

Proportionality

An article on justified interference, judicial method, and rights-sensitive technology design in EU law

By Dr M.R. Leiser (Mark)

Abstract

Proportionality is often invoked as if the word itself supplies judgement. It does not. In EU law, the principle is neither a universal solvent nor a single test with a fixed intensity. It is a family of justificatory disciplines that operate in different legal locations: Article 5(4) TEU controls the content and form of Union action; Article 52(1) of the Charter governs limitations on Charter rights; the GDPR and the AI Act embed narrower tests of necessity, balancing, risk reduction and remedial discretion; and courts use proportionality to calibrate remedies. This article reconstructs those disciplines as the constitutional law of technological architecture. Its central claim is that power becomes legally intelligible only when the design of an interference can be traced to a lawful and sufficiently precise reason.

Does the design of the interference remain within the limits of the reason that justifies it?

The argument proceeds in four stages.

1. It traces the principle from older ideas of measured authority, through German administrative and constitutional law, Strasbourg's fair-balance reasoning, the Court of Justice's general principles, and the Charter.
2. It develops proportionality as a judicial method. It distinguishes several modes of review: deferential legislative review, strict rights review, remedial proportionality, infrastructure proportionality, lawful-basis proportionality, safeguards proportionality and explanation proportionality.
3. It reads the hard technology cases as conflicts among rights and legally protected freedoms rather than as privacy against nothing.
4. It proposes a doctrinally grounded protocol for GDPR and AI Act practice. The protocol starts with interference intensity, specifies aims operationally, tests suitability with evidence, treats necessity as a design comparison, makes safeguards constitutive, requires a residual burden review, and insists on a temporal review.

The article rejects both privacy absolutism, including the anti-proportionality rhetoric associated with Max Schrems, and managerial balancing, which treats rights as a negotiable cost in a business plan. Properly understood, proportionality does neither. It disciplines public authorities, supervisory bodies and regulated actors by requiring them to identify the legal source of their power, describe the interference, specify the aim, test causal fit, compare sufficiently effective alternatives, design safeguards and justify the

residual burden. The result is not a licence to trade away rights, but a structured account of why a particular limitation remains lawful.¹

Keywords: proportionality; EU law; Charter of Fundamental Rights; GDPR; AI Act; privacy; data protection; business freedom; judicial review; technology regulation; digital rights.

1. Introduction: The Discipline of Justified Interference

Proportionality begins with a simple proposition and quickly becomes difficult: power must not outrun the reason that justifies it. That proposition does not dictate that privacy always defeats security, expression always defeats reputation, property always defeats access to information, or business freedom must always yield to regulatory ambition. It requires something more exacting. The actor responsible for a rights burden must identify the legal authority for the measure, articulate the aim at a level that can be tested, establish a rational connection, identify sufficiently effective but less restrictive alternatives, establish safeguards, and accept a final judgement about excess. Each stage answers a different question; collapsing them into the language of “balance” conceals legal failure.²

Modern law constantly authorises interference. Data protection law authorises processing. Competition law authorises investigation. Platform law authorises duties of care. Security law authorises access. Child-protection law authorises verification and reporting. Consumer law authorises intervention in interface design. The legal problem is not interference as such. Law governs by interference. The problem is excess. An institution may act within its competence and still choose means that are overbroad, indiscriminate, weakly evidenced or poorly safeguarded. Proportionality targets that second failure. It asks whether lawful power remains inside the limits of its own justification.

Technology makes the point unavoidable. A database, recommender system, biometric gate, AdTech consent framework, age-assurance tool, fraud model, workplace-monitoring system or AI classifier does not merely execute a rule. It gives the rule an architecture. That architecture decides who enters the system, which data are captured, how long the burden persists, which inferences may follow, which actor may obtain access, which person can complain and which errors become sticky. Proportionality therefore travels from the form of law to the design of systems. It asks not only whether a legislature, controller, platform or regulator has named a legitimate aim. It asks whether the operational design respects that aim.³

The article's controlling claim is that EU technology law suffers less from the absence of proportionality than from a failure to distinguish and operationalise its different legal forms. Article 52(1) review of a legislative limitation is not the same exercise as a controller's necessity assessment under Article 6 GDPR, a data minimisation analysis under Article 5(1)(c), a DPIA under Article 35, a deployer's fundamental-rights impact assessment under Article 27 of the AI Act, or a supervisory authority's choice of corrective

¹ Consolidated Version of the Treaty on European Union [2012] OJ C326/13, art 5(4); Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 52(1); Regulation (EU) 2016/679 of the European Parliament and of the Council [2016] OJ L119/1, recital 4; Regulation (EU) 2024/1689 of the European Parliament and of the Council [2024] OJ L2024/1689, art 27.

² *R v Minister of Agriculture, Fisheries and Food, ex p Fedesa* (Case C-331/88) EU:C:1990:391, para 13; Charter, art 52(1).

³ *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238, paras 52-69; *Opinion 1/15 EU-Canada PNR Agreement* EU:C:2017:592, paras 140-232; *Ligue des droits humains ASBL v Conseil des ministres* (Case C-817/19) EU:C:2022:491, paras 117-228.

power. The grammar of justification connects those exercises, but their legal basis, addressee, evidential burden and remedy differ. The article therefore uses proportionality as an organising principle without allowing it to swallow the operative rules that give it legal form.

*Has the actor justified the rights burden created by the design?*⁴

That claim requires a legal-location rule. Article 52(1) addresses limitations attributable to public power within the Charter's scope; it is not itself a lawful basis for private processing. Controllers are subject to proportionality under the GDPR's operative provisions, and platforms or AI actors are subject to additional rules that bind them. Conversely, a regulator cannot justify a remedy merely by showing that the controller infringed a rule. The regulator must act within its corrective powers and justify the form and severity of intervention. Proportionality integrates these inquiries only if it preserves their distinct sources.

Two evasions distort the subject. The first is rights absolutism. Recital 4 of the GDPR correctly places data protection within a constitutional ecology in which privacy, expression, information, equality, property, business freedom, child protection, and effective remedies can all carry legal weight. The second is managerial balancing. Proportionality does not permit an organisation, regulator, or court to trade off a right for efficiency whenever a spreadsheet shows a net benefit. It requires reasons that the relevant legal order recognises, and it tests those reasons against evidence, alternatives, safeguards and the distribution of the remaining burden. Fundamentality therefore strengthens the demand for justification; it does not eliminate conflict or authorise informal trade-offs.⁵

The argument also needs limits. Proportionality cannot cure the absence of competence, an inadequate legal basis, unforeseeable law, impairment of the essence of a right, discrimination contrary to a hard prohibition, invalid consent or conduct that an operative rule forbids. Nor does Recital 4 create a free-standing lawful basis or permit a controller to disapply the GDPR's text in the name of balance. In *Schrems I*, for example, generalised access to the content of electronic communications compromised the essence of Article 7, while the absence of effective judicial protection compromised the essence of Article 47; ordinary balancing could not repair either defect. Proportionality governs legally permissible limitations. It does not perform legal alchemy on illegality.⁶

2. Historical Background: From Measured Power to Constitutional Grammar

2.1 Measure, Reason and the Refusal of Excess

The vocabulary of proportionality is modern, but the legal anxiety is older than EU law. Legal orders have long distrusted power that loses its relation to the reason for its existence. Older ideas of measure and due proportion did not contain the tripartite test now taught to lawyers, and the history should not be narrated as a frictionless progression from natural law to Karlsruhe and then Luxembourg. What persisted was a

⁴ Regulation (EU) 2016/679, arts 5, 6, 25 and 35; Regulation (EU) 2024/1689, arts 9-15 and 27; European Data Protection Supervisor, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (25 February 2019).

⁵ Regulation (EU) 2016/679, recital 4; Charter, arts 7, 8, 11, 16, 21, 24, 47 and 52(1).

⁶ Charter, art 52(1); *Schrems v Data Protection Commissioner* (Case C-362/14) EU:C:2015:650, paras 94-95; *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* (Case C-311/18) EU:C:2020:559, paras 171-202.

constitutional intuition: jurisdiction concerns whether an authority may act, whereas proportionality asks whether the means chosen remain connected to and bounded by the purpose that authorises the action. Early police, licensing and emergency powers made that distinction concrete because a measure could rest on statutory authority and still burden liberty more than the occasion warranted.⁷

That older account explains why proportionality should not be treated as politeness in the exercise of power. It controls the excess of power that claims legality. The distinction matters in privacy, data protection and platform regulation. A controller may identify a lawful basis; a public authority may invoke statutory competence; a regulator may point to a market failure; a platform may rely on contractual design. None of those moves answers the proportionality question. Authority permits the actor to act. Proportionality asks whether the actor has chosen means that remain within the limits of the reason for action.

The migration of proportionality into EU law was neither linear nor uniform. The principle has protected rights, market freedoms, Member States against excessive Union action and individuals against unnecessary administrative burdens. Its apparent unity therefore conceals different objects of protection and different standards of review. An interest-based taxonomy is indispensable in technology cases because the same system may be reviewed as Union legislation, a national restriction, a limitation on a Charter right, private processing under the GDPR and a regulatory remedy.⁸

2.2 German Public Law and the Architecture of *Verhältnismässigkeit*

German administrative and constitutional law gave the principle its most influential architecture. *Verhältnismässigkeit* separates suitability, necessity and proportionality in the strict sense. Suitability asks whether the measure can contribute to the stated aim. Necessity asks whether a sufficiently effective but less rights-restrictive option is available. Strict proportionality asks whether the residual burden is excessive in view of the importance and degree of achievement of the aim. The separation is not scholastic tidiness: it prevents a court from masking a failure of evidence as a final balance, or treating institutional preference as necessity. The model's migration into EU law was selective, however, and the Court of Justice has adapted its intensity to the protected interest, institutional setting and source of the measure rather than applying a single German template.⁹¹⁰

⁷ Takis Tridimas, *The General Principles of EU Law* (2nd edn, OUP 2006) 136-170; Paul Craig, *EU Administrative Law* (3rd edn, OUP 2018) 657-711.

⁸ Gráinne de Búrca, 'The Principle of Proportionality and its Application in EC Law' (1993) 13 *Yearbook of European Law* 105; Tor-Inge Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16 *European Law Journal* 158; Wolf Sauter, 'Proportionality in EU Law: A Balancing Act?' (2013) 15 *Cambridge Yearbook of European Legal Studies* 439; Vasiliki Kosta, 'The Principle of Proportionality in EU Law: An Interest-based Taxonomy' in Joana Mendes (ed), *EU Executive Discretion and the Limits of Law* (OUP 2019) 198.

⁹ Robert Alexy, *A Theory of Constitutional Rights* (Julian Rivers tr, OUP 2002) 66-69; Dieter Grimm, *Constitutionalism: Past, Present, and Future* (OUP 2016) 178-205; Aharon Barak, *Proportionality: Constitutional Rights and their Limitations* (CUP 2012) 131-175.

¹⁰ Gráinne de Búrca, 'The Principle of Proportionality and its Application in EC Law' (1993) 13 *Yearbook of European Law* 105; Tor-Inge Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16 *European Law Journal* 158; Wolf Sauter, 'Proportionality in EU Law: A Balancing Act?' (2013) 15 *Cambridge Yearbook of European Legal Studies* 439; Vasiliki Kosta, 'The

Suitability disciplines fantasy. A measure that does not contribute to the aim cannot justify a rights burden. Necessity disciplines institutional preference. A measure may help the actor, but a narrower design may do the same legal work with less interference. Strict proportionality disciplines overreach after fit and necessity have done their work. A system may be suitable and necessary in a limited sense yet still impose a rights cost that a constitutional order refuses to accept. That final judgement matters where a measure is population-wide, persistent, opaque, predictive, difficult to contest or capable of chilling ordinary conduct.

Post-war constitutionalism made proportionality more than administrative good sense. Fundamental rights did not merely block unlawful action; they shaped lawful action. A state could pursue public goods, but it had to pursue them through means that respected dignity, liberty, equality and legality. That development explains the contemporary force of proportionality. It does not say that rights never yield. It says that limitations are constitutional events. The authority that limits a right carries the burden of justification, and the quality of the justification must rise with the seriousness of the interference.

2.3 Strasbourg: legality, necessity, fair balance and procedural judgement

The European Convention on Human Rights supplied a parallel but not identical vocabulary. Articles 8 to 11 require that an interference be prescribed by law, pursue an enumerated legitimate aim, and be necessary in a democratic society; property cases also ask whether a fair balance has been struck. Strasbourg does not consistently articulate suitability, least restrictive means and strict proportionality as discrete stages. It works through pressing social need, relevant and sufficient reasons, fair balance, the severity of the sanction and the quality of domestic decision-making. That looser structure can hide conclusions, but it also reflects the Convention system's subsidiary role and its concern with whether national authorities have responsibly confronted the rights conflict.¹¹

The margin of appreciation is best understood as a doctrine of review intensity, not as a substantive answer. Strasbourg ordinarily allows greater latitude where democratic choice, moral pluralism, or complex social policy dominate, and less where secret surveillance, vulnerable groups, prior restraint, or the core of private life are at issue. Consensus, the importance of the right, the quality of domestic deliberation and the availability of safeguards can all affect the width of the margin. Variable intensity need not weaken proportionality, but unexplained deference does. A court should disclose why institutional reasons justify restraint and why the rights burden nevertheless remains subject to effective supervision.¹²¹³

Strasbourg also supplies a distinctive procedural proportionality. It asks whether domestic courts and authorities identified the competing interests, applied relevant criteria, provided sufficient reasons, and

Principle of Proportionality in EU Law: An Interest-based Taxonomy' in Joana Mendes (ed), *EU Executive Discretion and the Limits of Law* (OUP 2019) 198.

¹¹ Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended), arts 8-11; *Handyside v United Kingdom* (1976) 1 EHRR 737, para 48; *Sporrong and Lönnroth v Sweden* (1983) 5 EHRR 35, paras 69 and 73.

¹² *Sunday Times v United Kingdom (No 1)* (1979) 2 EHRR 245, paras 45-67; *Silver v United Kingdom* (1983) 5 EHRR 347, paras 85-90; Jonas Christoffersen, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights* (Martinus Nijhoff 2009) 31-71; Julian Rivers, 'Proportionality and Variable Intensity of Review' (2006) 65 *Cambridge Law Journal* 174.

¹³ Janneke Gerards, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466; Janneke Gerards and Eva Brems (eds), *Procedural Review in European Fundamental Rights Cases* (CUP 2017).

built safeguards against arbitrary power. Procedure is not a substitute for substance: a meticulously documented measure may still be excessive. Its value is epistemic and institutional. A reasoned process exposes the aim, evidence and distribution of burden before deference is granted. In *S and Marper*, the defect was therefore not biometric retention in the abstract but the failure of a blanket and indefinite regime to distinguish unconvicted persons from convicted persons, children from adults, minor matters from serious crime, and continuing need from administrative convenience.¹⁴¹⁵

The surveillance cases develop the same structural concern. *Roman Zakharov* treated the mere existence of a secret interception regime as capable of engaging Article 8 where the regime exposed persons to surveillance without effective safeguards. *Big Brother Watch* accepted that bulk interception need not be incompatible with the Convention in every form. Still, it required end-to-end safeguards, independent authorisation, meaningful selection rules, supervision and effective remedies. Strasbourg therefore differs from Luxembourg in tone and institutional posture, but not in the central demand. Secret or large-scale technological power needs a legal architecture that constrains discretion.¹⁶

2.4 Community law before the Charter

The European Communities did not begin with a codified catalogue of rights. The Court of Justice recognised fundamental rights as general principles of Community law by drawing on constitutional traditions common to the Member States and international human rights instruments. *Internationale Handelsgesellschaft* preserved the autonomy and supremacy of Community law while insisting that Community acts would be judged against the Community's fundamental rights. *Nold* reinforced the point. Proportionality fitted that environment because it could travel across legal systems. It offered a common technique for asking whether a measure within the Community legal order went too far.¹⁷

The early Community cases also show that proportionality did not belong exclusively to rights law. It operated in the review of EU legislation, administrative action and national restrictions on Treaty freedoms. Internal market adjudication forced courts to ask whether Member States could justify barriers to free movement. Union legislation compelled courts to ask whether institutions had overstepped the bounds of necessary action. That double life remains important. Article 5(4) TEU concerns the content and form of Union action; Article 52(1) of the Charter concerns limitations on Charter rights. They often interact, but they do not ask the same question.¹⁸

Fedesa supplies the classic EU formula: measures must be appropriate and necessary to attain legitimate objectives; where several appropriate measures are available, recourse must be had to the least onerous;

¹⁴ *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), paras 119-125.

¹⁵ Janneke Gerards, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466; Janneke Gerards and Eva Brems (eds), *Procedural Review in European Fundamental Rights Cases* (CUP 2017).

¹⁶ *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015), paras 229-305; *Big Brother Watch and Others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021), paras 334-425.

¹⁷ *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (Case 11/70) EU:C:1970:114, paras 3-4; *Nold KG v Commission* (Case 4/73) EU:C:1974:51, paras 13-14.

¹⁸ Treaty on European Union, art 5(4); Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality [2012] OJ C326/206; Charter, art 52(1).

and the disadvantages caused must not be disproportionate to the aims pursued. The Court nevertheless applied a manifestly inappropriate standard in a field involving broad legislative discretion. That standard is not an alternative definition of proportionality but a choice about intensity. EU doctrine is more intelligible when lawyers ask three prior questions: whose act is under review, which legally protected interest bears the burden, and what institutional reason supports deference? Scholarship has long shown that the review of Union legislation, Member State restrictions, and serious rights interferences does not proceed at a uniform level.^{19,20}

Schmidberger and *Omega* made the internal market visibly constitutional. In *Schmidberger*, Austria's tolerance of an environmental demonstration restricted the free movement of goods. The Court accepted that freedom of expression and assembly could justify the restriction where the national authorities had struck a proportionate balance. In *Omega*, a ban on a commercial laser game restricted the freedom to provide services, but human dignity supplied the public policy justification. These cases prevent a flat, market account of EU law. Economic freedoms matter. They operate inside a legal order that also protects fundamental rights. Proportionality provides the grammar for deciding whether one legally protected interest may limit another.²¹

2.5 The Charter, Article 8 and the Constitutionalisation of Limitation

The Charter gave rights proportionality a modern text. Article 52(1) requires any limitation on Charter rights to be provided for by law, respect the essence of the rights and freedoms, and, subject to proportionality, be necessary and genuinely meet an objective of general interest recognised by the Union or the need to protect the rights and freedoms of others. The sequence matters. Legality, essence and legitimate aim are not decorative gateways to a free-standing balance. An attractive objective cannot repair a vague rule; an impairment of essence cannot be outweighed by aggregate welfare; and an aim framed too broadly makes necessity untestable. Proportionality begins only after those conditions are satisfied.²²

Article 8 of the Charter deserves separate treatment. Data protection is not merely Article 7 privacy with a balancing clause attached. Article 8 gives the right its own constitutional architecture: fair processing, specified purposes, a legitimate basis laid down by law or consent, access, rectification and control by an independent authority. These requirements are not external concessions to data protection. They form part of the right. That structure matters because the best argument against data-protection absolutism does not

¹⁹ *Fedesa* (Case C-331/88) EU:C:1990:391 paras 13-14; *R v Secretary of State for Health, ex p British American Tobacco* (Case C-491/01) EU:C:2002:741, paras 122-126; *Vodafone Ltd v Secretary of State for Business, Enterprise and Regulatory Reform* (Case C-58/08) EU:C:2010:321, paras 51-71.

²⁰ Gráinne de Búrca, 'The Principle of Proportionality and its Application in EC Law' (1993) 13 *Yearbook of European Law* 105; Tor-Inge Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16 *European Law Journal* 158; Wolf Sauter, 'Proportionality in EU Law: A Balancing Act?' (2013) 15 *Cambridge Yearbook of European Legal Studies* 439; Vasiliki Kosta, 'The Principle of Proportionality in EU Law: An Interest-based Taxonomy' in Joana Mendes (ed), *EU Executive Discretion and the Limits of Law* (OUP 2019) 198.

²¹ *Eugen Schmidberger, Internationale Transporte und Planzüge v Republik Österreich* (Case C-112/00) EU:C:2003:333, paras 74-94; *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn* (Case C-36/02) EU:C:2004:614, paras 31-40.

²² Charter, art 52(1); Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 *German Law Journal* 779.

flatten Article 8 into a negotiable interest. It reads Article 8 as a structured right whose internal requirements already discipline proportionality.²³

The movement into data protection made that discipline unavoidable. *Österreichischer Rundfunk* rejected the notion that privacy problems arise only with intimate secrets. Processing and publishing income data for transparency purposes could interfere with private life and data protection interests. *Schecke* then required the legislature to distinguish among categories of subsidy recipients and to assess the necessity of disclosure rather than accept a blanket transparency rule. Those cases supply the bridge from privacy as secrecy to data protection as constitutional architecture. A datum that looks harmless in isolation may become rights-significant through aggregation, linkage, persistence, access and inference.²⁴

Article 52(1) also disciplines the language of the aim. A court cannot test proportionality against a slogan. Security, innovation, efficiency, platform integrity, child safety and administrative convenience do not carry the same constitutional weight. Nor do those words identify which persons, risks, data categories, or harms the measure addresses. The more general the aim, the easier it becomes to treat intrusive means as necessary. Proportionality therefore starts with description. The legal system must require the actor to name the risk with enough precision to make the fit, necessity and safeguards tests testable.

2.6 Recital 4 as Constitutional Instruction

Recital 4 GDPR is a constitutional instruction, but it is not an operative escape clause. It states that data protection is not absolute, must be considered in relation to its function in society and must be balanced with other fundamental rights in accordance with proportionality. That instruction guides the interpretation of the Regulation's operative provisions, especially where they expressly require a necessity or a balancing. It cannot derogate from clear text, create a lawful basis, validate defective consent or authorise processing that Articles 5, 6, 9 or 22 prohibit. EU law treats recitals as important interpretive material but denies them independent force to contradict an enactment's operative scheme.^{25,26}

Read within those limits, Recital 4 changes the tone of data protection analysis. It prevents Article 8 from being treated as a trump card in every dispute, while preventing controllers from treating the identification of a lawful basis as the end of analysis. The GDPR internalises proportionality through purpose limitation, data minimisation, necessity, balancing legitimate interests, privacy by design, DPIAs, calibrated security, and rights-sensitive remedies. A private controller does not become a miniature constitutional court with a power to limit Article 8. It must satisfy the statutory conditions through which the legislature has reconciled the rights at stake.

²³ Charter, art 8; Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 89-122; Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 201-236.

²⁴ *Rechnungshof v Österreichischer Rundfunk and Others* (Joined Cases C-465/00, C-138/01 and C-139/01) EU:C:2003:294, paras 73-90; *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* (Joined Cases C-92/09 and C-93/09) EU:C:2010:662, paras 48-86.

²⁵ Regulation (EU) 2016/679, recital 4; Charter, arts 7, 8, 16 and 52(1); *Productores de Música de España (Promusicae) v Telefónica de España SAU* (Case C-275/06) EU:C:2008:54, paras 62-70.

²⁶ *Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas* (Case C-136/04) EU:C:2005:716, para 32; *Grégor Puppincx and Others v European Commission* (Case C-418/18 P) EU:C:2019:1113, para 76.

This point matters equally for supervisory authorities. The digital supervisory state can reshape markets, advertising systems, platform design, expression and AI deployment through prohibitions, erasure orders, redesign requirements and fines. Regulatory independence protects authorities from external direction; it does not insulate their exercise of public power from legality, reason, judicial review, or the requirement that sanctions be effective, proportionate, and dissuasive. The stronger the intervention and the wider its collateral effects, the more clearly the authority should explain why the chosen remedy fits the identified infringement.

2.7 Digital Rights Ireland and Scale as a Constitutional Fact

Digital Rights Ireland made proportionality hard-edged. The Data Retention Directive pursued serious objectives: combating serious crime and protecting public security. The Court did not trivialise those objectives. It invalidated the Directive because the interference with Articles 7 and 8 of the Charter was vast and insufficiently circumscribed. The Directive covered almost the entire population, all means of electronic communication and traffic data capable of identifying the source, destination, date, time, duration and type of communication. It did so without differentiation, limitation or exception linked to the objective pursued.²⁷

The Court also treated safeguards as part of proportionality. It criticised the absence of clear and precise rules on access; objective criteria limiting access to serious crime; prior review by a court or an independent body; adequate differentiation in retention; security; and irreversible destruction at the end of the retention period. This reasoning matters for every data-intensive system. A measure may serve a legitimate aim and still fail because its architecture turns a targeted justification into general infrastructure. Scale, duration, access and review are not technical details. They decide constitutional legality.²⁸

The later retention cases have refined rather than abandoned that position. *Tele2 Sverige* and *Watson, Privacy International, G.D.*, and *SpaceNet* rejected the general and indiscriminate retention of traffic and location data for ordinary law-enforcement purposes. At the same time, *La Quadrature du Net* accepted exceptional measures for a genuine, present, or foreseeable serious threat to national security under strict temporal and substantive conditions. In *La Quadrature du Net II*, the Court then accepted general retention of IP addresses, and bounded access for copyright enforcement, where watertight separation from other data prevented the construction of detailed profiles and the system included safeguards against abuse. The development is not a simple retreat from strictness. It shows that technical separation, combination risk and access design can alter the legal intensity of an interference.^{29,30}

²⁷ *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238 paras 26-37 and 56-59.

²⁸ *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238 paras 60-69.

²⁹ *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970, paras 97-112; *La Quadrature du Net and Others v Premier ministre and Others* (Joined Cases C-511/18, C-512/18 and C-520/18) EU:C:2020:791, paras 134-192; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (Case C-623/17) EU:C:2020:790, paras 65-82.

³⁰ *G.D. v Commissioner of An Garda Síochána and Others* (Case C-140/20) EU:C:2022:258; *SpaceNet AG and Telekom Deutschland GmbH* (Joined Cases C-793/19 and C-794/19) EU:C:2022:702; *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (Case C-470/21) EU:C:2024:370; *Bezirkshauptmannschaft Landeck (Attempt to access personal data stored on a mobile telephone)* (Case C-548/21) EU:C:2024:830.

The historical lesson is not moderation in the abstract. Proportionality became a legal form of disciplined justification, but EU law deploys it for different protected interests and through different institutional arrangements. It can police the limits of Union competence, review a Member State restriction, protect a Charter right, interpret a statutory necessity condition or calibrate a remedy. Treating those uses as interchangeable produces doctrinal slippage; separating them reveals a common demand. Lawful power must remain connected to its purpose, and the quality of the justification must rise with the scope, persistence, opacity and practical irreversibility of the burden.

3. Judicial Method: The Grammar and Modes of Review

3.1 From claim to justification

A proportionality case starts before the proportionality test in the narrow sense. The court first identifies the protected right or interest. It then asks whether the measure interferes with that right or interest. In privacy and data protection cases, defendants often contest this step by characterising data as mundane, public, voluntarily supplied or technically processed without human attention. Both Luxembourg and Strasbourg resist that narrowness. Collection, retention, access, linkage, disclosure, indexing and automated analysis can each create an interference. The question is not whether the interference already feels dramatic. The question is whether the measure places legally relevant pressure on the protected interest.³¹

The court then asks whether the interference is attributable to a measure within the Charter's scope, has adequate legal authority and pursues a recognised objective. This ordering prevents proportionality from becoming a solvent. If the law is inaccessible, unforeseeable or insufficiently precise, the legality requirement fails. If the essence of a right is impaired, ordinary balancing never begins. If the aim is framed at an untestable level of abstraction, suitability and necessity become theatre. Good reasoning identifies the point of failure rather than allowing every defect to disappear into an undifferentiated final balance.³²

3.2 Legitimate aim and the problem of abstraction

Aim framing often decides the case because the level of abstraction determines the comparator. “Public security”, “service improvement”, “innovation” and “child safety” can make almost any measure appear useful. An operational aim identifies the persons, harm, context and success condition: detecting specified serious offences within a defined investigative setting; preventing account takeover within a particular service; or restricting access by a stated age group to a defined category of content. The aim must also be traced to the correct legal source. A public body cannot convert convenience into an objective of general interest, and a controller cannot redescribe a preferred business model as contractual necessity.

³¹ *Österreichischer Rundfunk* (Joined Cases C-465/00, C-138/01 and C-139/01) EU:C:2003:294; *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12) EU:C:2014:317, paras 80-81; *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) paras 66-86; *Benedik v Slovenia* App no 62357/14 (ECtHR, 24 April 2018), paras 101-116.

³² Charter, art 52(1); *Sunday Times v United Kingdom (No 1)* (1979) 2 EHRR 245 paras 47-49; *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) paras 228-234; *Opinion 1/15 EU-Canada PNR Agreement* EU:C:2017:592 paras 139-151.

Opinion 1/15 shows the discipline. The Court did not deny the legitimacy of combating terrorism and serious transnational crime. It examined categories of passenger data, purposes of processing, automated analysis, sensitive data, retention, access by Canadian authorities, independent oversight and redress. The aim survived; the architecture did not. The opinion matters because it treats security law as a form of legal design. A serious aim does not collapse proportionality. It raises the standard of explanation.³³

Strasbourg reaches the same point through the language of necessity in a democratic society. In *Bărbulescu*, the Grand Chamber did not deny that employers may protect productivity and discipline. It required domestic courts to examine the notice, the scope of monitoring, the degree of intrusion, legitimate reasons, less intrusive methods, and the consequences for the employee. The case is often taught as a workplace privacy case. It is better read as an aim-framing case: the employer's interest in workplace management could not justify unrestricted monitoring unless the domestic courts tested how the monitoring related to that interest.³⁴

3.3 *Fedesa* deference, Charter strictness and Review Intensity

The same formula does not always bite with the same force. In complex economic and social policy fields, the Court may grant the legislature broad discretion and ask whether a measure is manifestly inappropriate. Serious interference with privacy, data protection, the confidentiality of communications, or effective judicial protection requires strict necessity, precise rules, and strong safeguards. Intensity should depend on legally relevant reasons: the nature of the act, the protected interest, the severity and reversibility of the interference, epistemic uncertainty, democratic pedigree and the quality of prior assessment. It should not depend on an unspoken instinct that some institutions or technologies deserve trust.^{35,36}

The tension between *Fedesa* and *Digital Rights Ireland* therefore cannot be resolved by declaring one case deferential and the other rights-protective. The cases occupy different institutional and constitutional positions. A court reviewing a broad agricultural or market measure may hesitate before substituting its policy assessment for that of the legislature. A court reviewing population-wide communications infrastructure confronts a burden that is indiscriminate, difficult to detect and capable of reconstructing private life. Review intensity carries constitutional information: it tells the parties how much evidence, targeting, explanation and safeguard design the legal order requires, and it should be made express rather than smuggled into the application of a supposedly uniform test.

³³ *Opinion 1/15 EU-Canada PNR Agreement* EU:C:2017:592 paras 148-232.

³⁴ *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017), paras 120-122.

³⁵ *Fedesa* (Case C-331/88) EU:C:1990:391 para 14; *British American Tobacco* (Case C-491/01) EU:C:2002:741 para 123; *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238 paras 47-48; *Tele2 Sverige* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970 paras 96-112.

³⁶ Gráinne de Búrca, 'The Principle of Proportionality and its Application in EC Law' (1993) 13 *Yearbook of European Law* 105; Tor-Inge Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16 *European Law Journal* 158; Wolf Sauter, 'Proportionality in EU Law: A Balancing Act?' (2013) 15 *Cambridge Yearbook of European Legal Studies* 439; Vasiliki Kosta, 'The Principle of Proportionality in EU Law: An Interest-based Taxonomy' in Joana Mendes (ed), *EU Executive Discretion and the Limits of Law* (OUP 2019) 198.

La Quadrature du Net complicates the story productively. The seriousness of an aim can alter the architecture that the law permits, but it does not abolish justification. A genuine national-security threat may support time-limited general retention under conditions that ordinary crime prevention cannot satisfy. *La Quadrature du Net II* adds the converse point: a technically separated category of data may create a less serious interference and therefore support access for a less weighty aim. Both propositions require discipline. Courts must test whether the technical and organisational conditions that are supposedly meant to reduce intensity are real, durable and auditable, rather than treating a system label as proof.³⁷³⁸

3.4 Suitability: Rational Connection with Evidence

Suitability normally sets a low threshold: the measure must be capable of contributing to the objective. Low does not mean empty. In technology disputes, a product category, vendor assurance or accuracy headline cannot establish fit. A predictive-policing tool, biometric system, content classifier, fraud model, advertising signal, or credit score may be sophisticated and still fail in its deployment context because of false positives, false negatives, domain shift, weak labels, proxy effects, gaming, or a mismatch between the measured output and the legally recognised harm. Courts need not become engineers, but they must demand an intelligible causal account and evidence proportionate to the seriousness of the burden.³⁹

This evidential point protects rights and improves regulation. A system that floods human reviewers with false positives may not protect children, consumers or public funds. A remote identification system that fails disproportionately for particular groups may not provide reliable security. A content-moderation model that removes lawful speech in bulk may not serve public discourse. Suitability should ask whether the measure serves the aim the law actually recognises. Institutional hope cannot carry serious rights interference.

Evidence and deference must therefore remain distinct. Deference concerns the range of choice left to an institution after it has identified plausible options; it does not excuse the absence of reasons showing that an option is plausible. The actor should disclose the evidential base, material uncertainty, distribution of errors and conditions under which the claim may cease to hold. The more continuous, predictive or coercive the system, the less acceptable it is to rely on speculative benefit while externalising uncertainty onto affected persons. Judicial restraint without an evidential record is abdication, not proportionality.

3.5 Necessity: Usefulness is not Enough

Necessity is the most practical and often the most neglected stage. It requires a comparison between the chosen measure and a sufficiently effective, less rights-restrictive alternative. “Equally effective” cannot be defined so narrowly that every marginal gain renders the preferred design necessary, nor can the

³⁷ *La Quadrature du Net* (Joined Cases C-511/18, C-512/18 and C-520/18) EU:C:2020:791 paras 134-192.

³⁸ *G.D. v Commissioner of An Garda Síochána and Others* (Case C-140/20) EU:C:2022:258; *SpaceNet AG and Telekom Deutschland GmbH* (Joined Cases C-793/19 and C-794/19) EU:C:2022:702; *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (Case C-470/21) EU:C:2024:370; *Bezirkshauptmannschaft Landeck (Attempt to access personal data stored on a mobile telephone)* (Case C-548/21) EU:C:2024:830.

³⁹ *Afton Chemical Ltd v Secretary of State for Transport* (Case C-343/09) EU:C:2010:419, paras 45-46; Regulation (EU) 2024/1689, arts 9 and 15.

comparator be an imaginary zero-cost system. The actor must define the lawful objective and an acceptable level of achievement, disclose the trade-offs and explain why data reduction, shorter retention, local processing, targeting, sampling, role-based access, human triage or a non-automated route would materially frustrate that objective. Administrative convenience and cost may be relevant, but neither is self-justifying when the rights burden is serious.⁴⁰⁴¹

Digital Rights Ireland illustrates the point. Generalised retention of communications data may help law enforcement. Usefulness did not establish necessity. The Court demanded differentiation, limits and safeguards tied to the objective. The same logic applies outside security. A platform may find cross-service data combination profitable; that does not prove contractual necessity. A public authority may find bulk data matching convenient; that does not prove that every affected person should carry the rights burden. Necessity turns proportionality into system design because the comparison must happen at the level where the burden arises.⁴²

Mousse brings the same discipline into ordinary consumer interactions. SNCF Connect required customers to choose "Mr" or "Ms" when buying tickets online. The Court rejected the proposition that gendered titles were necessary for performing a rail transport contract. Neutral and inclusive forms of communication could achieve the service objective without collecting that data. *Mousse* is modest in facts and important in method. It shows that necessity not only constrains spectacular surveillance. It also constrains lazy data collection dressed up as custom, politeness or personalisation.⁴³

3.6 Proportionality *stricto sensu*, Safeguards and Remedial Fit

Proportionality in the strict sense asks whether the remaining burden is excessive after suitability and necessity have done their work. Critics rightly object that balancing can become impressionistic, hide moral choices behind numerical metaphors and weaken the special status of rights. Defenders answer that conflicts cannot be resolved by refusing to articulate why one legally protected claim limits another. The institutional response should not be an invented arithmetic. It should be a reasoned comparison of concrete burdens: scope, sensitivity, identifiability, inference, persistence, vulnerability, chilling effect, error correction, practical consequence and access to remedy, set against the importance and demonstrated degree of achievement of the aim.⁴⁴⁴⁵

⁴⁰ *Fedesa* (Case C-331/88) EU:C:1990:391 para 13; Regulation (EU) 2016/679, arts 5(1)(c) and 25; European Data Protection Supervisor, *Necessity Toolkit* (11 April 2017).

⁴¹ *Fedesa* (Case C-331/88) EU:C:1990:391, para 13; Gerards, 'How to Improve the Necessity Test' 466–490; European Data Protection Supervisor, *Necessity Toolkit* (11 April 2017).

