

European Pirate Party

Policy Position Paper on

Google's Android Developer Verification Requirement

March 2026

Executive Summary

In August 2025, Google announced the Android Developer Verification programme, requiring all developers who distribute apps on Android devices to register centrally with Google, pay a fee, submit government-issued identification, and upload evidence of their private cryptographic signing keys. From September 2026, apps from unverified developers will be blocked in standard installation flows on certified Android devices, covering the vast majority of Android-compatible devices outside China. A global rollout is planned from 2027 onwards.

The programme, framed by Google as a security measure, poses fundamental threats to software freedom, user privacy, and fair competition in the digital ecosystem. It effectively ends anonymous distribution of apps through normal Android installation channels, significantly expands corporate identity collection for Android developers, and structurally advantage Google's own distribution channel. We believe that it is also incompatible with Google's obligations as a designated gatekeeper under the EU Digital Markets Act (DMA).

More than 37 organisations including, the Electronic Frontier Foundation, Article 19, the Free Software Foundation, F-Droid, Fastmail, and Vivaldi, have signed an open letter calling on Google to reconsider. The European Pirate Party adds its voice to this coalition.

We call on Google and Alphabet to:

1. Withdraw the Android Developer Verification programme and commit to preserving Android's openness for developers distributing outside the Play Store.
2. Recognise alternative app stores and community repositories such as F-Droid as legitimate and protected components of the Android ecosystem.
3. Provide a written public commitment that sideloading will remain frictionless for all users and developers, regardless of Play Store registration status.

We call on the European Commission to:

4. Open a formal investigation into whether the Android Developer Verification programme breaches Alphabet's obligations under Article 6(4) of the Digital Markets Act.
5. Treat the programme as a priority enforcement matter, given Alphabet's existing record of non-compliance with DMA sideloading and app store obligations.

Who we are

The European Pirate Party represents a pan-European movement working across EU institutions, national parliaments, and local governments to defend digital rights and democratic participation in the technological age. Since our founding, we have championed internet freedom, civil liberties, and user empowerment against the concentration of power in both state surveillance and corporate control.

We understand that how software is distributed, who controls the conditions of that distribution, and whether developers can share their work freely with users, determines whether digital spaces remain open for creativity, dissent, and democratic participation, or become managed environments serving commercial gatekeepers.

What We Believe

Our position on the Android Developer Verification requirement flows directly from core principles shared by the Pirate movement across Europe.

We believe that free and open-source software is an essential infrastructure for a democratic society. Our manifesto states that software which can be “used, analysed, disseminated and changed by everyone” is essential for users’ control of their own technical systems and provides a significant contribution to strengthening the autonomy and privacy of all users. Any policy that makes the distribution of free software conditional on corporate approval undermines this foundation.

We also believe that the right to develop and share software anonymously is a civil liberties issue, not a technical preference. Many of the most important contributions to the open-source ecosystem have come from developers working pseudonymously, whether for personal safety, political protection, or simply the freedom to contribute without exposing their identity to a global corporation subject to the legal demands of every jurisdiction in which it operates.

When a single corporation controls the conditions under which software can be distributed on the world’s dominant mobile platform, it gains power over what citizens can access, install, and trust. That power must be subject to democratic oversight and competitive constraint. The EU Digital Markets Act exists precisely to impose those constraints on designated gatekeepers such as Alphabet. Thus, we affirm that market structure is not separate from fundamental rights.

The Android Developer Verification requirement is a test on whether Europe will enforce the rules it has written, or allow them to be bypassed through technical implementation choices framed as security measures.

Why We Are Responding

Android powers more than 70% of smartphones globally and, outside of China, more than 95% of certified Android devices will be subject to this programme once enforcement begins. The scale makes this not merely a developer relations dispute but a structural question about who controls software distribution for most of the world’s mobile users.

The programme was announced in August 2025, with verification opening to all developers in March 2026, enforcement beginning in Brazil, Indonesia, Singapore, and Thailand in

September 2026, and a global rollout planned from 2027 onwards. We are responding now because the window for regulatory and political intervention, is open and must be used before enforcement locks.

We are also responding because this issue sits at the intersection of three areas where the European Pirate Party has both expertise and a mandate: free software and the open ecosystem, civil liberties and the right to privacy, and competition law under the Digital Markets Act. Each dimension reinforces the others, and together they make a compelling case for regulatory intervention.

