

Submitted by: Event Industry Association of Ireland (EIAI)

Date: 14 September 2026

Observation 1

COP Sections 1.3, 1.4, 1.7 and 2.4.1: Application to temporary events and identification of the relevant third party

The Event Industry Association of Ireland recommends that the final Code, or accompanying practical guidance, expressly address the application of the framework to temporary events and other multi-party CCTV environments.

Event CCTV frequently operates differently from a permanent CCTV installation controlled and operated by a single organisation. A venue may own permanent cameras while an event organiser commissions an additional temporary system. A specialist CCTV supplier may install, configure and technically maintain the cameras, network and recording infrastructure, while a separate security provider staffs the control room and actively monitors the live feeds. The organiser or venue may determine the purposes for which the system is used, while information from CCTV may also be used within Event Control to support crowd management, public safety and security.

As a result, the organisation that owns the equipment, the organisation that provides technical administration, the organisation whose personnel physically operate the system and the organisation acting as data controller may not be the same entity. The person capable of displaying or controlling a particular camera feed may therefore work for an organisation that does not have legal responsibility for determining whether access should be provided.

These temporary arrangements may exist for only a few days, making it particularly important that the relevant responsibilities and points of contact are identified before the event begins.

EIAI recommends that the final guidance explain clearly how the relevant third party should be identified where ownership, technical control, live monitoring and data protection responsibilities are distributed between different organisations. It should also clarify who should receive an authorisation or approval, the role of a contracted security operator, and the position of a technical CCTV supplier that retains administrator access but does not undertake live monitoring.

These responsibilities should be capable of being determined before the event rather than requiring frontline personnel to resolve them during a live incident.

Observation 2

COP Sections 1.8 to 1.12 and 2.2: Authorised access, urgent access and multi-agency Event Control

EIAI recommends that the Code be supported by a clear operational process explaining how a third party should implement Garda access once an authorisation or approval has been granted. This should address how the identity and authority of the Garda personnel concerned can be verified, which cameras or areas are covered, any conditions or restrictions attached to the access, when the access begins and expires, and how it should subsequently be terminated.

This is particularly important in a major event environment. Event Control may include representatives of An Garda Síochána, local authorities, fire services, health or medical services, event management and private security. CCTV operators may therefore receive operational requests for information from several legitimate partners.

The guidance should make clear that access under this statutory framework is triggered only by an appropriately authorised Garda request. Operators should be able to distinguish such a request from other operational requests made by statutory, emergency-service or event partners who may be working alongside Garda personnel within Event Control.

Urgent circumstances also require particular clarity. During live incidents, CCTV operators may be required to act under considerable operational pressure, particularly where Garda personnel are physically present within Event Control or the CCTV control room.

Operational urgency does not remove the need for the statutory process to be followed.

Operators should therefore have a straightforward means of verifying the basis and scope of a request and an escalation route where anything is unclear. Frontline CCTV personnel should not be expected to make complex legal determinations while simultaneously managing a safety or security incident.

The objective should be to support rapid lawful access while ensuring that operators are not placed in a position where urgency, physical proximity or operational pressure results in required safeguards being bypassed.

Observation 3

COP Sections 1.7, 2.2 and 2.6: Continuity of event operations, operator capacity and technical resilience

EIAI recommends that implementation of Garda access take account of the continuing operational role of CCTV within an event. Event CCTV may simultaneously support crowd monitoring, incident identification, emergency access, perimeter management, security deployment and other safety-critical functions. Facilitating Garda access should not remove or materially reduce the event CCTV team's ability to continue carrying out these functions.

Processes for implementing access should therefore preserve continuity of event-safety monitoring and take account of operator workload and welfare. Additional access-related tasks should not place an operator in a position where their ability to maintain attention on safety-critical surveillance is compromised.

Temporary event CCTV can also have a different technical profile from a permanent installation. Systems may depend upon temporary power, wireless links, mobile communications infrastructure or equipment installed specifically for the event. These arrangements can introduce operational vulnerabilities that may not arise to the same extent within permanent installations.

Technical failure, degraded picture quality or loss of connectivity can occur despite appropriate planning and maintenance. The final guidance should therefore explain the expected response where authorised access is affected by camera failure, network interruption, communications failure, loss of power or wider system outage.

This should include any obligation to notify An Garda Síochána, the reasonable steps expected from the relevant third party and the limits of operator responsibility where the problem arises from circumstances outside that party's reasonable control.

Technical failure should not be misinterpreted as a refusal to comply with an authorised request, particularly where the failure arises from circumstances outside the operator's reasonable control.

EIAI also recommends practical guidance that can be incorporated into third-party event control-room procedures and operator briefings so that personnel facilitating access understand the process expected of them without having to interpret the legislation during a live operation.

Observation 4

COP Sections 1.4 and 1.5: Proportionality, multi-system environments and enhanced CCTV technology

EIAI strongly supports the emphasis placed on necessity, proportionality and the protection of fundamental rights within the draft Code.

Large events may involve extensive CCTV coverage and significant numbers of attendees. Access to an entire network could therefore involve the observation of many individuals who are unrelated to the policing purpose for which access has been sought.

