
PURPOSE & MEANS

PRACTITIONER REFERENCE · DPIA SERIES

The EU Charter of Fundamental Rights and Data Processing Risk

A working reference for data protection practitioners: mapping all 54 Charter articles to the processing activities most likely to engage each right. Titles I–VI contain 50 substantive articles (rights, freedoms and principles); Title VII (Arts. 51–54) sets out general provisions including scope and limitations.

Published October 2026 **Source** EU Charter of Fundamental Rights (OJ C 326/391, 2012, binding from December 2009)

Framework GDPR Art. 35 · Recital 75

Article 35 of the GDPR requires a data protection impact assessment where processing is likely to result in a high risk to the *rights and freedoms of natural persons*. Those rights and freedoms are not defined within the GDPR itself. GDPR Recital 4 states that the right to data protection is not absolute and must be considered in relation to its function in society; Recital 75 lists specific risks to rights and freedoms; and the supervisory authority guidelines on DPIAs (WP248 rev.01) make explicit that practitioners should look to the **EU Charter of Fundamental Rights** to identify which rights are engaged. The Charter became legally binding when the Lisbon Treaty entered into force in December 2009.

This reference maps all 54 articles across the Charter's seven titles. Titles I–VI contain 50 substantive articles (rights, freedoms and principles); Title VII (Arts. 51–54) sets out general provisions including scope and limitations. Note that some articles, in particular Arts. 25, 26, 37 and 38, are principles rather than directly enforceable rights; under Art. 52(5), principles may be relied on in judicial proceedings only to interpret implementing legislation. Under Art. 51(1), the Charter binds EU institutions directly and member states only when implementing EU law; it reaches private controllers mainly indirectly, through the GDPR, which must be read in conformity with the Charter. Articles marked **KEY** are those most frequently implicated in data processing risk assessments (author's selection). For each title, worked examples show how specific processing activities put those rights at risk in practice.

How to use this reference. During the scoping phase of a DPIA, work through the six substantive titles (I–VI), then Title VII for limitations and scope, and identify which articles are engaged by the processing activity under assessment. Not every article will apply to every activity. Once you have identified the relevant rights, your DPIA's risk assessment should articulate specifically how the processing puts those rights at risk, and not merely reference the article number.

TITLE I

Dignity

Arts. 1–5 · The foundational title from which all other Charter rights derive. Human dignity (Art. 1) and the prohibition of torture (Art. 4) are absolute and cannot be balanced away; the other Title I rights are subject to the general limitations in Art. 52.

Art. 1 Human dignity KEY <i>Inviolable; must be respected and protected. Engaged by any processing that reduces a person to a score or dataset without recourse.</i>	Art. 2 Right to life <i>Engaged by processing in critical systems (medical, infrastructure, emergency services) where automated decisions could endanger life. Note: military and national security activities are largely outside EU law and the GDPR (GDPR Art. 2(2); TEU Art. 4(2)).</i>
Art. 3 Right to integrity of the person KEY <i>Physical and mental integrity. Engaged by biometric processing, covert health monitoring, and processing that causes psychological harm.</i>	Art. 4 Prohibition of torture <i>Relevant where processing enables or supports interrogation, detention, or surveillance systems used to facilitate ill-treatment.</i>
Art. 5 Prohibition of slavery and forced labour <i>Engaged by processing that enables or facilitates forced labour or trafficking, for example systems used to monitor, control, or conceal exploitation of workers. The connection to typical commercial processing is indirect; include only where there is a credible trafficking or forced-labour nexus.</i>	

WORKED EXAMPLES: TITLE I

ART. 1: HUMAN DIGNITY

Automated scoring without review or recourse

Creditworthiness, employability, or recidivism scoring systems that assign individuals a risk score with significant real-world consequences (loan refusal, employment rejection, parole denial) where no human reviews the score and no viable mechanism for challenge exists. Where a person cannot understand why a decision was made or effectively contest it, their dignity as a rational agent capable of self-determination is undermined. The harm is acute where the score follows the individual across contexts through data sharing.

ART. 3: INTEGRITY OF THE PERSON

Biometric processing at scale

Facial recognition, gait analysis, or voice identification collected in public or semi-public spaces without the knowledge of data subjects. Unlike a password, biometric characteristics

cannot be changed if compromised. The mental integrity dimension is also engaged where covert monitoring of emotional state is conducted through workplace sensors, wearables, or behavioural inference, particularly where data subjects cannot meaningfully withdraw from the context in which monitoring occurs.

