PrivaLex Advisory
...Compliance Redefined, Privacy Secured

2024 Global Data Protection Fines

CONTACT US:

@PrivaLex Advisory @privalex_advisory

contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Executive Summary

As the year comes to an end, we present a highlight of some of the most significant data protection fines imposed globally in 2024. It highlights enforcement trends, regulatory focus areas, and compliance gaps that organisations must address to ensure adherence to privacy regulations. The fines emphasise the critical importance of data security, transparency, and lawful data processing.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Europe

LinkedIn – €310 million fine
Authority: Irish Data Protection Commission (DPC)
LinkedIn unlawfully processed personal data for targeted advertising, relying on invalid legal bases and failing to provide sufficient transparency about data usage, breaching GDPR's fairness principle.

Uber Technologies Inc., Uber B.V. – €290 million fine
Authority: Dutch Data Protection Authority (DPA)
Uber transferred sensitive driver data, including payment and identity details, to the U.S. without adequate safeguards, violating GDPR following the invalidation of the EU-U.S. Privacy Shield.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Meta Platforms Ireland Limited – €91 million fine
Authority: Irish Data Protection Commission (DPC)
Meta stored plaintext user passwords without encryption, breaching GDPR's integrity and confidentiality principles. Although Meta rectified the issue, the fine was issued for insufficient security measures.

Enel Energia SpA – €79.1 million fine
Authority: Italian Data Protection Authority (Garante)
Enel Energia engaged in telemarketing abuses and had weak security measures that allowed unauthorised access to customer data. An earlier €26.5 million penalty was cancelled before this larger fine was imposed.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Clearview AI Inc. - €30.5 million fine
Authority: Dutch Data Protection Authority (DPA)
Clearview AI unlawfully scraped 30 billion facial images to create a biometric database without consent, violating GDPR by lacking transparency and processing sensitive biometric data without legal justification.

Avast Software - €13.9 million fine
Authority: Czech Data Protection Authority (ÚOOÚ)
Avast transferred data from antivirus software users to a subsidiary without consent.
Inadequate anonymisation exposed users to re-identification, breaching GDPR's data protection standards.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Eni Plenitude S.p.A. - €6.4 million fine
Authority: Italian Data Protection Authority (Garante)
Eni Plenitude conducted unsolicited promotional calls without consent, including calls to numbers on the Do Not Call list, and failed to implement adequate data security and consent management practices.

Apoteket AB - €3.2 million fine
Authority: Swedish Authority for Privacy Protection (IMY)
Apoteket misconfigured Meta's Pixel tool, exposing sensitive data, including health-related purchases, to Meta's advertising platform, breaching GDPR due to insufficient data security protections.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Hellenic Post – €2.9 million fine
Authority: Hellenic Data Protection Authority (HDPA)
Hellenic Post suffered a cyberattack that compromised sensitive data published on the dark web. Weak access controls and encryption failures violated GDPR's security requirements.

UniCredit S.p.A. – €2.8 million fine
Authority: Italian Data Protection Authority (Garante)
UniCredit was fined for inadequate security measures following a 2018 cyberattack that compromised personal data. Delayed notifications and insufficient safeguards were cited as GDPR breaches.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Vinted – €2.3 million fine
Authority: Lithuanian State Data Protection Inspectorate (SDPI)
Vinted mishandled data erasure requests, engaged in "shadow blocking," and failed to demonstrate compliance, breaching GDPR's data processing and user rights principles.

TikTok – £1.8 million fine
Authority: Ofcom
TikTok provided inaccurate information about parental controls, delaying child safety assessments, and breaching transparency rules.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Avanza Bank AB – €1.3 million fine
Authority: Swedish Authority for Privacy Protection (IMY)
Avanza exposed sensitive customer data via Meta's Pixel tool due to poor technical measures and oversight.

CaixaBank S.A. – €1.2 million fine
Authority: Spanish Data Protection Authority (AEPD)
CaixaBank required consent to access social security data without offering withdrawal options, breaching GDPR processing principles.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

mBank – €940k fine
Authority: Polish Data Protection Authority
mBank failed to notify customers about a data breach exposing sensitive details, violating GDPR's transparency obligations.

Postel S.p.A. – €900k fine
Authority: Italian Data Protection Authority (Garante)
Postel suffered a ransomware attack due to poor security measures, exposing employee and applicant data.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Verkkokauppa.com – €856k fine
Authority: Finnish Data Protection Ombudsman
Verkkokauppa.com mandated account creation for purchases and stored data indefinitely without clear retention policies, violating GDPR.

