EUROPEAN CYCLING INDUSTRIES

POSITION PAPER
SEPTEMBER 2026

ANTI-TAMPERING IN ELECTRICALLY POWER ASSISTED CYCLES (EPACs)

Electrically Power Assisted Cycles (EPACs) have become a cornerstone of Europe's transition towards sustainable, accessible, and efficient mobility. Their success is built on a clear regulatory framework that distinguishes them from motor vehicles, ensuring that they remain safe, widely accessible, and compatible with cycling infrastructure.

However, the increasing incidence of tampering (where EPACs are modified to exceed legal and safety limits for speed, power delivery, torque, acceleration or overall vehicle dynamics) poses a direct threat to this framework. Advances in digital systems and the increasing availability of aftermarket modification tools have made such practices more widespread and easier to implement. The tampering of EPACs significantly alter intended performance characteristics, undermining road safety, distorting fair competition, and eroding trust in the EPAC category.

As evidenced by Annex II, the cycling industry has been working assiduously to address these issues by developing technical anti-tampering measures (through standardisation), and by establishing a strong industry commitment against tampering. Because its members remain united in their stance that tampering is unacceptable, European Cycling Industries (ECI) considers it essential to address this issue through a comprehensive approach that combines industry responsibility, stronger enforcement, targeted regulatory adjustments, and a clearer interpretation of technical standards.

Industry Commitment to Prevent Tampering

The European cycling industry recognises its responsibility to ensure that EPACs placed on the market are compliant by design and resistant to unauthorised modification. It also recognises that modifying EPACs to exceed factory settings not only compromises safety but fundamentally alters the nature of the vehicle. In such cases, a bicycle can effectively become a motor vehicle without meeting the corresponding regulatory requirements.

As such, the industry has collectively vowed to prevent the tampering of e-bikes, to ensure that all applicable anti-tampering requirements are respected, and to continuously improve technical solutions to make tampering more difficult. This pledge is not theoretical; it is formalised through an industry-wide self-commitment originally developed under the auspices of CONEBI, to which all ECI members are signatories. This shared commitment reflects a unified position across manufacturers, suppliers, and national associations that tampering is unacceptable.

End-to-end value chain collaboration

Importantly, the formalised commitment refers to efforts led across the entire value chain: from coordination with manufacturers, cooperation with/between market surveillance authorities and law enforcement, and awareness-raising among end users.

ECI believes it important to differentiate between the incentive to tamper and the capability to do so. It does not dispute that higher available power may well increase the incentive to tamper; but an incentive only turns into a tampered EPAC where the capability exists – and capability is governed by the robustness of the anti-tampering measures put in place. In essence, a well-secured high-torque system offers less tampering capability than a poorly secured low-power one.

Crucially, ECI believes that e-motor manufacturers must actively participate in the industry's next strategic steps – as they hold (1) the technical capacity to implement systems that successfully detect and react to unauthorized modifications, and (2) the resources to invest in innovation that stays ahead of potential future tampering techniques.

At the same time, the persistence of tampering demonstrates that industry action, while necessary, is not sufficient on its own. In reality, many users are unaware that modifying an EPAC beyond legal limits renders the vehicle ineligible as an EPAC under EU law, carrying severe consequences for insurance, liability, road use, product compliance, and warranty. Therefore, robust public awareness campaigns and clear information provided at the point of sale are also essential.

The need for stronger market surveillance and enforcement

The actions proposed above must be supported by effective enforcement and an updated regulatory framework. The current framework provides a solid basis for ensuring compliance, but its effectiveness depends on consistent and robust enforcement across the European Union. In practice, enforcement remains uneven, with significant differences in resources, expertise, and priorities among Member States.

Enforcement efforts should extend throughout the entire value chain, insofar as this can prevent the (technical) compliance onus from being shifted solely onto the manufacturers. Crucially, the increasing role of online sales channels complicates enforcement, by allowing tampering devices to enter the internal market and reach consumers directly and at scale. Notwithstanding, it is also important to tackle offline software/hardware-based modification services – offered by some e-bike retailers and independent service providers. Without effective deterrence, the incentives for such activities will persist, undermining both safety and fair competition.

To address the issues stated above, it is therefore necessary to strengthen market surveillance mechanisms and to ensure that police authorities are equipped with the tools and expertise[1] required to detect both hardware and software-based modifications. For that effect, greater cross-border enforcement cooperation between national authorities is encouraged, as it is essential to avoid fragmentation and ensure that rules are applied consistently within the European Union.

