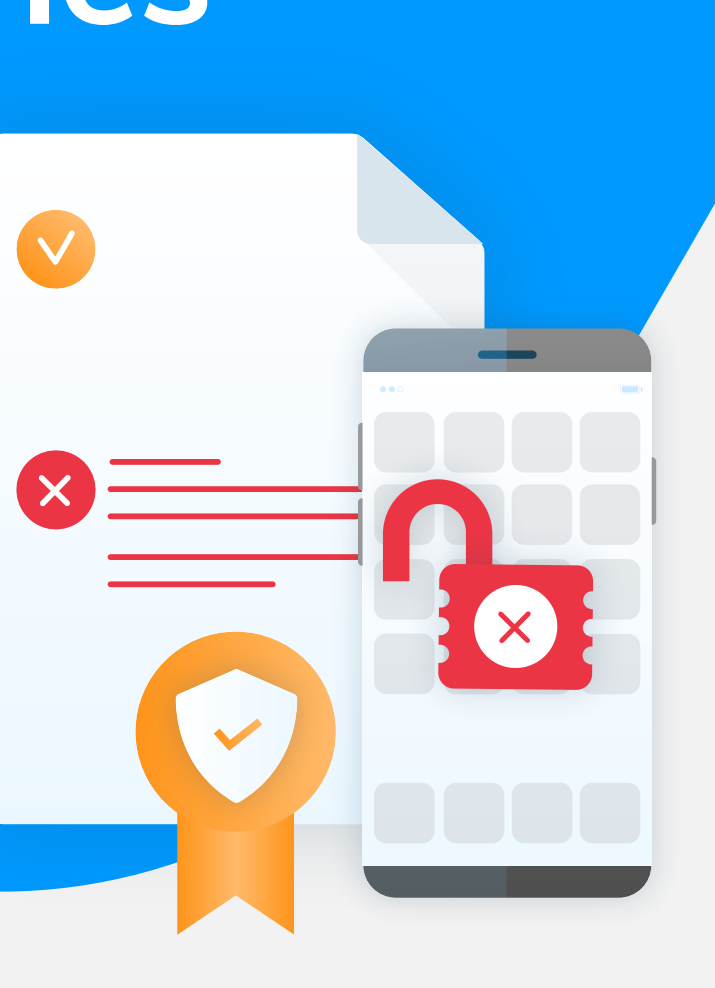
INFOGRAPHIC

NowSecure

Mobile App Privacy and Compliance: High-Profile Fines and Enforcement Actions

Infographic illustrates the cost of failing to comply with key mobile app privacy regulations such as GDPR, CCPA and COPPA.



The Federal Trade Commission (FTC) and other agencies are increasingly cracking down on mobile app security and privacy practices. Authorities aggressively enforce data protection policies such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) and assess significant fines for non-compliance.

Federal Trade Commission Protects Consumer Privacy & Security

Recent FTC settlements and fines demonstrate the agency's commitment to enforcing privacy regulations and safeguarding sensitive health information.

2024

May

Cerebral

The FTC proposed a $7M settlement with telehealth app maker **Cerebral** because it provided sensitive health information to third parties and misled consumers about cancellation policies. The company and its CEO also failed to properly secure data.[1]

2023

July

BetterHelp

The FTC banned online counseling service **BetterHelp** from sharing sensitive health data about mental health challenges with third parties and ordered it to pay $7.8M to consumers.[2]

May

Premom

Fertility app **Premom** was fined $100,000 for violating the Health Breach Notification Rule (HBNR) by sharing sensitive health information with third parties.[3] The Easy Healthcare app maker also paid a separate $100,000 fine to state attorney generals.[4]

February

GoodRx

Digital health platform **GoodRx** paid a $1.5M penalty for violating the HBNR by sharing consumers' sensitive health information with third parties.[5]

2022

Kurbo by WW

The FTC fined WW International $1.5M because its **Kurbo by WW** mobile app illegally collected kids' sensitive health data in violation of the Children's Online Privacy Protection Act (COPPA).[6]

