Acts implement Directive 2016/680 and operate as *lex specialis* alongside the general GDPR regime.

The Wpg and Wjsg architectures are structurally similar. Each provides for: specified purposes for which processing may be undertaken; categories of data that may be processed for each purpose; retention periods specified by purpose and category; rules on onward transfer to third parties; data-subject rights modulated by the criminal-justice context; and oversight by the AP and by sectoral bodies.

The substantive provisions of the Wpg and Wjsg are detailed and prescriptive. The Wjsg, in particular, specifies the categories of data that the OM may process for prosecutorial purposes, the conditions under which such data may be transferred to other actors in the criminal-justice system, and the retention periods that govern the data thereafter. The Wpg performs analogous functions for police data.

4.2 The NIFP's Position

The NIFP is not, in formal terms, a police body within the Wpg sense, nor is it the OM within the Wjsg sense. The NIFP is an executive agency of the Ministry of Justice and Security, operating as a forensic-medical institution that provides services to the OM, the courts, and the prison service. Its data-protection architecture is therefore a question of fit: does NIFP processing fall within the Wpg, the Wjsg, the residual GDPR regime, or some combination?

The functional answer is that NIFP processing is best characterised as residual-GDPR processing for forensic-medical purposes, conducted by an executive agency of the Ministry of Justice and Security, but triggered by, materially shaped by, and ultimately serving the prosecutorial process governed by the Wjsg. The data flows from the OM (Wjsg) to the NIFP (residual-GDPR) and back to the OM (Wjsg). The NIFP holds the data internally under what is, on its face, a GDPR-Article-9(2)(g)/(h) regime, but the data is integrated into a Wjsg-governed prosecutorial workflow.

The regulatory consequence of this functional fit is uncertainty. The NIFP's data-protection notices, data-subject-access procedures, retention schedules, and onward-transfer protocols sit at

the boundary of two regimes and have not been the subject of authoritative AP guidance. The structural recommendation developed in §11 below is for the AP to issue such guidance.

4.3 Onward Transfer

A specific concern arises in respect of onward transfer. A *pro Justitia* report is transmitted from the NIFP to the OM (Wjsg recipient); from the OM to the trial court (Wjsg actor); from the trial court to the defence (procedural disclosure); and, after conviction, to reclassering (Wjsg-adjacent), to prison medical services (residual-GDPR), and to any TBS-kliniek receiving the convicted defendant (residual-GDPR with Wjsg connection). Each transfer is a separate processing operation requiring its own Article 6/9/10 GDPR or Wpg/Wjsg basis. The cumulative architecture is complex and largely undocumented in NIFP-published materials.

The Dutch academic literature on the Wpg and Wjsg has not, to date, addressed the *pro Justitia* sequence in these terms. The structural opacity is, on its own, a transparency concern under Article 5(1)(a) GDPR.

5. The ECtHR Article 8 Jurisprudence on Sensitive-Data Processing by State Actors

5.1 *Z v. Finland: The Foundational Case*

The European Court of Human Rights established the foundational doctrine on sensitive-data processing by State actors in *Z v. Finland* (App. No. 22009/93, 25 February 1997). The case concerned the disclosure, in criminal proceedings against the applicant's husband for sexual offences, of the applicant's HIV-positive status and related medical information. The Court held that the protection of personal data, particularly medical data, is of fundamental importance to the enjoyment of the right to respect for private and family life under Article 8 ECHR. The Court emphasised that disclosure of medical information by State actors may engage Article 8 not only where the disclosure is to the public but also where it is to other State actors or to private persons in the course of legal proceedings. The interference must satisfy the standard Article 8(2) test: in accordance with the law, pursuing a legitimate aim, and necessary in a democratic society, with particular attention to proportionality.

Z v. Finland established that disclosure of medical data in legal proceedings is itself a regulated activity under the Convention. The Court did not preclude such disclosure where it is properly

grounded but required that the structural arrangements satisfy the Convention's requirements. The case is the parent of all subsequent ECtHR jurisprudence on State-led processing of sensitive data.

5.2 *M.S. v. Sweden: The Disclosure of Medical Records*

In *M.S. v. Sweden* (App. No. 20837/92, 27 August 1997), the Court considered the disclosure of medical records by a hospital to a state insurance authority for the purpose of evaluating an injury claim. The Court found a violation of Article 8, holding that the disclosure was disproportionate even though the legitimate aim was clear and the legal basis existed. The case is significant because it establishes that the existence of a legitimate aim and a legal basis does not exhaust the Article 8 analysis: the proportionality requirement operates as a substantive constraint on the conditions of disclosure.

The application to *pro Justitia* practice is direct. The transmission of NIFP-held medical-evaluative data to the OM, to the trial court, and to subsequent recipients is, on the *M.S.* analysis, an Article 8 event whose proportionality must be assessed at each stage. The current Dutch practice, which treats such transmission as a routine procedural matter, has not been subject to systematic proportionality scrutiny under Article 8.

5.3 *I v. Finland: Positive Obligations*

In *I v. Finland* (App. No. 20511/03, 17 July 2008), the Court held that Article 8 imposes positive obligations on the State to ensure the security of medical records. The case involved unauthorised access to medical records by hospital staff. The Court found a violation because the State had failed to take reasonable steps to prevent such unauthorised access. The doctrine has been extended in subsequent cases to require not only security against unauthorised access but also accuracy, relevance, and effective data-subject-access mechanisms.

