DG CNECT/GROW – Draft List of potentially unfair practices

- This document contains preliminary notes and observations on the leaked ‘blacklist/grey list’ of potentially unfair practices concerning platforms drafted by DG CNECT and DG GROW
- If implemented this could significantly impact App Association members
- Keep in mind this is an early draft, so these are initial thoughts and general observations
- As it’s an early stage document the scope of the list is still unclear, which could be a reason for concern for our small business members.
- Comments and questions by the App Associated are marked in red.

“BLACKLIST” (Prohibited practices)

Data Related Practices

1. **Prohibition of exclusive use of data, unless ensuring non-differentiated sharing**: Gatekeepers shall not use data generated and collected on the platform or on any of the gatekeepers’ other services for the purpose of its own commercial activities directed at consumers of the relevant platform, unless they are making this data accessible to business users (seeking to become) active in the same commercial activities.

   a. Alternative “white list” obligation: Gatekeepers that collect third party business users’ data generated and collected on the platform or gatekeepers’ services shall share such data with these third-party business users as well as other interested third parties subject to a consent by the third-party business users.

   b. Alternative DG COMP proposal: Gatekeepers shall not use data received from business users for advertising services for any other purpose than advertising services.

   - If it is gatekeeper/platform generated data, is this list item prohibiting them from using their own data? Or is it about the data generated by business users on the platform?
   - There are legitimate reasons for the platform to use data to provide essential services and improve functioning of the platform, such as running the app store, providing personalized suggestions, preventing fraud, and optimizing the user experience. Encouraging or forcing platforms to make this data available to third parties encourages platforms to breach the privacy of their users and goes against the spirit of foundational EU regulations such as GDPR.
   - Another question relates to consent from third-party business users. What about their own consumers? How does this impact the sharing of data of those third party’s own customers? Is GDPR compliance easily ensured, or does this put platforms or developers at risk of breaching user privacy?
   - Data sharing with business users is generally good, but the type of data included in this list item is too broad and should be clarified. The ‘white list’ item seems preferable.
   - The DG COMP proposal takes a narrower approach, focusing on only advertising services – this may be preferable. It may also be helpful for the Commission to share why they are requiring data sharing: is it because they think it is inherently anticompetitive for some companies to have access to more data or because they think platforms are misusing data?
   - Under this item, would all platforms have the same sharing obligations? Sharing obligations should be platform specific.
   - ‘Accessible to business users’ in which way? Would this facilitate tacit collusion in the market?
2. **Gatekeepers shall offer users the choice whether to combine off-site data with on-site data.**

- Who are the users addressed here? Consumers or business users?
- Is data protection taken into account when considering this obligation for a choice of data combination?
- Generally, combining on-site and off-site data does seem OK for our members as it gives them more data to operate with and less fragmentation/management of different data.
- Will ‘gatekeepers’ be able to access off-site data? If gatekeepers aren’t able to process data themselves, is it realistic to expect them to allow this for users?

**Self-preferencing practices**

3. **Ban of preferential display/ranking:** Gatekeepers shall not provide preferential display/ranking in online search engines or online intermediation services for their own downstream services/offers.

- Not having preferential display/ranking of own services is beneficial to our members, as transparent and fair ranking practices on app stores is crucial to their success.
- This preferential ranking of own services also goes against what users want. If a user has temporarily removed the default mail app and a few days later they are once again looking at mail apps in the app store, it’s likely that the may want to install their old mail app. Prohibiting platforms from suggesting the default mail app creates a much worse user experience.
- This provision should be carefully worded so it does not prohibit all ranking on app stores. The P2B regulation requires platforms to disclose the main determining factors of their ranking algorithms to facilitate app store optimization and enable developers to tailor their products so they can be found more easily.
- App stores don’t do preferential ranking/display. This was a problem in the past, but app stores have taken recent steps to change their own practices so that ranking algorithms no longer privilege their own products.
- What would happen if gatekeeper products are ranked/rated the highest solely through the regular ranking criteria?