We join the 37 organisations that signed the open letter published by the F-Droid team in February 2026, including the Electronic Frontier Foundation, Article 19, the Free Software Foundation, Fastmail, and Vivaldi. Their letter correctly identifies the programme as an extension of Google's gatekeeping authority beyond its own marketplace into distribution channels where it has no legitimate operational role.

Opportunities and Risks

We recognise that platform security is a legitimate concern. Malware distributed through sideloading causes real harm to users, and a system that improves developer accountability without restricting software freedom would be worth building. Android already maintains multiple security mechanisms such as, Google Play Protect, which scans apps regardless of their source, and the existing permission and signing key infrastructure, that address these concerns without requiring developer identity registration.

The genuine opportunity here is for Google and regulators to strengthen those existing mechanisms, improve user-facing security information, and support community-run verification systems like F-Droid's, rather than replacing distributed, open processes with centralised corporate control.

The risks of the programme as currently designed are threefold and each is examined in detail in the sections below.

First, it ends the free software ecosystem on Android as it currently exists, making community repositories like F-Droid structurally incompatible with the platform.

Second, it creates an unprecedented identity database of developers worldwide, with serious implications for anonymous development and the safety of developers in vulnerable contexts.

Third, it constitutes a de facto breach of Alphabet's obligations under the EU Digital Markets Act, which explicitly requires gatekeepers to allow and technically enable the installation of third-party software without interposing themselves as unavoidable intermediaries.

1. Free Software, Open Ecosystems and the Public Interest

Android's openness has, until now, been one of its defining characteristics. Unlike Apple's iOS, Android has allowed a practice known as sideloading, where users could install software from sources other than the official app store. This has enabled the creation of a diverse and innovative software ecosystem that exists independently of commercial platform approval.

The most significant example is F-Droid, a community-run repository dedicated to free and open-source Android applications. F-Droid builds applications directly from publicly available source code, verifies them independently, and distributes them without requiring developers to register with any central authority or commercial platform. Many of the applications in the F-Droid repository deliberately avoid the tracking technologies common in commercial app marketplaces, making them the distribution channel of choice for users who prioritise privacy, software freedom, or both.

The Android Developer Verification programme is structurally incompatible with how F-Droid operates. F-Droid builds from source code maintained by volunteers, researchers, and small teams, and does not operate as a registered developer in the conventional sense. Under the new programme, every application in the F-Droid repository would need to be registered by a Google-verified developer. As the F-Droid maintainers explained in their open letter, this “applies regardless of whether your software is distributed commercially on a competitive app store like the Samsung Galaxy Store, or through a non-commercial community app repository like F-Droid, or even by offering your app as a direct download from a web page.”¹

The practical consequences extend far beyond F-Droid. Independent developers who distribute apps directly to users, through their own websites, peer-to-peer sharing, or community forums, would all be required to register with Google. Developers who contribute to open-source projects using pseudonyms would face a choice between revealing their identity to a US corporation subject to the legal demands of dozens of jurisdictions, or ceasing to distribute their work on Android.

Google’s stated justification is security as the programme is framed as equivalent to an ID check, intended to hold bad actors accountable. But this analogy obscures the scale of what is being proposed. The Android Developer Verification programme would create a private, corporate identity database of every person who writes software for the world’s dominant mobile platform, operated by a company that is simultaneously a commercial competitor to the developers it would now control.

Also, the security justification is not proportionate. Android already operates Google Play Protect, which scans more than 100 billion apps daily for malware regardless of their distribution source. The platform already requires cryptographic signing of applications, which provides a chain of integrity without requiring developer identity to be disclosed to Google. The F-Droid open letter, signed by 37 organisations, identifies this directly: “the Android platform already includes multiple security mechanisms that do not require central registration.”²

The European Pirate Party’s manifesto is explicit on this point. Free and open-source software is essential for users’ control of their own technical systems and provides a significant contribution to strengthening the autonomy and privacy of all users. A policy that makes the distribution of such software conditional on Google’s approval directly contradicts this principle.

¹ <https://keepandroidopen.org/>

² Prux, M. et al. / F-Droid (February 2026). An Open Letter Opposing Android Developer Verification. <https://f-droid.org/en/2026/02/24/open-letter-opposing-developer-verification.html>

We call on Google and Alphabet to withdraw the verification requirement for developers distributing outside the Play Store, and to publicly recognise alternative app stores and community repositories as legitimate and protected components of the Android ecosystem.