I v. Finland is doctrinally significant for *pro Justitia* practice because it establishes that the State's responsibility under Article 8 is not exhausted by the lawfulness of the initial processing but extends to the structural conditions surrounding the data over its entire lifecycle. The application to long-term retention of *pro Justitia* materials in NIFP files is direct: the State must take reasonable steps to ensure that such materials are protected against unauthorised access, are accurate and relevant, and are subject to appropriate retention periods.

5.4 *L.H. v. Latvia and the Boundaries of Medical-Data Processing for State Purposes*

In *L.H. v. Latvia* (App. No. 52019/07, 29 April 2014), the Court considered the unauthorised collection of personal medical data by a state body (the Inspectorate for Health) for the purpose of investigating a complaint. The Court found a violation of Article 8, holding that the legal basis for the collection was insufficiently clear and that the collection was therefore not “in accordance with the law” within the Article 8(2) sense. The case establishes that the legal-basis requirement of Article 8(2) is substantive: vague or general statutory authorisation does not satisfy the requirement; the legal basis must be specific enough to permit the data subject to foresee the consequences of the processing.

The application to *pro Justitia* practice is significant. The Dutch statutory framework on forensic-evaluation processing — the *Wetboek van Strafvordering* provisions, the Wet BIG, the Wpg and Wjsg, and the residual GDPR — is, on the *L.H.* analysis, plausibly insufficiently specific in respect of the comprehensive third-party-data processing that *pro Justitia* reports routinely involve. The argument for substantive ECHR-incompatibility on this ground is preserved for §7 below.

5.5 *Y.Y. v. Russia and Psychiatric Records*

In *Y.Y. v. Russia* (App. No. 40378/06, 23 February 2016), the Court addressed the disclosure of psychiatric records by a state psychiatric institution to court proceedings concerning the applicant’s parental rights. The Court found a violation of Article 8, holding that the disclosure was not justified by the procedural needs of the underlying proceedings and that the disclosure procedures lacked adequate safeguards. The case is directly relevant to *pro Justitia* practice because it engages the disclosure of psychiatric records by a state institution to court proceedings — the structurally identical configuration.

5.6 *Surikov v. Ukraine and Long-Term Retention*

In *Surikov v. Ukraine* (App. No. 42788/06, 26 January 2017), the Court considered the long-term retention of mental-health information by a state institution and its effect on the applicant’s employment and broader social participation. The Court found a violation of Article 8, holding that the retention was disproportionate to any legitimate aim and that the structural conditions surrounding the retention failed the proportionality requirement. The case is significant for *pro Justitia* practice because the long-term retention of forensic-evaluation material in NIFP files raises analogous structural concerns.

5.7 Avilkina v. Russia and Unconsented Disclosure

In *Avilkina v. Russia* (App. No. 1585/09, 6 June 2013), the Court addressed the disclosure of medical information without consent in the context of state investigation. The Court found a violation of Article 8, emphasising that consent (or its lawful substitute) is a foundational element of the protection of medical data and that disclosure without consent requires particularly stringent justification.

5.8 S. and Marper v. United Kingdom: Indefinite Retention as Independent Concern

The Grand Chamber's judgment in *S. and Marper v. United Kingdom* (App. Nos. 30562/04 and 30566/04, 4 December 2008) addressed the indefinite retention of fingerprints and DNA samples of persons who had been arrested but not convicted. The Court found a violation of Article 8, holding that indefinite retention of such sensitive data by State actors is, in itself, an independent Article 8 concern requiring justification. The case is doctrinally significant because it establishes that retention is not merely an ancillary aspect of the initial processing but a separate Article 8 event subject to its own proportionality analysis.

The application to *pro Justitia* practice is direct. The retention of forensic-evaluation materials in NIFP files, particularly in respect of persons whose proceedings have concluded without conviction or with acquittal, raises *S. and Marper*-type concerns. The current Dutch retention practice has not been subject to systematic ECHR-compatibility analysis.

5.9 The Composite Standard

The cumulative ECtHR jurisprudence under Article 8 establishes a composite standard for State-led sensitive-data processing. The processing must be: - *In accordance with the law*: with a substantive, foreseeable legal basis specific enough to permit the data subject to foresee the consequences; - *In pursuit of a legitimate aim*: of the kind enumerated in Article 8(2); - *Necessary in a democratic society*: reflecting a pressing social need; - *Proportionate*: in the strict sense, calibrated to the legitimate aim and going no further than necessary; - *With adequate safeguards*: structural, not merely formal, against abuse and against arbitrary onward use; - *Subject to retention limits*: with indefinite retention itself a structural concern requiring independent justification; - *Open to effective remedy*: with the data subject's procedural position permitting meaningful challenge to the processing.

The argument of this article, developed across the substantive sections that follow, is that NIFP-affiliated *pro Justitia* practice does not, in its current form, satisfy each of these elements consistently. Specific failures are identified at each subsequent step.

6. CJEU Jurisprudence on Sensitive-Data Processing in Criminal-Justice Contexts

6.1 The CJEU Framework in Outline

The Court of Justice of the European Union has, in a series of judgments since the entry into force of the GDPR and its predecessors, articulated a substantial jurisprudence on the limits of sensitive-data processing in criminal-justice contexts. The framework operates in parallel with the ECtHR jurisprudence under Article 8 ECHR, with the additional doctrinal framework of the Charter of Fundamental Rights of the European Union (Articles 7 and 8) and the structural role of the Court of Justice in interpreting EU secondary legislation.