Major events may also be covered by several CCTV systems operating concurrently, creating a combined surveillance footprint that is significantly larger than any individual system. Temporary event CCTV may operate alongside permanent venue CCTV and, under separate legal arrangements, other public or transport CCTV infrastructure.

EIAI's recommendation is not that systems falling outside the scope of this Code should be brought within it. Rather, where Garda access under this framework operates alongside access to other CCTV systems under separate legal arrangements, the overall surveillance footprint should, where relevant, be considered as part of the proportionality assessment.

The assessment should consider whether the policing purpose can be achieved using fewer cameras, a smaller area or a shorter period of access. Particular care is warranted where coverage includes children, medical or welfare facilities, locations where individuals may have an increased expectation of privacy, or lawful demonstrations and assemblies.

EIAI also recommends clarification of the position where third-party CCTV incorporates analytical functionality such as crowd-density monitoring, automated alerts, object tracking or other forms of video analytics. The final guidance should make clear whether an authorisation for a live feed extends only to the underlying video or may also include analytical outputs generated by the third-party system.

Where systems incorporate facial recognition, biometric identification or other particularly sensitive forms of processing, the relationship between those functions and an authorisation for live CCTV access should be expressly addressed.

Garda access should not itself be interpreted as expanding the third party's lawful basis for carrying out separate analytical processing or legitimising additional processing beyond that for which an appropriate lawful basis already exists.

Observation 5

COP Sections 2.1 to 2.6 and Sections 1.10 to 1.12: Governance, audit trail, handover and post-event accountability

EIAI welcomes the distinction within the draft framework between access to a live CCTV feed and access to stored footage. This distinction should be made particularly clear to third-party operators so that facilitating authorised live access is not incorrectly understood as authority to provide recorded material.

Where An Garda Síochána subsequently requires stored footage for investigative or evidential purposes, the appropriate legal and evidential process should remain separate. This is particularly important in event environments where responsibility for facilitating a live connection may not be the same as responsibility for exporting, retaining or releasing recorded footage.

EIAI also recommends practical guidance for third parties on the minimum record that should be maintained when Garda access is facilitated. This could include the relevant authorisation or approval reference, appropriate Garda contact details, the individual who facilitated access, the cameras or areas involved, commencement and termination times, relevant conditions or restrictions and any technical or operational issues that occurred.

The guidance should clarify whether any particular retention period applies to such third-party operational records and which organisation is responsible for retaining them. This is especially important for temporary events, where control rooms may close and specialist contractors may leave the site shortly after the event concludes.

Event CCTV can also operate across several shifts. Where authorised Garda access remains active during a shift change, the incoming operator should be informed of the authority under which access is being provided, its scope, any applicable conditions or restrictions, its expiry or review time and any relevant operational issues.

Similarly, the Code or accompanying guidance should address what happens where a temporary system is dismantled, responsibility transfers to another organisation, a security contractor changes or control reverts from the event organiser to a venue or supplier while an authorisation remains in force.

The responsible post-event contact should remain identifiable even where the temporary control room has closed and the contractors involved have left the site.

This is important because An Garda Síochána may subsequently require clarification about the access provided, the individual who facilitated it or any technical or operational issue that occurred. Clear post-event responsibility would support accountability for both An Garda Síochána and the third party.

Additional Comments

The Event Industry Association of Ireland welcomes the opportunity to respond to this consultation and supports the establishment of a clear, lawful and proportionate framework through which An Garda Síochána may access third-party live CCTV for legitimate policing, public-order and public-safety purposes.

Our observations focus on the practical application of the proposed Code within festivals, concerts, sporting fixtures, exhibitions and other temporary or large-scale events. These environments can differ significantly from a conventional permanent CCTV installation controlled by a single organisation.

An event CCTV system may be commissioned by an organiser, technically supplied and maintained by a specialist company, operated by a separate security contractor and connected to infrastructure owned by a venue. Different organisations may therefore hold legal, contractual, technical and operational responsibilities for the same overall CCTV function.

The system may also operate as part of a multi-agency Event Control structure, alongside several other CCTV systems, while continuing to perform essential event-safety functions. Temporary event CCTV may rely upon temporary power, wireless networks or mobile communications infrastructure, operate across several control-room shifts and exist for only a short period before being dismantled or transferred back to another party.

These characteristics make advance clarity particularly important. Frontline operators should be able to understand who may request access, the authority under which that access is provided, its scope and duration, the steps required to facilitate it and the point at which their responsibilities end. Organisers, venues, security providers and CCTV suppliers should likewise be able to determine their respective responsibilities before an incident occurs.

EIAI does not seek to alter the safeguards or statutory authorisation requirements contained within the proposed framework. Rather, we recommend that the final Code, or accompanying practical guidance, expressly recognise temporary events and other multi-party CCTV environments.

Clear guidance on responsibility, authorisation, multi-agency boundaries, technical implementation, continuity of event-safety monitoring, operator competence and workload, technical failure, proportionality, audit trails, shift handovers and changes of control would support the policing objectives of the legislation while giving the event industry the practical certainty required to comply effectively and lawfully.