2. Privacy, Civil Liberties and the Right to Anonymous Development

The Android Developer Verification programme requires developers to submit their legal name and address. This information is verified by uploading an official government identity document, along with a contact email, phone number, and for organisations, a D-U-N-S business identification number. Developers must also register all current and future application package names and prove control of their cryptographic signing keys. This information would be held by Google with no public commitment on retention periods, access conditions, or the circumstances under which it would be disclosed to law enforcement or government authorities.

This creates an unprecedented corporate identity registry of everyone who writes software for Android. The privacy implications are serious for all developers. They are existential for those working in vulnerable contexts.

2.1 The Surveillance Risk

Google has a documented record of complying with government demands to remove applications in authoritarian jurisdictions. A developer of censorship circumvention tools, a journalist's source protection application, or a human rights monitoring tool who registers their identity with Google is simultaneously registering that identity with every government that can reach Google through legal process, and potentially beyond. The Electronic Frontier Foundation has warned explicitly that developers of VPN and circumvention tools, face direct danger if their identities reach hostile governments through this mechanism.

Additionally, the signing key requirement adds a further dimension. Cryptographic signing keys are the foundation of software supply-chain integrity. Uploading evidence of these keys to a central corporate registry creates a single point of vulnerability. If that registry is breached, compromised, or accessed by hostile actors, the integrity of every registered application is at risk.

Under Articles 7 and 8 of the EU Charter of Fundamental Rights, as well as Articles 5(1)(c) and 25 of the GDPR, any system that processes this volume of sensitive personal data must satisfy strict proportionality, data minimisation, and privacy-by-design requirements. The verification programme, as currently described, provides no framework for any of these obligations. It collects identity data without publicly clarifying the legal basis for its processing, retention period, or mechanism for developer access to or deletion of their own data.

2.2 The Chilling Effect on Anonymous Development

Anonymous and pseudonymous development has been fundamental to free software since its origins. Some of the most widely used open-source tools, including privacy-protective applications, security research tools, and censorship circumvention software, have been developed and maintained by contributors who work under pseudonyms for entirely legitimate reasons.

The mandatory identification requirement ends this on Android. The argument is structurally identical to those the Pirate Party has made against Chat Control and age verification mandates: requiring identification to exercise a fundamental right, in this case, the right to write and share software, suppresses legitimate activity far more broadly than it deters bad actors. A dissident building a censorship circumvention tool cannot safely provide their passport to a US corporation operating across every jurisdiction on earth.

Article 11 of the EU Charter of Fundamental Rights guarantees freedom of expression, including the freedom to impart information without interference. The freedom to distribute software is an expression of this right. Conditioning it on identification to a private corporation, with no democratic accountability for how that identification is used, constitutes interference that must be assessed against the proportionality requirements of Article 52(1) of the Charter. No such assessment has been provided by Google.

2.3 Structural Disadvantage for Privacy-Protective Software

The verification programme also creates a structural disadvantage for privacy-focused applications. Applications that generate revenue through surveillance-based advertising can absorb the cost and friction of registration. Applications that are community-funded, volunteer-built, or designed specifically to minimise data collection cannot. The result is a regulatory design that advantages the business models that European data protection law was intended to constrain.

We call on the Commission to require a Data Protection Impact Assessment of the verification programme under Article 35 GDPR before enforcement begins, and to assess whether the programme is compatible with the GDPR's data minimisation and purpose limitation principles.

3. Competition Law and the Digital Markets Act

On 5 September 2023, the European Commission designated Alphabet as a gatekeeper under the Digital Markets Act, with Android among its designated core platform services. From 7 March 2024, Alphabet has been required to comply with the full obligations of the DMA, including those governing app distribution and sideloading. We believe that the Android Developer Verification requirement may be incompatible with those obligations.

3.1 Article 6(4) of the Digital Markets Act

Article 6(4) of the DMA requires that gatekeepers “shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper.”^{3,4}

³ EU Digital Markets Act, Article 6(4) — Obligations for gatekeepers susceptible of being further specified. https://www.eu-digital-markets-act.com/Digital_Markets_Act_Article_6.html

⁴ Regulation (EU) 2022/1925 (Digital Markets Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1925>

The developer verification programme directly prevents this. By requiring every developer who distributes software on Android regardless of whether they use the Play Store to register with Google, accept its terms and conditions, and obtain its approval, the programme establishes Google as an unavoidable intermediary in every software installation on certified Android devices. This is precisely the gatekeeping the DMA was designed to prevent.

The DMA does permit measures to protect system integrity, but these are subject to a proportionality test: they must be “strictly necessary and proportionate.” As detailed in Section 1 above, Android already operates security infrastructure i.e., Play Protect, cryptographic signing, permission controls, that addresses the stated security objective without requiring developer identity registration. The programme therefore fails the proportionality test required by the DMA.

