

Sprinting to Respond to Data Subject Access Requests

Contending with the Hurdles of GDPR

Tom Barce, Vice President of Thought Leadership, KLDISCOVERY

Helmut Sauro, Regional Director EMEA, KLDISCOVERY

January 19th 2019

LR 2019, Page 1 to 4 (overall 4 Pages)

Before the European General Data Protection Regulation went into effect, seemingly everyone was talking about the pending requirements and potential penalties. Requirements such as the “right to be forgotten,” data pseudonymization, privacy by design, oversight of data processors, appointment of Data Protection Officers, readiness assessments, data breach disclosure requirements and concerns about fines up to 4% of annual global turnover garnered much attention. Now, most lawyers, technology experts and corporate leaders fall into one of four categories: sufficiently compliant, behind schedule, unconcerned or engrossed in responses to Data Subjects. While some believe they are in compliance with all of the substantial requirements to protect personal data, others are scrambling because their initiatives are behind schedule. Moreover, a few business leaders have decided to chance using a minimally compliant strategy by not significantly investing in initiatives such as data pseudonymization or simply hiring a third party representative to act as their Data Protection Officer; and taking a “wait and see” approach to how the GDPR is leveraged by Data Subjects and enforced by authorities. Meanwhile, an increasing group of companies are contending with a growing number of access, deletion and remediation requests from Data Subjects.

1

Many organizations who must comply with the GDPR have been focused on appointing a Data Privacy Officer, displaying GDPR compliant notices on their websites, updating employment contracts, training staff, organizing a response plan, assessing their organization’s readiness, requesting compliance agreements from subcontractors and software providers, and maybe even conferring with outside counsel. Some readers who should be more compliant with the GDPR by now are uncomfortable because they are behind schedule on a number of the aforementioned initiatives already. The GDPR requires routine, well integrated maintenance, while nevertheless, managing your business every day. In fact, the required rigor is increasing.

2

I. Motivating Factors

Individuals are progressively relying on Data Subject Access Requests (DSARs) to learn what information a company might have about them in light of increased public awareness, interest and, sometimes, outcry about personal data security and management. This phenomenon stems from the proliferation and global distribution of digital data. So, companies are learning firsthand what all the commotion leading up to the effective date was about. The GDPR is chief amongst global legislation that increasingly favors the rights of Data Subjects over employers, controllers and processors. International organizations are also wise (or forewarned) to heed the material impacts of the regulations because they apply to any organizations concerned with personal data of Data Subjects within the EU, "...regardless of whether the processing itself takes place within the Union."¹ 3

Naturally, corporate concerns are intensifying about the potential impacts of DSARs on active or potential legal claims, 30-day deadlines, precise responses, sensitive company data, scrutiny from authorities, concerns about fines and budgetary pressures. In addition, various sources or locations of data potentially relevant to a routine DSAR cannot be underscored enough. The rate of innovation, adoption and replacement in technologies, especially communication mechanisms, creates an on-going conflict with effective responses to DSARs. Often times, requestors such as former employees or savvy customers have prior knowledge about how your organization generates and stores information. This leaves room for responses to be scrutinized, deemed incomplete and successfully appealed, thereby opening up potential scrutiny from the Information Commissioner's Office or other authorities. 4

II. Winning the DSAR Race

As we have seen an exceptional influx of DSAR projects, organizations are alleviating the burdens of the DSAR process through the use of cutting-edge technology and professional experts. Many years of experience in successful, precise data retrieval and production are necessary to effectively collaborate on and execute strategies for systemically addressing DSARs. By aligning seasoned experience and technology driven by experts with the specific requirements of DSARs, companies responding to requests can maintain a repeatable strategy, proven to effectively and defensibly respond to requestors by utilizing an interdisciplinary approach to deliver streamlined, cost effective and high quality results. 5

In our experience, a unique and thorough response to DSARs can be achieved through the combination of the following strategies: 6

¹ Paragraph 22 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Official Journal of the European Union, 4 May 2016

- Thoughtful data identification and collection, combined with excellent data processing, searching, and de-duplication to specifically, appropriately and thoroughly target unique documents that are most likely to be relevant.
- A customizable document categorization framework, which by default, is set up to allow reviewers to tag documents that can be disclosed, need to be redacted, should be reviewed for sensitive information or might be withheld based on specified grounds for exemption.
- Automated workflows for documents to be routed to specific reviewers, based on document tagging, timeframe for review or language.
- A custom review and production solution, which simplifies the approach to documents requiring numerous pages of redactions, by enabling clients to simply identify the individual page(s) to produce and eliminating the need to redact completely non-responsive pages. This, combined with Native Spreadsheet Redaction, is especially useful to many organizations as data about Subjects are often found in large compilations, reports or spreadsheets and also intermingled with sensitive information.
- Native Spreadsheet Redaction, which allows reviewers to redact content from Excel files without the need to convert to tiff images. Options for redactions include removal of rows, columns, worksheets, formulas, cells, and standard text redactions.
- Strategic and thoughtful use of Artificial Intelligence, data analytics and predictive coding to identify and prioritize highly relevant material.
- European based Advanced Review Services teams, who are accustomed to utilizing all of the above approaches to finalize responses.
- Weekend and evening support, especially in light of the time-sensitive nature of responses to DSARs.

III. Running the Marathon

More than ever before, companies and their counsel need reliable solutions to manage responses to DSARs. Answering every DSAR amidst more incoming demands for information creates competing priorities. Therefore, respondents and stakeholders need to formulate sustainable, long term strategies to improve their overall approach to requests. There is little reason to believe demands for data from EU Subjects will decline, especially when responding corporations bare all of the costs. While there tends to be inherent contentions between innovation, profit and sound data management, these differences need to be overcome in order to avoid DSAR missives. In addition to the immediate success path to any response discussed above, stakeholders can be well served in the long run by considering the following strategies:

- Be proactive about instituting streamlined day-to-day data management strategies and managing information as well as any other tangible asset.

- Align with a reliable technology enabled service providers who can deliver a DSAR response strategy that will help mitigate risk, namely through the following measures.
- Consider technology that can help you identify personal data in real time; remediate personal data on file shares and other data sources; and manage data retention.
- Ensure GDPR compliance is extended to backup tapes, including audit, migration, recovery, and personal data remediation.
- Maintain erasure verification services to establish proof of disposition and generate records demonstrating appropriate technical safeguards.
- Consider data erasure software and hardware to securely dispose of end-of-life data on any type of storage media.
- Office 365 Security and Compliance subscribers can leverage the power of Microsoft's GDPR investments to improve compliance.

Confidently beating the clock to respond in time requires preparation. Through all of the aforementioned considerations, those with a stake in DSARs will enter the GDPR arena knowing exactly where they stand. Companies should be ready to respond by lining up the best expertise, procedures and technology including all of the elements and solutions discussed above.

9