NTT Data Italia S.P.A – €800k fine
Authority: Italian Data Protection Authority (Garante)
NTT Data subcontracted tasks without UniCredit's approval and delayed reporting vulnerabilities tied to a data breach.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Apohem AB – €698k fine
Authority: Swedish Authority for Privacy Protection (IMY)
Apohem exposed sensitive data through Meta's Pixel tool, failing to meet GDPR's security requirements.

Netflix – €4.75 million fine
Authority: Dutch Data Protection Authority (DPA)
Netflix failed to provide clear information about data collection, sharing, and retention in its privacy statements, violating GDPR transparency rules.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

HelloFresh – £140,000 Fine
Authority: Information Commissioner's Office (ICO)
Fined in January 2024 for sending 79 million spam emails and 1 million spam texts over seven months, breaching the Privacy and Electronic Communications Regulations (PECR).

LADH Limited – £50,000 Fine
Authority: Information Commissioner's Office (ICO)
Fined in January 2024 for sending tens of thousands of spam text messages, violating PECR.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Outsource Strategies Ltd (OSL) – £240,000 Fine
Authority: Information Commissioner's Office (ICO)
Fined for making 1.43 million unsolicited marketing calls between February 2021 and March 2022 to people registered on the Telephone Preference Service (TPS). The calls targeted elderly and vulnerable individuals, leading to 76 complaints about aggressive tactics.

Dr Telemarketing Ltd (DRT) – £100,000 Fine
Authority: Information Commissioner's Office (ICO)
Fined for making 1.43 million unsolicited marketing calls to people listed on the TPS register, breaching PECR. The calls demonstrated aggressive and exploitative behaviour toward vulnerable consumers.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Advanced Computer Software Group Ltd – £6.09 Million (Provisional Fine)
Authority: Information Commissioner's Office (ICO)
Provisionally fined in August 2024 following a 2022 ransomware attack that compromised the personal information of 82,946 people, including sensitive data. The final decision is pending.

Police Service of Northern Ireland (PSNI) – £750,000 (Potential Fine)
Authority: Information Commissioner's Office (ICO)
Facing a potential fine following a spreadsheet error that exposed the personal information of its entire workforce. The final decision is pending.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

America

T-Mobile USA - $80.08 million fine
Authority: Federal Communications Commission (FCC)
T-Mobile was fined $80.08 million for failing to protect customer location data, which was disclosed to third parties without consent. Initially fined $91.63 million, the amount was reduced following T-Mobile's comments. The FCC underscored the need for telecommunications providers to enforce stringent data protection measures.

AT&T - $57.27 million fine
Authority: FCC
AT&T was fined $57.27 million for selling customer location data to third parties without consent and failing to secure customer information adequately. This enforcement action emphasized privacy obligations for telecommunications providers.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Verizon Communications - $46.9 million fine
Authority: FCC
Verizon was fined $46.9 million for sharing customer location data without consent and failing to safeguard the data. The FCC stressed that telecommunications companies must protect sensitive customer information.

Sprint Corporation (T-Mobile USA) - $12.24 million fine
Authority: FCC
Sprint, now part of T-Mobile, was fined $12.24 million for providing customer location data to third parties without consent and failing to adopt measures to secure the data. This case reinforced the importance of data privacy compliance post-merger.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Geico – $9.75 million fine
Authority: New York Attorney General's Office
Geico was fined $9.75 million for a data breach that compromised the personal information of 116,000 drivers. This enforcement action highlighted accountability in securing customer data.

Cerebral, Inc. – $7.08 million fine
Authority: FTC
Cerebral, Inc. was fined $7.08 million for disclosing sensitive health data of 3.2 million consumers to third parties, including LinkedIn, Snapchat, and TikTok, without consent. The FTC imposed restrictions on its data-sharing practices and required it to provide opt-out options.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Avast – $16.5 million fine
Authority: FTC
Avast was fined $16.5 million for selling web browsing data to third parties despite assurances that its products would protect users from online tracking. Avast was also prohibited from further selling such data.

