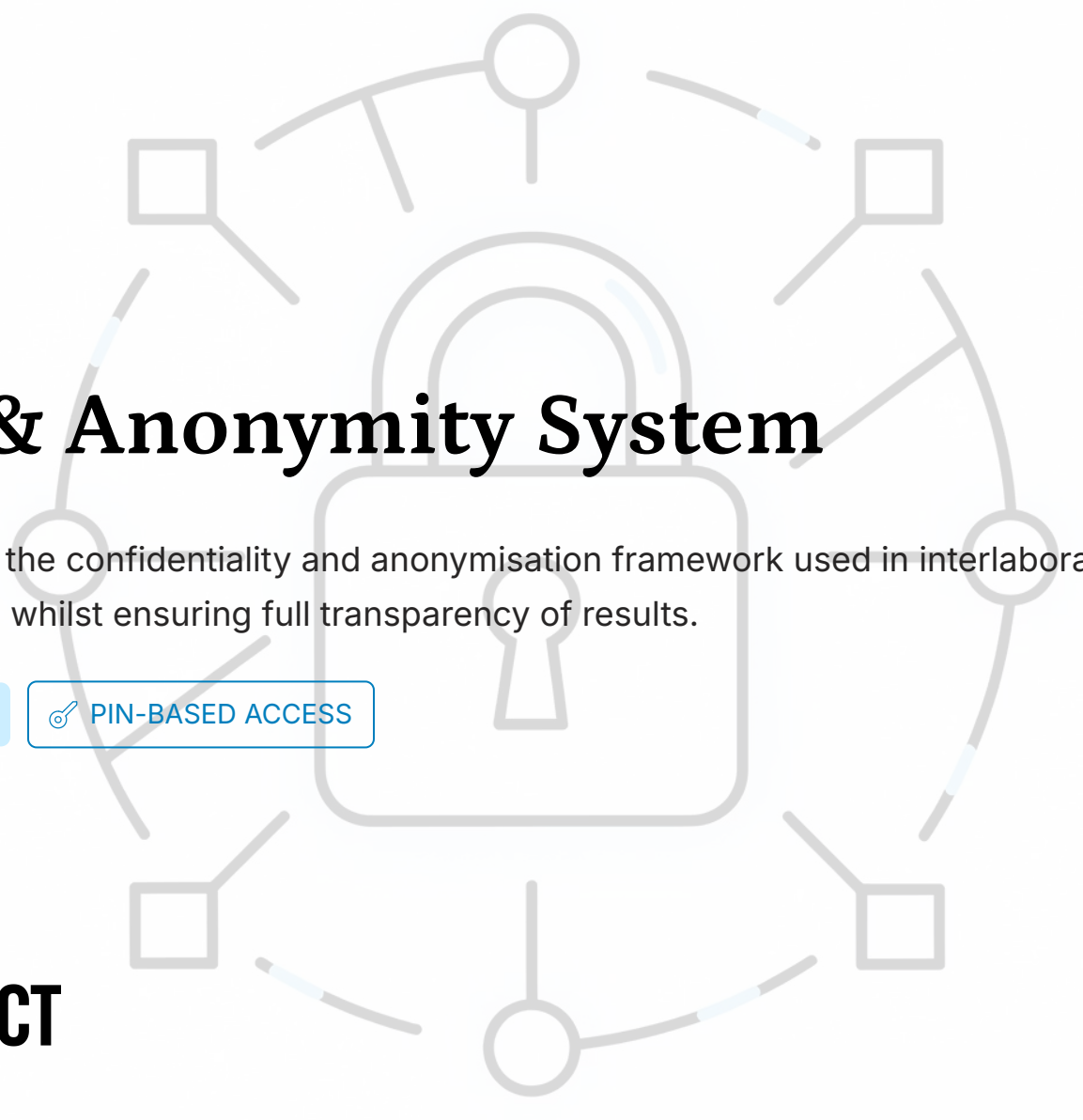




PIN Code & Anonymity System

A comprehensive guide to the confidentiality and anonymisation framework used in interlaboratory tests — designed to protect participant identity whilst ensuring full transparency of results.

