Seal
CONTRACT DISCOVERY AND ANALYTICS

GENERAL DATA PROTECTION REGULATION (GDPR)
ARE YOU READY?

Protection of Personal Information

In most parts of the world, there are rules and regulations for how companies must protect and manage personally identifiable information (PII). PII includes information such as passport data, credit card and banking information, healthcare information, or any other sensitive data that can be associated to an individual.

Laws have been inconsistent and have varied widely in the level of data protection they mandate, but it had not been a major concern as breaches of PII were relatively rare.

In recent years, the amount of personal data stored by companies and governments has exploded, prompting the creation of a new and standardized regulation called **General Data Protection Regulation** or GDPR.

What is GDPR?

GDPR is a comprehensive set of new rules defining how PII data must be managed. While drafted and enacted by the EU Parliament, it is not just for European companies but any company doing business in Europe or with European customers. GDPR becomes enforceable May 25th of 2018, and penalties for non-compliance are harsh. They include fines up to €20,000,000 or 4% of annual revenues for certain offenses, and companies are now scrambling to set up and implement GDPR compliance initiatives.

While GDPR includes a comprehensive set of mandates addressing the processing and management of PII, the extraction and analysis of data within contracts plays a very important role in compliance.

There are 3 specific areas where contracts are key to GDPR compliance, including:

1. Ensuring data breach definitions and obligations, as defined in contract documents, are understood and comply with GDPR requirements.
2. The location of all PII (passport data, credit card and banking information, healthcare information, etc.,) that may exist as “dark data” within the organization.
3. Confirming contractual agreements with data processors or other vendors that may come into contact with PII have appropriate clauses and a defined scope.

Ensuring Contracts Have Proper Language for Data Breach

The goal of GDPR is reduce or prevent exposure of sensitive personal information in the event of a data leak, so preparation is key. Contracts must contain language which describes what exactly constitutes a data breach, and then the specific obligations and legal rights in the event one occurs.

The definition of a breach is vague, but is considered to occur if the breach may "result in a risk for the rights and freedoms of individuals." When there is a breach, it is important to understand the point of entrance for the breach, and also the obligations of all parties for notification. Did it occur through the fault a vendor/supplier? If yes, do contracts have indemnification language allowing for compensation for any loss? Are there proper insurance clauses and coverage that covers for any loss? It is important to ensure adequate protections are built into all contracts.

Notification or other obligations as a result of data breach are also now being mandated in GDPR rules, meaning obligation clauses in existing contracts are no longer valid. Obligation language should be found and revised in all contracts to reflect GDPR rules, and to avoid any confusion by either party in case one occurs.

Shedding Light on "Dark Data"

A serious challenge with GDPR compliance is the untold amounts of "dark data," or data hidden in unstructured content. This can be in both searchable and unsearchable document formats across an organization, and if dark data includes sensitive information such a payment information, passport information, health information, or other PII, it needs to be identified and processed according to GDPR regulations.

Seal Contract Discovery and Analytics locates dark data. It converts unsearchable documents to a searchable format, and then locates and extracts the PII within documents. Once found, an organization can protect the data and process it accordingly.

GDPR also allows for individuals to ask if their personal data is being captured and processed, and if it is, the organization must be able to produce copies of their personal data in electronic format. This is another reason why finding PII in dark data is critical.

Proper Language in Vendor Contracts

Organizations are also tasked with ensuring contracts contain provisions regarding the tasks and responsibilities of any suppliers or agents that might be handling data. This includes how and when data will be returned or deleted after processing, and the details of the processing, such as subject-matter, duration, nature, purpose, type of data and categories of data subjects.

Proper Language in Vendor Contracts (continued)

This presents a challenge as some of this data may come in the form of scanned documentation in image formats, and digitized contracts are often spread across an organization's entire contract corpus. And even if all of an organizations processor contracts are located in a central repository, these contracts will still have to be manually reviewed; a long and expensive process.

How Seal Can Help

GDPR requires a clear understanding of PII, whether it is hidden in dark data or not. Seal can discover contracts across the network, OCR image and non-searchable formats, and locate and extract PII data. It also analyzes contract data to:

- Let you know if contracts have a viable definition of a breach.
- Search for proper indemnification language.
- Discover proper insurance language.
- Extract and index data breach obligation language.
- Segregate buy-side agreements from sell-side agreements and other contract type docs.
- Provide a capability called "Analyze this Now" (ATN), allowing business users to quickly modify their contracts for GDPR compliance right from within MS Word.

GDPR is a complex and comprehensive new regulation affecting most organizations. This is why a technology solution such as Seal is needed to dramatically reduce the time, cost, and disruption of scouring through documents for GDPR compliance. Seal will help find PII data, and all other data associated with data breach processing and procedures, helping companies dramatically reduce the threat of GDPR penalties.

What Should You Do Now...

If your organization needs answers to your contract questions, reach out to us at info@seal-software.com, and we will answer those questions and show you Seal Contract Discovery and Analytics in action.

Contact Seal

Americas HQ
1990 N. California Blvd. Suite 500
Walnut Creek, CA 94596. USA.
T: + 1 650 938-SEAL (7325)

info@seal-software.com

European HQ
1-2 Hatfields, Waterloo
London
SE1 9PG, United
Kingdom.
T: + 44 203 735 9898