The relevant cases cluster into two doctrinal lines. *First*, cases concerning mass or undifferentiated retention of communications and personal data: *Tele2 Sverige and Watson* (Joined Cases C-203/15 and C-698/15, 21 December 2016); *La Quadrature du Net and Others* (Joined Cases C-511/18, C-512/18, C-520/18, 6 October 2020); *Privacy International* (Case C-623/17, 6 October 2020); *H.K. v. Prokuratuur* (Case C-746/18, 2 March 2021); *Commissioner of An Garda Síochána* (Case C-140/20, 5 April 2022). *Second*, cases concerning specific sensitive-data processing in identifiable individual contexts: *Bara* (Case C-201/14, 1 October 2015); *G.C. v. CNIL* (Case C-136/17, 24 September 2019); *Ligue des droits humains* (Case C-817/19, 21 June 2022); *Norra Stockholm Bygg* (Case C-268/21, 2 March 2023).

6.2 The Mass-Retention Line and Its Lessons

The mass-retention line is doctrinally significant for *pro Justitia* practice, even though the cases concern communications-data retention rather than forensic-evaluation retention. The Court's reasoning establishes general principles that apply across the spectrum of sensitive-data processing.

The Court has repeatedly held that undifferentiated retention of personal data, on a national scale, for criminal-justice purposes is incompatible with Articles 7, 8, and 11 of the Charter. The Court requires retention to be targeted, proportionate, and subject to substantive procedural safeguards.

The doctrinal core is that sensitive-data retention is not a freely available investigative tool; it is an interference with fundamental rights that must be specifically justified at every stage.

The application to *pro Justitia* practice is structural. NIFP-held forensic-evaluation materials are not “mass” in the Tele2 sense — they are individual files, not aggregate datasets — but the underlying logic of the cases is that sensitive-data processing in criminal-justice contexts is subject to substantive proportionality requirements that the State cannot satisfy by general assertion. The Court’s resistance to undifferentiated retention applies to individually-targeted indefinite retention with the same force.

6.3 *Ligue des droits humains: Sensitive-Data Processing for Criminal-Justice Purposes*

The most directly relevant case is *Ligue des droits humains* (Case C-817/19, 21 June 2022), in which the Court considered the EU PNR Directive (Directive (EU) 2016/681) and its compatibility with the Charter. The Court held that the processing of passenger data for criminal-justice purposes — even within the framework of an EU instrument — must satisfy substantive proportionality requirements; that the processing must be limited to what is strictly necessary; that retention beyond the immediate operational use of the data is itself a separate concern; and that the structural conditions surrounding the processing must permit effective challenge by data subjects.

The Court’s reasoning in *Ligue des droits humains* maps closely onto the *pro Justitia* configuration. The Court rejected the argument that the criminal-justice purpose is, in itself, sufficient to justify comprehensive sensitive-data processing. The justification must be specific to the processing in question; the proportionality must be assessed on the actual scope of the processing; the retention must be limited; and the structural conditions must support effective remedy.

6.4 *G.C. v. CNIL and the Right to Erasure*

In *G.C. v. CNIL* (Case C-136/17, 24 September 2019), the Court addressed the right to erasure under the GDPR in the context of search engines and the processing of sensitive data. The Court held that the right to erasure operates with particular force in respect of sensitive-data processing, that the data subject’s interests in erasure carry presumptive weight against competing interests in continued processing, and that the controller must make a specific and substantive assessment in each case.

The application to NIFP retention is significant. A defendant whose proceedings have concluded — particularly where they have concluded without conviction or with acquittal — has a presumptive right under Article 17 GDPR (and Article 16 of the Law Enforcement Directive) to the erasure of forensic-evaluation materials that no longer serve a legitimate ongoing purpose. The current Dutch practice on retention does not, on its face, give effect to this right.

6.5 *Bara* and the Information Obligations

In *Bara* (Case C-201/14, 1 October 2015), the Court addressed the transfer of personal data between two state bodies (a tax authority and a health-insurance body) and the consequent processing for purposes different from those for which the data was originally collected. The Court held that the data subject must be informed of the transfer and the new processing; that the absence of such information is a violation of the foundational transparency obligation; and that the transfer requires its own lawful basis distinct from the original collection.

The application to the *pro Justitia* sequence is direct. The dossier transmission from the OM to the NIFP, the recommendation transmission from the NIFP to the OM, the report transmission from the NIFP to the OM, the report transmission from the OM to the trial court, and each subsequent transmission constitutes a *Bara*-type transfer requiring its own lawful basis and triggering its own information obligation. The current practice does not, on its face, satisfy these requirements with the consistency that *Bara* requires.

6.6 The Composite CJEU Standard

Synthesising the CJEU jurisprudence, the standard for *pro Justitia* processing of sensitive data and criminal-conviction data is structurally aligned with the ECtHR Article 8 standard but adds specific elements drawn from the Charter framework: strict-necessity proportionality; targeted rather than undifferentiated processing; substantive transparency including specific information at each transfer; the data subject's right to challenge processing through effective procedural mechanisms; and the right to erasure operating with particular force in respect of sensitive data once the operational purpose has been served.