TITLE II

Freedoms

Arts. 6–19 · The largest title (14 articles) and the most directly engaged in data processing risk assessments. Art. 8 is the Charter's dedicated data protection right; Art. 7 protects private and family life.

Art. 6 Right to liberty and security <i>Covers liberty: protection against unlawful arrest and detention. Engaged where processing enables or facilitates deprivation of liberty, for example automated risk scoring that feeds into pre-trial detention decisions. Not concerned with freedom of movement, which is Art. 45.</i>	Art. 7 Respect for private and family life KEY <i>Home and communications. Closely linked to Art. 8 (data protection) but distinct: Art. 7 protects the sphere of private life, while Art. 8 governs the processing of personal data as such. Both are routinely engaged together in tracking, profiling, and communications monitoring.</i>
Art. 8 Protection of personal data KEY <i>The Charter's dedicated data protection right and the direct constitutional basis for the GDPR (see also Art. 16 TFEU and GDPR Recital 1). Requires fair processing on a specified basis, a legitimate purpose, access and rectification rights, and oversight by an independent authority (Art. 8(3)). Applies to all processing.</i>	Art. 9 Right to marry <i>Rarely directly engaged, but implicated where processing reveals or infers relationship data used to discriminate or coerce.</i>
Art. 10 Freedom of thought, conscience, religion KEY <i>Engaged by processing that infers or reveals religious or political belief, including location data near places of worship, association networks, spending patterns.</i>	Art. 11 Freedom of expression and information KEY <i>Chilling effects. Engaged by surveillance of communications, content moderation systems, and monitoring of public expression.</i>
Art. 12 Freedom of assembly and association <i>Engaged by monitoring of participation in lawful assemblies, trade union membership data, and processing of association networks.</i>	Art. 13 Freedom of the arts and sciences <i>Engaged where surveillance, data collection, or processing restrictions constrain researchers, journalists, or artists, for example monitoring of academic communications or data access restrictions that impede scientific research.</i>
Art. 14 Right to education <i>Engaged by processing in educational technology: student monitoring, algorithmic grading, data sharing with third parties, where this limits fair access to education.</i>	Art. 15 Freedom to choose an occupation <i>Engaged by automated hiring decisions, background screening databases, and algorithmic reputation systems that restrict employment access.</i>
Art. 16 Freedom to conduct a business	Art. 17 Right to property

Engaged where algorithmic ranking or exclusion by dominant platforms materially affects the commercial freedom of sole traders or small businesses.

Art. 17(2) explicitly protects intellectual property. Engaged where processing involves unauthorised use or reproduction of copyright-protected works, or where algorithmic systems infringe IP rights at scale.

Art. 18 Right to asylum

Engaged where processing is used in asylum decision-making systems or where data sharing exposes asylum seekers to third-country risks.

Art. 19 Protection in the event of removal/expulsion

Engaged where processing supports deportation or removal decisions, particularly where algorithmic risk assessment is used to prioritise enforcement.

WORKED EXAMPLES: TITLE II

ARTS. 7 & 8: PRIVATE LIFE & PERSONAL DATA

Cross-context tracking and secondary use

Persistent device fingerprinting and cross-context tracking that builds detailed profiles of individuals' behaviour without their awareness, where tracking continues even after a user takes steps to limit it. The Art. 8 dimension is directly engaged where health data collected for medical care is later used for insurance underwriting or marketing without a lawful basis. Where data subjects could not reasonably have anticipated the secondary use, both the right to private life and the right to data protection are infringed.

ARTS. 7 & 11: PRIVATE LIFE & EXPRESSION

Workplace monitoring and chilling effects

Broad monitoring of employee communications (email, messaging, file access logs, keylogging) where scope is disproportionate to any legitimate business aim. The ECtHR's Grand Chamber in *Bărbulescu v Romania* (2017) established a multi-factor balancing test for assessing the lawfulness of employee monitoring: whether the employee was notified in advance, how far the monitoring went, whether less intrusive means were available, the proportionality of consequences, and whether adequate safeguards existed. Prior notice is one factor among several, not a standalone rule. The same chilling effect risk applies to public surveillance that records participation in lawful assemblies or political activity. Both Arts. 7 (private life) and 11 (expression) are engaged where monitoring causes individuals to self-censor.

ART. 10: FREEDOM OF THOUGHT AND RELIGION

Inference of belief from behavioural data

Processing of location data, payment records, or social network connections that, in combination, allows inference of an individual's religious practice, political beliefs, or ideological affiliation, even where no explicit declaration has been made. The risk is not merely disclosure but the existence of a persistent inferred profile that can be acted upon by state or private actors. Processing that creates this inference, even as a by-product of a different primary purpose, engages Art. 10 directly.