2021

Flo Health

Fertility tracking app **Flo Health** must obtain user consent before sharing their personal information with third parties and had to undergo an independent review of its privacy practices after disclosing sensitive health data to marketing and analytics services.[7]

2020

HyperBeard

App maker **HyperBeard** violated COPPA by unlawfully collecting personal information from children without parental consent. The company agreed to pay $150,000 and delete illegally collected personal information.[8]

2019

Retina-X Studios

Stalking app developer **Retina-X Studios** settled with the FTC over its failure to secure data collected by its apps and ensure the apps were used for legitimate purposes.[9]

---

[1] FTC, "Proposed FTC Order Will Prohibit Telehealth Firm Cerebral from Using or Disclosing Sensitive Data for Advertising Purposes, and Require It to Pay $7 Million," April 15, 2024

[2] Federal Trade Commission, "FTC Gives Final Approval to Order Banning BetterHelp from Sharing Sensitive Health Data for Advertising, Requiring It to Pay $7.8 Million," July 14, 2023

[3] Federal Trade Commission, "Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order," May 17, 2023

[4] Arnold & Porter, "FTC Settles with Premom App Developer for Privacy and Security Violations," June 1, 2023

[5] Federal Trade Commission, "FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising," Feb. 1, 2023

[6] Federal Trade Commission, "FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data," March 4, 2022

[7] Federal Trade Commission, "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others," June 22, 2021

[8] Federal Trade Commission, "Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data without Parental Consent," June 4, 2020

[9] Federal Trade Commission, "FTC Gives Final Approval to Settlement with Stalking Apps Developer," March 27, 2020

General Data Protection Regulation Increases Enforcement

European Union (EU) countries such as Ireland have intensified scrutiny of tech companies operating in the region to encourage widespread GDPR compliance.

2023

September

Grindr

Norway upheld a €5.8M fine levied by the Norwegian Data Protection Authority against **Grindr** for sharing user data such as GPS location and profile with third parties.[10]

TikTok

The Ireland Data Protection Commission (DPC) fined **TikTok** €345M for wrongfully collecting and processing the personal data of children and setting their accounts to public by default.[11] Earlier in 2023, the UK ICO fined TikTok £12.7M for misusing children's data[12] and in 2021, Dutch authorities levied a €750,000 fine for insufficiently protecting children's privacy.[13]

May

Facebook

The Ireland DPC fined **Meta** a record-breaking €1.2B for transferring Facebook data from the EU/EEA to the United States, violating GDPR international transfer guidelines.[14]

January

Facebook & Instagram

The Ireland DPC fined Meta €390M for breaking EU data rules over its targeted advertising practices on **Facebook** and **Instagram** and not allowing users to opt out.[15]

WhatsApp

The Ireland DPC fined Meta €5.5 million for lack of transparency about **WhatsApp** data processing practices.[16]

2022

Instagram

The Ireland DPC fined **Instagram** €405M for violating children's privacy by exposing their phone numbers and email addresses.[17]

2021

WhatsApp

The Ireland DPC fined **WhatsApp** €225M for lack of transparency about its data processing practices.[18]

Vinted

French, Polish and Lithuanian authorities joined a European Data Protection Board investigation of secondhand fashion app **Vinted** for its personal data storage and data processing practices.[19]

2020

British Airways

The UK ICO fined British Airways £20 million for a mobile app and web breach that leaked the personal data of nearly 400,000 customers.[20]

2019

La Liga

The AEPD Spanish data protection authority fined the La Liga professional soccer league €250,000 for using its mobile app to improperly access users' microphones and location data to detect unauthorized broadcasts of soccer matches.[21]

---

[10] Noyb, "€5,8 million for Grindr confirmed," Sept. 29, 2023

[11] Data Protection Commission, "Irish Data Protection Commission announces €345 million fine of TikTok," Sept. 15, 2023

[12] ICO, "ICO fines TikTok £12.7 million for misusing children's data," April 4, 2023

[13] European Data Protection Board, "TikTok fined for violating children's privacy," July 22, 2021

[14] The New York Times, "Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules," May 22, 2023