 CONFIDENTIAL BY DESIGN

 PIN-BASED ACCESS

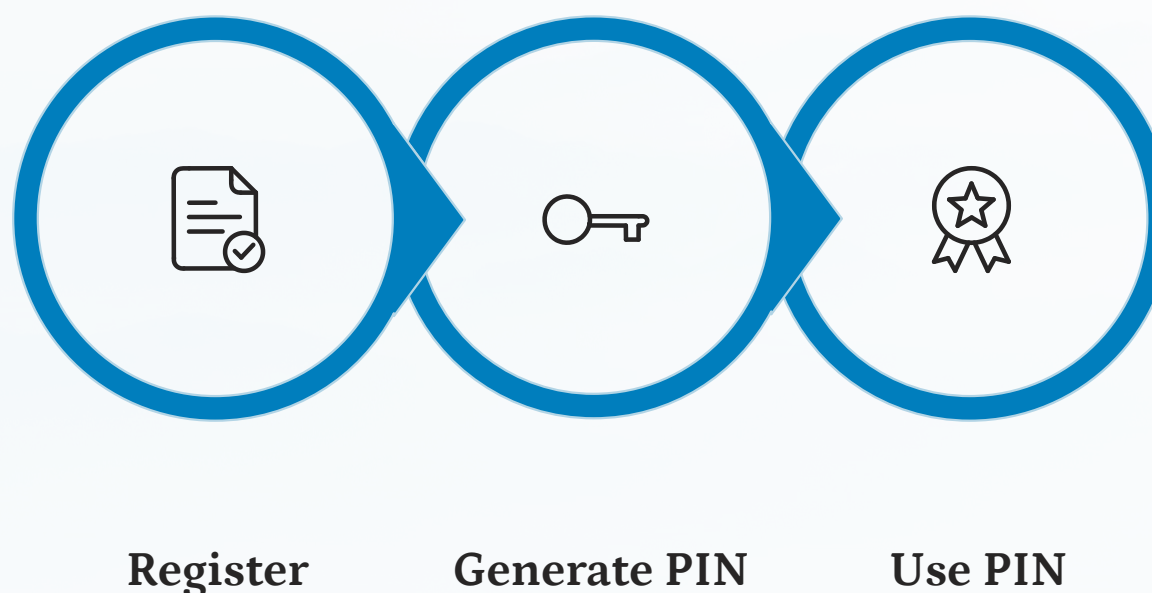


**FOOD CONTACT
SERVICES**

How the System Works

The interlaboratory test management system departs fundamentally from traditional approaches. Rather than linking results directly to company identities, it employs an innovative mechanism built entirely around anonymous codes. This design places participant confidentiality at the heart of every stage of the process — from initial registration through to publication of final results.

Each time a company registers for a test, the system automatically generates a unique PIN code that is valid exclusively for that specific test. This code becomes the sole identifier used throughout all subsequent stages, replacing any reference to the company's name or registration details. No other identifier is ever associated with a participant's submitted data.



This architecture ensures that results can be reported, compared, and published without ever exposing the identity of any individual laboratory or organisation. The system achieves a careful balance between the transparency required for scientific rigour and the privacy protection that participants rightfully expect.

Independent Technical Management

To guarantee maximum security and impartiality, the technical management of the anonymisation system has been entrusted to an external specialised entity. This deliberate organisational choice is central to the integrity of the entire framework.

By delegating technical oversight to an independent third party, a complete structural separation is established between company identity data and test result data. This separation is not merely procedural — it is enforced at the architectural level, making any direct or indirect association between a participant and their results technically impossible, even for those with administrative access to the system.

What the External Entity Manages

- PIN code generation and assignment
- Secure separation of identity and result data
- Technical infrastructure and encrypted protocols
- Operational impartiality and audit readiness

What the External Entity Cannot Do

- Link any PIN code to a specific company
- Identify individual participants from result data
- Retrieve or recover a lost PIN code
- Access registration details alongside results

Full Anonymisation: The Core Principle



The foundational principle underpinning the entire system is **full anonymisation**. A brand-new PIN code is created for each individual test registration, with no connection whatsoever to the registration data provided by the company. This means there is no persistent identifier that could be used to build a profile of a participant's activity over time.

This approach has a significant practical implication for companies that participate in multiple tests: a different PIN code will be assigned on each occasion. Even if the same laboratory registers for five separate tests across several years, it will receive five entirely distinct and unrelated codes. It is therefore structurally impossible for any party to track participation patterns, compare results across tests, or identify repeat participants.

One Test, One Code

Each registration event generates a fresh PIN code, independent of all previous registrations — even by the same company.

No Cross-Test Linkage

Different codes across tests make it impossible to trace or correlate a single participant's involvement over time.

No Registration Data Connection

The generated PIN carries no embedded reference to the company name, contact details, or any other identifying information submitted during registration.

Accessing Your Results



Once all submissions have been processed, test results are compiled and published in a final report, made available on the website for all stakeholders. This publication ensures transparency across the interlaboratory community and allows for meaningful comparisons of performance across participating laboratories.

However, the ability to identify any specific participant's data within that report is strictly controlled. Access to an individual participant's results is possible **only through the assigned PIN code**. Only those who possess the correct code can locate and interpret their own data within the published report — all other entries remain anonymous and indistinguishable.



