What is GDPR?

GDPR, or the General Data Protection Regulation, is a privacy law established by the European Parliament to increase security for the PII of EU citizens. Its objective is to return control of personal data to individuals, and facilitate international business by creating a standard across the EU. The regulation will come into full effect on May 25th, 2018.

Some notable impacts of the law include:

- Mandatory appointment of Data Protection Officers for corporations that have personal data processing as core activities
- Notification of a supervisory authority after a breach of personal data (typically not more than 72 hours after the breach was realized
- Encouraged pseudonymization (rendering data anonymous or the subject unidentifiable) with personal data assets
- Support for the right to erasure ("right to be forgotten") from data collections / searches

Of these, "the concept of personally identifiable information [PII] lies at the core of the GDPR," writes the International Association of Privacy Professionals (IAPP). From the GDPR, IAPP specifically refers to Recital 75, which instructs controllers to "implement appropriate safeguards to prevent the 'unauthorized reversal of pseudonymization.' To mitigate the risk, controllers should have in place appropriate technical (e.g., encryption, hashing, or tokenization) and organizational (e.g., agreements, policies, privacy by design) measures separating pseudonymous data from an identification key."

Proven Data Protection

With these new regulations, it will not only be a good idea to protect PII, but it will be required by law. The penalties for non-compliance are severe: up to €20,000,000 or 4% of the previous year's worldwide turnover, whichever is greater. The best time to ensure your compliance is not shortly before (or, even worse, after) the regulation has gone into effect. Proactive compliance with the law will protect you when it goes into effect, and will provide you a buffer to guarantee the law is followed before you risk being sanctioned.

For the GDPR, as with other data privacy laws worldwide, it is important to have a powerful and extensible technology to protect PII. Proven PII discovery and anonymization software in the award-winning IRI Data Protector Suite -- include the IRI FieldShield (or IRI CellShield) data masking products and the IRI Chakra Max database firewall -- or the full-stack IRI Voracity data management and governance platform, deliver the rule- and role-based data-centric audit and protection capabilities you need to locate and classify, mask (encrypt, pseudonymize, redact, etc.) PII, remove records of those wishing to be forgotten, and prove compliance with the GDPR.

IRI's PII discovery capabilities work across any database and legacy / document file format, and its masking capabilities work in structured and semi-structured sources (with unstructured sources pending). Affordable licensing, implementation, and support services are available from authorized IRI representatives throughout the EU and beyond.

Related Articles

Breached But Still Protected

Format-Preserving Encryption

What is Data Pseudonymization?