⁴² *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238 paras 57–59; *Meta Platforms Inc and Others v Bundeskartellamt* (Case C-252/21) EU:C:2023:537, paras 98–125.

⁴³ *Mousse v Commission nationale de l'informatique et des libertés (CNIL) and SNCF Connect* (Case C-394/23) EU:C:2025:2, paras 48–61.

⁴⁴ Alexy, *A Theory of Constitutional Rights* 102–110; Barak, *Proportionality* 340–370; Stavros Tsakyrakis, 'Proportionality: An Assault on Human Rights?' (2009) 7 *International Journal of Constitutional Law* 468.

⁴⁵ Stavros Tsakyrakis, 'Proportionality: An Assault on Human Rights?' (2009) 7 *International Journal of Constitutional Law* 468; Kai Möller, 'Proportionality: Challenging the Critics' (2012) 10 *International Journal of Constitutional Law* 709; Francisco J Urbina, *A Critique of Proportionality and Balancing* (CUP 2017).

Safeguards belong inside this judgement because they can alter both the probability and gravity of harm. Prior authorisation, narrow access, purpose separation, deletion, audit trails, explanation, and contestability can make two systems that use the same data constitutionally different. Safeguards nevertheless have limits. They cannot supply missing legal authority, cure an indiscriminate measure whose breadth is the defect, or restore confidentiality after a system has eliminated it. The inquiry is therefore counterfactual and specific: which identified interference does each safeguard reduce, by what mechanism, and what burden remains if the safeguard fails?⁴⁶

Proportionality also has remedial bite. At Union level, excessive interference may invalidate an act; within the scope of EU law, national courts may interpret a measure narrowly, disapply conflicting provisions or require safeguards. In data protection disputes, the available responses may include deletion, dereferencing, restriction, narrowed access, redesigned governance, suspension, or cessation. The remedy should follow the defect. Overbroad scope calls for narrowing; missing safeguards may justify conditions or suspension; an unlawful basis may require cessation; impairment of essence admits no balancing cure. A remedy that reaches further than the infringement reproduces the very proportionality failure it is meant to correct.⁴⁷

Dun & Bradstreet Austria gives that point a modern algorithmic form. Article 15(1)(h) GDPR requires the affected person to receive meaningful information about the procedure and principles actually applied to use the data and obtain the result, expressed in a concise and intelligible form. A controller cannot satisfy the duty with a formula dump, nor can it invoke trade secrets as a complete shield. Where protected third-party data or trade secrets genuinely arise, the information must be made available to the competent authority or court so that it can reconcile the interests and determine what the data subject may receive. Explanation is therefore a designed remedy: enough understanding to verify and contest the decision, without assuming that publication of every protected input is always necessary.⁴⁸

3.7 Eight Modes of Proportionality Reasoning

The case law becomes clearer when proportionality is treated as a family of techniques rather than as a single test mechanically applied to different facts. The first mode is invalidating proportionality: *Digital Rights Ireland*, *Schrems I*, *Schrems II*, and Opinion 1/15 reject legal architectures whose scale, safeguards, or transfer conditions fail to meet Charter standards. The second is saving proportionality through conforming interpretation: *Ligue des droits humains* preserves the PNR Directive only by narrowing the purposes, data, automated assessment, retention and review that the text may permit. The distinction matters because interpretation cannot be allowed to rewrite legislation beyond its plausible limits. Yet,

⁴⁶ *Tele2 Sverige* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970 paras 109-125; *Ligue des droits humains* (Case C-817/19) EU:C:2022:491 paras 205-228; *Big Brother Watch and Others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) paras 334-425.

⁴⁷ *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238; *Google Spain* (Case C-131/12) EU:C:2014:317; *Schrems v Data Protection Commissioner* (Case C-362/14) EU:C:2015:650; *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/18) EU:C:2020:559.

⁴⁸ *CK v Magistrat der Stadt Wien and Dun & Bradstreet Austria* (Case C-203/22) EU:C:2025:117, paras 58-66 and 73-76.

invalidation should not be the automatic response where a rights-consistent construction is genuinely available.⁴⁹

The third mode is remedial proportionality. *Google Spain, GC and Others, Google v CNIL* and *Hurbain* ask which intervention targets the actual burden: de-referencing rather than deletion, territorial calibration rather than an assumed global rule, or anonymisation rather than suppression of an archive. The fourth is infrastructure proportionality. *Promusicae, Scarlet Extended, SABAM v Netlog* and *UPC Telekabel* examine whether enforcement design turns a specific claim into general monitoring, burdens intermediaries excessively or suppresses lawful information. In both modes, the court follows the interference to the layer—indexing, filtering, blocking or archiving—where technical design changes its intensity.⁵⁰

The fifth mode is statutory or lawful-basis proportionality. *Meta Platforms, Schrems v Meta, Mousse* and *KNLTB* apply necessity and balancing inside the GDPR's operative concepts rather than through a free-standing Article 52 review. The sixth is safeguards proportionality in the retention, access and PNR cases. The seventh is explanation proportionality in *SCHUFA* and *Dun & Bradstreet Austria*, where intelligibility and contestability affect legality. The eighth is supervisory proportionality: *Land Hessen* requires a supervisory authority to choose a response that is appropriate, necessary and proportionate to remedy the infringement and secure full enforcement. The taxonomy is not cosmetic. It identifies the source, addressee, intensity and remedial consequence of the justificatory exercise.^{51 52}

4. Competing Rights and Proportionate Accommodation

4.1 The Charter Map

The hard cases in EU technology law rarely present rights against nothing. They present privacy and data protection against security; expression against data protection; intellectual property against information freedom; business freedom against regulatory duties; child protection against confidentiality; equality against automation; or effective enforcement against intermediary autonomy. The first task is mapping. Articles 7 and 8 protect private life and data protection. Article 11 protects expression and information. Article 16 protects the freedom to conduct a business. Article 17 protects property. Article 21 protects non-

⁴⁹ *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238; *Schrems v Data Protection Commissioner* (Case C-362/14) EU:C:2015:650; *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* (Case C-311/18) EU:C:2020:559; *Opinion 1/15 EU-Canada PNR Agreement* EU:C:2017:592; *Ligue des droits humains* (Case C-817/19) EU:C:2022:491.

⁵⁰ *Google Spain* (Case C-131/12) EU:C:2014:317; *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* (Case C-136/17) EU:C:2019:773, paras 66-78; *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (Case C-507/17) EU:C:2019:772, paras 60-72; *Hurbain v Belgium App no 57292/16* (ECtHR, 4 July 2023), paras 201-242; *Promusicae* (Case C-275/06) EU:C:2008:54; *Scarlet Extended SA v SABAM* (Case C-70/10) EU:C:2011:771; *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (Case C-360/10) EU:C:2012:85; *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (Case C-314/12) EU:C:2014:192.

⁵¹ *Meta Platforms* (Case C-252/21) EU:C:2023:537; *Maximilian Schrems v Meta Platforms Ireland Ltd* (Case C-446/21) EU:C:2024:834; *Mousse* (Case C-394/23) EU:C:2025:2; *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens* (Case C-621/22) EU:C:2024:858; *SCHUFA Holding (Scoring)* (Case C-634/21) EU:C:2023:957; *Dun & Bradstreet Austria* (Case C-203/22) EU:C:2025:117.

⁵² *Land Hessen (Obligation to act by the data protection authority)* (Case C-768/21) EU:C:2024:785, paras 32–42; Regulation (EU) 2016/679, arts 58(2) and 83(1).

discrimination. Article 24 protects the rights of the child. Article 47 protects effective judicial protection. Article 52(1) structures limitation.⁵³

Mapping prevents common errors, but it does not flatten every interest into an equal-weighted right or turn private actors into constitutional adjudicators. Privacy lawyers may misdescribe countervailing rights as mere policy; industry lawyers may redescribe data protection as compliance friction; security lawyers may treat a weighty aim as an answer. The legal source still controls. A legislature limiting a Charter right must satisfy Article 52(1); a controller must satisfy the GDPR provision on which it relies; a platform must comply with the DSA's due diligence architecture; and a court may need to reconcile horizontally affected rights under those rules. Proportionality structures the accommodation but does not erase the statute that mediates it.

4.2 Business Freedom: Real, Qualified and Contextual

Article 16 deserves more serious treatment than privacy scholarship sometimes gives it. It protects economic activity, contractual freedom and aspects of competitive autonomy, but its wording recognises the freedom in accordance with Union law and national laws and practices. The Court also treats it in relation to its social function. Data restrictions, design duties, interoperability, audits and limits on contractual exploitation can therefore engage Article 16 without making every revenue model constitutionally protected. The intensity of the burden, the undertaking's ability to adapt, the regulatory context and the countervailing rights all matter.⁵⁴

Sky Österreich offers the better model. Rules allowed broadcasters to use short excerpts from high-interest public events even when another broadcaster held exclusive rights to them. The rules limited commercial exploitation and engaged Article 16. The Court accepted the limitation because it protected freedom to receive information and media pluralism, and because the measure remained confined. Extracts were short, conditions applied, and compensation was limited to additional costs directly incurred. The case shows how proportionality should work: acknowledge the business burden, identify the countervailing right, then test the precision of the accommodation.⁵⁵

Alemo-Herron is the more troubling case. The Court used Article 16 to resist an interpretation of the Acquired Rights Directive that would bind a transferee dynamically to collective agreements negotiated after transfer when the transferee could not participate. The criticism is not that business freedom was legally irrelevant, but that the judgment risked treating contractual autonomy as more important than the Directive's social purpose without adequately examining worker vulnerability, sectoral bargaining arrangements, or less disruptive accommodations. The methodological lesson is that recognition of Article

⁵³ Charter, arts 7, 8, 11, 16, 17, 21, 24, 47 and 52(1).

⁵⁴ Charter, art 16; *Sky Österreich GmbH v Österreichischer Rundfunk* (Case C-283/11) EU:C:2013:28, paras 42-50; *Alemo-Herron and Others v Parkwood Leisure Ltd* (Case C-426/11) EU:C:2013:521, paras 30-35.

⁵⁵ *Sky Österreich* (Case C-283/11) EU:C:2013:28 paras 51-67.

16 must be followed by contextual analysis, not by an assumption that regulatory cost itself establishes disproportionality.⁵⁶

Meta Platforms v Bundeskartellamt brings Article 16 into the platform economy. The Court did not deny that Meta's advertising model had economic value; it denied that a controller's chosen architecture could define contractual necessity. Article 6(1)(b) GDPR asks whether processing is objectively indispensable to the specific contractual service, not whether the controller has made the service profitable by processing. Article 16 remains relevant to the burden of regulation and the design of remedies. Still, it does not convert surveillance advertising, cross-service combination or any other incumbent model into a constitutional entitlement.⁵⁷

4.3 Expression, Privacy and De-referencing

Google Spain is often presented as a privacy victory. Its deeper significance lies in proportionality. The original newspaper notice remained lawful. The issue was whether search-engine indexing by name continued to make outdated information prominent in ways that burdened privacy and data protection. The Court required a balance between the data subject's rights and internet users' interests in access to information. Time, relevance, public role and the nature of the information mattered. De-referencing was not a deletion reflex. It was a remedy directed at search visibility as a distinct rights burden.⁵⁸

Later, de-referencing cases refine the method. *GC and Others* required particular care with sensitive data, criminal allegations and the continuing public interest in access. *Google v CNIL* rejected a general EU-law duty of global de-referencing while accepting that search engines must make de-referencing effective within the Union and that national authorities may order wider measures where justified. These cases show temporal and territorial proportionality. Information can lose relevance with time, but public interest may persist. Privacy may require de-referencing in one legal order, but the global balance between privacy and information cannot be assumed to be identical everywhere.⁵⁹

Strasbourg's Article 8 and Article 10 cases sharpen the same point. *Axel Springer* and *Von Hannover* require courts to examine the contribution to a debate of general interest, the person's public role, prior conduct, the method of obtaining information, the content and form, and the consequences and severity of the sanction. *Hurbain* then applied a tailored version of that analysis to online archives and anonymisation. The Grand Chamber did not endorse a general erasure of history. It accepted a narrow anonymisation order after examining the article's age, continuing public interest, impact on the person, availability of the archived article and the remedy's limited effect on the newspaper archive. That is proportionality in granular form.⁶⁰

⁵⁶ *Alemo-Herron* (Case C-426/11) EU:C:2013:521; Jeremias Prassl, 'Freedom of Contract as a General Principle of EU Law? Transfers of Undertakings and the Protection of Employer Rights in EU Labour Law' (2013) 42 Industrial Law Journal 434.