Published Final Report

Results are compiled and made publicly available on the website, enabling transparency and benchmarking across all participants.



PIN-Gated Access

Your unique PIN code is the only key to identifying your own results within the report. Without it, your data remains indistinguishable from all other anonymous entries.



Your Privacy Preserved

Even while accessing your own results, the anonymity of all other participants is fully maintained. No participant can identify another.



The PIN Code Is Shown Only Once



One of the most critical operational aspects of this system is the moment at which the PIN code is generated and displayed. The code appears **only once** — immediately after the company submits the file containing its test data. This is the sole opportunity to record it.

Once that screen is navigated away from, the PIN code cannot be retrieved, recovered, or reissued by any party. Because the system is designed so that no entity holds a record of which PIN belongs to which company, there is no administrative mechanism for recovery. This is not a limitation of the system — it is a deliberate feature that reinforces the anonymity guarantee.

 **Important Action Required:** It is the sole responsibility of the company to save or print the PIN code at the moment it is displayed. Please ensure that the relevant staff member is prepared to do so before submitting the test data file. Loss of the PIN code means permanent loss of access to your individual results within the final report.

We strongly recommend establishing a simple internal procedure to manage PIN codes — for example, printing the code immediately and filing it with your test documentation, or saving it to a secure password manager or internal records system. Given the consequences of losing the code, a brief moment of care at submission will prevent significant inconvenience later.

Cybersecurity Measures

Beyond the anonymisation architecture, the system incorporates robust cybersecurity measures to protect data at every stage of the process — from the moment a company begins its initial registration through to the final upload of test data.



Encrypted Communications

All data exchanged between users and the server is protected using encrypted communication protocols, ensuring that information cannot be intercepted or read by unauthorised third parties during transmission.



Secure Connections

Every operation — registration, data upload, and result access — is conducted exclusively through secure connections. Unprotected channels are not supported at any stage.



Data Integrity

Encrypted protocols also guarantee that data cannot be altered in transit. What you submit is exactly what is received and processed by the system, with no risk of tampering.



Server-Side Protection

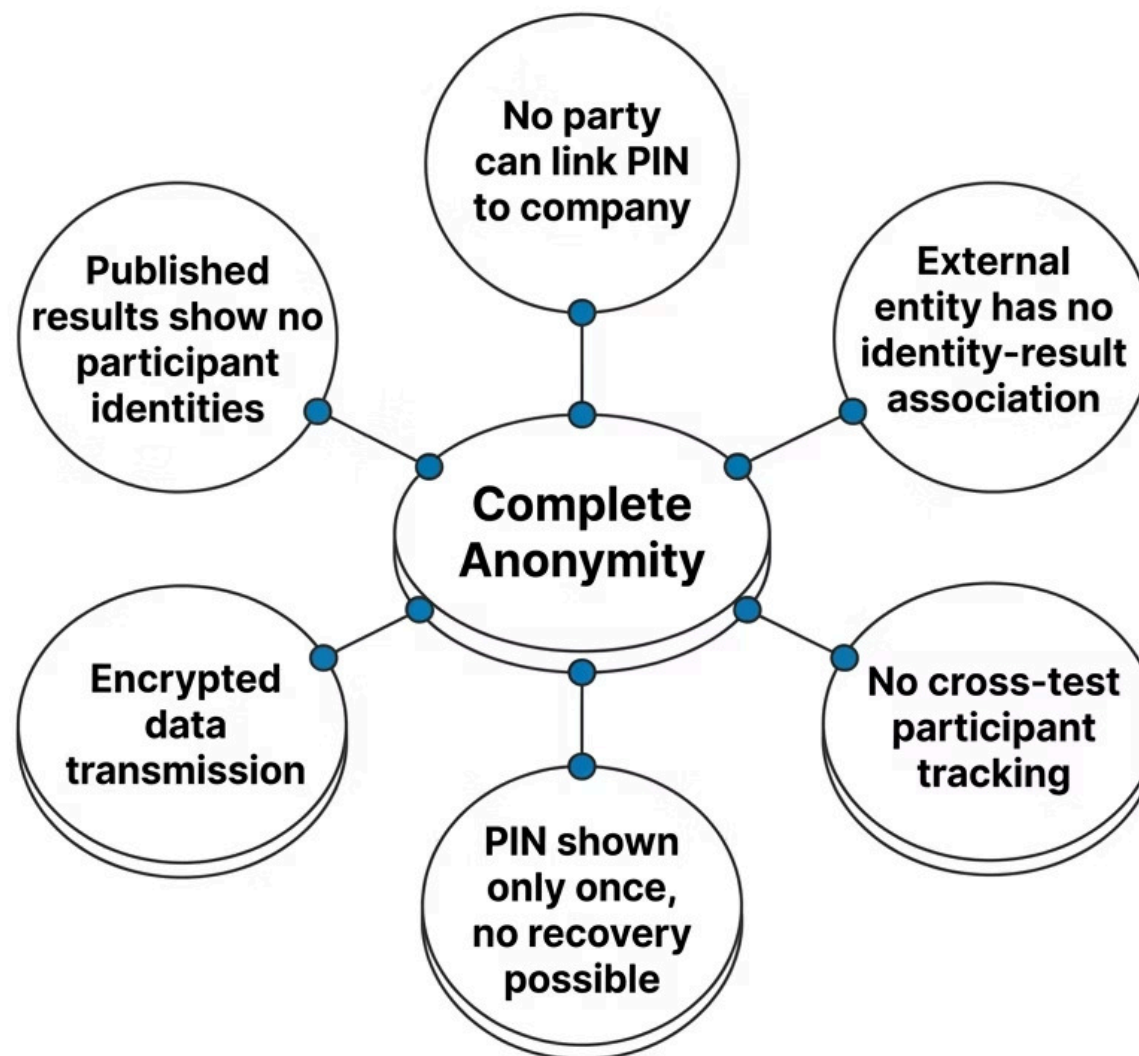
The technical infrastructure maintained by the external entity incorporates server-side protections, ensuring that stored data remains safe from unauthorised access or breach.

