MAY 21, 2019

Legaltech news ONLINE

An ALM Publication

GDPR: Brave New World or Business as Usual for E-Discovery?

BY BENJAMIN SEXTON, JND AND MAREN STRANDEVOLD

In the first year since its adoption, the General Data Protection Regulation (GDPR) has caused widespread panic, much of which is due to its slightly impenetrable drafting. A proliferation of misinformation has resulted in many businesses and industries addressing data privacy with a nearly-paralyzing level of caution. This article explores the impact of the GDPR on the e-discovery industry and demystifies some of the less-discussed provisions and exemptions.

Photo Credit: mrmuhh/Shutterstock.com

When Does the GDPR Apply?

On its surface, the GDPR appears to have a broad reach: It applies to all processing of personal data where the data forms part of a filing system. As such, it may appear that the GDPR applies to all activities typically undertaken in an e-discovery project ("processing") and to almost every circumstance where information about an individual exists ("personal data").

However, in reality, the GDPR is focused on protecting individuals and safeguarding data from data processing giants like Facebook and Google, not on restricting the flow of information or legitimate uses of data. This is evidenced by paragraph 15 of the preamble:

"Files or sets of files [...] which are not structured according to specific criteria should not fall within the scope of this Regulation"

This provision is important because it establishes a distinction between normal, everyday usage of data such as an individual's mailbox and loose files (unstructured data) and carefully structured pools of information such as a customer database of contact details (structured data).

Structured vs. Unstructured Data

In the information age, we are constantly contributing to a subterranean mountain of structured data. As we know, a single Google search can forever alter the ad content curated across your social media channels. Somewhere in a climate-controlled catacomb of servers, a carefully organized database stores a record with your name, age, sex, location, and search history, alongside billions of data points on other consumers. For advertising giants, fraudsters and identity thieves, such data is a gold mine.

This is structured data—precisely what the GDPR is designed to protect, and it's no wonder why. Due to the prevalence of personal information and the ease of access, structured data presents a much higher risk of exposing personal information than unstructured data.

In a recent consumer protection matter, among the usual ESI, MSGs, PDFs and MS Office files, we were asked to collect a single .BAK file containing a SQL database of consumer information—structured data. The single file contained 225MM account records with the name, sex, age, location, financials, and social security numbers for each individual. While all data deserves protection, this single file of structured data could do far more damage in the wrong hands than the rest of the discovery combined.

Those of us who have spent time in the trenches will note that unstructured data comprises the vast majority of electronic discovery. Understandably so, as electronic evidence more commonly resides in the form of a communication, contract or meeting minutes than in a database of consumer purchase histories.

According to Anant Jhingran of IBM Research, 85% of ESI stored by businesses is unstructured. Consequently, classifying the types of data owned by a corporation is a critical step in understanding your obligations under the GDPR because, in many cases, the more stringent aspects may not apply.

The Litigation Exemption

For data that does fall in-scope of the regulation, GDPR provides that Member States may provide exemptions for data that is being processed as part of legal proceedings, but they are not required to do so. It is important therefore, to check the local law on this point to determine whether you fall within the scope of the GDPR.

By way of example, the French Data Protection Act allows processing of data without consent where it is required to comply with any legal obligation. It also allows for transfer of data out of the jurisdiction if it is required to meet legal obligations or to pursue or defend legal claims.

In England, there is an exemption where a data controller is required to disclose data by an enactment, rule of law or an order of a court or tribunal. This provision is broad enough to capture discovery in connection with legal proceedings including prospective legal proceedings and taking legal advice.

On that basis, e-discovery activities such as data collection and processing would be exempted from the GDPR, even when undertaken proactively at the start of a dispute but before legal proceedings have officially commenced.

It is important to note, however, that the litigation exemption only reduces the obligations relating to the processing of data, and provisions regarding data security will still apply.

Actionable Takeaways

- The more stringent aspects of the GDPR do not apply where discovery only includes mailboxes and loose files. Sensitive data should still, of course, be safeguarded according to industry best practices.
- If you encounter structured data during e-discovery, be particularly mindful of obligations to safeguard the data and the penalties for breaching those obligations.
- Most jurisdictions have exemptions for the processing of data pursuant to litigation or legal obligations.
- An EU corporation may be fully compliant with the GDPR while utilizing a U.S. vendor for processing and hosting. U.S. e-discovery companies should consult with overseas clients to understand the types of data at issue, and any jurisdictional obligations their clients face.

When it comes to the privacy and security of personal information, a cautious approach is prudent and should always be the default. However, it's important to remember that the GDPR wasn't designed to hamstring litigators, and, for e-discovery practitioners, often may not apply. If your practices pre-GDPR were robust and defensible, it may be that nothing needs to change. However, be aware of the types of data you deal with most and know your specific jurisdictional regulatory environment.

Benjamin D. Sexton *is Vice President of eDiscovery and Analytics at JND in Minneapolis, where he advises corporations on deploying the proper policy, process and technology to meet discovery goals and reduce risk. JND is a RelativityOne Certified Partner. He can be reached at ben.sexton@jndla.com.* ***Maren Strandevold*** *is a commercial litigation Attorney at Haynes & Boone, LLP in London, UK. Maren's practice focuses on disputes in the energy and infrastructure sector, ranging from offshore construction and shipbuilding to agency and commercial contracts. Maren can be reached at maren.strandevold@haynesboone.com.*