Furthermore, the EU must close the e-commerce accountability gap to safeguard the Internal Market. Specifically, every product sold to European consumers must trace back to a clearly identifiable and responsible actor within EU jurisdiction who has verified its compliance prior to market entry.

A more proactive and coordinated approach to enforcement would reduce the prevalence of tampering while reinforcing confidence in the regulatory framework.

[1] Police and market control authorities should collaborate with the bicycle industry to develop and evaluate criteria that can indicate illegal tuning. Based on these evaluated criteria, the bicycle industry should also provide police authorities with appropriate tools (soft- and hardware). Because basic speed sensors are easy to trick, the industry supports exploring tamper-proof data logging.

Annex I: Interpretation and Application of Standards

Both EN 15194:2017+A1:2023 and the CEN Technical Specification CEN/TS 17831:2023 provide the foundation for demonstrating compliance with EPAC requirements. It remains a robust and widely accepted reference framework for the European cycling industry.

ECI notes that work relating to the interpretation and evolution of the standards EN 15194 and CEN/TS 17831:2023 is already taking place within the relevant standardisation committees for cycles – with active participation from many industry stakeholders. In this context, ECI wishes to clarify how certain concepts within the current standard ought to be interpreted in order to allow for the proper and consistent enforcement of the standard: particularlry, the concepts of "authorized person" and "state of the art".

With regard to the concept of an "authorized person" to make changes to a bicycle's parameters, ECI considers that this should be interpreted strictly as referring to the systems manufacturer, the original equipment manufacturer (OEM), or an entity explicitly authorised by either (including authorized dealers and service partners) – and only where there is a clearly justified technical necessity requiring such changes. Furthermore, a future standards revision should require state of the art cryptographic methods to ensure integrity according to EN 15194:2026 (E) 4.3.23.

Allowing broader or undefined categories of actors to modify system parameters would create significant risks in terms of tampering, cybersecurity, product liability, and consumer safety. However, the interpretation above must not restrict or prevent the legitimate technical access required by accredited testing laboratories, market surveillance authorities, technical services, independent expert witnesses, and recognized research institutions for the purposes of conformity assessment, independent safety investigations, forensic examinations, or scientific research.

In addition, "state of the art" should be understood as requiring that EPACs are designed and manufactured in such a way that tampering is not reasonably possible using commonly available tools and methods[2]. This implies the systematic integration of proportionate and effective security measures into both hardware and software (reflecting current technological capabilities and recognised industry practices), as well as the consistent monitoring of (aftersale) EPAC use (aimed at detecting and responding to new forms of tampering which may arise). Crucially, these anti-tampering measures must be proportionate and technically feasible, remaining fully compatible with legitimate maintenance, diagnostics, repair, compliance verification, and the preservation of independent technical expertise.

ECI believes that a clear and consistent interpretation of these concepts is essential to maintaining the integrity of EPAC systems, supporting market surveillance authorities, and ensuring a level playing field across the European market through the proper enforcement of the standard.

As technologies and tampering methods continue to evolve, the ongoing work within the relevant standardisation bodies will remain important in ensuring that EN 15194 continues to provide an effective and technologically relevant framework for compliance and consumer safety.

[2] Examples of "state of the art" anti-tampering measures/tools for EPACs are listed in Annex III.

Annex II – Timeline of EU cycling industry actions to safeguard against tampering of EPACs

2017	E-bike standard EN 15194:2009 is thoroughly revised and new 2017 edition published with specific section relating to anti-tampering. This new edition is shortly after approved by the EU as a harmonised standard for the Machinery Directive.
2019	CONEBI meets to discuss growing concerns around tampering, deciding to formalise an industry self-commitment against tampering (and to support further improvements in EN15194 anti-tampering measures)
2020	Standardisation committee CEN TC333 forms a drafting team to review the anti-tampering clauses in EN 15194
2021	Industry self-commitment is signed and announced.
2022	After considerable industry input, CEN review of anti-tampering measures in EN 15194 is completed and submitted for publication as a separate Technical Specification, intended for incorporation into the next revision of EN 15194. In December 2022 CONEBI presents the industry self-commitment at the EU Forum for the Exchange of Information on Enforcement.
2023	CEN/TS 17831:2023 – "Cycles. Electrically power assisted cycles. Anti-tampering measures", is published.
2026	Multiple ongoing actions: CEN/TS 17831:2023 is due for regular review under CEN procedures EN 15194 is also under 'fast review' for compliance with Machinery Regulation: will include cyber security requirements with anti-tampering implications, publication expected Q4 2026 EN 15194 'deep revision' is also underway and will include further improved anti-tampering measures, either within EN 15194 or by referring to a separate standard which may be developed based on CEN/TS 17831:2023