These measures collectively ensure that both the confidentiality of participant identities and the integrity of submitted test data are safeguarded against external threats. Participants can engage with the system with full confidence in the security of their communications.

Complete Anonymity: No Party Can Link PIN to Company

Perhaps the most significant assurance the system provides is this: **no party involved in the process — including the organisation responsible for its technical management — is able to link a specific PIN code to a particular company.** This is not simply a policy commitment; it is an architectural reality enforced by the way the system is designed.

This guarantee eliminates several categories of risk that exist in less rigorous systems. There is no possibility of results being disclosed to a competitor, no risk of a data breach exposing a company's performance, and no potential for any form of bias or preferential treatment based on knowledge of participant identities.



This level of anonymity is especially valuable in competitive industrial sectors, where the performance data generated by interlaboratory tests could, if exposed, carry commercial or reputational implications. The system's design ensures that participation is genuinely risk-free from a confidentiality standpoint.

Transparency and Privacy in Balance



A common concern with anonymisation systems is that they may compromise the transparency and scientific utility of published results. This system is specifically designed to resolve that tension — achieving both objectives simultaneously without sacrificing either.

The published final report provides the interlaboratory community with full visibility of aggregate performance data, statistical distributions, and comparative benchmarks. This transparency supports quality improvement, regulatory compliance, and scientific rigour. At the same time, individual participants retain complete control over whether their identity is ever connected to their results — and by default, it never is.

Transparency Achieved

- Final results published openly on the website
- Full statistical and comparative data available
- Supports benchmarking and quality improvement
- Enables regulatory and accreditation compliance
- Scientific integrity maintained throughout

Privacy Protected

- No company identity ever published alongside results
- PIN access restricts individual result identification
- No cross-test tracking or longitudinal profiling
- No party holds a complete identity-result mapping
- Participation is confidential and risk-free

This balance means that participation in interlaboratory tests carries no reputational risk from a disclosure perspective. Laboratories and organisations can engage fully and honestly with the process, knowing that their results will inform their own quality management without being exposed to external scrutiny.

Further Technical Documentation

For laboratory managers, quality assurance officers, and administrators who require a deeper understanding of the system's architecture, procedures, and technical specifications, comprehensive technical documentation is available. This documentation provides a full description of all processes — from PIN generation through to result publication — as well as the security protocols and anonymisation mechanisms in place.

→ **System Architecture Overview**

Detailed technical description of how the anonymisation framework is structured, including the role of the external management entity and the data flow between components.

→ **Step-by-Step Procedural Guides**

Practical walkthroughs for each stage of participation — registration, file submission, PIN code management, and result retrieval — designed for laboratory administrators.

→ **Security and Compliance Information**

Full details of the cybersecurity measures, encryption standards, and data protection compliance frameworks that underpin the system's operation.

→ **Frequently Asked Questions**

Answers to the most common queries raised by participants, covering topics from PIN code loss through to the interpretation of published reports.

 **Access the Documentation:** Comprehensive technical documentation is available on the website. If you have specific questions not addressed in the documentation, please contact the test coordination team directly.

We encourage all participating organisations to familiarise themselves with the documentation before their first test submission. Understanding the system fully will help ensure that PIN codes are managed correctly and that results can be accessed without difficulty once the final report is published.