datasafeguard
intelligently protecting data

Enterprise Data Privacy

Accelerated Risk:

The advent of COVID-19 has accelerated the need for digital transformation and market driven digitization. This has created an opportunity for the beginning of a new Privacy Technology era. This advent has also opened new opportunities to hacker communities and state sponsored actors resulting in record setting data breaches and cyber-attacks on companies, government, and individuals. These sophisticated and collaborated attacks by hackers and state actors have been carried out with state-of-the-art technologies. Consequently, there are significantly higher risks to data breaches and financial losses for enterprises and governments all around the globe.

Data Safeguard Incorporated was formed to provide Data Privacy solutions for global enterprises and government organizations around the world by redacting (ID-Redact™) and masking (ID-Mask™) sensitive and personal data using AI/ML technology. Data Safeguard is quickly becoming the first line of defense for sensitive and personal data, while meeting global Data Privacy compliance policies including but not limited to GDPR, NIST, CCPA and other global data privacy laws in countries around the world.

Evolving Challenge:

Data Privacy and stopping the unwanted proliferation of sensitive and personal data is a complex and ever evolving problem. The dynamics of data privacy will continue to shift with business and product demands, public sentiment, global and country-based data privacy compliance requirements that are ever changing to meet the influx of unstructured, semi-structured and structured data generated by, entering into, and leaving from the enterprise.

The highlights of privacy laws can be summarized as follows:

1. easier access to user's own data,
2. clarifying the "right to be forgotten",
3. the right to know when a user's data has been compromised,
4. one-stop-shop with a single data supervisory authority,
5. a right to data portability for easier transfer of personal data between service providers,
6. continual updates to regional laws keeping current with evolving sensitive and personal data privacy needs.

Global Rules and Regulations:

For global Data Privacy regulations, the difficulty of identity and privacy identification is accomplished by the concept of any data defining a "natural person". By using "natural person", the privacy regulations are saying data regarding companies, which are sometimes considered "legal persons," are not personal data. This puts the obligation on the enterprise to be context aware and protect personal information from proliferating. A final caveat is that this person must be alive. Data related to the deceased are not considered personal data in most cases.

Consumers and their elected representatives are seeking some level of sensitive and personal data privacy and discretion. Consumers do not want passwords, family finances, details of personal relationships, medical history, location, purchase history, and private discussions being exposed and used for unintentional purposes. The results are made public. consumers various forms of pervasive spam, phishing, unsolicited sales calls, blackmail, and ransom. Privacy does not necessarily have to be about hiding something. Rather, privacy is about limiting the provided sensitive and personal data to its explicit and intended use only.

At the same time, we realize that too little privacy can undermine commerce, liberty, and the reporting of victimizations. Too little privacy, without oversight, can also inadvertently give access of sensitive and personal data to unintended entities, resulting in disruption and loss of productivity. Conversely, too much privacy can allow criminal actors to hide from authorities, resulting in increasing artificial identities and growing cybercrime against individuals and corporations. Such artificial identities are being used to steal from and undermine individual as well as corporations. At Data Safeguard these artificial identities are classified as Frankenstein Identities.

Conclusion:

The global perspective on sensitive and personal data is that it should only be kept in a form which permits identification of data subjects for as long as is necessary, and for the purposes for which the personal data are explicitly intended.

It is crucial for enterprises' Data Privacy Policies to preserve productivity and stop the proliferation of sensitive and personal data. The industry leading solution being offered today ensure appropriate levels of security and confidentiality for existing data, data being generated and in motion within the enterprise. This level of data privacy includes protection against 1) unauthorized or unlawful access to and use of such personal data, 2) gaining access to the equipment which stores and processes such personal data, and 3) accidental loss, destruction, and leaks of such data.

Enterprises are being held accountable for, and must be able to demonstrate, their compliance with all the above-named principles of Data Privacy. Enterprises are taking responsibility for their processing of sensitive and personal data and how they comply with the privacy laws and regulations, like GDPR, and be able to demonstrate (through appropriate records and measures) their compliance.

Data Safeguard's portfolio of products include provisions for current and future trends in Data Privacy requirements. "We believe the best solution is for the enterprise to control data proliferation across unstructured, semi-structured and structured data within the ecosystem" said Mr. Lowen, Chief Privacy Officer at Data Safeguard Inc. "I am excited about our Data Privacy suite of products that control the proliferation of data in the enterprise environment". Our products (ID-Redact™ and ID-mask™) are built using our core AI/ML based Cognitive Computing Engine™, to prevent sensitive and personal data from inadvertently spreading and being used in unintended ways. This is accomplished by redacting or masking personally identifiable data at its origin. In addition, the Cognitive Computing Engine™, an AI/ML based tool safeguards personally identifiable information (PII) at its source and tracks the lineage across the environment.