4. **Ban on exclusive pre-installation:** Gatekeepers shall not pre-install exclusively their own applications nor require from any third-party operating system developers or hardware manufacturers to pre-install exclusively gatekeepers’ own applications.

- It can be argued that there is an advantage for preinstalled apps – but both app stores constantly highlight alternatives to their own app and many of those competitors that aren’t preinstalled are much more successful (e.g., Apple Music vs. Spotify, Microsoft Office vs. Google equivalents).
- Consumers reasonably expect phones to come with certain things preinstalled (e.g., internet browsers, messaging, calling, email clients). These apps can now largely be uninstalled.
- In Apple’s case, they manufacture their devices – so, is it not an infringement on their freedom to conduct business to prohibit the installation of the apps Apple wants on its devices?
- This provision is a Pandora’s box. How is decided which other apps should be pre-installed and who decides what they are? This only provides an additional advantage to incumbent popular apps and prohibits up-and-coming innovative apps from small SMEs from joining the party (because they are too small/unpopular/lack financial resources to be pre-installed). Instead, a
regulation where platforms can offer alternatives to pre-installed apps, that are easily searchable and discoverable but not installed, would be preferable.

5. **Gatekeepers shall not, through contractual clauses or technical measures or otherwise, prevent users from uninstalling any (of the pre-installed) apps.**

- Apple and Google both have several more of their own apps that are preinstalled, which are a core part of the user experience. Removing these apps would only cause user confusion.
- Some of the preinstalled apps may be central to the functioning of a device and uninstalling them may affect the integrity/security/functioning of the phone. If users are permitted to uninstall whatever apps they want, perhaps they should be shown a warning that they may corrupt the device/invalidate their warranty.

6. **Ban of narrow parity/ban of side-loading for app stores:** Gatekeepers shall not restrict the ability of business users to offer the same goods and services to consumers under different conditions through other online intermediation services or online search engines than through their own platform or services.

- This seems like a non-issue for app stores. Mobile apps can be available on multiple stores under different conditions with a wide variety of business models.
- App stores already don’t restrict ability of business users to offer the same goods/services through other app stores or platforms; most apps you can find on one store will have several apps on the other platforms that offer equivalent functionality.
- Even platforms themselves support most apps on multiple stores (e.g., you can get Google Mail on your iPhone or listen to Apple Music on an Android OS phone).
- Side-loading risks installing lower quality apps that potentially pose security risks and could decrease consumer trust in mobile apps as side-loaded apps have potentially not gone through a rigorous review process. This will harm consumer trust and therefore make it less likely for consumers to trust apps from SMEs who don’t have an established brand.

7. **Anti-steering ban and side-loading ban:** Gatekeepers shall not, through contractual or any other measure with equivalent effect, prevent:
   a. Third-party sellers from promoting offers to their customers and from concluding contracts with these customers for the provision of these customers’ services outside of the gatekeeper’s platform or services (anti-steering ban).
   b. The installation of applications by third-party business users outside the gatekeeper’s platform or service (ban on side-loading)

- Seems like a duplication of the previous point. Both should be defined in greater detail to clarify what the difference is.
- Apple and Google do ‘steering’ in some way, but so do app makers, and there are universally accepted workarounds. For example, Spotify, Netflix, and numerous other apps all only offer subscription outside their apps and the platforms do not prohibit this.
- Platforms do prohibit actively promoting other offers and payments in the apps, but this is an issue primarily exclusive to big brands. For small businesses and consumers, centralized payments and refunds are safe and convenient.
• Side-loading risks installing lower quality apps that potentially pose security risks and could decrease consumer trust in mobile apps as side-loaded apps have potentially not gone through a rigorous review process. This would reduce consumer trust which only benefits big brands and causes substantial harm to SMEs.
• Having multiple app stores available on a smartphone increases the financial burden for small businesses to be present on each one to gain access to the maximum number of customers.

