

Data Subject Request (DSR) Automation

Challenges you face:



Incomplete and Disconnected Data Landscape

Personal data is often dispersed across cloud platforms, legacy systems, and third parties. Organizations lack a unified view, resulting in significant effort and resources to fulfil Data Subject requests.

> Risk: Partial responses expose the organization to regulatory penalties and undermine accountability.



Unclear or Difficult-to-Understand Responses

Even when data is retrieved, responses are frequently unclear, poorly formatted, or difficult for the data subject to interpret.

> Risk: This erodes trust and increases the likelihood of complaints or investigations, as seen in recent high-profile enforcement actions.



Missed Compliance Deadlines & Fragmented Workflows

Disconnected emails, spreadsheets, and manual ticketing tools create significant coordination challenges across teams. These inefficiencies frequently lead to delayed responses and missed regulatory deadlines, increasing the risk of penalties and compliance failures.

> Risk: High reliance on manual coordination results in inconsistent execution, scaling issues, and heightened exposure to enforcement actions.



High Cost-to-Serve and Resource Strain

Legal, IT, and privacy teams spend disproportionate time on manual, repetitive tasks such as data retrieval, redaction, and fulfilment.

> Risk: Operational costs increase, and strategic capacity is diverted away from higher-value privacy initiatives.



Poor Data Subject Experience

Data subjects often face long wait times, lack of status updates, and confusing submission portals or responses.

> Risk: Negative experiences can damage brand reputation, trigger formal complaints, and undermine the company's privacy posture.



Limited Oversight and Optimization

Without centralized tracking and analytics, organizations lack real-time visibility into DSR performance, bottlenecks, and SLA compliance.

> Risk: Inhibits continuous improvement and creates gaps in audit readiness, especially in multi-jurisdictional environments.

With an automated DSR approach you can:



Faster request fulfillment



Lower operational costs



Unified platform & insights



Improved compliance demonstration

Our approach:

We position OneTrust as an orchestrator within your DSR operations — enabling seamless coordination across intake, enrichment, data retrieval, and response assembly. While OneTrust supports automation and system integration, KPMG defines the process, governs execution, and aligns every step with your internal controls, compliance needs, and organizational structure.

Phase	What We Deliver
Intake Management	- Assess your current DSR intake process and identify operational pain points - Set up secure, user-friendly channels for individuals to submit requests - Apply identity verification and SLA configurations
Request Enrichment	- Enhance incoming requests with internal references (account IDs, user metadata) - Verify that requests are structured and ready for downstream processing
Data Retrieval & Response Assembly	- Retrieve personal data from connected systems and repositories - Compile GDPR-compliant responses, including metadata and required disclosures
Fulfilment Tracking & Reporting	- Deliver responses securely and in the subject's preferred language - Monitor request progress in real time via dashboards - Track SLA adherence and support audit reporting



**Request
Intake**



**Data
Enrichment**



**Data
Retrieval**



**Response
Assembly**

Added value:

- Tailored to your environment** — Built around your processes, teams, and regulatory needs
- Instant coordination** — Systems are notified within milliseconds to reduce delays
- Less manual work** — Internal effort is reduced, freeing up valuable resources
- Real-time visibility** — Track every request with full transparency and SLA control

Contacts



Benny Bogaerts
Partner

T: +32 (0)38211893
E: bbogaerts@kpmg.com



Laurens Mols
Senior Manager Advisor

T: +32 (0)38211916
E: lmols@kpmg.com



Stephan Idema
Director

T: +31 (0)652755924
E: Idema.Stephan@kpmg.nl



Sebastiaan van Vliet
Manager

T: +31 (0)633028505
E: vanVliet.Sebastiaan@kpmg.nl

Privacy Technology services

KPMG has over 5,000 Technology specialists globally, including deep integration experts to help embed Privacy Technology into your systems of record. We work together with the OneTrust leading privacy platform and global alliance partners to embed KPMG advice and expertise into leading digital platforms.



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2025 KPMG Advisory, a Belgian BV/SRL and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.