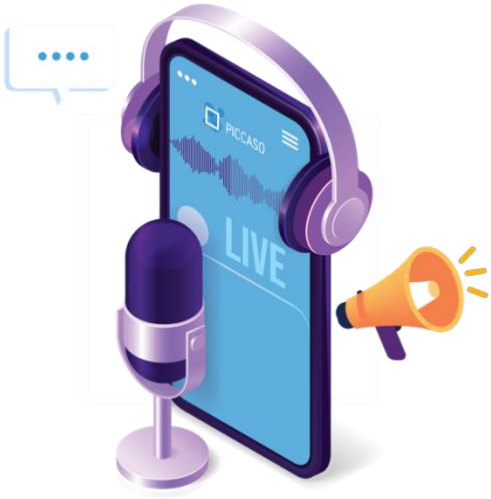
PICCASO

Privacy & Security Insights with PICCASO




# Retention & Deletion

## The Data Lifecycle

Paul Jordan

Chair, PICCASO

PICCASO

Sponsored by

PrivacyCulture

# Retention & Deletion

## The Data Lifecycle

From my viewpoint, one of the more compelling and continuous challenges for organisations in terms of their data processing operations is maintaining stringent and compliant data policies in line with the retention & deletion provisions under the EU-UK versions of GDPR, and or other legal and international data privacy laws. Almost every company and organisation processes personal data. Where data is collected, organised and stored, updated, augmented and further used, possibly forwarded, and then - hopefully and eventually - deleted. The set of processing operations that personal data undergoes forms the life cycle of personal data and needs careful planning and documentation.

As we embrace the digital age with pace, companies and organisations are collecting increasingly vaster quantities of personal (as well as non-personal data) to advance their own relevance and growth strategies to the benefit of both organisations and consumers. With the advent of advanced technology, AI techniques and applications, data processing is becoming more complex and serving increasingly to establish commercial and competitive advantage. Arguably, within this context retention and deletion as an aspect of fundamental and good data governance is one that many organisations may overlook, where the energy and focus is predominantly on how they use and process data. The message here should be a clear one, privacy is no longer an option.

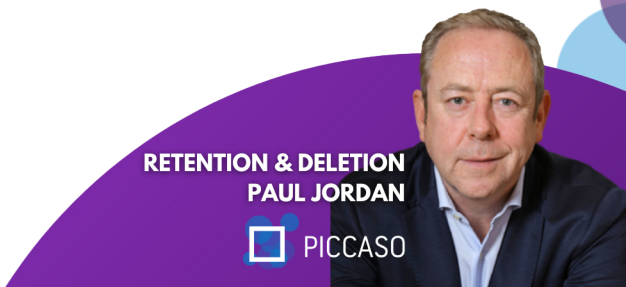
One of the biggest compliance missteps companies make is keeping too much data for too long. In many cases, this can expose an organization to unnecessary risk: It's a bright target for bad actors and compliance officers alike. Not to mention, it can open your organization up to tremendous legal exposure, enforcement action, and reputational damage.

The key principles of data lifecycle management are designed to guide organizations in handling data in a legal, secure, efficient, and compliant manner throughout its entire lifecycle. These principles apply to various data management processes, including data collection, storage, processing, usage, retention, and deletion. Let's look at the guiding principles that will help strengthen your data retention and deletion processes -and your records of processing activities (ROPA) - reducing risk and ensuring greater protection of individual privacy rights under GDPR:

1. **Lawful basis for data retention**: Before collecting and storing any personal data, ensure that you have a legitimate reason and a lawful basis for doing so. This might include the necessity for fulfilling a contract, legal obligations, consent from the individual, vital interests, public task, or legitimate interests.
2. **Define retention periods**: Establish clear and documented organisational policies on how long you will retain different types of personal data. The retention periods should be determined based on the purpose for which the data was collected and any legal requirements or industry standards.
3. **Minimise data collected**: Collect only the minimum amount of personal data required to fulfill the purpose for which it was collected. Avoid unnecessary data collection to reduce potential risks associated with retention. Identify and list the categories of personal data that are processed (ROPA).

4. **Secure data storage**: Ensure that the data you retain is stored securely to prevent unauthorized access, loss, or disclosure. Implement as appropriate encryption, access controls, and regular security audits to safeguard the data.
5. **Inform data subjects**: Inform individuals about the data retention period when collecting their personal data. Provide a clear and concise privacy notice outlining the retention policies and the rights they have under GDPR.
6. **Consent management**: If you rely on consent as the lawful basis for processing data, remember that consent must be freely given, specific, informed, and unambiguous. Allow individuals to easily withdraw their consent at any time, and promptly disuse/ delete their data when consent is withdrawn in adherence with legal obligations.
7. **Data subject rights**: Be prepared to respond to data subject requests promptly. Individuals have the right to access their data, rectify inaccuracies, erase their data (the "right to be forgotten"), and restrict or object to processing under certain circumstances.
8. **Automated data deletion**: Implement automated processes that delete or anonymize personal data when the retention period expires or when it is no longer necessary for the original purpose.
9. **Regular reviews**: Conduct periodic reviews of the data you retain to ensure compliance with GDPR principles. Regularly assess whether the data is still necessary, and if not, proceed with secure deletion. Keep your records of processing activities up-to-date.
10. **Data Protection Officer** (DPO): If you haven't done so, appoint a DPO or a data governance function, as necessary, to oversee data protection and privacy practices, including data retention and deletion across your organisation.

The upside to adhering to these key principles, is that organisations can foster and promote a greater trust with their customers, mitigate legal liability risk, and ensure that data is managed responsibly and with integrity to a high standard of protection.



PICCASO

## Listen now on:

Spotify®

Google Podcasts

YouTube

Apple Podcasts

## About us:

We are a UK based non-for-profit privacy special interest group, led by seasoned volunteers who are senior leaders in privacy and data protection.

The primary aim of PICCASO is to create a community of professionals that share the value of exchanging 'know how', insights, clarity and explanation on specific privacy and data protection topics designed to distinguish between legal requirements, operational implementation, and strategic objectives, with the aim of greater understanding in how to achieve optimal outcomes based on good practice and thought leadership.

The PICCASO community is drawn from across the UK, Europe, and beyond, and from all industry sectors.

## Contact us:

www.piccaso.org
Bouverie House | 154-160 Fleet St | London | EC4A 2DQ
T. +44 (0) 207 112 9360 | hello@PICCASO.org
https://www.linkedin.com/company/piccaso/