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

How long can data be retained?

EU and UK GDPR data retention dilemmas in the age of cyber fraud

1. Introduction

Data retention is one of the most debated, yet also one of the most misunderstood, areas of data protection. When a business asks how long it may retain the personal data of its customers, employees or partners, the answer is not simply a list of statutory deadlines, but a deeper understanding of the principle of purpose limitation.

The EU's General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and its British counterpart, the UK GDPR, now also amended by the Data (Use and Access) Act 2025 (DUAA)[1], both elevate the storage limitation principle to a cornerstone: personal data may only be kept for as long as the purpose of processing continues to apply.[2]
This may look like a simple rule, but in practice it amounts to a complex balancing exercise.

The situation is further complicated by the rapid spread of cyber fraud, data breaches and ransomware attacks. On the one hand, organisations ask themselves whether they are retaining enough data in case of possible court proceedings or regulatory investigations. On the other hand, it is precisely the longer retention of data that increases the potential damage in the event of a cyberattack.

This contradiction leads to a paradox of “the more, the safer” versus “the less, the more protected”.
The purpose of this article is to provide a comprehensive, source-based overview of the EU and UK GDPR data retention rules, the differences between the two regimes, current trends in regulatory enforcement, and how these issues fit into the current, increasingly severe reality of cyber fraud and data security incidents.

2. Legal foundations of the retention principle

2.1 The EU GDPR storage limitation

Article 5(1)(e) of the GDPR provides that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.[3] This is not merely a recommendation but a binding principle, breach of which can directly give rise to the supervisory authorities' power to impose fines.
It is important to stress that the GDPR itself does not set specific, generally binding retention periods for the vast majority of data categories. The controller itself, taking into account the applicable legal norms, must determine and document the period during which the purpose of processing justifies retention.[4] This requires industry benchmarks, legal risk assessment, internal policy and sector-specific legislation alike.

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

Exceptions naturally exist: archiving in the public interest, scientific research, statistics, or mandatory statutory retention periods (e.g. accounting law, employment law rules) may justify longer retention.[5] These are, however, exceptions, and the principle of purpose limitation must always be applied in parallel.

2.2 The UK GDPR and the changes under the DUAA 2025

Since Brexit, the United Kingdom has applied its own data protection framework: the UK GDPR and the Data Protection Act 2018. The Information Commissioner's Office (ICO) confirms that the UK GDPR likewise does not prescribe specific retention periods; these must be determined by controllers depending on the purpose of processing.[6]
The Data (Use and Access) Act 2025 (DUAA) received Royal Assent on 19 June 2025, and its phased entry into force continues until mid-2026.[7] The Act amends the UK GDPR in a number of respects: it introduces the new lawful basis of recognised legitimate interests[8], clarifies the exceptions relating to processing and further processing for scientific research purposes[9], and, notably, also imposes retention and preservation obligations on certain organisations in connection with child death reviews.[10]

Under the DUAA, from 19 June 2026 individuals will be able to complain directly to the controller about its data retention practices before going to the ICO - this places a new administrative burden on controllers.[11]

3. Sector-specific retention periods: a compass for practice

Although the GDPR itself does not set specific deadlines, national legislation, regulatory guidance and industry standards set out benchmarks for numerous sectors. The following are generally accepted reference frameworks:

- Employee data (HR): generally 5 years after termination of employment; for payroll matters and social security records, up to 10 years may be justified, based on employment law and social security obligations.
- Customer data (commercial): 3 years from the end of the active contractual relationship, or until the end of the limitation period in the event of a legal claim (generally 5–8 years).
- Accounting documents: 10 years in most EU member states (and in the UK), based on local accounting legislation.
- Health data: highly sector-dependent; in many member states periods of 15–30 years may apply under specific regulation.
- Marketing data (consent-based): until consent is withdrawn, but no more than 2–3 years without active contact; after this, an obligation to erase arises.[12]
- The findings of the EDPB's 2025 coordinated enforcement action (based on the CEF report adopted on 10 February 2026) highlighted that most organisations lack internal data classification systems and automated erasure mechanisms, which is the most

common and most serious shortcoming in complying with the storage limitation principle.[13]

4. The impact of cyber fraud and data security incidents on retention decisions

4.1 Data minimisation as a cybersecurity tool

The global rise in cyber fraud and ransomware attacks is directly linked to retention decisions: the more personal data an organisation stores, the greater the potential damage in the event of a successful attack. This means that a retention policy is not merely a data protection compliance matter, but also a direct cybersecurity strategy.
The principle of data minimisation under Article 5(1)(c) of the GDPR and the storage limitation principle under point (e) are therefore mutually reinforcing principles: deleting unnecessary data reduces the attack surface, while the accumulation of sensitive data in databases represents an ever-increasing security burden.

4.2 The retention dilemma: evidence vs data protection

The retrospective investigation of data breach and cyber fraud incidents creates a particular tension in relation to data retention. On the one hand, affected organisations may need log files, communication records and transaction data for investigative, civil law or other legal proceedings. On the other hand, these are precisely the data that the GDPR requires to be kept for the shortest possible time.
The case of the French CNIL, in which an online payment platform was fined because it failed to delete user accounts that had been inactive for more than ten years, despite its own retention policy, meaning that the data of tens of thousands of accounts remained in the system in searchable form for effectively indefinite periods, illustrates this contradiction well.[14]
The authority found that deactivating an account is not equivalent to erasing personal data, and that retaining data stripped of its purpose infringes Article 5(1)(e).
Similar questions are raised by a 2024 CNIL investigation concerning the data processor of a music streaming platform: the processor retained the personal data of more than 46 million users even after termination of the contract, and even used it for its own purposes.[15]
This case shows that retention obligations apply not only to controllers, but also to processors.

4.3 Backups: the blind spot of compliance

The EDPB's CEF 2025 report found that almost half of organisations have no specific procedure for erasing data from backup systems.[16] This is particularly concerning, since in the event of a ransomware attack, restoring encrypted backup files may bring back to light data that the organisation has already deleted from its live systems. Backups are therefore not exempt from data retention rules, and the erasure obligation extends to the whole of them.

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

5. Enforcement trends and fining practice

5.1 Strengthening enforcement at EU level

By 2025, the aggregate fining activity of EU data protection authorities had increased significantly. In 2025, European regulators imposed a total of approximately EUR 1.2 billion in GDPR fines, a 22% increase compared to the previous year.[17] According to the CMS Enforcement Tracker's 2025 data, by March 2025 cumulative GDPR fines had reached EUR 5.65 billion, across a total of 2,245 enforcement proceedings.[18]
According to CNIL's 2024 annual report, the French authority took 303 corrective measures, of which 87 were sanctions, totalling more than EUR 55 million.[19]
In the proceedings against Free Mobile and its parent company Free, triggered by a 2024 cyberattack affecting around 24 million customer contracts, one element of the fine related precisely to inadequate data retention and erasure practices.[20]
The Dutch data protection authority (AP) fined a well-known streaming provider EUR 4.75 million in 2024 for failing to adequately specify the purposes and legal bases of its processing; the proceedings lasted five years, indicating that the authority is capable of examining an organisation's retention and transparency practices over an extremely long period.[21]

5.2 CEF 2025: the right to erasure in the EDPB's spotlight

The EDPB's 2025 coordinated enforcement action (CEF 2025) focused on the right to erasure (Article 17 GDPR). In the report adopted on 10 February 2026, the EDPB summarised the investigative experience of 32 national supervisory authorities, covering 764 controllers.[22]

The key findings:

- **Missing internal procedures:** many organisations have no documented process for handling erasure requests.
- **Ineffective anonymisation:** many controllers use inadequate anonymisation techniques instead of actual erasure.
- **Undefined retention periods:** a significant proportion of data categories are not assigned a specific retention period.
- **Backup systems:** half of organisations are unable to erase data from their backups.[23]

The EDPB stressed that the findings of CEF 2025 will feed into the sector-specific inspection plans of national authorities for 2026, meaning that the next wave of investigations will focus on enforcing the storage limitation principle.

5.3 The United Kingdom: a pragmatic approach, growing demands

The ICO has traditionally applied a more flexible enforcement approach, particularly towards the public sector.[24] However, the changes introduced by the DUAA 2025 strengthen individual complaint mechanisms and the ICO's powers; it is expected that data retention issues will also receive stronger regulatory attention in the United Kingdom from next year.

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

It is particularly notable that the DUAA brought into immediate effect, as early as 19 June 2025, amendments to data retention provisions relating to counter-terrorism,[25] indicating how strongly law enforcement and national security considerations weigh on traditional data protection principles.

6. Recommended compliance framework

Below we summarise the key steps an organisation should practically take to meet the EU and UK GDPR data retention requirements, with particular regard to cybersecurity risks:

1. **Data retention register:** For every data category, document the purpose of processing, the legal basis and the specific retention period (ROPA). This is not optional, but a mandatory element of the accountability principle under Article 5(2) of the GDPR.

2. **Automated erasure mechanisms:** Without automatic erasure functions built into IT systems, a retention policy that exists only on paper remains an empty document. CEF 2025 identified precisely this shortcoming as the most serious and recurring problem.

