educage.
info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

The Next Great Challenge for the GDPR: AI, Encryption and Cybercrime in the EU and the United Kingdom

1. Introduction

The General Data Protection Regulation of the European Union, Regulation (EU) 2016/679 (GDPR), has been a defining point of reference in global data protection law since its entry into force on 25 May 2018. The Regulation pursued a dual objective: to provide a uniform, high level of data protection for EU citizens and to reduce the legal uncertainty arising from divergent regulatory approaches across Member States. In recent years, however, the technological and threat landscape has changed radically. The exponential development of artificial intelligence (AI), the widespread adoption of end-to-end encryption, and the industrialisation of cybercrime all pose challenges to the GDPR and to the authorities and courts that interpret it challenges that the Regulation's drafters in 2016 could not have fully foreseen.[1]

The United Kingdom's withdrawal from the European Union (Brexit) set in motion a parallel trajectory of regulatory development.
The UK data protection regime, whose backbone is the UK-retained GDPR (UK GDPR) and the Data Protection Act 2018 (DPA 2018), shows divergences from the EU approach. This article aims to examine these three key challenges AI, encryption, and cybercrime and to assess the extent to which the current legal frameworks are capable of addressing the conflicts that arise, and what direction legislative and enforcement trends are pointing.[8,9]

2. The GDPR and AI: From Profiling to Autonomous Decision-Making

2.1. Rules on Automated Decision-Making

Article 22 of the GDPR establishes as a general rule that a data subject shall not be subject to a decision based solely on automated processing - including profiling - which produces legal effects concerning them or similarly significantly affects them. This provision applies directly to AI-based credit scoring, job application screening, or insurance pricing systems. The exceptions are narrow: automated processing is permissible where the data subject has given explicit consent, where it is authorised by law, or where it is necessary for the performance of a contract, but in every case, the possibility of human intervention, the right to contest the decision, and the right to express one's point of view must be ensured.

The emergence of generative AI, however, gives rise to serious interpretive difficulties. Do the outputs of large language models (LLMs) - for example, the responses of a system that evaluates job applicants - qualify as decisions based "solely on automated processing" if a human user subsequently endorses them? The European Data Protection Board (EDPB) provides an important interpretive framework for the application of the GDPR in its guidelines on

automated individual decision-making and profiling. However, comprehensive and specific EDPB guidance addressing the data protection implications of generative AI systems is not yet available; accordingly, the assessment of such technologies currently rests primarily on the existing data protection principles and general guidelines. The situation is further complicated by the fact that AI systems increasingly serve parallel processing purposes, simultaneously participating in display, analysis, and decision-support processes a development that also renders enforcement of the purpose limitation principle (Article 5(1)(b) GDPR) problematic.

2.2. The Interaction Between the AI Act and the GDPR

Regulation (EU) 2024/1689 of the European Parliament and of the Council - the so-called AI Act - is the world's first comprehensive, risk-based AI regulation. The Regulation introduces the concept of the "high-risk AI system", which encompasses applications related to employment, education, law enforcement, and the administration of justice. In this category, a fundamental rights impact assessment is mandatory, closely linked to the data protection impact assessment (DPIA) under Article 35 of the GDPR. The two instruments create parallel compliance obligations.[2]

Controllers and operators of AI systems must simultaneously comply with the requirements of both regimes.

The AI Act sets out explicit requirements regarding data governance and the quality of training, validation, and testing datasets. These requirements are closely linked to the principles of data minimisation and accuracy enshrined in the GDPR, since the proper functioning of AI systems can only be ensured through the use of relevant, adequately high-quality, and sufficiently accurate data.[2]

No comprehensive AI regulation comparable to the EU AI Act has yet been adopted in the United Kingdom. The UK Government has instead opted for a so-called "pro-innovation" approach, under which individual sectoral regulators - including the Information Commissioner's Office (ICO) - address AI-related risks through the application of existing legal frameworks.
The AI and Data Protection Risk Toolkit developed by the ICO provides practical guidance for assessing AI-related processing activities in compliance with the UK GDPR and for managing the associated data protection risks. However, it remains a matter of debate in the literature whether a decentralised, innovation-centred regulatory model is capable, in the long term, of ensuring the effective protection of data subjects' fundamental rights.[9]

3. Encryption and Data Protection: The "Backdoor" Debate

3.1. Encryption as the Cornerstone of Data Protection

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

Article 32 of the GDPR obliges controllers and processors to implement technical and organisational measures appropriate to the level of risk in order to ensure the security of personal data; in this context, the Regulation explicitly refers to the encryption of personal data. The guidelines of the European Union Agency for Cybersecurity (ENISA) and the opinions of the EDPB consistently confirm that end-to-end encryption is one of the most effective tools for the secure processing of personal data. The CJEU's judgment in Schrems II highlighted the fact that technical safeguards applied in the context of transfers to third countries - in particular effective encryption - can play a significant role in maintaining the level of data protection guaranteed under EU law[1,13]

