



General Data Protection Regulation (GDPR) Right to Erasure Risk Audit

Prepare for GDPR Compliance

After years of negotiations, the European Union General Data Protection Regulation (GDPR) will come into effect on May 25, 2018, replacing the 22 year-old EU Data Protection Directive. GDPR is likely to be recognized as a watershed moment for data security, as it applies to all businesses that hold the data of EU citizens, regardless of whether they are a member of the EU community or have a physical presence in the region. This means that organizations in the UK, US and the rest of the world will have to comply if they've ever done business with an EU resident.

The GDPR Difference

Unlike many checkbox-driven compliance programs, GDPR is a risk-based framework. Because it covers personal data, it's focused on having the right governance structure, policies and operational practices, as well as monitoring, detection, and response capabilities. Significant components of GDPR include:

- Requirements for privacy by design and default, data portability and the right to erasure
- Fines as high as 4% of global annual revenue, or €20 million, whichever is greater
- 28,000 new Data Protection Officers required in Europe

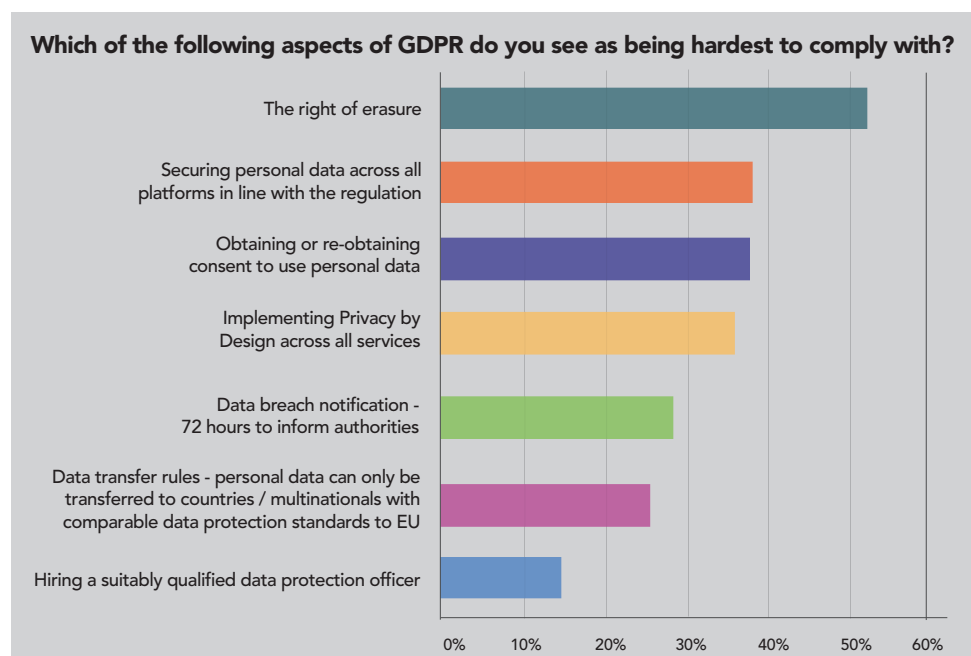
EU Citizens Live Everywhere

As a DPO or the person in charge of safeguarding your organization's data, you should be aiming for GDPR-like compliance with all transactions involving your current and future customers, formally declared as EU citizens or not. Why? Because trying to identify your organization's relevant exposure will eventually become an intolerable burden.

And, the nature of what data needs protection is multiplying with every effort you're making to better serve the customer's interest. We all understand the core data like birthdates, addresses, payment methods, social medicine numbers, etc. but consider the growing data points regarding URL visits, shopping habits, social media relationships, and more. Better to provide the point of protection now and avoid future loss notifications and identity protection service offerings.

