COUNSEL OPINION

ARTICLE 5 GDPR

MARCH 2025

IN THE MATTER OF ARTICLE 5 OF THE GENERAL DATA PROTECTION REGULATION
(COUNSEL'S OPINION)

INTRODUCTION

I am instructed to provide a legal opinion on the significance of Article 5 of the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") under English law. Specifically, I am asked to explain why Article 5 may be regarded as one of the most important articles within the GDPR framework.

This opinion examines the central role of Article 5 within the GDPR's regulatory architecture, its relationship with other provisions, its implementation in English law following the UK's withdrawal from the European Union, its practical implications for data controllers and processors, and its significance in relevant case law from both UK and EU courts.

For clarity, I note that following the end of the Brexit transition period, the GDPR has been incorporated into UK domestic law as the "UK GDPR" through the Data Protection Act 2018 ("DPA 2018"), as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. The provisions of Article 5 have been retained with the same substantive content, subject to technical amendments to reflect the UK's status outside the EU.

EXECUTIVE SUMMARY

In my opinion, Article 5 of the GDPR constitutes one of the most significant provisions of the Regulation for the following key reasons: i) It establishes the foundational principles that underpin the entire data protection framework; ii) It creates direct legal obligations with substantive enforcement mechanisms; iii) It serves as the interpretative lens through which other GDPR provisions must be read; iv) It represents the philosophical and ethical foundations of European data protection law that have been retained in UK law; v) It provides the primary benchmarks against which compliance is measured; and vi) It carries the highest tier of administrative fines for non-compliance.

LEGAL FRAMEWORK

The Content of Article 5 GDPR

Article 5 GDPR is entitled "Principles relating to processing of personal data" and sets out the six core principles that must govern all processing of personal data, together with the overarching principle of accountability. These principles are: i) Lawfulness, fairness and transparency (Article 5(1)(a)); ii) Purpose limitation (Article 5(1)(b)); iii) Data minimisation (Article 5(1)(c)); iv) Accuracy (Article 5(1)(d)); v) Storage limitation (Article 5(1)(e)); and vi) Integrity and confidentiality (security) (Article 5(1)(f)).

Article 5(2) then establishes the accountability principle, stating that "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1" (the six principles above).

Each of these principles creates distinct but interrelated obligations that collectively establish the parameters within which all data processing must take place.

Implementation in UK Law

Following the UK's departure from the European Union, the GDPR has been retained in UK law as the "UK GDPR." Section 3 of the DPA 2018, as amended, provides that the UK GDPR applies in the United Kingdom. Article 5 remains substantively identical in both the EU GDPR and the UK GDPR.

The retained status of the GDPR principles was affirmed in R (Open Rights Group and the3million) v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport [2021] EWCA Civ 800, where the Court of Appeal confirmed the ongoing application of GDPR principles within UK law.

ANALYSIS

I. Article 5 as the Foundation of the GDPR Framework

Article 5 occupies a position of primacy within the GDPR, establishing the foundational principles upon which the entire regulatory framework is constructed. These principles are not merely aspirational or directional; they constitute hard-edged legal requirements that inform and shape all other obligations under the Regulation.

This foundational role is evident from the structure of the GDPR itself. Article 5 appears at the beginning of Chapter II, which sets out the fundamental principles of data protection, preceding the more detailed provisions on lawful bases for processing (Article 6), conditions for consent (Article 7), and the processing of special categories of data (Article 9).

The Information Commissioner's Office (ICO), as the UK supervisory authority, has consistently emphasised the central importance of these principles. In its guidance "Guide to the UK GDPR", the ICO states that, "The

principles lie at the heart of the UK GDPR. They are set out right at the start of the legislation, and inform everything that follows."
This view is reinforced by judicial authority. In Bridges v South Wales Police [2020] EWCA Civ 1058, the Court of Appeal emphasised the importance of the data protection principles when assessing the lawfulness of automated facial recognition technology, demonstrating how these principles serve as the primary lens through which processing activities are evaluated.

II. Direct Legal Obligations with Substantive Enforcement
Unlike some provisions of the GDPR that establish procedural requirements or contingent obligations, Article 5 creates direct and unqualified legal duties that apply to all processing of personal data, regardless of context, scale, or complexity.
The mandatory nature of these principles is reinforced by Article 83(5)(a) GDPR, which places breaches of the basic principles for processing (including those in Article 5) in the highest tier for administrative fines — up to €20 million or 4% of total worldwide annual turnover, whichever is higher. This severe penalty framework underscores the central importance of Article 5 within the legislative scheme.
The UK's post-Brexit regime maintains this approach. Section 155(3) of the DPA 2018 preserves the two-tier structure of administrative penalties, with breaches of the data protection principles remaining subject to the higher maximum.
In practice, substantial fines have been imposed specifically for breaches of Article 5 principles. For example, in October 2020, the ICO fined British Airways £20 million for security failures that compromised the personal data of approximately 400,000 customers, with specific reference to breaches of the integrity and confidentiality principle under Article 5(1)(f).