⁵⁷ *Meta Platforms* (Case C-252/21) EU:C:2023:537 paras 98-125; *Schrems v Meta* (Case C-446/21) EU:C:2024:834 paras 61-65.

⁵⁸ *Google Spain* (Case C-131/12) EU:C:2014:317 paras 80-99.

⁵⁹ *GC and Others* (Case C-136/17) EU:C:2019:773 paras 66-78; *Google v CNIL* (Case C-507/17) EU:C:2019:772 paras 60-72.

⁶⁰ *Axel Springer AG v Germany* App no 39954/08 (ECtHR, 7 February 2012), paras 89-95; *Von Hannover v Germany (No 2)* App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), paras 108-113; *Hurbain v Belgium* App no 57292/16 (ECtHR, 4 July 2023) paras 201-242.

The combined lesson matters for digital regulation. Search, ranking and archiving change the intensity of expression and privacy burdens. A lawful publication can become a new privacy burden through name-search visibility. A privacy remedy can become a new expression burden if it rewrites archives or suppresses public-interest information. Proportionality asks the court to intervene at the layer where the burden arises, not at an abstract level where one value is declared superior.

4.4 Intellectual property, Privacy and Platform Infrastructure

The copyright enforcement cases are foundational for digital proportionality because they focus on intermediary architecture. *Promusicae* required Member States to interpret directives in a manner that allowed a fair balance between fundamental rights, including intellectual property, effective judicial protection and data protection. The judgment did not turn copyright enforcement into a data-disclosure trump. It required national law to accommodate the rights at stake within the limits of EU law.⁶¹

Scarlet Extended then rejected an injunction requiring an internet access provider to install a general filtering system to prevent copyright infringement. The system would have been general, preventive, costly, indefinite and indiscriminate. It would have burdened the provider's business freedom, users' data protection and users' freedom to receive or impart information. *SABAM v Netlog* confirmed the point for hosting services. The Court did not devalue intellectual property. It rejected an enforcement architecture whose burden fell too broadly across users, communications, information freedom and intermediary operations. General monitoring duties become constitutionally suspect when they convert a specific enforcement aim into standing surveillance infrastructure.⁶²

UPC Telekabel adds nuance. The Court accepted that a blocking injunction against an intermediary could be compatible with EU law if it protected copyright, left the intermediary free to choose technical means and did not unnecessarily deprive users of lawful access to information. This is a proportionate implementation. Law may set an objective without dictating an excessive method. The intermediary's business freedom and users' information rights remain part of the design space. That lesson travels beyond copyright. Whenever law delegates implementation to a platform, proportionality must govern the translation of legal obligation into technical architecture.⁶³

Delfi shows the Strasbourg counterpart. The Grand Chamber accepted liability for an online news portal for manifestly unlawful reader comments. Still, it emphasised the portal's commercial and professional nature, the extreme nature of the comments, the measures available to prevent harm, the conduct of the injured persons and the modest sanction. One may criticise *Delfi* for chilling user-generated expression. Still, the Court's reasoning is recognisably proportionality reasoning: it turned liability on context, control, harm, safeguards and sanction, not on an abstract claim that platforms are always publishers or never publishers.⁶⁴

⁶¹ *Promusicae* (Case C-275/06) EU:C:2008:54 paras 62-70.

⁶² *Scarlet Extended* (Case C-70/10) EU:C:2011:771 paras 40-53; *SABAM v Netlog* (Case C-360/10) EU:C:2012:85 paras 38-52.

⁶³ *UPC Telekabel* (Case C-314/12) EU:C:2014:192 paras 52-64.

⁶⁴ *Delfi AS v Estonia* App no 64569/09 (ECtHR, 16 June 2015), paras 131-162.

4.5 Platform business models, adtech and automated decisions

Meta Platforms v Bundeskartellamt is a central modern case on data-driven business models because it separates regulatory perspective from legal standard. A competition authority may take GDPR compliance into account when assessing abuse of dominance. Still, it must cooperate sincerely with the competent data protection authorities and may not disregard an existing decision. On substance, the Court read contractual necessity strictly and treated platform power as relevant to whether consent is freely given. The judgment therefore shows that competition, data protection and business freedom may describe the same architecture from different legal directions without collapsing into one another.⁶⁵

C-446/21 Schrems v Meta Platforms deepens the point through data minimisation. The Court held that Article 5(1)(c) GDPR precludes an online social network from aggregating, analysing and processing all personal data obtained from the data subject or third parties, on and off the platform, for targeted advertising without restriction as to time and without distinction by type of data. The judgment is not anti-advertising. It is anti-indiscriminate accumulation. It treats time, data type and source as legally relevant features of proportionality under the GDPR principles.⁶⁶

The same judgment also shows why special-category data cannot be treated as contaminated and then freely exploited once some related fact has entered the public domain. Mr Schrems had referred publicly to his sexual orientation during a panel discussion. The Court accepted that a statement in a public event may, subject to verification, amount to making that information manifestly public for Article 9(2)(e). It then drew the crucial line: that fact does not authorise the platform to process other data relating to sexual orientation, including data obtained outside the platform, for personalised advertising. Public disclosure of one fact does not turn the person into open season for inferential profiling.⁶⁷

IAB Europe shows that consent infrastructure can itself become personal-data infrastructure. The Transparency and Consent Framework produces a TC String that records user preferences and passes signals through the advertising ecosystem. The Court held that the string may be personal data where it can be associated with an identifier, and that *IAB Europe* may be a joint controller for defined processing operations where it influences purposes and means. The lesson is broader than classification. In complex ecosystems, rights burdens arise at the level of governance architecture, not only at the point where an advert appears on a screen. Proportionality and accountability must therefore operate at the system level.⁶⁸

KNLTB stops the pendulum swinging into the opposite error. A commercial interest is not excluded in principle from Article 6(1)(f) GDPR. Still, the controller must identify an interest that is lawful, real, and present, demonstrate its necessity, and show that the data subject's interests and fundamental rights do not override it. Reasonable expectations, the source and sensitivity of the data, the relationship with the controller, the effects of processing and safeguards all belong in the assessment. The decision does not

⁶⁵ *Meta Platforms* (Case C-252/21) EU:C:2023:537 paras 47-63 and 98-125.

⁶⁶ *Schrems v Meta* (Case C-446/21) EU:C:2024:834 paras 61-65 and operative part 1.

⁶⁷ *Schrems v Meta* (Case C-446/21) EU:C:2024:834 paras 78-83 and operative part 2.

⁶⁸ *IAB Europe v Gegevensbeschermingsautoriteit* (Case C-604/22) EU:C:2024:214, paras 43-69 and 74-84.

constitutionalise commerce; it prevents the legal analysis from treating commerciality as a substitute for applying the statutory test.⁶⁹

The position had acquired a second regulatory layer by July 2026. In April 2025, the Commission found Meta's binary consent-or-pay model non-compliant with Article 5(2) of the DMA and imposed a €200 million fine; after dialogue, Meta undertook to present EU users with a less personalised but equivalent advertising option, which was introduced in January 2026. That DMA development does not determine whether consent is valid under Articles 4(11) and 7 GDPR, because gatekeeper contestability and data-protection law use different legal tests. It does show that meaningful choice can be designed as a spectrum rather than a binary, and that cross-regulatory proportionality requires institutional cooperation rather than doctrinal merger.⁷⁰

SCHUFA and *Dun & Bradstreet Austria* bring automated scoring into the same field. *SCHUFA* held that an automatically produced probability value falls within Article 22 where a third party gives it a determining role in deciding whether to establish, implement or terminate a contract. *Dun & Bradstreet Austria* then required intelligible information about the procedure and principles actually applied. Together, the cases reject the formal allocation of responsibility: an upstream score is not neutral merely because a downstream institution signs off on the decision, and nominal human involvement does not preclude automation when the score effectively determines the result.⁷¹

4.6 Security, Retention, Access and PNR

Security cases test proportionality at its most demanding because the objectives are weighty and the infrastructures are capable of generalised surveillance. *Digital Rights Ireland*, *Tele2 Sverige*, *Watson*, *G.D.*, and *SpaceNet* reject the proposition that serious crime alone makes general traffic and location data retention necessary. *La Quadrature du Net* recognises a narrower national-security exception. At the same time, *La Quadrature du Net II* shows that IP-address retention may be classified differently where watertight separation prevents detailed profiling. The line is difficult, but its organising idea is stable: the permissible aim, duration, targeting and safeguards depend on the actual informational power created by retention and access, not on the database's label.^{72,73}

⁶⁹ *KNLTB* (Case C-621/22) EU:C:2024:858 paras 37-58; Regulation (EU) 2016/679, recital 47.

⁷⁰ European Commission, 'Commission finds Apple and Meta in breach of the Digital Markets Act' (23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085> accessed 14 July 2026; European Commission, 'Meta commits to give EU users choice on personalised ads under Digital Markets Act' (8 December 2025) <https://digital-markets-act.ec.europa.eu/meta-commits-give-eu-users-choice-personalised-ads-under-digital-markets-act-2025-12-08_en> accessed 14 July 2026; European Commission, *Annual Report on the Digital Markets Act 2025*, COM(2026) 247 final (21 May 2026).

⁷¹ *SCHUFA* (Case C-634/21) EU:C:2023:957 paras 43-73; *Dun & Bradstreet Austria* (Case C-203/22) EU:C:2025:117 paras 58-66.

⁷² *Tele2 Sverige* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970 paras 97-112; *La Quadrature du Net* (Joined Cases C-511/18, C-512/18 and C-520/18) EU:C:2020:791 paras 134-192.

⁷³ *G.D. v Commissioner of An Garda Síochána and Others* (Case C-140/20) EU:C:2022:258; *SpaceNet AG and Telekom Deutschland GmbH* (Joined Cases C-793/19 and C-794/19) EU:C:2022:702; *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (Case C-470/21) EU:C:2024:370; *Bezirkshauptmannschaft Landeck (Attempt to access personal data stored on a mobile telephone)* (Case C-548/21) EU:C:2024:830.

The access cases make the analysis more granular. *Ministerio Fiscal*, *Prokuratuur*, *Privacy International*, and *Bezirkshauptmannschaft Landeck* distinguish between the seriousness of the objective and the seriousness of access. Data capable of yielding precise conclusions about private life ordinarily require a correspondingly weighty aim, prior review by a court or an independent body, and objective criteria. Access to a mobile telephone may be permitted for offences beyond the most serious category, but national law must define the factors governing proportionality and prior authorisation remains essential. Retention and access are related but distinct interferences; lawful storage does not make every subsequent query lawful.⁷⁴⁷⁵

Passenger Name Record litigation shows a different judicial technique. *Opinion 1/15* rejected the draft EU-Canada PNR agreement as incompatible with the Charter. *Ligue des droits humains* upheld the PNR Directive only through a strict Charter-compliant interpretation. The Court narrowed purposes, sensitive data use, automated assessment, human review, retention and oversight. Proportionality sometimes invalidates. Sometimes it saves a regime by remaking the legal architecture. In both settings, the question is the same: has security law confined itself to the risk that justifies it?⁷⁶

The ECtHR surveillance cases strengthen this analysis by focusing on institutional safeguards. In *Zakharov*, the danger lay not only in interception but in direct technical access and weak legal controls. In *Big Brother Watch*, the Grand Chamber required safeguards across the whole life cycle: authorisation, selection, examination, retention, sharing, oversight and remedy. That end-to-end perspective matters for EU technology law. A system can be disproportionate because it collects too much, but also because it allows too many actors to search, combine, retain, share or reuse what it collects.⁷⁷

4.7 Biometrics, AI and Encrypted Communications

Biometrics and AI move proportionality from stored information to automated identification, classification and inference. The AI Act prohibits specified practices and regulates high-risk systems, but classification does not exhaust Charter or Convention review. *Glukhin v Russia* is instructive: the use of facial recognition to identify and arrest a peaceful protester for a minor offence was highly intrusive, unsupported by adequate rules and safeguards, and capable of chilling expression. The proportionality question therefore follows the system into context: why this use, against whom, with what error and combination risks, for how long, with what human authority and with what route to challenge?⁷⁸⁷⁹

⁷⁴ *Ministerio Fiscal* (Case C-207/16) EU:C:2018:788, paras 55-62; *HK v Prokuratuur* (Case C-746/18) EU:C:2021:152, paras 35-59; *Privacy International* (Case C-623/17) EU:C:2020:790 paras 65-82.