Marriott International – $52 million settlement
Authority: FTC and State Attorneys General
Marriott agreed to a $52 million settlement and enhanced security measures following multiple data breaches affecting 300 million customers. Poor data security practices led to breaches spanning 2014–2020.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Global Tel Link Corp. - Enforcement Order
Authority: FTC
The FTC issued an enforcement order requiring Global Tel Link to implement better data security practices after failing to adequately protect user data and failing to notify affected individuals about a breach.

Meta Platforms (Texas Settlement) - $1.4 billion fine
Authority: State of Texas
Meta (Facebook) was fined $1.4 billion for unlawfully collecting biometric data from millions of Texans without consent, violating state privacy laws. This is the largest fine obtained by a U.S. state for privacy violations.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

T-Mobile – $60 million CFIUS penalty
Authority: Committee on Foreign Investment in the United States (CFIUS)
T-Mobile was fined $60 million for failing to prevent and report unauthorized access to sensitive data, breaching a mitigation agreement tied to its Sprint acquisition.

Oracle America, Inc. - $115 million settlement
Authority: Class Action Lawsuit
Oracle settled for $115 million after allegations of collecting and selling personal data without consent. Individuals affected were eligible to claim compensation.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

ZoomInfo - $29.55 million settlement
Authority: State Regulators
ZoomInfo agreed to pay $29.55 million in settlements for violating data privacy laws by improperly handling personal information. Residents of four states were eligible for payments.

Travelers Indemnity Company - $1.55 million fine
Authority: New York Attorney General's Office
Travelers was fined $1.55 million for a data breach affecting approximately 4,000 individuals. The breach exposed sensitive data due to insufficient security controls.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Meta Platforms (Brazil) - Daily fines and suspension

Authority: Brazil's National Data Protection Authority (ANPD)

Meta was ordered to halt the use of Brazilian personal data for AI model training. Daily fines of 50,000 Brazilian Reais (approximately $8,836) were imposed for non-compliance. The suspension reflects increasing scrutiny over AI and data use.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Australia

Meta Platforms (Facebook) – A$50 Million Settlement
Authority: OAIC
Meta settled for A$50 million ($31.85 million) in December 2024 over the Cambridge Analytica scandal. Data of 311,127 Australian users was improperly shared via the "This is Your Digital Life" app, breaching the Privacy Act 1988.

Medibank – Legal Proceedings Initiated
Authority: OAIC
In June 2024, the OAIC sued Medibank for a breach affecting 9.7 million customers. Medibank allegedly failed to secure sensitive data, with fines potentially reaching A$2.22 million per violation.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Africa

Nigeria: Meta Platforms – $220 Million Fine
Authority: Federal Competition and Consumer Protection Commission (FCCPC)
Meta Platforms was fined $220 million on July 19, 2024, for unauthorized data sharing, lack of user consent, and discriminatory practices, violating Nigeria's data protection and consumer rights laws.

Nigeria: Fidelity Bank – N400 Million Fine
Authority: Nigeria Data Protection Commission (NDPC)
Fidelity Bank was fined N400 million ($358,580) on August 22, 2024, for collecting personal data without consent during account opening and using unauthorized tools, breaching data privacy laws.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

South Africa: Department of Justice – ZAR 5 Million Fine
Authority: Information Regulator (IR)
The Department of Justice was fined ZAR 5 million ($279,000) in July 2023 for failing to comply with the Protection of Personal Information Act (POPIA) after a 2021 data breach compromised 1,200 files due to expired antivirus licenses.

Kenya: WPP Scangroup – KES 1.95 Million Fine
Authority: Office of the Data Protection Commissioner (ODPC)
WPP Scangroup was fined KES 1.95 million ($13,000) on October 31, 2024, for mishandling personal data belonging to its former CEO, violating Kenya's Data Protection Act.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Asia

South Korea: Meta Platforms – 21.6 Billion Fine
Authority: Personal Information Protection Commission (PIPC)
Meta was fined 21.6 billion ($15 million) in November 2024 for collecting sensitive personal data from 980,000 users without consent and sharing it with 4,000 advertisers. The data included political views, religion, and sexual orientation, violating South Korea's privacy laws requiring explicit consent.

India: WhatsApp (Meta Platforms) – $25.4 Million Fine
Authority: Competition Commission of India (CCI)
In November 2024, the CCI fined WhatsApp $25.4 million and ordered it to stop sharing user data with Meta for advertising purposes for five years. The decision followed a 2021 investigation into WhatsApp's privacy policy, which required users to agree to data sharing.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Turkey: Twitch (Amazon) – ₺2 Million Fine
Authority: Personal Data Protection Board (KVKK)
Turkey fined Twitch ₺2 million ($58,000) in November 2024 for a data breach affecting 35,274 individuals. KVKK cited inadequate security measures and delays in breach reporting as violations.

