The GDPR (EU and UK) and Recent Developments

1. Introduction

The General Data Protection Regulation (GDPR or the Regulation) 2016/679, has been in force since 25 May 2018 and remains the central framework governing the protection of personal data within the European Union (EU). Following the United Kingdom's withdrawal from the European Union, the GDPR has been retained in domestic law as the UK GDPR, supplemented by the Data Protection Act 2018.

The United Kingdom has since enacted the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent in June 2025 and began taking effect from August 2025. The Act reforms and relaxes aspects of the UK regime with the stated aim of promoting economic growth and clarifying the use of data while maintaining a framework broadly aligned with the GDPR. It introduces changes in areas including consent, automated decision-making, data sharing for research and protections for children online. These reforms mark a measured divergence between the UK and EU regimes, though the underlying structure remains recognisably similar. The GDPR continues to regulate the processing of personal data, while the Data Act introduces a parallel regime governing access to and use of data more broadly, including non-personal data.

Accordingly, data protection law now operates in parallel regimes in the EU and the UK. Since its coming into force, the GDPR has been shaped by decisions of the Court of Justice of the European Union (CJEU). In the United Kingdom, those decisions remain highly persuasive, though not formally binding in all circumstances, and the regime is interpreted and enforced by the Information Commissioner's Office. At EU level the framework has also been supplemented by further legislation, in particular Regulation (EU) 2023/2854 (the Data Act).

At the heart of both EU and UK regimes remain the principles of lawfulness, fairness, transparency, purpose limitation and data minimisation.

2. Main Elements

2.1 Territorial jurisdiction

Under the EU GDPR, the Regulation applies where personal data of individuals in the Union is processed in connection with the offering of goods or services or the monitoring of behaviour within the Union. The UK GDPR applies on a similar basis to individuals in the United Kingdom. Both regimes therefore have broad extraterritorial

reach and may apply in parallel where activities target both markets.

2.2 Consent

Consent must be freely given, specific, informed and unambiguous, given by a clear affirmative act and capable of withdrawal at any time. The DUAA introduces a more flexible approach in certain UK contexts, including streamlined cookie consent for low-risk processing.

2.3 Right to be forgotten

The right to erasure, developed in *Google Spain v Costeja* C-131/12 and codified in Article 17, permits deletion of personal data in defined circumstances and may extend to informing third parties where data has been made public. Its scope has been clarified in *Google v CNIL* C-507/17, confirming limits to territorial reach. The scope of the right to erasure has also been shaped by case law addressing its interaction with freedom of expression under Article 10 ECHR and Article 11 of the Charter. In *Google LLC v CNIL* (above) the Court confirmed that de-referencing obligations are generally limited to the EU domain. In *GC and Others v CNIL,* C-136/17, the Court further clarified that search engine operators must assess, on a case-by-case basis, whether continued indexing is strictly necessary for protecting the public's right to information, particularly in relation to sensitive data.

In the United Kingdom, the courts have adopted a similar balancing approach. In *NT1 & NT2 v Google LLC* [2018] EWHC 799 (QB), the High Court considered competing rights under data protection law and Article 10, granting de-referencing in one case while refusing it in another, emphasizing factors such as the claimant's role in public life, the nature of the information and the continuing public interest. More recently, in *ZXC v Bloomberg LP* [2022] UKSC 5, the Supreme Court confirmed that individuals under criminal investigation have, a reasonable expectation of privacy, reinforcing the importance of careful balancing between privacy rights and freedom of expression.

2.4 Data Portability

Article 20 provides a right to receive personal data in a structured, commonly used and machine-readable format and to transmit it to another controller where technically feasible. The position is aligned across EU and UK regimes.

2.5 Data Breach Notification

Controllers must notify breaches within 72 hours unless unlikely to result in risk, and notify individuals where high risk arises.

2.6 Automated decision-making and profiling

Individuals have rights relating to automated decisions. The DUAA permits greater use subject to safeguards. The ICO is consulting on updated guidance in this area.

2.7 Privacy by design

Controllers must implement appropriate technical and organisational measures and conduct impact assessments where appropriate.

2.8 Transfers

Personal data may only be transferred outside the relevant jurisdiction where an adequate level of protection is ensured. Following Schrems II, the EU–US Privacy Shield was invalidated. In the EU transfers can rely on mechanisms such as standard contractual clauses together with assessment of the recipient jurisdiction. A new EU–US Data Privacy Framework was adopted on 10 July 2023, and the DPF is currently in force and enables data transfers to self-certified U.S. companies without needing additional safeguards like Standard Contractual Clauses (SCCs). On 3 September 2025, the EU General Court dismissed a major challenge to the DPF, confirming that on the date of its adoption, the U.S. provided an "essentially equivalent" level of protection though its durability remains open to challenge. This was a direct legal action for annulment filed by Philippe Latombe, a French Member of Parliament, before the General Court of the European Union, Case T-553/23.