7. The Third-Party Data Problem

7.1 The Phenomenology

A *pro Justitia* report routinely contains personal data concerning persons other than the subject of evaluation. The categories typically include: members of the defendant's household (partners, children, cohabiting relatives); family of origin (parents, siblings, persons in the home country); current and former professional contacts; current and former personal contacts; prior healthcare providers; and any further persons identified through the evaluator's contact with the dossier and with the defendant's interview material.

The data concerning these third parties is typically processed at multiple levels of detail. *Identification data* (name, relationship to the defendant, occupation, residence) is routinely included. *Behavioural and characterological data* — descriptions of conduct, patterns of relationship, evaluative observations — is frequently included. *Health and mental-health data* concerning third parties is included where the third parties have themselves received healthcare and the records are accessible to the evaluator. *Sensitive-category data* — religious or political identification, sexual or relational matters, ethnic or national origin — is included where the evaluator regards it as relevant to the forensic question.

The volume and detail of third-party data in a typical *pro Justitia* report is, in the present author's experience and on the available comparative material, considerable. The disciplinary literature in Dutch tuchtrecht has occasionally addressed individual instances of disproportionate third-party-data inclusion, but no systematic structural analysis has been undertaken in either the academic literature or the regulatory output.

7.2 The Data-Subject Status of Third Parties

Under Article 4(1) GDPR, the third parties whose data is processed in a *pro Justitia* report are themselves data subjects in respect of that processing. They are, however, structurally different from the principal data subject (the defendant) in several respects. *They have not consented* to the processing — and in most cases have not been informed of it. *They have no procedural standing* in the underlying criminal proceedings to object to the processing. *They have limited practical access* to the data: the report is in the criminal-procedural file, not directly accessible to non-parties. *Their data-subject rights*, formally available under Articles 12–22 GDPR, are practically attenuated by these structural features.

The result is that the third parties bear the data-protection consequences of the processing without the procedural mechanisms that would normally permit the defence of those consequences. The

structural asymmetry is, on its face, a substantial concern under Articles 5 (fairness, transparency), 6 (lawfulness), 9 (special-category data), and 12–22 (data-subject rights) GDPR.

7.3 The Lawfulness Analysis

The lawfulness of third-party-data inclusion in a *pro Justitia* report turns on the application of Articles 6 and 9 GDPR (or the LED equivalents under the Wpg/Wjsg). The available lawful bases are limited. Consent (Article 6(1)(a); 9(2)(a)) is typically absent, and the *Bara* obligations of information and the GDPR's strict consent requirements would be hard to satisfy. Vital interests (6(1)(d); 9(2)(c)) are typically not engaged. The plausible bases are public interest (6(1)(e)) read with substantial-public-interest processing under 9(2)(g); legal-claims processing under 9(2)(f); or the LED equivalent.

For each of these bases, the proportionality requirement of Article 6(3) GDPR (and the analogous LED requirements) operates as a substantive constraint. The question is whether the inclusion of the specific third-party data is *necessary* for the legitimate forensic purpose and is *limited to what is necessary*. The data-minimisation principle (Article 5(1)(c) GDPR) requires that processing be limited to what is necessary; the inclusion of comprehensive third-party material in *pro Justitia* reports goes well beyond necessity in many cases.

The structural argument is that current *pro Justitia* practice systematically over-includes third-party data relative to what data minimisation requires. The over-inclusion is not a matter of individual evaluator choice but a feature of the institutional practice: the dossier contains comprehensive third-party material; the evaluator absorbs and organises that material; the report integrates it. The structural protection for the third parties — minimisation, purpose limitation, rights — is not given practical effect.

7.4 The Article 8 ECHR Analysis

The Article 8 ECHR analysis of third-party data inclusion in *pro Justitia* reports operates in parallel. The ECtHR has held in *Z v. Finland*, *M.S. v. Sweden*, *L.H. v. Latvia*, and *Y.Y. v. Russia* that the disclosure of medical and analogous sensitive data by State actors engages Article 8 and requires justification under the Article 8(2) framework. Where the data subject is a third party who has not consented to the disclosure and has no procedural standing in the proceedings to which the disclosure relates, the proportionality of the disclosure is at its weakest.

The doctrinal extension to *pro Justitia* third-party data is straightforward. The third party is in the position of having sensitive personal data — health or analogous data — disclosed by a State actor to other State actors and to a court, in proceedings to which the third party is not a party. The Article 8 protection of the third party operates independently of the Article 8 protection of the defendant. The disclosure must be justified under Article 8(2) on grounds specific to the third party’s position.

The current Dutch practice does not, on its face, conduct this Article 8(2) analysis at the third-party level. The practice treats the third-party data as ancillary to the defendant’s data, processed under the lawful basis that justifies the defendant’s data. This conflation is, on the *Z v. Finland / M.S. / L.H.* analysis, doctrinally inadequate.

7.5 The Practical Position of Third Parties

A practical concern reinforces the doctrinal one. Third parties whose data is included in a *pro Justitia* report typically have no notification of the processing, no opportunity to object, no procedural standing in the underlying criminal proceedings, and no effective remedy. The data-subject-access right under Article 15 GDPR is, formally, available to the third party — but the practical exercise requires the third party to know that the processing has occurred and to identify the controller. Neither knowledge nor identification is structurally provided.