3.2. Law Enforcement Access and the Online Safety Dilemma

The UK Online Safety Act 2023 (OSA) has generated considerable controversy regarding the balance between encrypted communications and law enforcement interests. The Act enables Ofcom to require, in certain circumstances, the application of technological measures to detect illegal content relating to the online sexual abuse of children.[10]
Critics argue that the practical implementation of these obligations could lead to a reduction in the effectiveness of end-to-end encryption (E2EE), since content inspection can only take place either before encryption or after decryption. As a result, there are widespread concerns that the legislation may in practice incentivise the deployment of "client-side scanning" solutions.
During the preparation and adoption of the legislation, representatives of Signal, WhatsApp, and Proton indicated on multiple occasions that they would consider withdrawing their services from the UK market if implementation of the Online Safety Act were to necessitate the weakening of end-to-end encryption or the establishment of backdoor access mechanisms. On the EU side, the European Commission published a legislative proposal in 2022 aimed at combating online child sexual abuse material (CSAM) the so-called "Chat Control" proposal. Certain provisions of the proposal would impose detection obligations on electronic communications service providers that numerous experts consider difficult to reconcile with end-to-end encryption. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) emphasised in a joint opinion that general and indiscriminate surveillance measures may raise serious concerns with regard to the right to privacy guaranteed by Article 7 of the Charter of Fundamental Rights of the European Union, and the right to the protection of personal data enshrined in Article 8. The case-law of the Court of Justice of the European Union, in particular *La Quadrature du Net and Others* (Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791), has likewise confirmed that the general and indiscriminate surveillance of communications is, as a general rule, incompatible with EU fundamental rights requirements.[6,14]

3.3. Encryption and Data Transfers

Chapter V of the GDPR sets out detailed rules governing the transfer of personal data to third countries. Among the most important instruments for providing appropriate safeguards under Article 46 are the Standard Contractual Clauses (SCCs) adopted by the European Commission

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

in 2021. The SCCs require the assessment of risks associated with data transfers, as well as the implementation and documentation of appropriate technical and organisational measures, among which encryption may play a prominent role. A particularly sensitive area is the flow of data between the European Union and the United Kingdom. The European Commission adopted an adequacy decision in respect of the United Kingdom in 2021, enabling the free flow of personal data between the EU and the UK. However, the adequacy decision cannot be considered permanent: the European Commission assesses, through a periodic review, whether the United Kingdom continues to ensure a level of data protection essentially equivalent to that guaranteed under EU law. Should the development of the UK legal system result in a significant divergence from EU data protection standards, the Commission is entitled to amend, suspend, or repeal the adequacy decision. Such a decision would materially affect the legal framework governing the flow of personal data between the European Union and the United Kingdom.[4;5]

4. Cybercrime, Data Breaches, and the GDPR's Liability Framework

4.1. The Obligation to Notify Personal Data Breaches

Under Article 33 of the GDPR, the controller is required to notify the competent supervisory authority of a personal data breach within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Under Article 34, the affected data subjects must also be notified where the breach is likely to result in a high risk. Ransomware attacks - in which criminals encrypt the victim's data and demand a ransom - pose particularly significant data protection and incident management challenges.[1]

EDPB Guidelines 9/2022 on personal data breach notification address ransomware attacks in detail and emphasise that the loss of availability of personal data, or a significant restriction of such availability, may in itself constitute a personal data breach within the meaning of the GDPR. In practice, data protection authorities are taking an increasingly stringent approach to GDPR infringements. This is well illustrated by the fine of EUR 225 million imposed on WhatsApp by the Irish Data Protection Commission (DPC) in 2021, and the EUR 1.2 billion sanction applied against Meta in 2023, which ranks amongst the largest data protection fines ever imposed for infringement of data protection rules in the European Union.

4.2. The Relationship Between the NIS2 Directive and the GDPR

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2) has significantly expanded the range of sectors deemed critical from a cybersecurity perspective, and has tightened risk management, incident handling, and reporting obligations. The Directive distinguishes between the categories of "essential" and "important" entities and, under Article 23, introduces a multi-stage notification system for significant incidents, the first element of which is an early warning to be submitted within 24 hours. The parallel application of NIS2 and the GDPR raises coordination questions, particularly in the

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

area of incident notification obligations, thereby increasing the importance of cooperation between data protection and cybersecurity authorities. The United Kingdom is not obliged to transpose the NIS2 Directive following its withdrawal from the European Union; however, a review of the Network and Information Systems Regulations 2018 is under way. Moreover, the guidance issued by the National Cyber Security Centre (NCSC) reflects requirements that, in many areas, are comparable to EU cybersecurity standards.[3]

4.3. Liability and Sanctions: The Dilemma of Public Authorities and Private Undertakings

Article 82 of the GDPR provides data subjects with a right to compensation for material and non-material damage resulting from an infringement of the GDPR. In Case C-340/21 (*Natsionalna agentsia za prihodite*), the Court of Justice of the European Union held in 2023 that the unauthorised access to personal data as a result of an external cyberattack does not in itself exempt the controller from liability. The controller must demonstrate that it had implemented appropriate technical and organisational measures as required by the GDPR, and that it bears no responsibility whatsoever for the event that caused the damage. The judgment further confirmed that, in certain circumstances, a well-founded fear of misuse of personal data may in itself give rise to non-material damage. The ruling has a significant impact on corporate cybersecurity practices, highlighting that falling victim to a cyberattack is not, in itself, sufficient to escape liability under the GDPR.[15]