3. **Managing backups:** The erasure obligation also applies to backup systems. A documented procedure is needed for how individual erasure requests or expired retention periods are enforced within backup systems.

4. **Data minimisation as a cybersecurity strategy:** Deleting unnecessary data directly reduces the damage that can be suffered in the event of a cyberattack. This is a rare intersection of business interest and statutory obligation.

5. **Linking DPIAs with retention questions:** When carrying out data protection impact assessments (DPIAs), examining the retention period and the erasure mechanism is a mandatory element - several authorities specifically emphasise this.

6. **Monitoring differences between UK and EU rules:** The phased entry into force of the DUAA 2025 is ongoing. Organisations also operating in the United Kingdom need to monitor the ICO's updated guidance.

7. Summary

The question of data retention is not a static list of statutory rules, but a dynamic compliance task shaped by two seemingly opposing pressures. From one direction pulls the principle of **privacy protection and data minimisation**, according to which personal data should be kept for the shortest possible time. From the other direction push **law enforcement and cybersecurity interests**: organisations need data to preserve evidence and logs, to support regulatory investigations, and for the purposes of enforcing legal claims.

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

The EDPB's CEF 2025 report, the 2024–2025 CNIL, AP and ICO fines, and the UK's DUAA 2025 all point in the same direction: regulators' patience is running out with the absence of documented retention policies and implemented automated erasure systems.

In the age of cyber fraud, the safest data is that which is no longer stored. Today, the ROPA is no longer just a document that ends up in the data protection officer's desk drawer, but one of the most important elements of IT security strategy, business risk management and the regulatory compliance programme.

Bibliography

[1] Data (Use and Access) Act 2025 (DUAA), Royal Assent: 19 June 2025. Source:

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), Article 5(1)(e) - Storage limitation principle.

[3] GDPR Article 5(1)(e); see also: Legiscope, GDPR Storage Limitation: Retention Periods by Sector (2026), May 2026.

[4] Pitch Law, Data Retention Policies: How Long Should You Keep Personal Data?, 25 February 2026.

[5] GDPR Article 89 - Exceptions for processing for archiving purposes in the public interest, scientific research and statistical purposes.

[6] ICO (Information Commissioner's Office), 'Principle (e): Storage limitation', UK GDPR Guidance.

[7] Farrer & Co, Data (Use and Access) Act 2025: five key changes for businesses, May 2026.

[8] DUAA 2025 - introduction of the Recognised Legitimate Interests lawful basis; Womble Bond Dickinson, Understanding the Data (Use and Access) Act', 2025.

[9] DUAA 2025 - retention exceptions relating to scientific research; Farrer & Co, op. cit.

[10] Leadership Through Data, The UK Data (Use and Access) Act 2025: What stage is it currently at, 12 February 2026.

[11] National Law Review, 'The Data (Use and Access) Act 2025 and the New Right for Individuals to Complain to Controllers, June 2026.

[12] Legiscope, op. cit.; Secure Privacy, 'GDPR Data Retention Policy & Storage Limitation, March 2026.

[13] EDPB, CEF 2025: Coordinated Enforcement Action - Implementation of the right to erasure by controllers, adopted: 10 February 2026.

[14] CNIL, Decision No. SAN-2023-023 (29 December 2023)

[15] Gibson Dunn, Europe Data Protection - January 2026, 15 January 2026. (CNIL proceedings: music streaming platform's data processor, 46 million users' data).

[16] EDPB CEF 2025 Report, op. cit.; Lexology/Reed Smith, 'EDPB report on the right to erasure: Key takeaways, 9 March 2026.

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

[17] Improvado, GDPR Fines in 2026: A Complete Guide to Enforcement, Penalties, and Compliance', 2026.

[18] Legiscope, op. cit. - based on CMS Enforcement Tracker Report 2025 data, EUR 5.65 billion cumulative fines, 2,245 proceedings.

[19] National Law Review, CNIL 2024 Annual Report: GDPR Fines, AI Rules & Data Breaches, 30 April 2025.

[20] Skillcast, Biggest GDPR Fines of 2026

[21] Smith Law, GDPR Enforcement is Alive and Well - Key Considerations in 2025, February 2025.

[22] EDPB, Coordinated Enforcement Action - Implementation of the right to erasure by controllers, CEF 2025 report, 10 February 2026.

[23] Lexology, EDPB report: Key takeaways - 2025 Coordinated Enforcement Action', 9 March 2026.; Legiscope Comprehensive GDPR Data Storage Compliance Guide 2024 (updated 2026).

[24] Stephenson Harwood, Data Protection update - January 2025,

[25] Corporate Assist, Understanding the Data (Use and Access) Act 2025, October 2025.