The structural recommendation, developed in §11 below, is that *pro Justitia* practice incorporate notification mechanisms for third-party data subjects and that the AP issue guidance specifying the required procedural standards.

8. Purpose Limitation and Mandate Drift

8.1 The Article 5(1)(b) Framework

Article 5(1)(b) GDPR requires that personal data be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”. The principle of purpose limitation is one of the most fundamental data-protection principles, articulated in earlier instruments including the Council of Europe Convention 108 and the predecessor Data Protection Directive 95/46/EC, and operating across both the GDPR and the LED.

The principle has two components. *First*, processing must be conducted for specified, explicit, and legitimate purposes — the purpose-specification requirement. *Second*, further processing must be compatible with those purposes — the use-limitation requirement. Where further processing is for a purpose incompatible with the original specification, it requires its own lawful basis and triggers its own information obligation under the *Bara* doctrine.

8.2 The Mandate of the *Pro Justitia* Evaluation

The mandate of a *pro Justitia* evaluation is, in formal terms, narrowly defined. The research questions address the defendant's mental state at the time of the alleged offence, criminal responsibility under the Dutch *toerekeningsvatbaarheid* framework, the prerequisites for measures of *terbeschikkingstelling* (TBS), and the risk of recidivism and treatability. The mandate does not include, and cannot include without specific authorisation, evaluation of the defendant's political views, religious commitments, geopolitical concerns, separate legal proceedings, family-of-origin trauma history, or general life narrative beyond what is strictly necessary for the forensic question.

The §12 of the original article (DOI 10.5281/zenodo.19812911) developed the methodological concept of *mandate drift* — the phenomenon by which a forensic evaluation expands beyond its formal scope into adjacent topics. The methodological analysis identified mandate drift as a structural risk to the integrity of forensic evaluation. The data-protection analysis identifies it, in addition, as a violation of the purpose-limitation principle under Article 5(1)(b) GDPR.

8.3 Mandate Drift as Purpose-Limitation Breach

When an evaluator introduces topics outside the legitimate forensic mandate — political views, religious commitments, ethnic identification, geopolitical concerns — the evaluator processes personal data for purposes incompatible with the specified forensic purpose. The data subject has not consented to processing for these adjacent purposes; the State has not authorised processing for these purposes; the institutional framework has not specified these purposes. The processing is, on its face, a violation of the purpose-limitation principle.

The structural significance of this characterisation is that it shifts the analysis from a methodological concern (the integrity of the forensic evaluation) to a regulatory concern (the lawfulness of the data processing). Methodological concerns are addressed through *tuchtrecht* and through cross-examination at trial; regulatory concerns are addressed through the AP and through

the GDPR enforcement framework. The two channels run in parallel and provide structurally different forms of remedy.

8.4 The Application to Parket Nr 18-104657-25

The disciplinary complaint pending before the *Regionaal Tuchtcollege voor de Gezondheidszorg te Zwolle* in respect of the *pro Justitia* report by Mw. V. Rama dated 20 November 2025 alleges, among other matters, that the evaluation engaged topics outside the legitimate forensic mandate including the defendant's religious and ethnic identification, his foreign-policy views and concerns, and matters separate from the underlying criminal allegations. The disciplinary tribunal will determine, in due course, whether the allegations are made out.

For the doctrinal purposes of this article, the relevance of these allegations is structural. If allegations of this kind are substantiated in the disciplinary proceedings, they constitute simultaneously a methodological breach (the subject of the disciplinary track) and a data-protection breach (the subject of an AP complaint and of an Article 8 ECHR analysis). The two characterisations are not in competition; they are parallel descriptions of the same underlying conduct. The structural recommendation in §10 below is that the data-protection track be activated independently and in parallel with the disciplinary track.

9. Storage Limitation and Onward Disclosure

9.1 The Article 5(1)(e) Framework

Article 5(1)(e) GDPR requires that personal data be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”. The principle of storage limitation imposes a substantive obligation: data must be retained only as long as the legitimate purpose requires and must be deleted, anonymised, or otherwise rendered non-identifiable thereafter.

The Wpg and Wjsg provide for specific retention periods in respect of the data they govern. The retention periods are typically generous — measured in years or decades, with periodic review obligations — but they are specified and they are bounded. The residual GDPR regime applicable to NIFP-held forensic-evaluation material is less prescriptive, but the underlying principle of storage limitation continues to apply.

9.2 NIFP Retention Practice

The publicly available information on NIFP retention practice is limited. The NIFP's data-protection notices and annual reports do not provide comprehensive specification of the retention periods applicable to *pro Justitia* materials, nor do they specify the conditions under which materials are reviewed for continued necessity. The practical position appears to be that *pro Justitia* materials are retained indefinitely or for very long periods, with limited review.

The *S. and Marper v. UK* doctrine, examined at §5.8 above, establishes that indefinite retention of sensitive data by State actors is itself an Article 8 concern requiring independent justification. The *G.C. v. CNIL* doctrine establishes that the right to erasure operates with particular force in respect of sensitive-data processing. Together, these doctrines impose substantive constraints on NIFP retention practice that have not, to date, been the subject of authoritative AP guidance or judicial determination.

