

Does the European Union have the Technical Expertise to locate GDPR Indirect Identifiers in your disparate Data?

If so, passing an EU GDPR audit may be more difficult than you expected.

Indirect identifiers are fields that give you the ability to identify personal information exposed through indirect relationships with a direct identifier, such as a diagnosis id, a phone number or some other value that allows positive identification of an individual. If personal information is exposed, either directly or indirectly, the burden is on companies under GDPR guidelines to reasonably protect the identity of individuals.

The real obstacles will be having methods that can identify the information in your customer hubs and legacy systems that provide the means to indirectly identify personal information. Such information, whether contained in database table, PDFs stored on your portal, metadata tagging images stored in your image processing system or word documents and other desktop sourced documents stored in your email server will come under the scrutiny of the regulators enforcing the European Union's General Data Protection Regulations (GDPR).

The EU has promised to make examples of those intentionally or unintentionally failing to meet the scrutiny of protecting consumer information as required by the GDPR regulations. To date, the EU has made examples of Facebook and Google, and is intent on requiring companies to protect consumer data even if it means bankrupting those taking the regulations lightly.

[Alphabet's latest earnings call](#) was somewhat bittersweet, as the company exceeded expectations [yet again](#), but also faced a decline in profits owing to the [record fine of £2.1bn \(\\$2.7bn\)](#) imposed on it by the European Union. Google's parent company brought in \$26bn (£19bn) in revenues, a 21% growth year-over-year, while the profits for the three months ending June 2017 were \$3.5bn, a 30% decline as compared to last year. Interestingly, without the fine, the profits would have been almost 40% higher. The company is [preparing an appeal against the verdict](#) which, should the corporation be successful, could boost the company's revenues in the future. On the flip side, however, the EU is also preparing to deal out [another huge fine](#), which could spell out more troubles for the Mountain View-based firm.

Many companies have built services around the assurance that customer information will be available to their teams according to the team's area of operation, and that access to this data will be granted through corralled cloud services and big data repositories. Teams will have access to this personal information whether their members or partners are located in New York, London or Tokyo.

We have all witnessed examples of exposure of personal and financial data through cyber-thefts, and have begun to witness companies, such as Dow Jones, who have placed this highly sensitive personal information in the cloud so that subscribers of theirs could access the necessary information to enrich their understanding of consumers they are interfacing with. Cloud leak, or the unintentional exposure of this personal information through insufficient controls engaged by partners housing data on behalf of companies, such as Dow Jones is not a defense for failure to meet the demands of GDPR regulations.

A software product that could identify and sequester such exposures, whether housed within the four walls of an enterprise or pushed into the domain of a partner who houses such data on behalf of the enterprise, is required to easily identify direct and indirect identifiers of consumer information that could be construed as violating GDPR, CDP, PrivacyShield, or other regulations surfacing around the globe intended to protect individuals from cyber-threats posed against organizations housing their data.

BigDataRevealed does have a single software product currently available, running on a single open source platform (Apache Hadoop), with the above capabilities. Our process of protecting the identity of individuals through direct and indirect relationships is accomplished using our SecureSequester processes. We believe we are the only firm that can make that claim.

BigDataRevealed will be releasing its release 2.3 of the software for limited production release during mid-August 2017, which will include the capability of assisting in meeting the GDPR obligations companies have in protecting the identify of individuals, whether exposed through direct identifiers or exposed through indirect relationships, whether data is sourced from database tables, portals, cloud sources, big data environments or streams of data. info@bigdatarevealed.com www.bigdatarevealed.com <https://vimeo.com/224269768>