⁷⁵ *G.D. v Commissioner of An Garda Síochána and Others* (Case C-140/20) EU:C:2022:258; *SpaceNet AG and Telekom Deutschland GmbH* (Joined Cases C-793/19 and C-794/19) EU:C:2022:702; *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (Case C-470/21) EU:C:2024:370; *Bezirkshauptmannschaft Landeck (Attempt to access personal data stored on a mobile telephone)* (Case C-548/21) EU:C:2024:830.

⁷⁶ *Opinion 1/15 EU-Canada PNR Agreement* EU:C:2017:592; *Ligue des droits humains* (Case C-817/19) EU:C:2022:491 paras 117-228.

⁷⁷ *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) paras 229-305; *Big Brother Watch and Others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) paras 334-425.

⁷⁸ Regulation (EU) 2024/1689, arts 5-6, 9-15 and Annex III; Charter, arts 7, 8, 21 and 52(1).

⁷⁹ *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023), paras 72-91; Regulation (EU) 2024/1689, arts 5, 26 and Annex III.

Timing now matters to that analysis. The AI Act's prohibitions and AI-literacy duty apply from February 2025, and its governance and general-purpose AI obligations apply from August 2025; many other provisions apply from 2 August 2026. A political agreement reached on 7 May 2026 would, if formally enacted, defer the main high-risk rules for Annex III systems to 2 December 2027 and product-related systems to 2 August 2028. The deferral does not suspend the Charter, GDPR, equality law or sectoral duties. It reinforces the article's central distinction: regulatory classification and conformity timetables do not exhaust the present legality of deployment.⁸⁰

Encrypted messaging and client-side scanning present a different conflict. Child protection and the prevention of sexual abuse are objectives of the highest importance, while Articles 7, 8, 11 and 24 protect secure communications, privacy, expression and children themselves. As of 14 July 2026, the permanent EU child sexual abuse proposal remained under negotiation, while the debate over the temporary ePrivacy derogation continued to distinguish between voluntary and mandatory measures and to contest the treatment of end-to-end encrypted communications. Proportionality requires further distinctions that political slogans often suppress: known-hash matching, novel-content detection, and grooming analysis do not impose the same error, confidentiality, or monitoring burden; targeted detection and population-wide scanning are not equivalent; and a safeguard cannot be assessed without the technical layer at which scanning occurs.^{81 82}

Effective judicial protection completes the map. Article 47 matters because a burden that cannot be discovered, understood or challenged is more severe and more likely to persist. In retention and PNR cases, prior review and independent oversight constrain access. In automated decisions, intelligible reasons and a person with authority to alter the outcome determine whether contestability is real. In platform cases, complaint routes, statements of reasons and restoration mechanisms affect expression. Procedure is not a universal cure, but the absence of a remedy is itself part of the proportionality analysis and may, at the limit, engage the essence of Article 47.⁸³

The competing-rights cases produce a stable lesson. The court should not ask which value wins in the abstract. It should name every right and freedom, specify each interference, test the aim, compare alternatives, examine safeguards and judge residual burden. That discipline protects privacy from dilution and protects other rights from erasure. It also improves regulation. A measure that survives serious

⁸⁰ Regulation (EU) 2024/1689, arts 26, 27, 86 and 113; European Commission, 'AI Act' <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 14 July 2026 (reporting the political agreement of 7 May 2026 on revised dates for high-risk systems).

⁸¹ Charter, arts 7, 8, 11, 16, 24 and 52(1).

⁸² European Commission, Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final; Council of the European Union, 'Child sexual abuse: Council reaches position on law protecting children from online abuse' (26 November 2025) <<https://www.consilium.europa.eu/en/press/press-releases/2025/11/26/child-sexual-abuse-council-reaches-position-on-law-protecting-children-from-online-abuse/>> accessed 14 July 2026; European Parliament, 'Combating child sexual abuse: support for a more limited ePrivacy derogation' (9 July 2026) <<https://www.europarl.europa.eu/news/en/press-room/20260706IPR46318/combating-child-sexual-abuse-support-for-a-more-limited-eprivacy-derogation>> accessed 14 July 2026; EDPB–EDPS, *Joint Opinion 04/2022* (28 July 2022).

⁸³ Charter, art 47; *Ligue des droits humains* (Case C-817/19) EU:C:2022:491 paras 205–228; *HK v Prokuratuur* (Case C-746/18) EU:C:2021:152 paras 50–59.

proportionality analysis tends to be narrower, more accountable and more intelligible than a measure justified by slogans.

5. A Framework for Technology and Privacy

5.1 Legal Status: A Proportionality Protocol, not a New Test

The framework proposed here is a doctrinally grounded proportionality protocol, not a free-standing legal test. It translates Article 52(1) of the Charter, the operative necessity and balancing provisions of the GDPR, data protection by design and DPIAs, the AI Act's risk-management and deployer obligations, and the remedial case law into a record that courts can test. Recital 4 supplies interpretive orientation but no independent lawful basis. Article 27 of the AI Act requires an FRIA only from specified categories of deployer and for specified high-risk systems; it should not be described as a universal private-sector duty. These limits make the protocol more legally credible by preserving the distinction between constitutional review and statutory compliance.⁸⁴⁸⁵⁸⁶

The protocol's legal consequences vary by actor and setting. A legislature that fails to examine less restrictive means may face invalidity or a rights-consistent interpretation where the text permits one. A supervisory authority that selects an excessive remedy may expose its decision to annulment. A controller that cannot explain alternatives or safeguards may fail to meet accountability, minimisation, legitimate interests, or DPIA duties. A deployer within Article 27 may produce an inadequate FRIA; a deployer outside it may still face GDPR, equality, sectoral and Charter-mediated obligations. The protocol does not manufacture a cause of action. It organises the reasons and evidence through which existing causes of action are decided.

The framework rests on four distinctions. First, Article 5(4) TEU competence proportionality is not the same as Article 52(1) rights proportionality. Secondly, public-law review is not identical to the necessity and balancing conditions that bind private processing. Thirdly, controller-side justification differs from the proportionality that governs a supervisory authority's remedy. Fourthly, AI Act classification, conformity assessment, and FRIA obligations do not themselves answer whether a deployment is lawful under the Charter, the GDPR, equality law, or sectoral rules. The same grammar connects these fields, but the legal source controls the burden, intensity and remedy.

Modern compliance practice often stops too early. A GDPR file may contain a lawful-basis memorandum, notice, retention schedule and DPIA; an AI file may contain a risk category, technical documentation, conformity language and a human-oversight label. Those artefacts can evidence compliance but are not self-validating. A controller may name a lawful basis while processing beyond the stated purpose; a deployer may complete a form while using a system whose errors and power asymmetries make the

⁸⁴ Regulation (EU) 2016/679, recital 4 and arts 5, 6, 25 and 35; Regulation (EU) 2024/1689, art 27; Charter, art 52(1).

⁸⁵ *Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas* (Case C-136/04) EU:C:2005:716, para 32; *Grégor Puppink and Others v European Commission* (Case C-418/18 P) EU:C:2019:1113, para 76.

⁸⁶ Regulation (EU) 2024/1689, arts 26, 27, 86 and 113; European Commission, 'AI Act' <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 14 July 2026 (reporting the political agreement of 7 May 2026 on revised dates for high-risk systems).

deployment excessive. The protocol therefore tests the substance behind the artefact and requires the record to remain open to revision.

5.2 The Schrems Error: Fundamental Rights without Proportionality

Max Schrems has done more than most private litigants to force EU data protection law to confront power. Safe Harbour, Privacy Shield, international transfers and Meta's advertising architecture became contestable because he refused to accept comfortable compliance fictions. That achievement should be acknowledged before criticising the rhetoric. The recurring claims that fundamental rights cannot be “for sale”, that charging for a privacy-respecting option approaches abolition of the right, or that consent-or-pay necessarily produces “fake consent” identify genuine risks of dependence and economic coercion. They do not, without further analysis, supply the legal test.⁸⁷

The first error is doctrinal only if fundamentality is treated as the conclusion rather than the premise. A fundamental right may be subject to structured limitation, but Recital 4 does not authorise a controller to balance away the conditions for valid consent. Article 7 and recitals 42 and 43 govern whether consent is freely given; Article 6(1)(f) separately requires a legitimate interest, necessity and an overriding-interests assessment; Article 5 continues to require fairness and minimisation. *KNLTB* confirms that a commercial interest may, in principle, count, not that it will prevail. The correct response to absolutism is therefore statutory discipline, not a free-floating appeal to balance.^{88 89}

The second error is rhetorical. “Fundamental rights cannot be for sale” can express two different claims: an anti-waiver claim that no economic condition may ever accompany a choice, or an empirical claim that a particular fee and market structure destroy genuine freedom. The first is too broad; the second is legally testable. The relevant evidence includes the size and presentation of the fee, platform dependence, equivalence of the alternatives, detriment for refusal, granularity, withdrawal costs, market power, reasonable expectations and the availability of a genuinely less intrusive service. Money is not irrelevant, but its appearance does not decide voluntariness without context.

The third error is evidential. Very high acceptance rates in consent-or-pay environments are powerful evidence of design pressure, but they do not identify its source or legal consequence without further inquiry. The EDPB's Opinion 08/2024 is more careful: for large online platforms, a binary choice between behavioural advertising and a fee will in most cases fail to produce valid consent, while an equivalent free alternative without behavioural advertising is particularly important. The Opinion is context-specific, and the broader EDPB guidelines remained on the 2026–2027 work programme as of the date of writing.

⁸⁷ noyb, 'Meta (Facebook / Instagram) to move to a "Pay for your Rights" approach' (3 October 2023) <https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach> accessed 14 July 2026; noyb, 'Pay or Okay - the beginning of the end?' (11 April 2023) <https://noyb.eu/en/pay-or-okay-beginning-end> accessed 14 July 2026; noyb, 'Pay or OK at DER SPIEGEL: noyb sues Hamburg DPA' (1 August 2024) <https://noyb.eu/en/pay-or-ok-der-spiegel-noyb-sues-hamburg-dpa> accessed 14 July 2026.

⁸⁸ Regulation (EU) 2016/679, recital 4 and art 6(1)(f); Charter, art 52(1); *KNLTB* (Case C-621/22) EU:C:2024:858 paras 37–58.

⁸⁹ *Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas* (Case C-136/04) EU:C:2005:716, para 32; *Grégor Puppink and Others v European Commission* (Case C-418/18 P) EU:C:2019:1113, para 76.

Meanwhile, DMA enforcement has required a less-personalised but equivalent choice for gatekeepers. The regimes converge on meaningful choice but do so under different legal tests.⁹⁰⁹¹⁹²

The fourth error is institutional. Anti-proportionality rhetoric can invite authorities to announce the morally attractive outcome without exposing the legal path. That is dangerous even when the outcome protects privacy. An authority challenging a consent architecture should identify the operative requirement, the power imbalance and design pressure that undermine free choice, the alternatives that would preserve the service with less intrusion, and the remedy that matches the infringement. An authority permitting the model should meet the same burden. Public reasons protect data subjects because they make under-enforcement visible; they also protect legality against enforcement by slogan.

The strongest reading of the Court's *Meta* and *Schrems* line is therefore neither *Meta*'s nor *Schrems*'s caricature. *Meta Platforms* rejects an attempt to make the incumbent business model the defining criterion for contractual necessity. *Schrems v Meta* applies data minimisation across time, source, and data type, and refuses to treat a single public statement as permission for broader inferential profiling. *Mousse* rejects customary data collection when a neutral alternative serves the contract. *KNLTB* recognises commercial interests only inside a demanding statutory assessment. The later DMA response adds a less-personalised equivalent option without deciding every GDPR consent question. The coherent principle is constrained choice architecture, not privacy absolutism or commercial entitlement.⁹³⁹⁴

5.3 Supervisory Proportionality: Reasons as Discipline

The framework must bind both regulators and regulated actors, and *Land Hessen* now provides direct doctrinal support. The Court held that a supervisory authority that establishes an infringement must respond appropriately to remedy it and ensure full enforcement, but need not exercise corrective power in every case. The chosen response must be appropriate, necessary and proportionate in light of all the circumstances; exceptionally, no corrective power may be required where the controller has ended the

⁹⁰ European Data Protection Board, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms* (17 April 2024), paras 176-181.