9.3 The Onward-Disclosure Problem

A second structural concern arises in respect of onward disclosure. A *pro Justitia* report, once produced, is transmitted from the NIFP to the OM and from the OM to the trial court. The trial court provides copies to the defence and, in the course of the proceedings, the report becomes part of the criminal-procedural file accessible to subsequent recipients including: appellate courts; reclassering at the post-conviction stage; prison medical services where the defendant is detained; receiving TBS-klinieken; and subsequent forensic evaluators in any future proceedings. Each disclosure is a separate processing event under the GDPR/LED framework.

The practical position is that a *pro Justitia* report, once issued, becomes a long-lived document with multiple subsequent recipients and uses. The *Bara* doctrine (each transfer requires its own lawful basis and triggers its own information obligation) and the *S. and Marper* doctrine (long-term retention is an independent concern) together impose substantive structural requirements that are not, on the publicly available material, systematically given effect.

9.4 The Cumulative Effect

The cumulative effect of indefinite retention and onward disclosure is that a *pro Justitia* report functions as a permanent, multiply-disseminated record of the defendant's mental-health evaluation, available to a wide range of State and adjacent actors, with limited mechanisms for

review, correction, or erasure. The structural conditions under which such a record exists require sustained scrutiny under the GDPR/LED architecture and under Article 8 ECHR. The current practice, in the present author's analysis, does not consistently satisfy that scrutiny.

10. Remedies: The Autoriteit Persoonsgegevens, Civil Claims, and Parallel Tracks

10.1 The AP Complaint Procedure

The *Autoriteit Persoonsgegevens* (AP) is the Dutch supervisory authority designated under Article 51 GDPR and Article 41 of the Law Enforcement Directive. The AP exercises supervisory and enforcement powers in respect of GDPR-governed and LED-governed processing in the Netherlands. A data subject who considers that processing of his or her personal data infringes the GDPR or the *Uitvoeringswet AVG* may lodge a complaint with the AP under Article 77 GDPR, which the AP must investigate and respond to.

The AP procedure has several practical features that recommend it as a parallel forum to the criminal court. *First*, no exhaustion-of-domestic-remedies barrier applies; the AP complaint may be filed at any time. *Second*, the AP procedure is administrative and operates on shorter timescales than criminal proceedings. *Third*, the AP may issue findings, impose corrective measures, and (where appropriate) administrative fines, generating regulatory output usable in parallel proceedings. *Fourth*, the AP's findings are subject to judicial review through the *bestuursrechter*, providing a separate route to judicial determination on data-protection questions.

A complaint against NIFP-affiliated *pro Justitia* practice would address: the lawful basis of the third-party-data processing; the proportionality of the data inclusion; the purpose-limitation analysis where mandate drift has occurred; the onward-transfer architecture; the retention regime; and the data-subject-access and rectification mechanisms. Each of these issues maps onto established AP enforcement priorities and could be the subject of structured submission.

10.2 Data-Subject Rights under Articles 15–22 GDPR

The GDPR's data-subject rights operate in addition to the AP complaint procedure and may be exercised directly against the controller. The most relevant rights for *pro Justitia* contexts are:

- *Right of access* (Article 15): the data subject may request access to personal data processed by the controller. In *pro Justitia* contexts, the right operates against the NIFP as controller of the forensic-evaluation processing.
- *Right to rectification* (Article 16): the data subject may request correction of inaccurate data. In forensic contexts, this engages the question of whether evaluative characterisations as well as factual data are subject to rectification.
- *Right to erasure* (Article 17): the data subject may request erasure of data that is no longer necessary, that has been unlawfully processed, or that has been processed without consent where consent was the basis. In forensic contexts, the right operates with particular force after the conclusion of proceedings, especially where the proceedings have concluded without conviction or with acquittal.
- *Right to restriction* (Article 18): the data subject may request restriction of processing pending verification of accuracy or in other specified circumstances.
- *Right to object* (Article 21): the data subject may object to processing on grounds relating to his or her particular situation.

The exercise of these rights against the NIFP is, in practice, attenuated by the structural conditions of forensic processing. The NIFP's response to data-subject-access requests has not, on the publicly available material, been the subject of systematic AP audit. The structural recommendation in §11 below is that the AP undertake such audit.

10.3 Civil Claims under Article 82 GDPR

Article 82 GDPR provides that any person who has suffered material or non-material damage as a result of an infringement of the Regulation has the right to compensation from the controller or processor. The provision establishes a private right of action that operates in addition to the regulatory enforcement framework.

The CJEU has, in cases including *UI v. Österreichische Post* (Case C-300/21, 4 May 2023), addressed the requirements for damages under Article 82, holding that the existence of an infringement does not automatically entitle the data subject to damages and that the data subject must demonstrate damage and a causal link. Subsequent CJEU jurisprudence has elaborated the

standards for non-material damage, with the trend favouring lower thresholds than initially proposed.

For *pro Justitia* contexts, an Article 82 claim is doctrinally available where the data subject can demonstrate: an infringement of the GDPR (the substantive analysis developed in §§3–9 above); damage flowing from the infringement (which in sensitive-data processing contexts may include reputational, professional, and emotional harm); and a causal link. The damages framework operates in parallel with the AP regulatory track and with civil claims under Dutch *onrechtmatige daad* doctrine (Article 6:162 BW).

