

Update May 2019: What Changed?

Four things you may not know about the legal right to possess legacy GDPR data!

What has changed based on feedback from Data Protection Authorities in the one year since GDPR?

- 1. New Risk of Expensive Compliance Orders:** Did you know that recent GDPR audits by the UK Information Commissioner's Office (the ICO) and other EU Data Protection Authorities (DPAs) include the question **"What did you do to transform the legal basis for processing pre-GDPR data so it continues to be legal to possess?"** Penalties include: **(i)** temporary or permanent bans on processing; **(ii)** orders to rectify, restrict or erase data; and **(iii)** fines of up to 4% of annual global turnover or €20 million, whichever is greater, because it involves infringement of rights under GDPR Article 5 (principles) and Article 6 (lawfulness).
- 2. Old Data Can Be Bad Data:** Did you know that under GDPR Recital 171, relating to consent, all data collected using approaches that were legal at the time of collection -- but which fail to comply with the newly-heightened GDPR requirements for consent -- **are now illegal to possess?**
- 3. New Burdens on Data Retention Disclosures:** Are you aware that under Article 15(d), data controllers should disclose in responses to Data Subject Access Request (DSARs) the time period which they envisage storing data collected using consent approaches that were legal at the time of initial data collection but which fail to comply with new GDPR consent requirements?
- 4. Data Controller Obligations and Actions:** Did you know that data controllers have obligations: **(i)** under GDPR Article 30, to document actions taken pursuant to the Guidelines on Consent under Regulation 2016/679 (wp259rev.01) to transform noncompliant data so that it continues to be legal to possess; and **(ii)** under Articles 13 and 14, to disclose the purposes of the processing as well as the legal basis for the processing of previously noncompliant data? Data that was collected in noncompliance with GDPR requirements needs to be transformed so that it is legal for Analytics, AI and Machine Learning -- doing nothing means the data is illegal under Recital 171 since the **GDPR does not have any "grandfather" or savings clause.**

Which of These Actions Works Best for Your Company?

The Guidelines on Consent Require Data Controllers to Select from One of the Following Four Actions for Analytics, AI & Machine Learning to be Lawful Using Pre-GDPR Legacy Data:

- Reconsenting the data:** achieving 100% re-consent to transform data collected in noncompliance with GDPR requirements has been proven impracticable.
- Deleting the data:** thus, eliminating all value for Analytics, AI and Machine Learning;
- Anonymizing the data:** making it impossible to relink to identifying information thereby dramatically reducing the value for Analytics, AI and Machine Learning; or
- Transforming the data to a new legal basis** while ensuring that processing for Analytics, AI and Machine Learning is fair and accounted for, by satisfying at a minimum each of the following:
 - Legitimate Interest processing** in compliance with Article 5(1)(a) and 6.1(f);
 - Purpose Limitation** in compliance with Article 5(1)(b) and 6(4);
 - Data Minimisation** in compliance with Article 5(1)(c) and 25(1); and
 - Storage Limitation** in compliance with Article 5(1)(e) and 89(1).

The only realistic option available for retaining personal data collected in noncompliance with GDPR requirements for lawful Analytics, AI and Machine Learning is to transform the data to another legal basis.

See 5-minute explainer video at anonos.com/video for an overview of what has changed, or contact us at SaveYourData@anonos.com

WHAT HAS CHANGED?

Recent GDPR audits and DPA rulings mean you must promptly reassess whether you have the legal right to possess personal data collected in noncompliance with the GDPR. The following matrix compares how different technologies perform against the requirements for transforming noncompliant data, so it is legal for Analytics, AI and Machine Learning.

See 5-minute explainer video at anonos.com/video for an overview of what has changed, or contact us at SaveYourData@anonos.com

Requirements for Transforming Pre-GDPR Data to be Legal

You Must Satisfy Each of the Following GDPR Principles to Transform Pre-GDPR Data to be Legal:	Anonos SaveYourData GDPR compliant pseudonymization software	Differential Privacy (Privitar, Epsilon)	3rd Party Anonymization Trusts (TrustArc, TrustArc, Data Republic)	Homomorphic Encryption (Inpher)	Encryption/ static Tokenization (Immuta, Protegrity, Privacy Analytics)	Privacy Compliance (OneTrust, TrustArc)
i. Legitimate Interest processing (in compliance with GDPR Article 5(1)(a) and 6.1(f))						
Centralized processing support for "Functional Separation" (cited eight times in WP 217 Opinion on Legitimate Interest)	✓	✓	✗	✓	✗	✗
Distributed processing support for "Functional Separation" (cited eight times in WP 217 Opinion on Legitimate Interest)	✓	✗	✗	✗	✗	✗
ii. Purpose Limitation (in compliance with GDPR Article 5(1)(b) and 6(4))						
Centralized processing support for "Functional Separation" (cited fourteen times in WP 203 Opinion on Purpose Limitation)	✓	✓	✗	✓	✗	✗
Distributed processing support for "Functional Separation" (cited fourteen times in WP 203 Opinion on Purpose Limitation)	✓	✗	✗	✗	✗	✗
Article 6(4) enumerated safeguard	✓	✗	✗	✓	✓	✗
iii. Data Minimisation (in compliance with Article 5(1)(c) and 25(1))						
Centralized processing support for limiting data processed to only that necessary for authorized purposes	✓	✓	✓	✓	✗	✗
Distributed processing support for limiting data processed to only that necessary for authorized purpose	✓	✗	✗	✗	✗	✗
Article 25(1) enumerated safeguard	✓	✗	✗	✗	✗	✗
iv. Storage Limitation (in compliance with Article 5(1)(e) and 89(1))						
Support for ongoing storage of data for statistical purposes using Article 89(1) enumerated safeguard	✓	✗	✗	✗	✗	✗

Contact us at: SaveYourData@anonos.com