#ForensicPerspectives

GDPR and E-Discovery

Eight ways to adapt electronic discovery to the general data protection regulation

1 Align the data processor, client, vendor, and law firm

In lieu of direct consent from the subject of the information, the GDPR allows processing of personal data for "legitimate interests pursued by the controller (or by a third party to which the data is disclosed) except where the controller's interests are overridden by the interests, rights or freedoms of the affected data subjects.)" Assuming the effort is reasonable and necessary, as well as sensitive to data privacy rules, most e-discovery participants would be acceptable processors.

2 Re-evaluate your indemnification provisions

Given the shared responsibilities of data controllers and data processors, it is critical for litigants to recognize the risks and renegotiate their indemnification provisions.

3 Obtain consents

A data subject can provide valid consent through a written statement, which can be electronic, or an oral statement, such as affirmatively checking a box on a web page, rather than agreeing to a box that is pre-checked. This is a critical distinction when attempting to collect ESI.

4 Honor data access requests by former employees

Controllers must provide access within 30 days to documents requested by former employees who are EU citizens, requiring rapid collection, processing, and hosting.

5 Recognize the right to be forgotten

E-discovery professionals can provide guidance on identifying and filtering material for defensible disposition.

CRA Charles River Associates

6 Redefine the location of data

Remotely accessing data that is physically in the EU from outside of the EU constitutes a cross-border data transfer. To prevent data location disputes, it is critical for data controllers and processors to engage in detailed information mapping and classification. This should include routine assessments and a periodic gap analysis.

7 Avoid confusion in the cloud

A data controller must report a breach within 72 hours, or explain why it could not do so, and alert the person to whom the information belongs. The processor must notify the controller. Both will likely need to implement more advanced technology that can adhere to the accelerated time frame.

8 Work with an outside provider to ensure compliance

- With a myriad of changes, many new definitions, and millions of dollars in potential fines, engaging an outside provider may provide a key competitive advantage.
- Compliance requires support for information mapping, data classification, assessments, gap analyses, policy drafting, procedure development, and defensible data disposition.
- Many organizations are also enlisting outside support for information governance training.
- Savvy teams recognize the need for mobile solutions when locally processing and hosting data on site. They use briefcase data centers and secure online hosting, featuring the ability to search, review, and produce records.

Work with independent e-discovery experts

GDPR enforcement will continue to evolve and complicate e-discovery. CRA's Forensic Services team offers expert guidance in these matters. Our experts combine expertise in forensic accounting, computer forensics, technology, valuation, and business intelligence. To continue the conversation, please contact one of the experts listed below.

Kristofer Swanson, CPA/CFF, CFE, CAMS
Vice President & Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com

Josh Hass, CFE, CEDS
Vice President, Forensic Services
+1-212-520-7139 | jhass@crai.com