[15] CPO, "Irish DPC Orders €390 Million Fine to Meta Over Targeted Advertising, Orders Implementation of Ability to Opt Out," Jan. 9, 2023

[16] InfoSecurity Magazine, "WhatsApp Hit with €5.5 Million Fine for GDPR Violations," Jan. 20, 2023

[17] BBC, "Instagram fined €405 million over children's data privacy," Sept. 5, 2022

[18] The New York Times, "Facebook's WhatsApp is fined for breaking E.U.'s data protection law," Sept 2, 2021

[19] OneTrust DataGuidance, "EU: EDPB announces compliance investigation of Vinted," Nov. 19, 2021

[20] BBC, "British Airways fined £20 million over data breach," Oct. 16, 2020

[21] Forbes, "La Liga Handed $280,000 GDPR Fine for 'Spying' on Fans Watching Pirated Streams," June 12, 2019

California Consumer Privacy Act Holds Businesses Accountable

The robust data privacy law requires companies operating in the Golden State to safeguard user privacy and respect consumer choice.

2024

DoorDash

California fined online food delivery app **DoorDash** $375,000 for selling customers' personal information and ordered it to provide annual compliance reports.[22]

2023

Retail Shopping, Travel & Food Service Apps

The California AG warned popular **retail, travel and food services** mobile apps that fail to comply with opt-out requests or offer a mechanism for consumers to halt the sale of their data.[23]

2022

Sephora

Beauty retailer **Sephora** agreed to pay a $1.2M fine and provide regular compliance reporting for failing to inform website and mobile app users that it was selling their information.[24]

---

[22] State of California Department of Justice Office of the Attorney General, "Attorney General Bonta Announces Settlement with DoorDash, Investigation Finds Company Violated Multiple Consumer Privacy Laws," Feb. 21, 2024

[23] State of California Department of Justice Office of the Attorney General,"Ahead of Data Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act," Jan. 27, 2023

[24] State of California Department of Justice Office of the Attorney General,"Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of the California Consumer Privacy Act," Aug. 24, 2022

New York State Attorney General Cracks Down on Privacy Abuse

Currently led by Letitia James, the office has acted against companies that fail to comply with the law and protect consumer data.

2023

Spyware Apps

The New York Attorney General secured $410,000 from the maker of several **spyware apps** that monitor peoples' mobile devices without their awareness and ordered the company to modify their apps to notify device owners that they're being monitored.[25]

2022

Shein & Romwe

The Empire State fined Zoetop, parent company of shopping apps **Shein** and **Romwe**, $1.9M for mishandling a data breach that exposed the personal information of more than 39 million customers and attempting to cover up the incident.[26]

2019

Credit Sesame, Equifax, Priceline, Spark Networks & Western Union

Credit Sesame, Equifax, Priceline, Spark Networks and **Western Union** failed to secure sensitive information on their mobile apps and agreed in a settlement to implement comprehensive mobile security programs.[27]

2017

Cardiio, Matis & Runtastic

The state fined mHealth app makers **Cardiio, Matis** and **Runtastic** $30,000 over misleading claims and irresponsible privacy practices and ordered them to make changes to safeguard consumer privacy.[28]

---

[25] Office of the New York State Attorney General, "Attorney General James Secures $410,000 from Tech Companies for Illegally Promoting Spyware and Violating New Yorkers' Privacy," Feb. 2, 2023

[26] Office of the New York State Attorney General, "Attorney General James Secures $1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers' Data," Oct. 12, 2022

[27] National Law Review, "N.Y. Attorney General Enforces Mobile App Security Initiative, Announces Settlements with Five Companies," Jan. 29, 2019

[28] Casetext, "NY AG Announces Settlement with Health App Developers Over Marketing and Privacy Practices," March 28, 2017

Reduce Compliance Risk

Organizations must thoroughly assess their mobile apps for security, privacy and compliance risks prior to release. Get a demo of the NowSecure Platform automated mobile application security and privacy testing solution to see how it and its manual complement, NowSecure Mobile Pen Testing as a Service (PTaaS), can help ensure highly sensitive mobile apps meet compliance requirements.

© 2024 NowSecure. All Rights Reserved.