GDPR Article 17 – Right To Erasure

Nearly 50% of UK consumers plan GDPR "Right to Erasure" requests, but surveys indicate this is the most challenging requirement of GDPR. Many companies will fail to comply because current 360-degree Single Customer View CRM, Customer Data Integration (CDI), Master Customer Information File (MCIF), and Master Data Management (MDM) hubs are intentionally skewed for high False-Negative match error rates (records not matched that are actually the same person). This creates the risk of future GDPR Article 17 compliance failures.



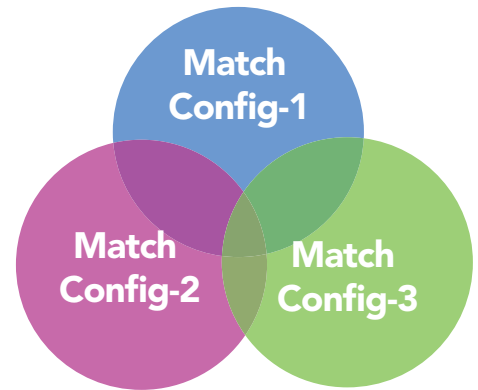
The Right of Erasure is the Top GDPR Compliance Concern, Computing, May 2017.

For a Product Demonstration or Risk Audit Information call 1-800-MELISSA

The Problem of False Negatives

Many companies will fail to comply because current 360-degree Single Customer View CRM, Customer Data Integration (CDI), Master Customer Information File (MCIF), and Master Data Management (MDM) hubs are intentionally skewed for high False-Negative match error rates (records not matched that are actually the same person). This creates the risk of future GDPR Article 17 compliance failures.

DataDelta analyzes this risk by using identity triangulation to compare test iteration results of loose configurations of your current match tool to see how high your false negative match error rates are.



DataDelta’s “Identity Triangulation” on false negatives via alternate match configuration iterations.

Erasure Risk Audit – Powered by Melissa

DataDelta offers two levels of Erasure Ricks audits of your entire customer data hub (not just samples), powered by Melissa Data Quality, to help you understand your risk so you can avoid fines, bad PR and business disruption by demonstrating due diligence to the ICO and other regulatory bodies. Armed with this knowledge you can enhance and extend your current customer match technology investments for GDPR compliance.

- **Fast Audit:** a 1 week analysis and upper bounds estimate of the number of records at risk, requiring no PII (Personally Identifiable Information) and thus avoiding data privacy access delays
- **Deep Audit:** a 4 week rigorous analysis of system at-risk record trends using a copy of your full customer data that remains protected at your datacenter and never leaves your environment

TAX_ID	Lname	Fname	DOB	Gender	Phone	Street	City	ST	ZIP
284725931	Smith	Mario	12/25/06	M	303-699-0606	123 ELM	DENVER	CO	80210
	Smith	M	12/25/06	U	303-699-0606	123 ELM	DENVER	CO	80210
284725932	Smith	Maria	12/25/06	F	303-699-0606	123 ELM	DENVER	CO	80210

Case Detail Report Example: “False Negative” with First Name Typo – or “False Positive” Twins?

About DataDelta

Since 2004 DataDelta, recognized as a Gartner “MDM Cool Vendor”, has been the leader in Match Accuracy Analytics. DataDelta’s patent-pending technology uniquely analyzes entire customer hubs to help optimize match algorithm accuracy for all MDM, CRM and Data Quality vendors, including proprietary home-grown match engines. DataDelta has assisted some of the largest Fortune 500 customer hubs over 1 Billion records in size across industries such as banking, finance, healthcare, pharma and consumer goods.

About Melissa

Since 1985, Melissa has specialized in global intelligence solutions to help organizations unlock accurate data for a more compelling customer view. More than 10,000 clients worldwide in arenas such as retail, education, healthcare, insurance, finance, and government, rely on Melissa data quality and ID verification software, including data matching, validation, and enhancement services to gain critical insight and drive meaningful customer relationships.

Melissa

22382 Avenida Empresa RSM, CA 92688-2112 | 1-800-MELISSA | www.melissa.com

Find us on: