THE ITALIAN COMPETITION AUTHORITY CLOSES ITS INVESTIGATION AGAINST GOOGLE ACCEPTING ITS COMMITMENTS ON CONSENT MECHANISMS FOR CROSS-SERVICE DATA LINKING.

By Enzo Marasà (partner), Irene Picciano (partner), Giulio Novellini (partner)

The Italian Competition Authority ("**AGCM**" or "**Authority**") has closed its investigation of Google's cross-service data linking consent practices by accepting binding commitments aimed at substantially amending Google's current consent request interface. Launched in July 2024, the proceedings ended on November 4, 2025. The Authority wanted to assess whether Google's request for user consent to "link" personal data across its services constituted an unfair commercial practice against consumers. However, instead of finding an infringement and imposing a fine, the Authority accepted Google's commitments and made them binding under the Italian Consumer Code[1].

Google will now have to implement enhanced transparency, granular consent options, and user notifications to ensure consent is duly informed and freely given, thus also aligning with obligations for digital gatekeepers designated under the Digital Markets Act ("**DMA**"). Indeed, this decision is another notable instance of how different pieces of legislations and the related public objectives – the protection of consumers, personal data and competition – may interplay over a same conduct regarding personal data in the digital sphere; and it also marks how the AGCM is able to retain jurisdiction and the role of main regulator in the digital field in Italy despite the overlap of competences with the European Commission and with Member States' privacy watchdogs.

The scope of the investigation and its composite legal framework: overlap and partition of competences.

The Authority's investigation specifically targeted Google's pop-up consent notice (the "**pop-up notice**") asking logged-in users on services like Search, YouTube, and Google Play (Google's digital marketplace for mobile apps) to allow combined and cross-use of personal data across Google's services. Notably, Google as a designated gatekeeper under Article 5(2) DMA must obtain user consent before linking data between its core platform services. Since enforcement of the DMA is primarily an EU-level competence, the AGCM asserted jurisdiction under Italy's consumer protection rules (Articles 20–25 of the Consumer Code, which reflect the provisions of Articles 5-9 of Directive 2005/29/CE) to contest an unfair commercial practice in how the consent was gathered, although coordination with the European Commission's DMA enforcement unit was maintained throughout the proceedings.

While the DMA mandates a consent mechanism to protect user choice and the ability of gatekeepers' challengers to contend valuable user data in the digital markets, national authorities may remain alternatively or additionally competent to apply consumer protection law to ensure that the provider's interface is not misleading or coercing consumers into consent. By contrast, given the existence of more specific EU law provisions governing consent requirements for digital gatekeepers, the scope for GDPR enforcement and privacy authorities to retain a prevailing or concurrent role in this area appears limited. Such authorities may nonetheless intervene in cases of total absence of consent or within the context of broader privacy violations, provided that cooperation with the European Commission is ensured. Further, consent practices by digital gatekeepers over the use of personal data may also overlap with pure competition law rules on abuse of dominance (Article 102 TFEU and the national equivalent), as also highlighted by another recently issued decision of the AGCM against a different gatekeeper with respect to consent tracking requirements it imposed on third-party app developers[2].

However, the issue of partition of competences in regulating and investigating conduct relating to personal data in digital markets is not dealt with in this decision of the AGCM. Notably, this matter has been the object of previous Italian judgements of the last instance administrative court (namely, Judgments of the Council of

[1] PS12714 – *Google/Consent for linking of services*, Decision N. 3172 of 4 November 2025 (see here).
[2] A561 – *App tracking transparency di Apple*, Decision N. 31772 of 22 December 2025 (see here).

State N. 2361/2021, N. 497/2024 and N. 80/2025), which – by relying on the principles set out in the judgement of the CJEU in Case C-54/17 and C-55/17 – confirmed the jurisdiction of the AGCM to investigate and sanction digital platforms' conduct concerning the collection or treatment of user data under EU and national consumer protection rules. The courts in these cases also established that, as a condition for legality of its action, the Authority must comply with a duty to coordinate and loyally cooperate its intervention and final decision with the other potentially competent authorities over the same conduct (including in other Member States), to avoid the risk of conflicting decisions, disproportionate fines or double jeopardy.