Annex III – Anti-tampering tools/methods

"State of the art"	
Secure updates & anti-rollback	Over the air and workshop updates shall be cryptographically verified and protected against manipulation, downgrade attacks, vulnerable older versions
Strong access rights management	Critical parameters and regional configurations shall be protected by cryptographic keys, certificates, or equivalent mechanisms; generic PINs and shared codes shall not be sufficient
Role-based least privilege	Separated access rights for relevant stakeholder groups as defined by the manufacturer (which may include OEM, authorised workshop, service, diagnostics, conformity assessment, and authority functions), with each implemented role limited to its legitimate purpose
Secure component authentication	Components, including motor, controller, or gateway, and battery/BMS, where relevant, authenticate each other to prevent spoofing, or insertion of manipulated components
Sensor plausibility & multi-signal checks	Speed-sensor signals verified by software algorithms and checked for consistency with one or more of the following parameters: vehicle speed, cadence, motor speed, wheel circumference, acceleration, torque, and other available system information
Detection of sensor-signal manipulation	Detection of and resistance against manipulation by magnets, tone or impulse wheels, sensor-alignment changes, pulse-frequency manipulation, external signal devices, and man-in-the-middle tuning kits
Defined response to manipulation	Detection of strongly suspected manipulation triggers a proportionate and fault-tolerant response, such as a diagnostic trouble code, logged security event, reduced assistance, service inspection requirement, or safe operating state
Tamper-resistant logging	Critical parameter changes, regional configurations, software versions, access events, detected manipulation, assistance beyond legal limits, and security events are logged with time stamp, actor or role where available, operation type, and integrity protection against unauthorised deletion or alteration
Secure diagnostic, service, & debug interfaces	Protection of communication via CAN, UART, BLE, USB, NFC, JTAG, SWD, and comparable interfaces; disabling or cryptographically locking of production debug interfaces
Time-limited service authorisations	Compliance-relevant diagnostic and service functions accessible only to authorised tools or persons using role-specific, revocable, and time-limited permissions
Protected drive-mode controls	System prevents unauthorised activation or reconfiguration of throttles, launch modes, walk-assist functions, or other drive modes that could allow operation outside legal EPAC limits

NOT "State of the art"	
User-accessible compliance changes	Region, speed, power, torque, throttle, or assistance settings can be changed exceeding the legal restrictions via app, web account, display or service menu, QR pairing, VPN, location spoofing, or similar user action
Simple on-bike unlocking	Speed limits or drive modes can be changed through button combinations, hidden menus, factory or default codes, common PINs, or similar low-threshold interactions
Weak protection of critical parameters	Settings are protected only by short PINs, default or shared passwords, unprotected Bluetooth or USB access, or unauthenticated service tools
Unsigned or rollback-prone software	Modified or older firmware, apps, controller software, or configuration packages can be installed or executed without cryptographic verification, and anti-rollback protection
Uncontrolled and accessible critical configuration	Wheel circumference, regional configuration, motor mapping, power, torque, acceleration, assistance cut-off, or throttle settings can be altered without strong authorisation, integrity protection, and traceability
Undetected sensor manipulation	External tuning devices, man-in-the-middle devices, magnets, tone or impulse wheels, sensor-position changes, or signal generators can alter, divide, delay, simulate, or suppress speed signals without detection and response
Single-signal reliance	The system relies on a basic speed-sensor signal without plausibility or consistency checks against cadence, motor speed, wheel circumference, acceleration, torque, and other relevant signals
Unsecured interfaces	CAN, UART, BLE, USB, NFC, JTAG, SWD, or comparable interfaces allow reading, writing, flashing, debugging, unlocking, or parameter changes without strong authentication, encryption where appropriate, and access control
Generic service access and weak key management	Service access uses permanent, transferable, or broadly shared credentials, or keys, tokens, certificates, and unlock credentials can be extracted, copied, replayed, or reused
No tamper-resistant logging or response	Critical changes, software versions, regional configurations, access events, or manipulation events are not logged in a tamper-resistant manner, or detection does not trigger a defined system response
Reliance on obscurity alone	Protection depends mainly on hidden menus, unpublished codes, undocumented connectors, proprietary obscurity, or the assumption that tuning instructions will not become publicly available