⁹¹ European Commission, 'Commission finds Apple and Meta in breach of the Digital Markets Act' (23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085> accessed 14 July 2026; European Commission, 'Meta commits to give EU users choice on personalised ads under Digital Markets Act' (8 December 2025) <https://digital-markets-act.ec.europa.eu/meta-commits-give-eu-users-choice-personalised-ads-under-digital-markets-act-2025-12-08_en> accessed 14 July 2026; European Commission, *Annual Report on the Digital Markets Act 2025*, COM(2026) 247 final (21 May 2026).

⁹² European Data Protection Board, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms* (17 April 2024); European Data Protection Board, *Work Programme 2026–2027* (11 February 2026) 2–3.

⁹³ *Meta Platforms* (Case C-252/21) EU:C:2023:537 paras 98-125; *Schrems v Meta* (Case C-446/21) EU:C:2024:834 paras 61-65 and 78-83; *Mousse* (Case C-394/23) EU:C:2025:2 paras 48-61; *KNLTB* (Case C-621/22) EU:C:2024:858 paras 37-58.

⁹⁴ European Commission, 'Commission finds Apple and Meta in breach of the Digital Markets Act' (23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085> accessed 14 July 2026; European Commission, 'Meta commits to give EU users choice on personalised ads under Digital Markets Act' (8 December 2025) <https://digital-markets-act.ec.europa.eu/meta-commits-give-eu-users-choice-personalised-ads-under-digital-markets-act-2025-12-08_en> accessed 14 July 2026; European Commission, *Annual Report on the Digital Markets Act 2025*, COM(2026) 247 final (21 May 2026).

breach and prevented recurrence. A complainant therefore has no subjective right to demand an administrative fine merely because an infringement occurred.⁹⁵⁹⁶

The institutional foundation is stronger than Recital 4 alone can provide. Articles 58 and 83 of the GDPR establish corrective powers and require that fines be effective, proportionate and dissuasive; the duty to give reasons and Article 47 support effective judicial control. A prohibition, erasure order, suspension, redesign requirement or fine should identify the infringement, the persons and rights affected, the remedial objective, the alternatives considered and the collateral burdens of the selected response. Proportionality does not weaken enforcement. It distinguishes effective correction from symbolic severity.

The same point applies to courts reviewing supervisory decisions. Respect for expertise is compatible with asking whether the authority framed the problem correctly, considered material evidence and alternatives, addressed genuinely engaged rights such as expression or business freedom, and selected a remedy that follows the defect. Review should not substitute a court's preferred policy for the regulator's within a lawful range; neither should it treat the regulator's conclusion as a black box. Proportionality marks the boundary between expert choice and unreasoned power.

5.4 Step One: Start with Interference Intensity

The first step reverses the usual organisational sequence. It starts with the pressure placed on persons rather than the organisation's preferred purpose. Scope asks how many people are affected, how frequently and across which contexts. Depth asks whether the system links sources, generates sensitive inferences, identifies persons or persists over time. Power asks whether affected persons can avoid the system and whether they are workers, children, patients, welfare recipients, migrants, suspects, students or dependent users. Consequence asks whether the system changes access, price, employment, movement, speech, suspicion or stigma.⁹⁷

This intensity assessment calibrates the required justification, but it should not be mistaken for an invented formal burden of proof. Low-intensity processing may be supported by ordinary reasons and controls; deep, persistent or population-scale interference demands precise aims, stronger evidence, serious comparison and independent oversight. Indiscriminate design is a warning sign because it disconnects burden from risk. Where the case law speaks of strict necessity, the record must show why targeting is infeasible and why exceptional scope is bounded by time, access and review.

Intensity also clarifies the comparator. A one-off list-cleaning exercise, contextual advert, fraud model, biometric gate and communications-retention regime do not warrant the same analysis. The more a system crosses contexts, infers protected traits, affects dependent users or controls essential services, the less acceptable it is to define success solely from the actor's perspective. The protocol therefore treats severity

⁹⁵ Regulation (EU) 2016/679, arts 57-58 and recital 4; Charter, arts 41, 47 and 52(1).

⁹⁶ *Land Hessen (Obligation to act by the data protection authority)* (Case C-768/21) EU:C:2024:785, paras 32-42; Regulation (EU) 2016/679, arts 58(2) and 83(1).

⁹⁷ *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238 paras 56-69; *Schrems v Meta* (Case C-446/21) EU:C:2024:834 paras 61-65; *SCHUFA* (Case C-634/21) EU:C:2023:957 paras 43-73.

and uncertainty as reasons for more justificatory labour, not as numerical weights that automatically decide the outcome.

5.5 Step Two: Specify the Aim Operationally

The second step specifies the aim at an operational and legally anchored level. “Improving safety” becomes preventing defined harms in a defined context; “fraud prevention” becomes identifying specified conduct at an articulated threshold; “child protection” becomes reducing a stated exposure or contact risk for a defined age group; “personalisation” becomes a particular recommendation, frequency-capping or advertising function. The actor must identify the provision or legally recognised interest that makes the aim legitimate and separate it from convenience, revenue preference and foreseeable function creep.⁹⁸

This separation matters where maximal data has become institutional habit. A platform may prefer cross-context profiling because it increases advertising yield; a public authority may prefer broad matching because it might reveal anomalies; a school may prefer remote proctoring because it lowers invigilation cost. Those considerations may enter the analysis, but they do not define necessity. An operational aim establishes the baseline against which causal fit and alternative designs can be compared, and it prevents an actor from laundering ambition through general words.

The aim should also state success and failure conditions. A fraud system should specify the conduct, desired reduction, acceptable error and burden on lawful users. An age-assurance method should identify the threshold, content or function, service risk and acceptable exclusion rate. A safety classifier should say whose safety, from what threat and through what mechanism. Without a success condition, evidence cannot falsify the claim and the actor can declare every output useful after the event.

5.6 Step Three: Test Suitability with Evidence, not Optimism

The third step asks whether the system plausibly advances the specified aim in the intended deployment context. The record should describe the causal mechanism, validation population, false positives and false negatives, calibration, subgroup performance, distribution shift, model drift and adversarial behaviour where relevant. Vendor claims and laboratory accuracy alone are not sufficient to detect serious interference. The AI Act’s documentation, risk management, and accuracy requirements can serve as evidence. Still, their staged application—and the 2026 political agreement to defer important high-risk obligations—makes it especially important not to confuse future conformity machinery with a present factual demonstration of suitability.^{99,100}

Suitability can fail in prosaic ways. Facial recognition may degrade under deployment lighting, camera, and crowd conditions. A welfare-fraud model may identify proxies for poverty rather than fraud. A

⁹⁸ Charter, art 52(1); *Opinion 1/15 EU-Canada PNR Agreement* EU:C:2017:592 paras 148-232; European Data Protection Supervisor, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (25 February 2019).

⁹⁹ Regulation (EU) 2024/1689, arts 9-15; *Afton Chemical* (Case C-343/09) EU:C:2010:419 paras 45-46.

¹⁰⁰ Regulation (EU) 2024/1689, arts 26, 27, 86 and 113; European Commission, ‘AI Act’ <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 14 July 2026 (reporting the political agreement of 7 May 2026 on revised dates for high-risk systems).

workplace system may measure keyboard activity rather than productive work. An age-estimation tool may exclude lawful users without materially reducing harmful exposure. These are not merely technical defects. They break the legal connection between burden and aim, and uncertainty about them must remain visible in the proportionality record.

Evidence should also address distribution and feedback. A model that reduces aggregate error by shifting false positives onto a protected group does not impose the same burden as a model whose errors are dispersed and easily corrected. A measure that “works” by chilling lawful speech may show apparent compliance while creating the very rights cost the legal order should count. Evidence should therefore include who receives the benefit, who bears the error, how quickly mistakes are corrected, and whether the operation changes the population or behaviour against which later performance is measured.

5.7 Step Four: Necessity as Design Comparison

The fourth step treats necessity as a documented design comparison. The actor should identify the baseline and a realistic set of less-restrictive alternatives, including data reduction, shorter retention periods, local or on-device processing, aggregation, pseudonymisation, functional separation, sampling, targeting, role-based access, threshold triggers, human triage, opt-outs, alternative channels, and non-automated routes. It should then compare effectiveness, rights burden, cost, latency and residual risk against the operational aim. Rejected options require reasons; a blank DPIA field or an assertion that the preferred product is “industry standard” does not establish necessity.¹⁰¹¹⁰²

This step gives concrete meaning to data minimisation and data protection by design. Article 5(1)(c) asks whether the data are adequate, relevant and limited to what is necessary for the purpose; Article 25 requires those principles to be implemented through design and defaults. A DPIA that inventories risks without comparing the design choices that create them records anxiety rather than justification. The comparison should occur before procurement and deployment, when the architecture can still change, and should be updated when a vendor, dataset, or use case changes.

Necessity also disciplines product rhetoric. Cross-context tracking is not necessary merely because it improves yield; remote proctoring is not necessary merely because it is cheaper; biometric entry is not necessary merely because it is convenient or fashionable. At the same time, a less intrusive alternative is not dispositive if it materially fails the lawful objective. The record must expose that trade-off so that a court or authority can decide whether the asserted loss of effectiveness is real, whether it is legally important and whether any marginal gain can justify the additional burden.

5.8 Step Five: Make Safeguards Constitutive

The fifth step builds safeguards corresponding to the interference mapped in step one. Thresholds, access controls, authorisation, human review, logs, explanation, contestability, deletion, purpose separation, independent oversight, staff limits, and public reporting perform different functions. If the risk is over-

¹⁰¹ Regulation (EU) 2016/679, arts 5(1)(c) and 25; European Data Protection Supervisor, *Necessity Toolkit* (11 April 2017).

¹⁰² *Fedesa* (Case C-331/88) EU:C:1990:391, para 13; Gerards, ‘How to Improve the Necessity Test’ 466–490; European Data Protection Supervisor, *Necessity Toolkit* (11 April 2017).

collection, training staff does not cure it; if the risk is error, encryption does not cure it; if the risk is function creep, a privacy notice does not cure it. Each control should identify the failure mode it addresses, its owner, evidence of operation and the consequence if it fails.¹⁰³

Safeguards change the residual burden only when they operate in practice. A data-access regime with prior independent review, strict purpose limits, short retention periods, and auditable queries differs from one with open access and weak logging. A biometric gate with local templates, no central history and a genuinely equivalent non-biometric route is different from a centralised system that records every movement. Yet safeguards are not coupons that can be accumulated to legitimate any architecture. Some measures remain excessive because their scale, chilling effect or destruction of confidentiality is the defect.

Algorithmic safeguards deserve particular care. “Human oversight” does not reduce a burden where the reviewer rubber-stamps an output, lacks time or authority to depart from it, cannot see the material inputs, or faces institutional penalties for disagreement. *SCHUFA* directs attention to the practical role of a score; *Dun & Bradstreet Austria* directs attention to the information needed to understand and contest it. Oversight should therefore be assessed through decision rights, competence, workload, access to evidence, override rates and consequences, not through the presence of a human name in a process diagram.¹⁰⁴

5.9 Step Six: Residual Burden, Temporal Proportionality and Limits

The sixth step asks whether the remaining burden is excessive after the actor has specified the aim, demonstrated fit, compared alternatives and designed safeguards. The judgement should be cumulative. An ordinary data point can become intrusive through continuous collection and linkage; an advisory score can control access in a dependent relationship; a rare sanction can chill speech if surveillance is invisible and pervasive. The residual assessment should explain the distribution of benefit and burden, the seriousness of uncertainty and whether consequences can be reversed before they become practically final.

Residual burden review should give special weight to vulnerability, chilling effect, and irreversible consequences, without assuming that vulnerability always dictates a single outcome. Children may lack comprehension and exit; workers may lack meaningful choice; welfare recipients may lose essential support before appeal; migrants and suspects may face coercive consequences; speakers may self-censor even where formal sanctions are rare. Those factors raise the required quality of reasons and safeguards. They also make delay, procedural opacity and error-correction time part of the substantive rights burden.

Proportionality also changes over time. A measure introduced for a specific risk may become excessive as the risk recedes; a database may attract secondary uses; a model may drift as populations and incentives change; a safeguard may become ineffective as deployment scales. The record should therefore specify retention limits, review intervals, performance and rights triggers, sunset clauses, rollback capacity and withdrawal criteria. GDPR storage limitation and AI Act monitoring duties support this temporal

¹⁰³ *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238 paras 60-69; *Tele2 Sverige* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970 paras 109-125; Regulation (EU) 2016/679, arts 12-22, 32 and 35.