8. **Ban on complaints:** Gatekeepers shall not, through contractual or any other measures with equivalent effect, prevent or discourage business users from complaining about gatekeepers’ practices.

• Which practices is this about? Not specific enough.
• This seems like a non-issue on the app stores. App makers and users can and do occasionally complain, and their complaints have resulted in policy changes (e.g., template apps).
• App stores have centralized complaints and dispute settlement systems that make it easy for developers to submit complaints.
• The P2B regulation already provides a process for this.
• They also have incentive for app makers to complain to ensure a great user experience on the app stores.
• This seems like it may overlap with the fundamental right to freedom of expression which may make it inappropriate to include in a blacklist.

9. **Gatekeepers shall not, through contractual or any other measures with equivalent effect, prevent or discourage business complaints against discriminatory access conditions, as well as closing of accounts and product delistings by gatekeeper platforms.**

• What are considered discriminatory access conditions? App store access conditions are the same for every business user.
• Can business users complain about legitimate account closures and product delistings?
• There are legitimate reasons to delist certain app makers from the platform. These reasons are not always entirely predictable. There’s a cat-and-mouse game between bad actors on the one hand, seeking to take advantage of users, and the platforms on the other hand, seeking to preserve safety and trust. For regulation to disturb this balance would be destructively disruptive.
• P2B already covers this by providing transparency and mediation tools.

**Bundling and tying practices**

10. **Gatekeepers shall not require a user to sign up/register with an email service of the platform when using another of its products.**

• When gatekeepers offer ways to provide enhanced privacy protection for users to sign-up or register, a regulation prohibiting the requirement to offer this service would be anti-privacy and anti-consumer.
• This is not the case for app stores
11. Gatekeepers shall not automatically sign users in to more than one of a gatekeeper’s products without giving users possibility to opt in to such a system.

- Sign-In with Apple, for example, is a great service, and not allowing Apple to require app makers to offer it is anti-consumer.

**Auditing of gatekeepers’ services – no comments on auditing**

12. Gatekeepers providing digital advertising services shall submit to an annual audit of their advertising metrics and reporting practices. The audit shall assess the degree of transparency and accuracy of information available for business users to evaluate the performance of the gatekeepers’ advertising services. It shall be made public. The audit shall be co-designed with the European Commission.

   a. Alternative DG COMP proposal: Gatekeepers shall transmit pricing data to advertisers and publishers combined with an obligation to provide access to advertisers and their agents to carry out their own independent verification.

13. Gatekeepers shall submit their consumer profiling practices to annual audit, which shall be made public. The audit shall focus in particular on cross-service tracking and their respect for EU data protection legislation including the GDPR and the e-Privacy Directive. The audit shall be co-designed with the European Commission.

**General Compliance Measures**

14. Gatekeepers shall provide to the competent regulatory authority any information that is necessary to ensure compliance with the rules and enable the same regulatory authority to monitor market developments.

- Who is the competent authority? Commission? Member State competition authorities?
- What constitutes ‘necessary information’? Is this information that shall be provided upon request or volunteered information?

15. Gatekeepers shall notify any planned mergers and acquisitions, as well as (technical) partnerships and new activities. Such notifications have no suspensive effects.

- Although there are no suspensive effects, this seems like overreach.
- ‘New activities’ – what does that mean? Research, development, business development?
- What constitutes a ‘technical partnership’?
- Such a notification scheme may deter businesses from these activities altogether.
- Who shall they send this notice to? If the gatekeeper is based in the United States and plans a merger with another U.S. company, would this require them to report that merger to the EU? If the gatekeeper is based in the EU and plans a merger with a U.S. company, are they obligated to report to both?