Thailand: J.I.B. Computer Group – 7 Million Fine
Authority: Personal Data Protection Committee (PDPC)
Thailand's PDPC fined J.I.B. Computer Group 7 million ($206,526) in August 2024 for a data breach that exposed personal information used in fraudulent schemes. This marked the first administrative fine under Thailand's PDPA.

PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Singapore: Various Organizations – SG$102,000 in Total Fines

Authority: Personal Data Protection Commission (PDPC)

In May 2024, Singapore's PDPC imposed SG$102,000 ($76,000) in fines for multiple breaches of its PDPA. The cases involved improper handling of personal data, and six organizations were required to improve their compliance measure

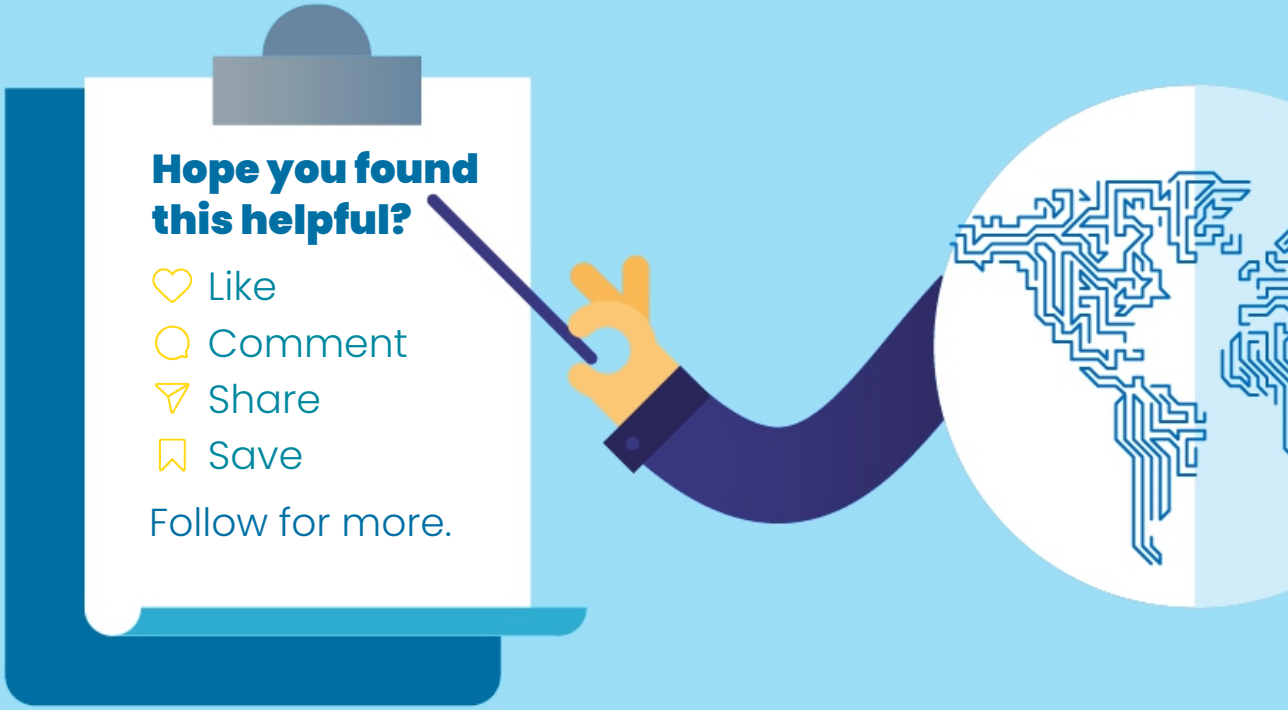
PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Conclusion

The year 2024 witnessed significant enforcement of data protection laws globally, with substantial fines highlighting the need for robust compliance programs. Organisations must prioritise data security, transparency, and user consent to avoid severe financial and reputational penalties.

@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com

PrivaLex Advisory
...Compliance Redefined, Privacy Secured



@PrivaLex Advisory @privalex_advisory
contact@privalexadvisory.com