The initial concerns of the Authority: consent request deficiencies.

The AGCM initiated the proceedings by preliminary alleging that Google's original consent prompt was possibly misleading and coercing consumers into providing consent. More specifically, the Authority argued that the mere reference to the linkage of data across Google services in the pop-up notice did not provide a sufficiently clear explanation of the extensive cross-service sharing of personal data that this entailed. Google was also omitting key information as it was failing to mention all Google services involved (including non-core services and upcoming AI features for Google's Gemini).

In addition, according to the Authority's preliminary view, Google stopped short of informing users that they could customize consent on a *per-service* basis. As to Google's conduct being "aggressive", the Authority noted that Google's practice of temporarily blocking access to services (like disabling Search functionality) until a choice was explicitly made exerted undue pressure on users, who could make a hurried and uninformed choice for fear of not being able to exploit important features of the service. Indeed, Google also warned users that if they declined consent, *"some features… will be limited or* unavailable", a formulation which might have pressured users into consent according to AGCM. Therefore, it preliminary considered these practices to be possibly in breach of the Consumer Code's provisions on misleading (Articles 21–22) and aggressive (Articles 24–25) practices.

Google's commitments: enhanced transparency and more user control.

To resolve these concerns, Google offered a comprehensive package of commitments, subsequently made binding by the decision of the Authority: Google committed to clarify the purpose and scope of data linking in the consent dialog, specifically by making it clear to users in the pop-up notice that when services are linked, they can share personal data with each other, and will reference the DMA legal basis for the consent requirement. Google will also provide clearer and more accurate information to users on the implications of consent for the use of their data, as well as on the range and volume of Google's services (including AI services, such as Gemini) where consent may involve the "combination" and "cross-use" of personal data."

In addition, Google will improve user choice mechanisms for a more granular consent: the interface will now allow users to tailor consent to specific services: a new control to "Select or deselect all" services at once will make it easier to refuse all data linking as it was to accept it.

Furthermore, the commitments will also tackle the perceived coercion in the original design as Google will modify the wording that previously emphasized loss of functionality upon denial of consent to data linking: the new notice will affirm that if services are not linked, *"the vast majority of features will remain unaffected"*, while only certain features (those inherently requiring inter-service data sharing) might be limited.

Individual notifications to users.

Google also committed to to reach out to users who have already responded to the previous consent prompt: once Google rolls out the new consent interface, a personalized email notification will be sent to all Italian users who previously made a choice (either consenting fully or partially or even refusing consent altogether). The message will summarize current consent settings, highlight what new information will now be provided

and provide the same clarifications and options for more transparency and user control over their data illustrate above.

Google committed to implement all these measures within six months of the AGCM's decision and must report back on compliance.

The implications of the decision - enforcement outlook.

AGCM's acceptance of Google's commitments marks a regulatory blueprint for digital platforms on how to collect user consent for data integration across services. More generally, it signals the Authority's willingness to retain a leading role in enforcing consumer protection laws in the digital sphere, as along with competition law, to curb interface designs that nudge or pressure users to provide consent in exploiting their personal data across services.

This is something that is especially relevant when the company holds a dominant position or is a designated digital gatekeeper under the DMA. However, irrespective of whether a digital platform holds a dominant position or can be designated as a gatekeeper, this decision and the set of commitments undertaken by Google serves as a guidance to what informative framework and consent mechanism for cross-linking of data (including with AI tools) the AGCM deems compliant with the high bar of protection of consumers that it is willing to enforce.

Despite the apparently prevailing competence of the European Commission and other authorities over similar conduct, The AGCM has proven particularly effective in keeping a leading enforcement role in the digital sectors within the EU block, thanks to its flexible approach in framing a broad range of conduct concerning the collection and use of personal data under different theories of harm, which may fit either with a breach of consumer laws or a competition law infringement. Technical skills in handling both regimes with a holistic and complementary approach, paired with ability and soft-power in cooperating and coordinating interventions with the other EU agencies, have made the AGCM's enforcement harm towards digital service providers particularly far reaching and dreadful to disregard.