A Review of U.S. vs Italian Data Protection Law

Data protection is one of the highest-risk and fastest-changing areas of law. Countries all over the world are continually adapting their privacy, security, and data protection laws to new and emerging technologies. In particular, the United States (US) and Italy have independently developed different data protection laws and regulations. As seen in the video above, there are several key factors to consider when transferring data between the US and Italy.

Italian Data Protection Law

Italian data protection law is managed by a central authority known as the Italian Data Protection Authority or Garante Privacy. Garante Privacy is a privacy code that is set up to implement the European Union's (EU) General Data Protection Regulation (GDPR) into national law. The national agency consists of four elected members on the Council and an Office to govern and manage according to the GDPR requirements.

Thus, in order to understand Italian data protection law, it is necessary to first explain the GDPR. As of 2018, the GDPR replaced the 1995 European Data Protection Directive as the key data protection legislation guiding all EU members, including Italy. The GDPR is a far-reaching, broad regulation that governs the processing of personal data in a "filing system." Briefly, it defines the (a) fundamental rights of data subjects, (b) requirements for those processing data, (c) compliance standards, and (d) enforcement and penalties for non-compliance.

GDPR enforcement is strong in Italy and the EU. In fact, data processors who fail to comply with data protection standards

face fines as large as about $23 million or 4% of their total global turnover, whichever is larger.



United States Data Protection Law

US data protection law is a complex, decentralized web of federal and state legislation. Unlike Italy, there is no central federal authority or requirement mandating data processors to register databases containing personal data. However, the federal government holds some power. For example, the Federal Trade Commission (FTC) has some authority to regulate the use and transfer of personal data. Additionally, legislation, such as the 47 US Code, establishes a right to privacy over personally identifiable data. Finally, Executive Order 14117 restricts some nations' access to sensitive personal data and establishes the Department of Justice's Data Security Program to protect citizens from foreign threats, data breaches, and data misuse. While the US federal government has a say in data protection law, its contributions are minimal, especially compared to the detailed, wide-reaching EU data protection laws.

Unlike in Italy, data protection in the US varies heavily by state and sector. Currently, only 20 states have introduced

comprehensive data protection and consumer privacy legislation (although this number is expected to increase). Among these states, the most significant, wide-reaching acts include the California Privacy Rights Act (CPRA), the Washington MHMD Act, and the Colorado Privacy Act (CPA). These acts were all implemented within the past decade and reflect an ongoing shift toward increasing data protection measures in the US.

US data protection laws also differ by sector. These differences occur because each industry requires access to different information at different levels. For example, in healthcare, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) safeguards sensitive healthcare data, reflecting privacy rights over medical decisions. Another example is in the banking and finance sector. In 1999, the Gramm-Leach-Bliley Act (GLBA) mandated financial and banking institutions to protect consumer financial data, showing a need for privacy over consumers' personal finances, such as credit, loans, or spending.

Data protection enforcement is relatively lax in the US, especially compared to EU standards. Compliance standards and penalties often vary by state, with most fines ranging from $2,500 to $20,000.

Comparing US and Italian Laws

The standardized and centralized data protection system across the EU creates consistency and minimizes the number of legal ambiguities and challenges within countries. By contrast, the unstandardized and decentralized data protection network in the US allows individual states to create and implement laws that are best suited to their local economy, but opens the door to more legal inconsistencies and challenges.

The GDPR is much broader and comprehensive than US data protection laws. These differences in legal standards largely arise from differences in legal and economic priorities. In

the past, the US favored rapid economic growth and vast technological innovation rather than detailed legal rules, regulations, and privacy initiatives.

On the other hand, the EU favors more aggressive, wide-reaching, and comprehensive data protection and privacy legislation. Instead of favoring rapid innovation among businesses, the GDPR offers a more thorough and transparent approach to data protection. Unlike in the US, data processors in Italy must carefully consider how to best align with the GDPR and the privacy implications of data processing and management decisions. Additionally, the incentive to remain aligned with data protection standards is much stronger in Italy than in the US. While failure to comply with data protection laws in the US yields a fine between $2,500 to $20,000, penalties in Italy are much more consequential and can be as high as $23 million.