¹⁰⁴ *SCHUFA* (Case C-634/21) EU:C:2023:957 paras 43-73; *Dun & Bradstreet Austria* (Case C-203/22) EU:C:2025:117 paras 58-66; Regulation (EU) 2024/1689, arts 14 and 27.

discipline. Still, the legal question remains broader: not only whether the system was proportionate at launch, but whether it continues to be proportionate in operation.¹⁰⁵

The framework must also know when to stop. Proportionality does not override the absence of a lawful basis, impairment of essence, invalid consent, unfairness, non-discrimination duties, statutory prohibitions or hard limits on AI practices. A manipulative interface that destroys free choice does not become lawful merely because the controller can describe a commercial benefit; a rights ledger cannot revive a prohibited AI practice; a measure that leaves no meaningful confidentiality or judicial protection may cross the line from limitation into destruction. The stop conditions should be stated at the beginning and checked again at the end.¹⁰⁶

5.10 The Proportionality Stack and Rights Ledger

The framework can be operationalised through a proportionality stack. At the norm layer, the actor identifies competence, legal basis, the precise aim, applicable Charter limits and any essence or prohibition threshold. At the system layer, it maps data flows, feature selection, retention, access, automation, human authority and safeguards. At the outcome layer, it assesses the effects on persons and groups, including the denial of opportunities, chilled behaviour, discrimination, error correction, remedies, and feedback loops. Passing one layer cannot compensate for failing another: a lawful purpose does not validate an excessive architecture, and a well-engineered system cannot supply missing legal authority.

The practical artefact is a rights ledger. For each right or freedom, it records the interference pathway, affected groups, intensity, evidence, alternatives considered, safeguards chosen, residual burden, material uncertainty, decision owner and review date. The ledger should link claims to underlying tests and monitoring rather than becoming a prose-heavy compliance form. Its value lies in legal memory and contestability: a court, regulator, auditor or affected person should be able to reconstruct why the design was selected and what evidence would require it to change.

¹⁰⁵ Regulation (EU) 2016/679, art 5(1)(e); *Google Spain* (Case C-131/12) EU:C:2014:317 paras 93-99; Regulation (EU) 2024/1689, arts 72-73.

¹⁰⁶ Charter, arts 21 and 52(1); Regulation (EU) 2024/1689, art 5; Regulation (EU) 2016/679, arts 5(1)(a), 6 and 7.

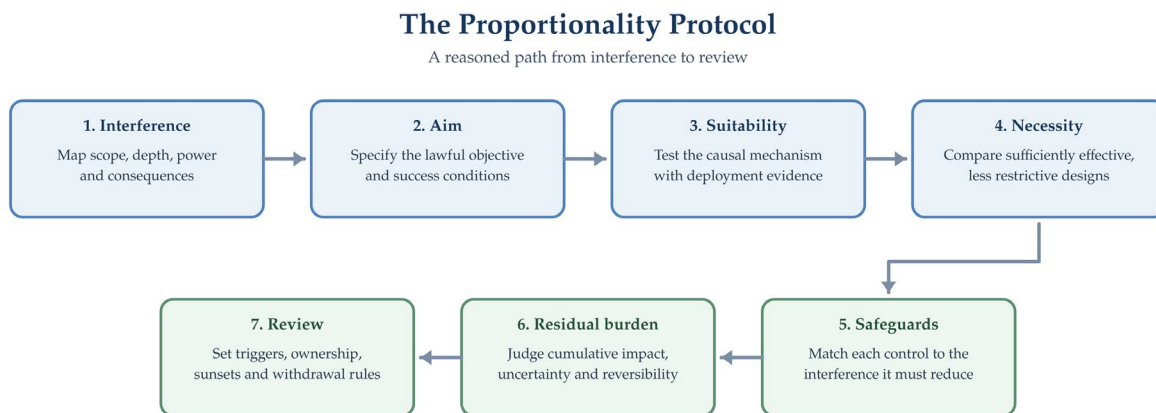


Figure 1. The proportionality protocol: a staged record of justified interference.

A rights ledger also improves supervisory decisions. If an authority orders cessation, it should identify which premise, legal condition or safeguard failed. If it accepts processing with conditions, it should explain how those conditions reduce the identified burden and how compliance will be verified. If it imposes a fine, it should link the sanction to the infringement and the criteria in Article 83. The ledger is not immunity from enforcement; it is the record against which the adequacy of both organisational and supervisory reasons can be tested.

5.11 Worked Applications

Age assurance demonstrates the value of the framework because child protection is weighty, while verification can burden privacy, data protection, expression, access to information, equality, and business freedom. Article 28 of the DSA requires appropriate and proportionate measures for platforms accessible to minors; the Commission's 2025 guidelines and age-verification blueprint, together with the EDPB's Statement 1/2025, emphasise risk-based, privacy-preserving implementation. The legal question is not whether children deserve protection, but which level of assurance a defined service risk justifies and what information the method reveals beyond the age threshold.^{107 108}

The aim must then be specified: which content or function, which age threshold, which harm, which service and which risk level? Suitability asks whether the method materially reduces that risk. Necessity asks whether graduated assurance, device-level controls, self-declaration with monitoring, attribute tokens or local estimation would be sufficiently effective. Stronger assurance may be justified for higher-risk access, but purpose separation, deletion, accessibility, non-document routes and appeal remain essential. An age

¹⁰⁷ Charter, arts 7, 8, 11, 16, 21, 24 and 52(1); Regulation (EU) 2016/679, arts 5, 25 and 35.

¹⁰⁸ Regulation (EU) 2022/2065, art 28; European Commission, *Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online* [2025] OJ C/2025/5519; European Data Protection Board, *Statement 1/2025 on Age Assurance* (11 February 2025), section 2.2; European Commission, 'The EU approach to age verification' <<https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification>> accessed 14 July 2026.

token that proves “over 18” without identity illustrates how architecture can protect children while reducing disclosure.¹⁰⁹

Adtech provides a different application. “Personalisation” may mean contextual advertising, first-party recommendations, frequency capping, measurement, cross-site behavioural targeting, or sensitive-interest inference; those activities cannot share a single necessity analysis. The interference grows as data cross contexts, persist, generate inferences and circulate through an ecosystem. *Meta Platforms*, *Schrems v Meta*, *IAB Europe*, and *KNLTB* govern GDPR questions, while Article 5(2) DMA separately constrains gatekeeper combinations and cross-use. The Commission's 2025 decision and Meta's January 2026 less-personalised option show why a proportionality record must identify the legal regime and the precise comparator rather than invoke “advertising” at large.¹¹⁰

Automated scoring provides a third application. The organisation should identify which data and proxies feed the score, the validation population, subgroup error, how the score changes over time, the role it plays downstream, what explanation the person receives and who can override it. The analysis must follow practical force across organisational boundaries. A credit bureau may produce the number and a lender may sign the decision, yet Article 22 can still apply where the number determines the result. Responsibility cannot be engineered away by splitting a decision into formally separate components.

Deceptive design and consent architectures provide a fourth application. A cookie banner, default, cancellation flow, or recommender interface may look minor in isolation, while repeated friction, salience, obstruction, and asymmetry can transfer autonomy, attention, and data at scale. GDPR fairness, consent, and design duties; Article 25 of the DSA; and the EDPB's deceptive-design guidance provide operative rules; proportionality helps explain why the intensity and accumulation of the design burden matter. It cannot save a pattern that invalidates consent or falls within a prohibition, but it can structure the comparison of legitimate service aims, alternative interfaces and residual effects.¹¹¹¹¹²

This point brings proportionality close to consumer protection without turning every irritating interface into a fundamental-rights case. Deceptive design often works through individually small frictions whose cumulative and distributional effects are large. Conventional disclosure analysis may ask whether a statement was visible; the protocol also asks whether the sequence, defaults and effort asymmetry materially impair free and informed choice, whether users bear the burden, and whether the claimed

¹⁰⁹ Regulation (EU) 2022/2065, art 28; European Commission, *Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online* [2025] OJ C/2025/5519; European Data Protection Board, *Statement 1/2025 on Age Assurance* (11 February 2025), section 2.2; European Commission, ‘The EU approach to age verification’ <<https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification>> accessed 14 July 2026.

¹¹⁰ European Commission, ‘Commission finds Apple and Meta in breach of the Digital Markets Act’ (23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085> accessed 14 July 2026; European Commission, ‘Meta commits to give EU users choice on personalised ads under Digital Markets Act’ (8 December 2025) <https://digital-markets-act.ec.europa.eu/meta-commits-give-eu-users-choice-personalised-ads-under-digital-markets-act-2025-12-08_en> accessed 14 July 2026; European Commission, *Annual Report on the Digital Markets Act 2025*, COM(2026) 247 final (21 May 2026).

¹¹¹ Regulation (EU) 2016/679, arts 5(1)(a), 6, 7 and 25; *Meta Platforms* (Case C-252/21) EU:C:2023:537; European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, version 1.1 (4 May 2020).

¹¹² Regulation (EU) 2022/2065, arts 25, 28 and 35; European Data Protection Board, *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces*, version 2.0 (14 February 2023).

service objective requires that architecture. The result is a more discriminating account of when persuasion becomes legally excessive design.

5.12 Seven Questions

The proposed framework can be reduced to seven questions.

1. What is the interference?
2. Who bears it and how intense is it?
3. What precise aim is pursued?
4. What evidence shows that the measure works for that aim in this context?
5. Which less restrictive designs were considered, and why were they rejected?
6. Which safeguards reduce the burden, and do they respond to the identified risks?
7. After alternatives and safeguards, is the residual burden justified, and when will the judgement be reviewed?

These questions do not replace doctrine. They force the user to identify which doctrine supplies the authority, standard and remedy, and then make the justificatory record visible. A court can use them to review a measure; a supervisory authority to select a corrective response; a controller to conduct a DPIA; an in-scope deployer to conduct an FRIA; or a procurement team to compare designs before lock-in. The method remains legal because it asks whether the actor has justified a burden under the rule that governs it; it becomes practical because it shows where evidence and reasons must appear.

The questions also answer the strongest objection to the article: that proportionality merely redescribes fairness, accountability, purpose limitation, minimisation, DPIAs and FRIAs. The answer is integration with limits. Proportionality explains why purpose, evidence, alternatives, safeguards, remedies and temporal review belong in one account of justified interference, while the operative provisions decide which elements are mandatory and what follows from breach. It neither replaces the GDPR and AI Act nor permits their requirements to be balanced away.

6. Conclusion

Proportionality is the legal form of disciplined justification, but its doctrinal plurality must remain visible. German law supplied an influential architecture; Strasbourg developed necessity, fair balance, procedural review and variable deference; Community law used proportionality across market freedoms, institutional discretion and general principles; Article 5 TEU and Article 52(1) of the Charter gave it distinct textual homes; and the GDPR, DSA and AI Act embed narrower necessity, design, risk and remedial obligations. The common demand is that lawful power remain connected to its reason. The legal route by which that demand operates depends on the actor and rule.

The method has teeth only when lawyers keep its stages and stop conditions separate. A legitimate aim must be legally anchored and operationally specified. Suitability must rest on deployment evidence rather than technological aura. Necessity must compare realistic, sufficiently effective designs rather than honour the organisation's first preference. Strict proportionality must address cumulative and distributed burdens without pretending to perform arithmetic. Safeguards must correspond to identified failure modes; the

intensity of review and institutional deference must be explained; remedies must follow from defects; and temporal controls must enable withdrawal.

The contemporary cases are not simple contests between privacy and policy. They require proportionate accommodation among privacy, data protection, expression, business freedom, property, equality, child protection, security and effective remedies. The case law is strongest when it rejects both absolutes and abstractions: *Digital Rights Ireland* on scale, the de-referencing cases on remedial targeting, the filtering cases on infrastructure, the retention line on informational power, *Meta Platforms* and *Schrems v Meta* on necessity and accumulation, *Mousse* on neutral alternatives, *SCHUFA* and *Dun & Bradstreet Austria* on practical automation, and *Land Hessen* on proportionate enforcement. *Glukhin* adds the chilling effect of biometric identification; the DSA, DMA, and the evolving AI Act show the same conflicts as they move into regulatory design.

The final step is application without doctrinal overreach. A lawful basis, DPIA, FRIA, risk category, conformity document, or supervisory decision may initiate the inquiry but cannot conclude it. The decisive question is whether the system and remedy go further than the governing legal aim can justify. A proportionality stack, rights ledger and temporal review make that question answerable before architecture hardens, while the stop conditions prevent “balance” from reviving what law forbids. Technology law becomes more honest when it accepts that interference is sometimes necessary and insists, with equal seriousness, that every material burden remain within the bounds of public reason.