



White Paper

APRIL 2018



Litigation and Practice Support

Leveraging Strategy and Modernizing Services

ABOUT ILTA

Technology solutions for law firms and legal departments get more complex every day. Connecting with your peers to exchange ideas with those who have “been there done that” has never been more valuable. For over three decades, the International Legal Technology Association has led the way in sharing knowledge and experience for those faced with challenges in their firms and legal departments. ILTA members include firms of all sizes and all areas of practice, all sharing a common need to have access to the latest information about products and support services that impact the legal profession.

STATEMENT OF PURPOSE

ILTA is the premier peer networking organization, providing information to members to maximize the value of technology in support of the legal profession.

DISCLAIMER

This report is designed for use as a general guide and is not intended to serve as a recommendation or to replace the advice of experienced professionals. If expert assistance is desired, the services of a competent professional should be sought. Neither ILTA nor any author or contributor shall have liability for any person's reliance on the content of or any errors or omissions in this publication.

COPYRIGHT NOTICE

Copyright © ILTA 2018. All rights reserved. No part of this report may be reproduced in any manner or medium whatsoever without the prior written permission of ILTA. Published by ILTA c/o Editor, 1431 Opus Place, Suite 110, Downers Grove, IL 60515.

We are pleased to present the 2018 ILTA Litigation Support white paper.

by Richard W. Brooman and Gillian Glass

This publication consists of two parts: educational articles and survey results. This cumulative intelligence provides insight into the business and practice of litigation support, where the industry is today, and how we are innovating for the future, from the perspective of your peers.

The articles reflect the broad spectrum of our work and the varied backgrounds of our writers. Litigation support is practiced in organizations large and small, locally, and across borders. The articles highlight the changing privacy and security landscape with GDPR, discuss the increased demand for professional development vis-à-vis certifications, and provide resources for managing your team. The content extends to modernizing operations, navigating mergers, and leveraging business intelligence to manage costs.

ILTA's annual Litigation Support survey complements the articles, uncovering the trends that drive our content. The survey results show the division of labor between in-house and service providers, growing maturity in the use of targeted analytics and machine learning, and heightened demand for industry certifications. While the polling suggests the billable hour still dominates, we see alternative pricing challenging the status quo. We also see the SaaS market growing as firms and legal departments move to cloud-based systems.

We hope you take a nugget of knowledge back to your legal department or firm, share with a colleague or friend, or pay it forward by educating others. A big *Thank You* to the [ILTA Litigation Support Content Coordinating Team](#) and the survey team for their leadership, ideas, and words, and the editorial staff for editing and curating the content!

GDPR and Privacy Law Evolution in the EU

by Debbie Reynolds



On May 25th, 2018 the EU's Global Data Protection Regulation (GDPR) goes into full enforcement. The GDPR is a new law that provides legal protection and redress rights to EU persons wanting to exercise their data privacy rights no matter where in the world their data resides. The GDPR was enacted to protect the data privacy rights of EU persons in countries like the United States that do not have the same stringent data privacy laws as the EU. Any company that provides goods or services to persons in the EU or handles their data must abide by this regulation or face fines of up to the greater of 4% of their company's worldwide annual gross revenue or 20 million pounds (currently about 27.9 million U.S. dollars).

Since World War II, when personal information was used by Nazi Germany to make life or death decisions about individuals, the EU has regarded individual privacy as a fundamental human right. As personal data flows across borders in our modern digital age, the GDPR is designed to help individuals, also known as "data subjects," exercise that fundamental right to privacy and make decisions about the use of their data. The GDPR replaces the EU's previous Data Protection Directive (95/46/EC) enacted in 1995. The GDPR is more expansive than the Data Protection Directive and is an enforceable law that applies immediately to all of the EU rather than requiring individual member states to pass legislation.

For organizations that use data from EU data subjects, the idea is that an individual's right to data privacy may supersede a company's right to use this data for business or legal purposes will cause a fundamental shift in how those organizations manage individual data privacy rights in the future. Three significant

issues addressed in the GDPR will impact any company dealing with EU data: management of consent, data breach notification, and privacy by design.

Consent

In order for EU data subjects to have ultimate control of their data, companies must provide them with a mechanism for obtaining and managing their consent. According to the GDPR Articles, consent must be given freely by the EU data subjects, who must be clearly instructed about the consent they are giving. Data subjects can request to see any data collected about them and can revoke consent at any time; they can also choose to have their data returned to them. If data must be

obtained from an EU data subject, the data controller/data processor - the company using the data - must have processes, procedures and technology in place to manage all the variables around an EU data subject's consent. For example, for handling GDPR consent as it relates to ediscovery data collection in litigation, it is recommended that EU data subjects be given notification much like a litigation hold notice that details the data sought, the reasons for requesting the data and when the data will be erased after use. Data from EU data subjects cannot be re-used for purposes other than those initially intended unless additional consent is obtained from the data subject. All data controllers/data processors must develop ways to erase or return data in instances where an EU data subject has revoked initial consent. Managing consent of EU data subjects will be a critical element in developing techniques to comply with the GDPR.

Data Breach Notification

The GDPR requires that companies who possess data of EU data subjects must inform the EU's supervising authorities of any company data breach within 72 hours of becoming aware of the breach and must also inform the individual EU data subjects of the breach in a timely manner. The 72-hour data breach notification timeline can be extraordinarily short and will require the data controller/data processor to have processes, procedures and technology in place to comply with the immediate data breach reporting requirements. The GDPR has outlined very detailed information that a data controller/data processor company must provide as part of breach notifications to both the supervising authorities and the EU data subjects.



**DEBBIE REYNOLDS**

Debbie Reynolds advises Fortune 500 companies on data privacy and the management of electronic evidence in high-stakes litigation. Ms. Reynolds is also an adjunct professor at Georgetown University, guest lecturer at various law schools, published author and speaker on the impact of global data privacy in legal matters.

Privacy by Design

Privacy by design will be one of the most challenging parts of the GDPR to achieve. Privacy by design and by default calls for all data controllers/data processors who deal with information of EU data subjects to proactively build privacy into policies, procedures and technology instead of being reactive to EU data privacy regulations in the GDPR. When companies have data complaints from EU data subjects, the GDPR's supervising authorities in the EU have the power to investigate the mechanisms companies have developed to comply with the GDPR as part of their business processes. The challenges with GDPR privacy by design was highlighted in a January 2018 German court ruling in a case brought by The Federation of German Consumer Organisations (VZBV) against Facebook. The German court found, among other things, that the design of Facebook's pre-ticked checkboxes in their privacy center violated the privacy by design and by default concepts under current German law. The same privacy by design and by default requirements are also found in the GDPR. Although the GDPR will not be fully enforced until May 2018, the privacy by design concept, as seen in the German Facebook case, will require some navigation from companies when they must manage data of EU data subjects.

The GDPR has been developed to create a cohesive data privacy framework governing the use of data belonging to persons in EU countries; once in full effect, it will be one of the most comprehensive data privacy laws in the world. GDPR readiness is a massive undertaking for any organization, and it remains to be seen how companies worldwide will manage compliance with the GDPR on May 25th, 2018 and beyond. **ILTA**