16. Gatekeepers shall appoint compliance officers to ensure compliance with rules laid down in the legal act.
• Which legal act? The DSA? This list?
• SMEs can be gatekeepers too and having a special employee for this may be a substantial burden. (In the IA on ex ante regulation, the definition of gatekeeping platforms included SMEs. The one on the DSA/liability rules didn’t. This should be clarified)

“GRAYLIST” (Unfair practices where intervention by the competent regulator is required)
Generally, this list should be more targeted and specific to each platform.

Data related practices
17. **Prohibition of access to one’s own customer data:** Gatekeepers shall not, through contractual or any other measures with equivalent effect, prevent third-party sellers from accessing essential information that gatekeepers collect on customers of these business users subject to consent of these customers for such sharing of information with third party-sellers.

• While this may be a reasonable request, this concern doesn’t acknowledge the benefits of safeguarding consumer privacy that platform practices generate.
• What is considered ‘essential information’?
• How will consent be obtained? General consent for all third-party data sharing or will new consent have to be given each time/for each new purpose? If general, privacy concerns. If not general, may be burdensome on consumers.

18. **Gatekeepers shall not collect personal data beyond what is necessary for the provision of their services to the users of their services**

• Who determines what is ‘necessary’ for provision of services?
• GDPR already mandates data minimization.
• Is this about business users or (end) consumers?
• Is the concern just about the collection of personal data or retention of it?

19. **Ban of restrictions on use of business users’ data:** Gatekeepers shall not restrict by technical or commercial means business users from accessing, handling or using the data they provide, receive or generate over the course of their use of the gatekeepers’ platforms or services

• This seems reasonable that businesses can access, handle, or use their own data in the (legal) ways they want.
• Gatekeepers may want to compete on privacy. They may want to say, “If you use our platform, you can rest assured that your data will not be used for [this purpose].” That’s a laudable way to compete, and the Commission should not prevent this in any way.

20. **Gatekeepers shall take appropriate and reasonable technical and contractual measures to enable the business users and consumers of their platform or services to use any other platform or service by means of providing enhanced portability of personal and non-data or forms of interoperability.**

• This also seems reasonable if done within the legal limits of EU data protection rules.
21. **Obligation to share click-and-query data**: Gatekeepers shall share their search and click data in relation to search and search advertising at a nominal price or under FRAND terms

- Concerning use of ‘FRAND’ in the data sharing context. FRAND commitments are done on a voluntary basis.
- Who should this data be shared with? Business users? Regulators?
- What purpose does this serve, and could it be an over-reach?
- Are we talking in aggregate or specific to a particular user? If it’s the latter, this would be a profound breach of privacy.

**Self-preferencing practices**
22. **Ban on restriction of options**: Gatekeepers shall not prevent, by any technical or commercial means, hardware manufacturers from providing their customers and business users with a choice of options for applications/services to be used on/accessed via the hardware.
   - Alternative: Gatekeepers, irrespective if they are hardware manufacturers or not, shall ensure that their customers and users have a choice of options for applications/services to be used on/accessed via the hardware.

- Users have choice/options on which apps to use on their devices. Any app is usually available on multiple app stores for any device. The only sticking point here may be that the app stores specifically are targeted for not giving customers/businesses a choice which one to use on Apple devices.
- Vertical integration is important for improving customer experience.

23. **Gatekeepers that are operating system developers or smartphone manufacturers shall allow third parties to access the same operating system or smartphone features that are available to/used by gatekeepers’ own products.**

- What’s available to Apple’s and Google’s apps is available to everyone else who makes apps: they can develop for the OS and be available on the same app store on which their own apps are available.
- Looking at features and interoperability, most of those issues (e.g., Spotify not being able to be opened via Siri have been addressed by APIs in new versions of iOS). Subscriptions to services like Spotify, Netflix, and the Financial Times have successfully signed up users independent of the App Store, through their own websites, and while users enjoy their services through apps – they are circumventing the features available to all apps.
- There’s a natural evolution where new features that are initially available to OS-specific apps later become available as an API. It’s not always easy to predict whether something will take off and become highly popular or whether a new feature will have limited acceptance. The standard process in place today, where the OS releases new features and over time makes API available, seems to be working well.