3.2 Alphabet’s Existing Record of Non-Compliance

The Commission has already opened non-compliance proceedings against Alphabet in relation to Google Play. In March 2025, the Commission issued preliminary findings that Google Play prevents app developers from freely steering consumers to better offers, in breach of Article 5(4) of the DMA. Civil society organisations have separately filed complaints arguing that Android’s failure to allow genuine uninstallation of pre-installed apps breaches Article 6(3). The Commission has confirmed that Alphabet’s DMA compliance is an active and ongoing enforcement priority.

The developer verification programme should be treated as part of this pattern. Each individual restriction whether on steering, on uninstallation, or on third-party distribution, narrows the practical openness of the Android ecosystem in ways that compound each other. Enforcement against the verification programme is a necessary component of ensuring that Alphabet’s DMA compliance is real rather than nominal.

3.3 Commercial Conflict of Interest

Google earns a commission on transactions made through the Google Play Store, historically up to 30% on in-app purchases, with a recently announced reduction to 20% for most transactions from June 2026 following antitrust pressure in the United States. The developer verification programme systematically disadvantages every competing distribution channel by imposing friction and cost on developers who operate outside the Play Store, while developers already registered with Play Console are largely already compliant.

The Electronic Frontier Foundation has noted that the programme was announced while Google was simultaneously fighting a US court order requiring it to stop penalising developers who used rival stores. The programme also gives Google access to a comprehensive dataset of Android development activity e.g., who is building what applications, which channels are they distributed. This constitutes a competitive intelligence advantage that should itself be treated as an antitrust concern.

The Epic Games settlement announced on 4 March 2026 makes this contradiction particularly clear. As part of that settlement, Google introduced a Registered App Stores programme, allowing third-party storefronts to apply for certification and receive a smoother installation flow for their users. On the surface, this appears to be a concession to openness.

However, the programme does not change the Developer Verification requirement. Individual developers distributing through any store, certified or otherwise, must still register their identity with Google, pay the applicable registration fee, and submit government identification. The store must be certified by Google, and the developer must be verified by Google. In practice, this means that on certified Android devices, software reaches users only through a system where Google exercises approval at both levels.

If the genuine objective were security, certifying the store could plausibly be sufficient. Trusted stores already vet the applications they distribute. Requiring separate developer identity registration on top of this suggests a broader objective: the creation of a comprehensive registry of developers building for Android, regardless of the distribution channel they use. This layered system of store certification and developer verification raises serious questions under the Digital Markets Act, which requires designated gatekeepers to allow and technically enable the distribution and effective use of third-party software and app stores without imposing unnecessary intermediary control.

A genuine security measure would target software behaviour, not developer identity. The programme's design, which collects identity and commercial intelligence about all Android development, is consistent with a market foreclosure strategy rather than a security objective.

We call on the European Commission to open a formal investigation into whether the Android Developer Verification programme breaches Article 6(4) of the DMA, and to treat this as a priority enforcement matter in light of Alphabet's existing compliance record. We also endorse the Keep Android Open letter and call on other European institutions and national competition authorities to add their voices.

Conclusion

The European Pirate Party represents those who believe that software freedom, privacy, and fair competition are not optional extras but the foundations of a democratic digital society. How software is distributed, who controls the conditions of that distribution, and whether developers can share their work without corporate gatekeeping determines whether the digital ecosystem serves citizens or commercial interests.

The Android Developer Verification programme presents itself as a security measure. In reality, it is a choice about what kind of mobile platform Android will be: open, as it has always claimed, or managed, as Google's commercial interests increasingly demand.

We put these questions to European legislators, regulators, and the Commission: Will we enforce the Digital Markets Act against a gatekeeper using security framing to extend its control over distribution channels it does not own? Will we protect the right of developers to contribute to free software without surrendering their identity to a private corporation? Will we ensure that privacy-focused applications can compete fairly, rather than being structurally disadvantaged by regulations that favour surveillance-based business models?

The Android Developer Verification programme, as currently designed, gives the wrong answers to all three questions. We recognise the legitimate goal of improving platform security. Android's existing mechanisms, address that goal without restricting software freedom. Those mechanisms should be strengthened, not replaced with a centralised identity registry that serves Google's commercial interests as much as its stated security objective.