Equality

Arts. 20–26 · Algorithmic systems and large-scale processing create substantial equality risks, particularly through proxy discrimination and scale effects.

Art. 20 Equality before the law <i>Engaged where algorithmic systems produce inconsistent outcomes for similarly situated individuals, or where data access determines legal outcomes.</i>	Art. 21 Non-discrimination KEY <i>Prohibits discrimination on any ground including sex, race, ethnic origin, political or any other opinion, religion, genetic features, disability, age, and sexual orientation: the grounds most relevant to data processing. Engaged by any algorithmic processing that perpetuates or amplifies discrimination on these grounds, including through proxy variables.</i>
Art. 22 Cultural, religious, linguistic diversity <i>Engaged where processing imposes a dominant cultural or linguistic framework, for example NLP systems that perform poorly for minority languages or name formats.</i>	Art. 23 Equality between women and men <i>Engaged by automated systems trained on gender-biased data: recruitment, credit, or healthcare systems that systematically disadvantage women.</i>
Art. 24 The rights of the child KEY <i>Best interests as primary consideration. Engaged by all processing involving minors, including educational technology, consumer apps, parental data sharing.</i>	Art. 25 Rights of the elderly <i>Engaged where digital-only service delivery excludes older people, or where processing of older adults' data (health, financial) creates specific exploitation risks.</i>
Art. 26 Integration of persons with disabilities <i>Engaged where automated systems create barriers for people with disabilities: inaccessible interfaces, biometric systems that fail for certain conditions, or processing that infers disability without consent.</i>	

WORKED EXAMPLES: TITLE III

ART. 21: NON-DISCRIMINATION

Proxy discrimination in algorithmic decision-making

Machine learning systems trained on historically biased datasets that learn and replicate patterns of discrimination. A recruitment tool trained on historical hiring decisions where certain demographic groups were systematically excluded. The model learns to associate protected characteristics, or their proxies (postcode, school, name), with outcomes. The harm operates at scale and at speed: a small discriminatory bias in a model processing thousands of applications produces discriminatory outcomes for large numbers of people, in ways that may be invisible without targeted testing. Amazon's internal recruitment tool (discontinued in early 2017, reported by Reuters in October 2018) illustrates the mechanism: trained predominantly on CVs from men, it systematically downgraded applications referencing women's organisations, raising concerns that discriminatory patterns could not be reliably eliminated. Amazon states the tool was never used by recruiters. Recruitment AI is classified as high-risk under Annex III, point 4 of the EU AI Act (2024).

ART. 24: RIGHTS OF THE CHILD

Data collection from child users for commercial purposes

Consumer-facing applications that collect data from child users through age-inappropriate design, absent effective age verification, or data shared by parents, and that data is used for behavioural profiling, targeted advertising, or sale to third parties. Art. 24(2) makes the child's best interests "a primary consideration" in all actions relating to children, not the only or automatically overriding one, but a consideration that must be actively weighed and documented. Particular care is required in educational or care settings where children have limited capacity to withdraw from the context, and where the controller holds a position of institutional authority.

TITLE IV

Solidarity

Arts. 27–38 · Workplace rights and social protections. Increasingly engaged as algorithmic management, HR analytics, and health data processing expand in scope.

Art. 27 Workers' right to information and consultation KEY <i>Engaged where workplace monitoring or algorithmic management is introduced without adequate information to workers or consultation with representatives.</i>	Art. 28 Right of collective bargaining and action <i>Engaged where processing targets or identifies trade union members, monitors collective bargaining activity, or is used to anticipate or disrupt industrial action.</i>
Art. 29 Right of access to placement services <i>Engaged where automated systems filter access to employment services, or where algorithmic blacklisting affects an individual's visibility to placement agencies.</i>	Art. 30 Protection in the event of unjustified dismissal <i>Engaged where termination decisions are made or informed by algorithmic performance monitoring, without adequate human review of the underlying data.</i>
Art. 31 Fair and just working conditions KEY <i>Engaged by pervasive monitoring, productivity tracking, and algorithmic scheduling that creates unfair or unsafe working conditions.</i>	Art. 32 Prohibition of child labour <i>Engaged where processing supports the identification, management, or exploitation of child workers, or where platforms fail to prevent minor users from being engaged in commercial activities.</i>
Art. 33 Family and professional life <i>Engaged where processing of parental status, family composition, or carer responsibilities is used in employment decisions, or where always-on monitoring erodes the boundary between work and family life.</i>	Art. 34 Social security and social assistance <i>Engaged where automated processing is used in social security eligibility decisions, including benefit fraud detection systems, automated sanctions, without adequate human oversight.</i>
Art. 35 Health care KEY <i>Engaged where processing of health data creates barriers to care, such as insurance risk scoring, algorithmic triage, or where</i>	Art. 36 Access to services of general economic interest <i>Engaged where processing leads to exclusion from services of general economic interest,</i>

health data is used for purposes incompatible with its collection.

such as banking and utilities are the clearest examples. Housing assistance falls under Art. 34(3) rather than Art. 36.

