POLICY BRIEF | REPUBLIC OF KOREA | SEPTEMBER 2026
ILF-ROK-PB-2026-02-EN

# From Reporting to Victim Protection: Building a Safe Digital-Sex-Crime Enforcement Chain

## Short Introduction

South Korea is expanding public reporting of digital sex crimes and illegal distribution channels. For reporting to produce meaningful victim protection, privacy safeguards, institutional accountability and traceable outcomes must govern the entire chain from report to removal, blocking and investigative referral.

## Action Needed

- Apply data minimisation and automatically redact unnecessary victim-identifying information from reports and takedown requests.
- Regulate transfers among public bodies, support organisations, platforms and third parties, including retention and onward disclosure.
- Track each case from receipt through verification, removal or blocking, investigative referral and follow-up.
- Publish victim-protection outcomes separately from raw reporting, URL and takedown volumes.
- Establish rapid notification, re-exposure monitoring, legal assistance and redress when victim information is exposed.

## What Is the Problem?

From 16 September to 31 December 2026, the Ministry of Gender Equality and Family and the Anti-Corruption and Civil Rights Commission are seeking public proposals concerning the prevention of digital sex crimes, victim protection and support, punishment and institutional improvement. The initiative also covers reports concerning illegal filming, sexually explicit deepfakes and child and youth sexual exploitation material. Information received may support removal, blocking and investigative referral.

This forms part of a broader shift in South Korea from individual takedown assistance toward an integrated enforcement system combining detection, site analysis, removal, blocking, investigation and inter-agency coordination. The government has also developed AI-supported continuous detection and automated takedown-request functions.

Yet the expansion of enforcement also expands the pathway through which victim and reporter information may travel. The Personal Information Protection Commission is investigating the external exposure of information connected to digital-sex-crime takedown requests transmitted to Google. Its inquiry includes the scope and categories of information disclosed, the period of disclosure, the lawful basis for third-party provision and the handling of sensitive information. The Commission has also identified the potential for secondary harm.

The performance of a reporting system should therefore not be judged by how much information it collects. It should be judged by whether illegal material can be identified and removed rapidly while using the minimum personal information necessary and preventing the protection process itself from creating a new exposure risk.

## What Can Be Done?

### 1. Minimise Personal Data at the Reporting Stage

Government should distinguish information needed to identify illegal content from information needed to identify a victim. A report concerning an illegal site or distribution channel should prioritise the URL, content category and other minimum information necessary for enforcement.

Victim names, contact details and other identifiers should not be required unless they are necessary for a defined operational purpose. When required, identifying information should be stored separately from case information and subject to stricter access controls.

The reporting process should also avoid encouraging users to download, reproduce or retransmit illegal material as proof. Clear instructions should allow reporting through URLs and minimum verification information wherever possible. This approach can expand reporting without unnecessarily reproducing illegal content or creating additional privacy exposure.

### 2. Control the Entire Information Pathway

Victim protection does not end when a public authority receives a report. If information is transmitted to a support organisation, investigative authority, platform or external entity, the system should identify who receives which information and for what purpose.

Government should establish minimum rules governing third-party provision, access rights, retention, onward disclosure, deletion and incident notification. Before identifying information is included in a platform takedown request, authorities should determine whether that information is actually necessary to obtain removal or blocking.

The Google investigation demonstrates that downstream disclosure is not merely a theoretical risk. A digital-sex-crime response system must remove harmful content without allowing the removal process itself to create another pathway through which victim information can become exposed.

### 3. Make Enforcement Traceable from Report to Outcome

Reporting volume alone cannot establish whether the system works. Each report should have a traceable pathway covering receipt, verification, takedown request, blocking, investigative referral, follow-up and closure.

Responsible institutions and baseline processing periods should be defined. Where appropriate, reporters or victims should be able to determine whether a report has been reviewed and what action followed.

Where the same content reappears under another URL or domain, the first successful removal should not automatically close the matter. A procedure for detecting and responding to redistribution is necessary. This would convert Korea's expanding detection, automated takedown and investigative infrastructure into a measurable enforcement chain.

### 4. Measure Victim Protection, Not Only Takedowns

Government statistics should distinguish reports, URLs, individual items of content, websites, affected victims, removals or blocks, and investigative referrals. These units are not interchangeable. A single

victim's material may generate hundreds of URLs, meaning that a rising takedown count cannot by itself establish either an increase in victims or an improvement in protection.

Performance reporting should include processing times, successful removals or blocks, detected redistribution, repeat domains, investigative referrals and available follow-up outcomes.

Where victim information itself has been exposed, notification, additional removal, monitoring, legal assistance and redress should also be measured separately. As Korea expands its digital-sex-crime response infrastructure, the central question should move from how much the system processed to what the system actually protected.

## Conclusion

Greater public participation can strengthen South Korea's response to digital sex crimes, but increased reporting does not itself guarantee victim protection. Data minimisation, controlled disclosure, traceable case handling and effective remediation should govern the entire information pathway from reporting through removal, blocking and investigative referral.

The recent exposure involving takedown-request information demonstrates that a process designed to remove harmful content can itself create a new privacy risk. The present policy-development period provides an opportunity to build these safeguards into the enforcement system before such failures become structural.

## Policy Intervention Stage

Pre-implementation policy intervention
Public participation period: 16 September–31 December 2026

## Primary Sources

Ministry of Gender Equality and Family and Anti-Corruption and Civil Rights Commission, public participation initiative on proposals to eradicate digital sex crimes, September 2026.

Personal Information Protection Commission, investigation concerning exposure of information associated with Google's digital-sex-crime takedown requests, 11 September 2026.

Ministry of Gender Equality and Family, government materials concerning digital-sex-crime victim support and AI-supported 24-hour detection and takedown assistance.