The European Pirate Party therefore calls for:

1. **Withdrawal of the verification programme for developers distributing outside the Play Store:** Google should commit publicly that sideloading will remain freely available without corporate identity registration.
2. **Recognition of alternative app stores and community repositories:** F-Droid, Accrescent, and similar community-run repositories must be recognised as legitimate and protected parts of the Android ecosystem.
3. **A formal DMA investigation by the European Commission:** The Commission should open proceedings under Article 20 DMA to determine whether the programme breaches Alphabet's obligations under Article 6(4).
4. **A mandatory Data Protection Impact Assessment:** Before any enforcement begins, Google must demonstrate compliance with GDPR data minimisation, purpose limitation, and privacy-by-design obligations.
5. **European institutional support for the Keep Android Open campaign:** We call on MEPs, national parliamentarians, and competition authorities to add their voices to the 37 organisations already on record.

The internet and the software ecosystem we build today determine the democracy we have tomorrow. Europe must choose to enforce the rules it has written.

References

- (EU), R. (n.d.). 2016/679. Retrieved from GDPR: <https://gdpr-info.eu/>
- 19, A. (2025, July). *Digital Markets Act: Civil society calls for investigation into Alphabet's non-compliance*. Retrieved from <https://www.article19.org/resources/digital-markets-act-civil-society-calls-for-investigation-into-alphabets-non-compliance/>
- 2022/1925, R. (. (2022). *Digital Markets Act*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1925>
- ACLU. (2025). *Your Smartphone, Their Rules: How App Stores Enable Corporate-Government Censorship*. Retrieved from American Civil Liberties Union : <https://www.aclu.org/news/free-speech/app-store-oligopoly>
- CFREU. (2012). *Charter of Fundamental Rights of the European Union*. Retrieved from European Union: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>
- Commission, E. (2023, September). *Designation of Alphabet as a gatekeeper under the DMA*. Retrieved from https://digital-markets-act.ec.europa.eu/events-poolpage/2025-alphabet-dma-compliance-workshop-2025-07-01_en
- EU Digital Markets Act, A. 6. (n.d.). *Obligations for gatekeepers susceptible of being further specified*. Retrieved from EU Digital Markets Act, Article 6(4): https://www.eu-digital-markets-act.com/Digital_Markets_Act_Article_6.html

- Foundation, E. F. (2025, November). *Application Gatekeeping: An Ever-Expanding Pathway to Internet Censorship*. Retrieved from Electronic Frontier Foundation : <https://www.eff.org/deeplinks/2025/11/application-gatekeeping-ever-expanding-pathway-internet-censorship>
- Foundation, I. F. (2025, November). *Google Clamps down On Android's Openness*. . Retrieved from Internet Freedom Foundation: <https://internetfreedom.in/google-clamps-down-on-androids-openness/>
- Google. (2025). *Android Developer Verification - Official Page*. Retrieved from <https://developer.android.com/developer-verification>
- Google. (2025, August). *Google Android Developers Blog. A new layer of security for certified Android devices*. Retrieved from <https://android-developers.googleblog.com/2025/08/elevating-android-security.html>
- LIEDTKE, M. (2026, March 5). *Google settles with Epic Games with offer to lower its app store commissions*. Retrieved from <https://apnews.com/article/google-play-store-changes-epic-games-1618d9a98b6a8b37ac2897be5aa105ad>
- Manifesto, E. P. (n.d.). Retrieved from <https://europeanpirates.eu/manifesto/>
- Manifesto, E. P. (n.d.). Retrieved from <https://europeanpirates.eu/manifesto/>
- Open, K. A. (2026). *Keep Android Open — campaign website and resources*. Retrieved from <https://keepandroidopen.org/>
- Prux, M. e. (2026, February). *F-Droid*. Retrieved from An Open Letter Opposing Android Developer Verification.: <https://f-droid.org/en/2026/02/24/open-letter-opposing-developer-verification.html>
- Register, T. (2026, February). *37 groups urge Google to drop ID checks for apps distributed outside Play*. . Retrieved from https://www.theregister.com/2026/02/24/google_android_developer_verification_plan/
- Tank, E. P. (2025, May). *Digital Markets Act enforcement: State of play*. Retrieved from <https://epthinktank.eu/2025/04/24/digital-markets-act-enforcement-state-of-play/>
- Technica, A. (2025, September). *F-Droid calls for regulators to stop Google's crackdown on sideloading*. Retrieved from <https://arstechnica.com/gadgets/2025/09/f-droid-calls-for-regulators-to-stop-googles-crackdown-on-sideloadings/>