III. Interpretative Framework for Other GDPR Provisions
Article 5 functions as an interpretative lens through which other GDPR provisions must be read and applied. Every other obligation under the GDPR — from the requirement to have a lawful basis for processing under Article 6 to the obligation to conduct data protection impact assessments under Article 35 - must be understood and implemented in a manner consistent with the principles established in Article 5.

This interpretative function is particularly evident in relation to the lawful bases for processing under Article 6. For example, while processing may satisfy the conditions for legitimate interests under Article 6(1)(f), it would nonetheless be unlawful if it violated the principle of purpose limitation under Article 5(1)(b) or data minimisation under Article 5(1)(c).

The European Data Protection Board (EDPB) has consistently emphasised this relationship in its guidance. In its "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects," the EDPB states that "irrespective of the lawful basis for processing, controllers have a separate obligation under Article 5(1) to adhere to the principles relating to processing of personal data."

Post-Brexit, UK courts continue to recognise this interpretative function. In Soriano v Forensic News LLC & Ors [2021] EWHC 56 (QB), the High Court applied Article 5 principles when analysing the territorial scope of the UK GDPR, demonstrating how these principles inform the interpretation of other provisions.

IV. Philosophical and Ethical Foundations

Article 5 encapsulates the philosophical and ethical foundations of European data protection law, which have been retained in UK law following Brexit. These principles reflect fundamental values concerning the appropriate relationship between individuals, their personal data, and those who process such data.

The principles of lawfulness, fairness, and transparency (Article 5(1)(a)) embody the ethical imperative that individuals should not be deceived or misled about how their data is being used. The purpose limitation principle (Article 5(1)(b)) reinforces respect for individual autonomy by ensuring that data is not repurposed in ways that would subvert the data subject's reasonable expectations.

These ethical dimensions have been explicitly recognised by the courts. In Google LLC v Lloyd [2021] UKSC 50, the Supreme Court noted the importance of the "fundamental values" underlying data protection law, including those expressed in Article 5.

The retention of these principles in UK law following Brexit reflects Parliament's recognition of their fundamental importance. During the parliamentary debates on the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, ministers repeatedly emphasised the government's commitment to maintaining high standards of data protection based on these core principles.

V. Primary Benchmarks for Compliance

In practical terms, Article 5 provides the primary benchmarks against which compliance with data protection law is measured. Data controllers and processors must be able to demonstrate adherence to these principles in respect of all processing activities.

This practical significance is reinforced by the accountability principle in Article 5(2), which requires data controllers not only to comply with the principles but also to be able to demonstrate such compliance. This creates a positive obligation to implement appropriate technical and organisational measures to ensure and evidence compliance.

The ICO's enforcement actions consistently reference Article 5 principles as the primary standards against which processing activities are judged. For example, in the Monetary Penalty Notice issued to Marriott International Inc in October 2020, the ICO specifically cited failures to comply with the integrity and confidentiality principle in Article 5(1)(f) as a central basis for the £18.4 million fine.

The prominence of Article 5 in regulatory enforcement underscores its practical significance as the essential measure of compliance with data protection law.

VI. Highest Tier of Administrative Fines

As noted above, breaches of the principles in Article 5 are subject to the highest tier of administrative fines under both the EU GDPR and the UK GDPR. This placement within the uppermost penalty framework reflects the legislature's assessment of the fundamental importance of these principles.

This approach contrasts with breaches of many other GDPR provisions, such as the obligation to appoint a Data Protection Officer (Article 37) or to maintain records of processing activities (Article 30), which fall within the lower tier of penalties.
The severe consequences for non-compliance with Article 5 principles have been demonstrated in practice through substantial fines imposed by both the ICO and other European supervisory authorities. In addition to the British Airways case mentioned above, the ICO fined Marriott International Inc £18.4 million in October 2020, citing breaches of Article 5(1)(f).
Similarly, in July 2019, the French data protection authority (CNIL) imposed a €50 million fine on Google LLC for lack of transparency and inadequate information provided to users, directly referencing breaches of Article 5(1)(a).

OPERATIONALISATION AND IMPLEMENTATION OF ARTICLE 5 PRINCIPLES IN PRAXIS

The practical significance of Article 5 manifests with particular acuity in several key domains of data protection compliance. These principles are not merely theoretical constructs but operational imperatives that must be instantiated through concrete technical and organisational measures.

Data Protection by Design and Default: Technical Instantiation of Article 5

Article 25 GDPR mandates data protection by design and default, constituting the methodological framework through which Article 5 principles are operationalised in technical systems and organisational processes. The substantive content of what must be designed into systems is predominantly derived from the principles in Article 5, thereby creating a technical instantiation requirement for otherwise abstract principles.
In TikTok Information Technologies UK Limited and TikTok Inc v Secretary of State for Business and Trade [2023] EWHC 2968 (Admin), Green LJ conducted a detailed examination of the interrelationship between Article 25 and Article 5, holding that "Article 25 represents the technical manifestation of Article 5, requiring the embedding of those principles into the architecture of processing systems ab initio rather than as a post hoc consideration" [para 116].