24. **Gatekeepers shall allow their customers to use identification services by third parties which provide the same level of security to access gatekeepers’ platforms or services.**

- Who determines the same level of security?
- Multiple identification services reduce consumer convenience.
• Having one identification service benefits privacy/GDPR compliance.

25. Gatekeepers shall ensure equal treatment between own activities and those of their business users in providing:
   a. Functionalities and quality of services of online intermediation services,
   b. Ancillary services to the gatekeeper’s online intermediation service directly related to the business users’ offers such as delivery, payment, or insurance services
   c. Identification service, which provide the same level of security to access gatekeepers’ platform or services

• By providing ancillary services like delivery, payment, etc., platforms have decreased entry barriers for small app developers. [Link](https://actonline.org/wp-content/uploads/ACT-Platforms-in-the-Digital-Economy-How-to-Preserve-a-Successful-Ecosystem.pdf)

• Functionality and quality of the app stores is a key priority to retain consumer trust and attract business users, so ‘gatekeepers’ already have strong incentives to ensure that these are equal for everyone.

• Re identification services: Who determines the same level of security? Multiple identification services reduce consumer convenience and having one identification service benefits privacy/GDPR compliance.

26. Gatekeepers shall not apply unfair or differentiated pricing conditions for the equal provision of platforms or services to third-party business users.

   • P2B addresses differentiated treatment already.
   • Pricing conditions are the same for everyone on the app store, various options are available to every business user (e.g., subscription models, in-app purchases, freemium, etc.)

27. Gatekeepers shall not refuse to interoperate/access for third-party ancillary services at the request of its business users or third-party service providers where the gatekeeper provides ancillary services to its online intermediation services (e.g. data analysis services, delivery, payment etc.)

   • This would mostly benefit big brands that have the resources to request access for their own ancillary services and leave small businesses behind.
   • Enables special treatment for those that can afford it.
   • Ignores the notion of ‘good’ gatekeeping that ensures security and safety, high-quality, and excellent customer experience.

28. Gatekeepers shall not discriminate in providing interconnection between their service and other services, or in the interoperability between their service and related services.
   a. Alternative: gatekeepers shall offer meaningful interconnection with and/or interoperability to their services.

   • How is a ‘related service’ defined? What kind of interoperability is under consideration here? What is the difference they understand between interconnection and interoperability?
   • The alternative is reasonable but most of the interoperability issues seem to resolve themselves/existing ones have been resolved.
   • How is ‘meaningful’ defined and who determines it?
29. **Gatekeepers shall not, through misleading technical or commercial means, encourage customers (of its business users) to replace services of business users with their own.**

- Does that mean gatekeepers can’t advertise their own products? That seems unreasonable.
- This depends on the definition of ‘misleading technical or commercial means’. If misleading only applies to technical means, then it sounds like they cannot use commercial means to advertise their own products. If it applies to both, then it seems to imply that misleading customers in any way is problematic, but legitimate commercial advertising is still acceptable.

**Building and tying practices**

30. **Gatekeepers shall not require the acceptance of supplementary conditions or services that, by their nature or according to commercial usage, have no connection with and are not necessary for the provision of the platform or services to its business users.**

   a. Alternative: Gatekeepers providing online intermediation services shall not differentiate the conditions for the provision of the relevant services for third party business users based on acceptance of supplementary services from third-party business users on their online marketplace.

- Who determines what has a connection and is necessary for the provision of the platform/services?
- Platforms should be able to set their own terms and conditions – freedom of doing business.
- Especially in the context of app stores, terms and conditions that apply the same for everyone are essential in providing quality, security, a better user experience, and level playing field.
- Without terms that protect the user experience, consumers welfare would decrease due to lower quality apps and security risks. The role of the app store terms and conditions in preserving consumer confidence is crucial for our members.