10.4 Onrechtmatige Daad Claims

A separate civil claim is available under Dutch *onrechtmatige daad* doctrine where the conduct of NIFP-affiliated actors has caused damage to the data subject through tortious conduct distinct from the strict GDPR-violation framework. The two tracks may overlap; the *onrechtmatige daad* track is broader in some respects and narrower in others. The combined civil framework provides multiple parallel routes to damages.

10.5 Strategic Sequencing

For a defendant in a configuration analogous to parket nr 18-104657-25, the strategic sequencing of the available remedies turns on the timing of the underlying criminal proceedings, the disciplinary proceedings, and the international submissions. The AP complaint can be filed immediately and runs in parallel; the AP’s findings, when issued, become evidence usable in the other proceedings. The civil damages claim is best filed after AP findings have issued and after the criminal proceedings have produced material on the consequences of the data-protection breach. The international submissions — to UN Special Procedures, the ECtHR, and the ICC OTP — can incorporate the AP findings as evidence of structural violation.

The cumulative architecture is that the data-protection track generates its own findings on its own timescale and feeds those findings into the broader system of remedies. The structural value of the parallel track is that it does not depend on the success or failure of the criminal proceedings; the AP complaint can succeed even where the criminal proceedings produce an unfavourable outcome for the defendant.

11. Reform Proposals and Structural Safeguards

The analysis developed in this article supports several categories of structural reform.

AP Guidance: The AP should issue authoritative guidance on the data-protection regime applicable to *pro Justitia* processing. The guidance should address: the controllership architecture; the applicable regime (GDPR, Wpg, Wjsg, or combinations); the lawful bases for third-party-data inclusion; the purpose-limitation requirements; the retention regime; the onward-transfer architecture; and the data-subject-rights mechanisms. The absence of such guidance is, in itself, a structural concern under Article 5(1)(a) GDPR (transparency).

Mandatory Data Protection Impact Assessments: The NIFP should be required to conduct Data Protection Impact Assessments under Article 35 GDPR for the *pro Justitia* programme as a whole and for any significant changes to the programme. The DPIAs should address each of the substantive concerns identified in §§7–9 above and should be subject to public consultation and AP review.

Structural Separation of NIFP Data Processing from Prosecuting-Authority Access: The current institutional architecture, in which NIFP data is integrated into a prosecutorial workflow without structural separation, creates the conditions for purpose-limitation breaches and for over-broad onward disclosure. Structural reform should consider mechanisms for separation: dedicated NIFP data-protection officers with mandate to scrutinise transfers; firewalls between forensic-evaluation data and broader OM access; and statutory restrictions on the use of *pro Justitia* materials beyond the immediate proceedings for which they were produced.

Mandatory Third-Party-Data Minimisation Protocols: NIFP practice should incorporate explicit protocols for the minimisation of third-party data in *pro Justitia* reports. The protocols should specify: the categories of third-party data that may be included; the proportionality assessment that must be conducted before inclusion; the notification obligations that must be discharged in respect of third-party data subjects (subject to any specific exceptions justified under the GDPR/LED framework); and the procedural mechanisms by which third parties may exercise data-subject rights.

Structured Retention Schedules with Periodic Review: NIFP retention of *pro Justitia* materials should be governed by published retention schedules specifying the duration of retention by category and purpose, with mandatory periodic review for continued necessity, and with default rules for erasure where the operational purpose has been served. The retention regime should give

effect to the *S. and Marper* doctrine on indefinite retention and to the *G.C. v. CNIL* doctrine on the right to erasure.

Data-Subject-Access Protocols Specific to the Forensic Context: The NIFP should publish data-subject-access protocols specific to forensic-evaluation processing, addressing the practical position of data subjects who seek access to materials within criminal-procedural contexts and providing mechanisms by which access can be effective in practice as well as in formal law.

Statutory Framework for Disciplinary/Regulatory Coordination: Where a *pro Justitia* report is the subject of a pending disciplinary complaint, a statutory framework should govern the parallel regulatory and disciplinary scrutiny. The framework should include: notification obligations between the AP and the relevant Tuchtcollege; coordination of findings; and explicit provision for the use of regulatory or disciplinary findings in the subsequent stages of the criminal proceedings.

12. Conclusion

This article has argued that NIFP-affiliated *pro Justitia* practice must be analysed not only as a criminal-procedural phenomenon but as a data processing operation subject to the substantive requirements of the GDPR, the Wpg, the Wjsg, and the parallel ECtHR Article 8 jurisprudence. The data-protection lens reveals structural concerns — the routine inclusion of third-party data, the operation of mandate drift as a purpose-limitation breach, the indefinite retention and broad onward disclosure of forensic materials, and the attenuated practical exercise of data-subject rights — that the criminal-procedural lens does not surface.

These concerns engage substantive normative requirements under EU law, under Dutch implementing legislation, and under the European Convention on Human Rights. The composite standard developed across the substantive sections of this article — lawful basis, proportionality, data minimisation, purpose limitation, storage limitation, transparency, data-subject rights, and effective remedy — is not, on the present author's analysis, consistently satisfied by current Dutch *pro Justitia* practice.

The remedial framework set out in §10 above provides multiple parallel routes for the data subject to address these concerns. The AP complaint procedure is filable now; the data-subject rights operate directly against the NIFP as controller; the civil-damages framework provides *ex post* remedies; the *onrechtmatige daad* claim provides a parallel civil route. Each track operates on its

own timescale and produces its own findings; the cumulative architecture does not depend on the success or failure of the underlying criminal proceedings.