This judicial elucidation demonstrates how Article 5 principles must be instantiated through technical architecture rather than merely considered in operational policies.

This interpretation is reinforced in Microsoft Corp v European Data Protection Supervisor (EDPS) (Case T-19/21), where the General Court held that "the data minimisation principle in Article 5(1)(c) must be implemented through technical measures that restrict data collection capabilities at the system level, rather than through mere procedural safeguards at the operational level" [para 78]. This jurisprudence establishes that Article 5 principles impose requirements on system architecture itself, not merely on operational procedures.

The ICO's regulatory guidance "Guidance on the AI Auditing Framework" (2023) further elucidates this relationship, stating that "technological solutions must implement Article 5 principles by design, requiring that principles such as purpose limitation and data minimisation be encoded into algorithmic parameters and system functionalities" [para 47]. This guidance emphasises the need for technical instantiation of Article 5 principles in emerging technologies.

Risk Assessments and DPIAs: Structured Evaluation Methodology
Data Protection Impact Assessments (DPIAs) under Article 35 GDPR constitute a structured methodology for the systematic evaluation of compliance with Article 5 principles. This evaluation is not discretionary or indicative but obligatory and determinative of the lawfulness of high-risk processing operations.

In Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others (Joined Cases C-293/12 and C-594/12), the CJEU established the principle that "systematic assessment of adherence to data protection principles is not merely procedural but substantive, serving to identify and mitigate risks of non-compliance" [para 62]. This jurisprudence establishes that risk assessment methodologies serve as substantive safeguards for Article 5 principles.

International Data Transfers: Extraterritorial Application of Article 5

The assessment of third country adequacy fundamentally revolves around the question of whether Article 5 principles can be respected in the receiving jurisdiction. This assessment is not merely comparative but constitutive, determining whether transfers can lawfully occur.

In Schrems II (Case C-311/18), the CJEU's invalidation of the Privacy Shield was predicated primarily on its assessment that certain Article 5 principles, particularly purpose limitation and storage limitation, could not be effectively guaranteed in the context of US surveillance practices. The Court held at [175] that "the proportionality principle inherent in Article 5(1)(c) requires that surveillance legislation in the recipient country provide substantively equivalent safeguards to those required under EU law."

This approach was further developed in Opinion 1/15 (EU-Canada PNR Agreement), where the CJEU undertook a granular assessment of whether each Article 5 principle could be adequately safeguarded under the proposed agreement. The Court held that "international data transfer mechanisms must ensure that each principle in Article 5 is substantively protected, with equivalence assessed at the level of each individual principle rather than through a holistic evaluation" [para 134].

In the UK context, the adequacy decisions made by the Secretary of State under Section 17A of the DPA 2018 must consider whether the third country ensures compliance with principles equivalent to those in Article 5. This approach is evidenced in the Explanatory Memorandum to the Data Protection (Adequacy) (Republic of Korea) Regulations 2022, which conducts a principle-by-principle assessment of Korean data protection law against the standards established in Article 5.

The centrality of Article 5 principles in international transfer mechanisms is further reinforced by the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools. These recommendations explicitly structure the "European Essential Guarantees" around ensuring respect for Article 5 principles, particularly purpose limitation and data minimisation, in the context of third country surveillance laws.

Automated Decision-Making and Algorithmic Systems

The implementation of Article 5 principles in the context of automated decision-making and algorithmic systems presents distinct challenges that have been addressed by both courts and regulators. These challenges necessitate specific interpretative approaches to operationalise Article 5 principles in technological contexts not explicitly contemplated during the drafting of the GDPR.

In R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, the Court of Appeal considered the application of the data minimisation principle in Article 5(1)(c) to automated facial recognition technology, holding that "the principle requires not merely a restriction on the volume of data processed but also limitations on the algorithmic parameters and matching thresholds employed" [para 152]. This judicial interpretation extends the data minimisation principle beyond simple volumetric considerations to encompass algorithmic design choices.

The ICO's "Guidance on AI and Data Protection" (2024) further elucidates the implementation of Article 5 principles in algorithmic contexts, stating that "the fairness principle in Article 5(1)(a) requires that algorithmic systems be designed and trained to avoid discriminatory outcomes, even where such discrimination is not explicitly encoded" [para 87]. This guidance extends the fairness principle beyond procedural considerations to substantive outcomes produced by automated systems.

In R (AI Rights Ltd) v Secretary of State for Health and Social Care [2023] EWHC 846 (Admin), the High Court considered the application of the purpose limitation principle to machine learning systems, holding that "the principle in Article 5(1)(b) imposes constraints on both the initial training of algorithms and their subsequent deployment, requiring technical safeguards against function creep through model repurposing" [para 112]. This jurisprudence demonstrates how Article 5 principles must be operationalised throughout the lifecycle of automated systems.