Title: Shifting toward "Structural Enforcement (Sanctions)" against State-Scale Digital Monopolies

1. Introduction: Overcoming the "Remedy Vacuum (Governance Gap)" in Multinational Value Chains

This draft of the Guidelines (Guidelines 04/2026) marks a pivotal advancement, as it formalizes the criteria for effectively combining the corrective powers and administrative fines stipulated under Article 58 of the GDPR. However, the contemporary digital ecosystem is dominated by "vertically integrated supply chains" that seamlessly unify space communications, autonomous frontier AI, and terrestrial legacy infrastructure (such as broadcast airwaves and power distribution systems).

Under such complex, multi-layered architectures, if cases arise where data subjects' biometric or neural telemetry data are collected and reverse-circulated entirely without informed consent, the traditional approach of imposing "individual fines on a single corporate entity" creates a structural "remedy vacuum." This position paper proposes revisions to the sentencing and fining criteria to effectively rectify the loophole wherein Big Tech conglomerates treat administrative penalties merely as a "cost of doing business," thereby evading true accountability.

2. Eliminating "Lizard’s Tail Cutting (Scapegoating)" within Multi-layered Architectures: The Necessity of Joint and Several Aggravated Sanctions for Joint Tortfeasors (Intervention in Step 3)

Top-tier multinational infrastructure owners (platform conglomerates) frequently utilize "terrestrial downstream commercial operators" within domestic jurisdictions, such as Japan, as intermediary communication nodes. When a data breach or infringement is detected, there is an exceptionally high risk that these mega-corporations will leverage their financial dominance to ignore economic sanctions, or scapegoat downstream peripheral entities ("cutting the lizard's tail") to escape into governance blind spots. Therefore, within Step 3 of the Guidelines (Assessment of the Seriousness of the Infringement), data protection authorities must incorporate the following criteria:

- **Proposed Amendment to the Criteria:** Where an infringement is systematically executed across a vertically integrated value chain spanning multiple operators, the upstream infrastructure owner shall bear an absolute governance obligation over downstream operational dynamics. If the upstream entity fails to halt automated deletion programs or execute emergency data kill-switches even after acquiring "actual knowledge" of the legal violation, such conduct must be redefined not as mere individual negligence, but as "structural gross negligence (willful omission)," serving as an absolute prerequisite for imposing maximum administrative penalties.

3. Seamless Interoperability and Evidentiary Transfer Between Administrative Corrective Powers and Criminal Prosecution Procedures

To truly manifest the effectiveness targeted by these Guidelines (Guidelines 04/2026), the application criteria for administrative fines must not operate in isolation. The non-consensual invasion of the biometric and neural domains via cutting-edge, vertically integrated supply chains constitutes not only a breach of data protection laws but concurrently exhibits the dimensions of a severe criminal offense (systemic rights infringement) against personal dignity.

Consequently, server logs, API communication histories, and processed biometric tag data forcibly extracted from defendant corporate groups by data protection authorities

leveraging their potent administrative audit and corrective powers must serve as decisive material evidence (the paper trail) for criminal investigations by law enforcement agencies, such as national prosecutors and police. Within these Guidelines, the EDPB must explicitly formalize a cooperation framework for "transferring and sharing administrative evidentiary logs secured by authorities to national criminal investigation and prosecution procedures without delay upon the data subject's request," thereby ensuring the complete concurrent application and interlocking operation of administrative sanctions and criminal prosecutions.

4. Stringency of Cumulative Enforcement Based on the "Duality of Purpose": Inseparable and Simultaneous Imposition of Emergency Injunctions and Administrative Fines (Intervention in Step 5)

We fully endorse the "duality of purpose" (the simultaneous achievement of normalizing the state of infringement and imposing social sanctions) within Step 5 of the Guidelines (Selection of Effective, Proportionate, and Dissuasive Measures).

To deter the runaway behavior of highly automated supply chains and the constant, non-consensual biometric identification and neural profiling, the mere imposition of monetary fines (administrative penalties) is insufficient; furthermore, corporations must not be permitted to subsequently excuse themselves by claiming, "We will comply with the order, so please waive the fine."

In response to severe human rights violations—such as the total collapse of the quality of life (QOL) or the destruction of bodily integrity currently endured by data subjects—the simultaneous and cumulative application (concurrent enforcement) of both an "emergency enforcement injunction (an order for the immediate physical and technical termination of the target lock)" under Article 66 of the GDPR and the "maximum tier of administrative fines (massive financial sanctions)" as an inseparable package constitutes a critical means to manifest a truly dissuasive outcome against mega-monopolies.