In the United Kingdom, a separate regime applies, including adequacy regulations and transfer tools such as the International Data Transfer Agreement and the UK addendum to standard contractual clauses. The EU has adopted an adequacy decision for the United Kingdom, permitting data flows from the EU to the UK, subject to periodic review. The renewed decision is valid until 27 December 2031, with strict "sunset clauses" and ongoing monitoring. The EU confirmed that UK legal frameworks, including the Data (Use and Access) Act, provide protection "essentially equivalent" to EU standards and this covers both commercial data transfers and law enforcement cooperation, allowing data flow without requiring additional safeguards like SCCs As a "living instrument," the decision is subject to continuous monitoring by the European Commission, with the ability to suspend or revoke the status if UK data protection standards diverge significantly from those of the EU.

2.9 Accountability

Controllers must demonstrate compliance through records, governance and impact assessments.

3. Additional Legislative Developments

The EU Data Act introduces rules on access and use of data, including sharing obligations and interoperability requirements.

4. Media issues

Special category data is restricted subject to exemptions. Freedom of expression must be balanced with data protection.

5. Case law

The Regulation has been significantly developed through decisions of the Court of Justice. *Schrems II*, C-311/18, confirmed the invalidity of the Privacy Shield and imposed stricter requirements on international transfers. *Meta Platforms* clarified limits on reliance upon contractual necessity in behavioural advertising. This was in May 2023, when the Irish Data Protection Commission (DPC) fined Meta Platforms Ireland Limited a record €1.2 billion for violating the GDPR by transferring European user data to the U.S. using SCC and failing to adequately protect it. The case, stemming from complaints mandated that Meta cease illegal data processing, including storage, in the U.S. within six months of the decision

In *Schufa* C-634/21, the Court of Justice restricted the use of automated credit scoring by agencies like SCHUFA. The court ruled that automated, high-probability scores that heavily influence loan decisions constitute a forbidden "automated decision" under GDPR if they lead to credit refusal. In *Österreichische Post*, C-300/21, the court confirmed that compensation for non-material damage requires proof of harm but no minimum threshold. Compensation under the UK GDPR also requires proof of actual material or non-material damage caused by the infringement; a mere breach is insufficient, but there is no minimum threshold of seriousness. See *Farley & Others v Paymaster (Equiniti)* [2025] EWCA Civ 1117.

Google v CNIL C-507/17 addressed territorial scope of erasure rights. *Bundeskartellamt v Meta* C-252/21 confirmed the interaction between data protection and competition law. More recently, the Court has clarified that subject access requests may, in limited circumstances, be refused where they are abusive, including where made solely to generate a damages claim.

In the United Kingdom, these EU authorities remain persuasive and are

likely to inform interpretation, subject to domestic judicial discretion.

6. Enforcement trends

Supervisory authorities in the European Union have adopted an increasingly assertive approach to enforcement, particularly in relation to large technology platforms. Meta has been subject to multiple significant fines, including the record €1.2 billion penalty in 2023 above, alongside further decisions concerning targeted advertising and the use of personal data without a valid legal basis. Google has also faced repeated enforcement action, including substantial fines imposed by the French authority for failures in transparency and valid consent in personalised advertising, as well as continued scrutiny of its advertising technologies.

Enforcement has also extended beyond the largest platforms. On 24 February 2026, the UK's Information Commissioner's Office (ICO) fined Reddit, Inc. £14.47 million for unlawfully processing children's personal data and failing to implement robust age assurance mechanisms. The investigation revealed that Reddit allowed children under 13 to use the platform, violating the UK's Children's Code. This regulatory action reflects a broader willingness to pursue online services. Across these cases, regulators have taken a strict approach to purpose limitation, lawful basis and the combination of data across services, with particular emphasis on behavioural advertising and tracking.

Recent developments also illustrate increasing judicial scrutiny of regulatory enforcement. In particular, the Administrative Court in Luxembourg annulled a €746 million fine imposed on Amazon on the basis that the regulator had failed adequately to assess whether the infringement was intentional or negligent, while nonetheless upholding the underlying findings of non-compliance.

There remains sustained focus on international transfers following Schrems II, requiring detailed transfer risk assessments and supplementary safeguards, and increased scrutiny of cookies and tracking technologies, with enforcement against non-compliant consent mechanisms.

In the United Kingdom, the Information Commissioner's Office has adopted an active but proportionate enforcement approach, combining guidance with sanctions. Enforcement has focused on data breaches, particularly those arising from cybersecurity failures, unlawful direct marketing and the use of personal data in political campaigning and

analytics. Recent enforcement includes action against Police Scotland for failures in handling highly sensitive personal data, reinforcing the importance of data minimisation and appropriate safeguards. There has also been sustained regulatory attention on children's data, building on the Age-Appropriate Design Code, alongside increasing alignment between data protection and online safety regulation, including joint activity with Ofcom in relation to age assurance.

The introduction of the DUAA is influencing enforcement priorities in the United Kingdom, particularly in relation to automated decision-making, data sharing for research and the treatment of lower-risk processing, while maintaining a focus on transparency and accountability.