For the defendant in a configuration analogous to parket nr 18-104657-25, the strategic value of the data-protection track is twofold. *First*, it provides a parallel forum operating on shorter timescales than the criminal court. *Second*, it generates regulatory and civil findings that feed into the broader system of remedies including the international submissions and any subsequent ECtHR application. The track is doctrinally available, regulatorily activatable, and structurally capable of contributing to the resolution of the underlying matter.

The wider point is the one made across the four-paper sequence to which this article belongs. The structural reform of NIFP-affiliated *pro Justitia* practice — driven by the convergence of criminal-procedural, expert-evidence, data-protection, and (in the next paper) Article 10 expression-protection requirements — is a project of substantial scope. The data-protection contribution to that project, articulated in the present article, is one component among others. Its specific value is the parallel-forum architecture and the regulatory-findings output that the AP track makes available, and the structural focus on data-subject rights that the criminal-procedural framework does not adequately incorporate.

References

Scholarly Literature

Cuijpers, C. *Privacy en strafrecht* (latest edition).

Hijmans, H. *The European Union as Guardian of Internet Privacy* (Springer, 2016).

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (Eds.). *The EU General Data Protection Regulation: A Commentary* (2nd edn, Oxford University Press, 2020).

Lynskey, O. *The Foundations of EU Data Protection Law* (Oxford University Press, 2015).

Voigt, P., & von dem Bussche, A. *The EU General Data Protection Regulation: A Practical Guide* (Springer, 2017).

Recurrent commentary in *Computerrecht, Tijdschrift voor Privacyrecht, Nederlands Juristenblad, Privacy & Informatie*.

EU Legal Instruments

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (Law Enforcement Directive), OJ L 119, 4.5.2016.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 (PNR Directive), OJ L 119, 4.5.2016.

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (Whistleblower Protection Directive), OJ L 305, 26.11.2019.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4.5.2016.

Court of Justice of the European Union — Selected Cases

Bara, Case C-201/14, 1 October 2015.

Commissioner of An Garda Síochána, Case C-140/20, 5 April 2022.

G.C. v. CNIL, Case C-136/17, 24 September 2019.

Google Spain, Case C-131/12, 13 May 2014.

H.K. v. Prokuratuur, Case C-746/18, 2 March 2021.

La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18, C-520/18, 6 October 2020.

Ligue des droits humains, Case C-817/19, 21 June 2022.

Norra Stockholm Bygg, Case C-268/21, 2 March 2023.

Privacy International, Case C-623/17, 6 October 2020.

Schrems I, Case C-362/14, 6 October 2015.

Schrems II, Case C-311/18, 16 July 2020.

Tele2 Sverige and Watson, Joined Cases C-203/15 and C-698/15, 21 December 2016.

UI v. Österreichische Post, Case C-300/21, 4 May 2023.

European Court of Human Rights — Article 8 (Sensitive-Data Processing)

Avilkina v. Russia, App. No. 1585/09, 6 June 2013.

Brunet v. France, App. No. 21010/10, 18 September 2014.

I v. Finland, App. No. 20511/03, 17 July 2008.

Khelili v. Switzerland, App. No. 16188/07, 18 October 2011.

L.H. v. Latvia, App. No. 52019/07, 29 April 2014.

M.S. v. Sweden, App. No. 20837/92, 27 August 1997.

S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04, Grand Chamber, 4 December 2008.

Surikov v. Ukraine, App. No. 42788/06, 26 January 2017.

Y.Y. v. Russia, App. No. 40378/06, 23 February 2016.

Z v. Finland, App. No. 22009/93, 25 February 1997.

Selected Dutch Legal Sources

Algemene wet bestuursrecht (Awb).

Burgerlijk Wetboek, Article 6:162 (onrechtmatige daad).

Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

Wet bescherming persoonsgegevens politie en justitie (provisions on enforcement).

Wet justitiële en strafvorderlijke gegevens (Wjsg).

Wet op de beroepen in de individuele gezondheidszorg (Wet BIG), Staatsblad 1993, 655.

Wet politiegegevens (Wpg).

Wetboek van Strafvordering (Sv), particularly Articles 196 and 227 et seq.

Companion Papers

Weaponised Forensic Psychiatry, Epistemic Risk, and Procedural Inequality: A Multilevel Analysis of Pro Justitia Reporting within European and International Human Rights Frameworks, expanded edition, April 2026, DOI 10.5281/zenodo.19812911.

The Weigerende Observandus and the Inversion of Winterwerp: NIFP Forensic Psychiatry, the Pieter Baan Centrum, and Article 196 Sv and Self-Incrimination Jurisprudence, April 2026, DOI 10.5281/zenodo.19817612.

This article is published under an open-access licence and is permanently archived at Zenodo under DOI [10.5281/zenodo.19825495](https://doi.org/10.5281/zenodo.19825495). The companion papers are archived under DOI [10.5281/zenodo.19812911](https://doi.org/10.5281/zenodo.19812911) and DOI [10.5281/zenodo.19817612](https://doi.org/10.5281/zenodo.19817612). Readers are invited to cite the persistent identifiers rather than any transient URL.