Art. 37 Environmental protection

Less directly engaged in typical processing contexts, but relevant where data-driven systems are used in environmental compliance or where processing enables environmental harm affecting communities.

Art. 38 Consumer protection

Engaged by personalised pricing, dark patterns, and processing for persuasive commerce that exploits consumer vulnerabilities identified through behavioural profiling.

WORKED EXAMPLES: TITLE IV

ARTS. 27 & 31: WORKERS' RIGHTS

Algorithmic management without information or consultation

Deployment of productivity monitoring software, task-completion tracking, or algorithmic scheduling in workplaces without meaningful information to workers or consultation with worker representatives. Where output rates, time-on-task data, or absence patterns inform performance management or termination decisions without workers knowing what data is being used or having any mechanism to challenge it, both the right to information and the right to fair working conditions are engaged. This risk is acute in platform and gig economy contexts where workers have limited bargaining power and no stable employment relationship through which to exercise their rights.

ART. 35: HEALTH CARE

Health data processing that creates barriers to care

Health data processed for insurance risk pricing that results in certain individuals, including those with chronic conditions, genetic predispositions, or prior diagnoses, being denied coverage or placed in prohibitively expensive risk pools. Similarly, automated triage or eligibility assessment systems in public healthcare that systematically route certain groups away from care, without clinical review, engage the Charter right to health care. The harm is structural: it does not require that any individual decision was incorrect, only that the system creates a class of people for whom access to care is systematically degraded.

TITLE V

Citizens' Rights

Arts. 39–46 · Rights specific to EU citizens. Increasingly engaged by processing that affects democratic participation, freedom of movement, and access to public administration.

Art. 39 Right to vote in European Parliament elections

Engaged where processing, including micro-targeting, disinformation, voter suppression

Art. 40 Right to vote in municipal elections

Mirrors Art. 39 for municipal elections in the member state of residence. Engaged where processing specifically targets voting rights in

through personalised content, that undermines the integrity of EU elections.	that context, for example data used to suppress or manipulate participation in municipal elections. Broader election-related processing risks engage Arts. 39, 7, and 11.
Art. 41 Right to good administration KEY Includes the right to have one's affairs handled impartially, and the right to reasons. Directly binds EU institutions and bodies only, not national authorities. Applies to national bodies as a general principle of EU law when they implement EU law (YS and Others, C-141/12).	Art. 42 Right of access to documents Binds EU institutions and bodies only. Engaged where automated processing of EU institution records creates opacity, or where access requests to EU bodies are denied on the basis of algorithmically managed classifications.
Art. 43 Ombudsman Relevant as an avenue of redress where processing by EU institutions or bodies causes maladministration, including automated processing without adequate oversight.	Art. 44 Right to petition Engaged where surveillance or monitoring of petitioners creates a chilling effect on the exercise of this democratic right.
Art. 45 Freedom of movement and of residence Concerned with cross-border movement between EU member states. Engaged where processing, including border surveillance,, passenger data sharing, Schengen data systems, that affects EU citizens' right to move freely between states. Chilling effects on movement within a single state are better mapped to Arts. 7, 10, and 12.	Art. 46 Diplomatic and consular protection Rarely directly engaged in commercial processing contexts; relevant where data sharing with third countries affects citizens' ability to seek consular protection.

WORKED EXAMPLES: TITLE V

ARTS. 7, 10 & 12: PRIVATE LIFE, BELIEF & ASSEMBLY

Location data and the chilling effect on lawful activity

Mobile network or app-derived location data retained over extended periods, allowing reconstruction of an individual's movements: where they live, worship, seek medical care, or meet with others. Even where individual data points appear innocuous, sustained location history can reveal political affiliation, religious practice, health status, and personal relationships. The chilling effect is real: individuals aware of persistent location tracking may avoid attending lawful assemblies, religious services, or medical facilities where stigma of attendance could be used against them by employers, insurers, or state actors. The relevant rights are Arts. 7 (private life), 10 (freedom of belief), and 12 (freedom of assembly), and not Art. 45, which concerns cross-border movement between member states.

