Global Data Privacy and Cybersecurity Handbook - United States

Penalties for Non-compliance

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What are the potential penalties / remedies for non-compliance with the key data privacy and cybersecurity laws in the jurisdiction?

*Last review date: 29 December 2023*

There are:

☒   administrative remedies/civil penalties imposed by regulators and law enforcement

Many of the privacy laws at the federal and state levels establish administrative remedies/civil penalties for non-compliance. For example, HHS may impose a civil money penalty on any person who violates the HIPAA Privacy Standards in the range from USD 100 to USD 50,000 per violation, with a total of USD 25,000 to USD 1.5 million for all violations of a single requirement in a calendar year.

The FTC may bring civil actions for civil monetary penalties of up to USD 40,000 per violation of the FTC Act or COPPA. Each day that non-compliance continues is considered a separate "violation" for purposes of the law.

If an organization enters into a consent decree with the FTC, any subsequent violations of the consent decree are subject to penalties of up to approximately USD 42,000 (periodically adjusted for inflation) per violation.

The FTC and financial regulatory authorities also have the power to bring civil actions for damages related to GLBA. In the context of the FTC, potential consequences include: rescission or reformation of contracts; monetary refunds or return of real property; restitution; disgorgement or compensation for unjust enrichment; monetary penalties; public notification of the violation; and limits on the violator's functions. Civil monetary penalties range from USD 5,000 to USD 1 million per day of violation if an individual knowingly violated the law.

States also establish such consequences for non-compliance with state privacy laws. For example, the CCPA provides for fines of up to USD 2,500 per violation or USD 7,500 per intentional violation, but notably does not place a cap on the total amount of fines. The VCDPA provides for civil penalties of up to USD 7,500 per each violation and injunctive relief. The CPA provides for civil penalties of up to USD 20,000 per violation and injunctive relief.

☒   criminal penalties from regulators and law enforcement

Violations of HIPAA can include criminal penalties, including up to ten years imprisonment in certain cases.

☒   private remedies

The CCPA provides for a private right of action for certain data breaches, including potential statutory damages of up to USD 750 per consumer per incident.

☐   other

# If data subjects have private remedies, what form can these remedies take?

*Last review date: 29 December 2023*

☒   individual personal actions

☐   representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

☒   class actions