

Are you trusting in the right Partner/Leader for your EU GDPR Compliance?



In the digital economy, it is information that is crucial to extracting, extending, capturing or protecting value. And privacy information is absolutely required to interface with consumers in Business to Business, Business to Consumers and Business to Business to Consumer frameworks so that information can be catalyzed into revenue generating transactions. Regulators have begun passing rules to protect consumers from cyberthreat, but organizations should be much more concerned about the willingness of consumers to participate in an organization's digital storefront than the potential payouts imposed by regulators. But both a willingness of consumers to participate in your digital storefront and satisfying regulators with the ability to comply with the likes of GDPR, PrivacyShield, IDP and a host of other regulations devised to give consumers the right to be forgotten. The following questions are devised to be a self-assessment of your ability to provide consumers their right to be forgotten.

- (1) Can you identify at any point in time what information about a consumer you have on hand, whether it is within your four walls, within a cloud environment or within a partner's environment for your convenience?
- (2) Do you have a mechanism to find personal information within all the files and databases that potentially store personal information, whether or not the information is stored in the data columns it was intended to reside in?
- (3) Do you have a well devised process to obfuscate personal information to protect yourself from successful hacks?
- (4) Do you have a defined secure environment to hold privacy information so it can be provided to people and systems with appropriate privacy keys? Is the method privacy information is extracted sufficiently complex so hacking attempts against the defined secure environment are marginalized?
- (5) Do you have a program so that when consumers demand to trigger their right to be forgotten from the systems within your four walls, on partner's environments, on platforms used in your digital ecosphere and backup environments residing onsite and offsite, you can react expeditiously without major effort and disruption, both of which will result in regulatory failure?
- (6) Do you have a program to secure the information housed for analysis, which in most cases includes personal identifiable information (PII). This information in many cases is stored in a big data environment to simplify the analysis, but also increases the ability for hackers to walk off with privacy information?
- (7) Does your privacy program include all information, such as that locked up in digital documents (Adobe PDFs with and without signatures), images (X-Rays, Insurance Claim pictures, contract images, etc.), all of which can be stripped of privacy information to the sophisticated hacker?
- (8) Is the program you devised autonomic, will it stop hacks without human intervention?
- (9) Have you developed a program to educate your employees and the employees of partners housing data for your convenience on what your program is and what you expect of them so that you can comply with regulations and protect the information required to participate in the digital economy?

If you would like to schedule a short session on discussing how BigDataRevealed approaches the right to be forgotten, have an expert discussion on what the risks and pitfalls of your privacy program are and understand what privacy rules you will be faced with for the foreseeable future, please contact us at privacyinfo@bigdatarevealed.com.