ART. 41 / EU GENERAL PRINCIPLE: GOOD ADMINISTRATION

Automated public administration decisions

Automated processing used to determine eligibility for social benefits, tax assessments, planning permissions, or regulatory decisions, where the algorithmic basis of the decision is opaque and the individual has no effective means of understanding or challenging it. Art. 41 directly binds EU institutions and bodies. For national authorities, the equivalent obligation

arises as a general principle of EU law when implementing EU law. In both cases, the right to be heard and the right to reasons for decisions are structurally difficult to meet where a decision is the output of a complex model rather than a reasoned administrative judgment.

TITLE VI

Justice

Arts. 47–50 · Rights of access to justice and fair process. Increasingly engaged by automated decision-making in law enforcement, financial services, and public administration.

Art. 47 **Right to an effective remedy and fair trial**
KEY
Engaged where automated decisions cannot be effectively challenged: black-box models, commercially confidential algorithms, opaque scoring systems.

Art. 48 **Presumption of innocence and right of defence** **KEY**
Engaged by pre-decisional risk scoring, watchlists, and predictive profiling that treats individuals as probable offenders before any legal finding.

Art. 49 **Principles of legality and proportionality**
Engaged where processing is used to determine criminal sanctions, or where automated enforcement decisions lack proportionality review.

Art. 50 **Right not to be tried or punished twice**
Engaged in data-sharing contexts where cross-border transfer of criminal justice data enables enforcement action in a second jurisdiction for the same conduct already prosecuted; the primary risk is in international data exchange rather than general processing activities.

WORKED EXAMPLES: TITLE VI

ART. 47: EFFECTIVE REMEDY

Predictive policing and opaque algorithmic outputs

Predictive policing systems that flag individuals as elevated risk based on algorithmic analysis of prior police contact, social network connections, or postcode, where this flag influences decisions about stop-and-search, arrest, or prosecution. Where the algorithm's reasoning is opaque, either technically (a black-box model) or legally (claimed as commercially confidential), and an individual subject to adverse action on the basis of its output has no meaningful ability to challenge the process. The effective remedy requirement is difficult to satisfy where the very basis for a decision is shielded from scrutiny, since any downstream review process depends on being able to identify and contest the specific grounds for the outcome.

ART. 48: PRESUMPTION OF INNOCENCE

Financial watchlists and sector-wide risk scoring

Fraud detection or anti-money laundering systems that place individuals on internal watchlists, restrict access to financial services, or trigger enhanced monitoring on the basis of

algorithmic risk assessment, without any legal process, notice to the individual, or right to respond. Where these assessments are shared across institutions through screening databases and persist over time, an individual who has committed no offence may find themselves treated as a higher-risk subject across the financial system, with limited means to understand or challenge why. Note that Art. 48 formally protects persons charged in criminal proceedings; the mapping here reflects the structural parallel: pre-decisional risk treatment without legal process, rather than a direct application of the article's strict scope.

TITLE VII

General Provisions

Arts. 51–54 · Scope, limitations, and relationship to other law. Essential context for any practitioner using the Charter in a DPIA.

Art. 51 Field of application **KEY**

The Charter binds EU institutions directly and member states only when implementing EU law. It reaches private controllers mainly indirectly, through the GDPR, which must be read and applied in conformity with the Charter. This is the primary mechanism making Charter rights relevant to private-sector DPIAs. Some articles (including Arts. 21 and 31(2)) have been recognised by the Court of Justice as capable of direct effect between private parties.

Art. 52 Scope and interpretation of rights and principles **KEY**

Limitations on Charter rights (Art. 52(1)) must be: provided for by law; respect the essence of the right; necessary; and genuinely meet an objective of general interest or protect others' rights. These are the legal elements of the proportionality analysis at the heart of any DPIA. Where a Charter right corresponds to an ECHR right (Art. 52(3)), it has the same meaning and scope, though EU law may provide broader protection. Directly engaged every time a DPIA weighs competing interests.

Art. 53 Level of protection

Nothing in the Charter may be interpreted as restricting human rights as protected under Union law, international law, the ECHR, or Member States' constitutions. The Charter sets a floor, not a ceiling, though under the primacy of EU law, higher national standards cannot be used to undermine the uniform application of EU law where EU law applies.

Art. 54 Prohibition of abuse of rights

No Charter right may be used to perform acts aimed at destroying the rights of others or at limiting them to a greater extent than the Charter allows. Rarely directly engaged in commercial processing contexts, but relevant where a claimed right (such as freedom of expression or contractual freedom) is invoked to override data subjects' protections.

GDPR RECITAL 75: REFERENCE TEXT

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and

freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements..."