Article 83 of the GDPR establishes a two-tier sanctioning system: for less serious infringements, fines of up to EUR 10 million or 2% of the undertaking's total worldwide annual turnover for the preceding financial year may be imposed, whilst for more serious infringements, fines of up to EUR 20 million or 4% of annual turnover may be applied - whichever is the higher amount. The enforcement of data processing obligations against public authorities presents particular challenges, however, as certain Member States apply different rules regarding the fining of public bodies. The EDPB noted in Guidelines 07/2020 that such divergences may affect the uniform application of the GDPR and the effectiveness of the sanctioning regime as a deterrent.[1]

5. The Question of EU–UK Legal Convergence and Divergence

Post-Brexit UK data protection regulation is currently subject to dual pressure. On one hand, maintaining the EU adequacy decision requires that the UK data protection regime remain essentially equivalent to the EU approach. On the other hand, the UK Government's reform ambitions - aimed at reducing the ICO's regulatory burden and corporate compliance costs - signal a drift away from the EU GDPR.
The Data (Use and Access) Act 2025 seeks to strike a balance between promoting innovation and preserving adequacy, but certain of its provisions - such as the expanded permissions for

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

processing aimed at scientific research and statistics - potentially narrow the scope of data subjects' rights.[11]
The divergence is even more pronounced in the area of AI regulation. Whilst the EU has enacted a binding, enforceable AI regulation, the United Kingdom relies on non-binding principles and sectoral regulatory guidance. This dual regulatory trajectory means that companies operating in both the EU and the UK face divergent AI compliance obligations. Regulatory gaps are particularly dangerous in relation to systems that process biometric data: Article 9 of the GDPR treats biometric data used for identification purposes as a special category of data, yet the legal assessment of real-time facial recognition systems for law enforcement purposes remains contested even under the AI Act.

6. Conclusions and Regulatory Perspectives

The GDPR has undoubtedly been a landmark piece of legislation, and its principles - lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability (Article 5) - represent enduring values. Nevertheless, the pace of technological development outstrips the natural revision cycles of legislation. Each of the three areas examined - AI, encryption, and cybercrime - reveals normative gaps that demand urgent legislative and enforcement responses.

- In the area of AI regulation, it is of paramount importance to ensure coherence between the provisions on automated decision-making in Article 22 of the GDPR and the requirements of the AI Act, with particular regard to the genuine and substantive exercise of human oversight.
- With regard to encryption, one of the most important challenges for EU legislation is to strike an appropriate balance between law enforcement interests and the protection of fundamental rights. In this context, solutions should be prioritised that enable lawful intervention by public authorities without disproportionately endangering the data security and confidentiality of communications guaranteed by end-to-end encryption.
- In the area of combating cybercrime, the coherent application of the regulatory frameworks established by the NIS2 Directive and the GDPR, the development of cross-border incident management mechanisms, and the effective enforcement of data subjects' right to compensation will continue to be of defining importance.

When the GDPR was adopted, the legislature sought primarily to address the data protection risks posed by digital platforms, online services, and large-scale data collection.
The technological developments of recent years, however, demonstrate that the Regulation must be applied in the face of new challenges that were only partially foreseeable when the legislation was enacted.
The emergence of generative artificial intelligence, the debates surrounding end-to-end encryption, and the growing complexity of cybersecurity threats all indicate that data protection can no longer be treated in isolation from other regulatory and societal objectives.

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

A common feature of the areas examined is that in none of these cases is the existence or necessity of data protection itself in dispute - rather, it is its boundaries that are contested.
Legislators, supervisory authorities, businesses, and courts alike are confronted with the task of determining the extent of data processing that is acceptable in the interests of fostering innovation, protecting public safety, or maintaining the operability of digital services. The significance of the GDPR lies precisely in the fact that it provides, during such conflicts, principles - in particular the requirements of necessity, proportionality, accountability, and transparency - that can continue to serve as a compass notwithstanding the emergence of new technologies.
The future success of the Regulation is therefore likely to depend not primarily on the adoption of further detailed rules, but rather on the extent to which the data protection principles prove applicable in an ever-changing technological environment.
The true test of the GDPR will not be whether it is capable of providing pre-formulated answers to every new technology, but whether it remains fit for the effective protection of individual rights in a digital ecosystem whose direction of development is becoming increasingly unpredictable.

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (AI Act).
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).
4. Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.
5. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
6. Charter of Fundamental Rights of the European Union.
7. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
8. Data Protection Act 2018 (c. 12).
9. UK General Data Protection Regulation (UK GDPR).
10. Online Safety Act 2023 (c. 50).
11. Data (Use and Access) Act 2025.
12. Network and Information Systems Regulations 2018 (SI 2018/506).
13. CJEU, C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559.
14. CJEU, C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others, ECLI:EU:C:2020:791.
15. CJEU, C-340/21, Natsionalna agentsia za prihodite, ECLI:EU:C:2023:381.
16. Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models