

What happens to your data

Karen Pendergrass · ORCID 0000-0002-2348-7259 · 2026-08-20

Karen Pendergrass. "What happens to your data". <https://heavymetalcertified.com/what-happens-to-your-data>. Retrieved 2026-10-06.

What happens to your data

Different data plays different roles across a certification, so it is held differently. The table below states, for each kind of data, who is the primary custodian, whether HMTc can access it, whether it becomes public, and the basis on which it is retained. The governing principle is simple: exploratory and readiness data stays in your custody by default, and only a certified product’s conformity status is published.

Data type	Primary custodian	HMTc access	Public	Retention basis
Standards lookup (no company name required)	None, or minimal logs	Limited	No	Security and analytics policy
Preliminary product profile	Brand and HMTc readiness function	Controlled	No	Readiness agreement
Exploratory raw laboratory report	Brand or laboratory by default	As authorized	No	Brand and laboratory policy
Remediation analysis	Brand and readiness function	Controlled	No	Corrective-action agreement
Official certification report	Certification operator	Full	Conformity status only	Certification scheme
Certificate and permissions	Certification operator	Full	Yes	Certificate lifecycle
Surveillance report	Certification operator and brand	Full	Status according to the published rules	Surveillance policy
Aggregate research data	Operator research-governance function	De-identified and aggregated	According to release policy	Research governance, pending the anonymization rule

No central repository of your raw results

HMTc retains the conformity evidence it needs to make and stand behind a certification decision. It does not aggregate brands’ raw exploratory test data into a central, searchable repository. Where category learning is useful, it is drawn from de-identified, aggregated data under minimum-cell-size controls.

De-identification is a governed method for limiting the risk of re-identification. It is not an absolute promise of anonymity, particularly where a product category, an origin, a formulation, or a supplier is distinctive enough to narrow the field. The correct standard, following the way bodies such as NIST describe it, is disclosure-risk management under governance, not a guarantee that a record can never be linked back. HMTc treats it that way and says so, rather than promising more than de-identification can deliver.

What is public, and what is not

A product becomes public when it is certified, or when an existing public certificate must change status under the published rules. Requesting a standard, running a readiness review, or working a correctable finding does not create a public record, and HMTc does not maintain a public list of brands that applied but were not yet ready to certify.

What custody does not do

Custody and confidentiality are commercial and operational controls. They are not attorney-client privilege, and they are not a promise that relevant evidence can never be reached through lawful process. They do not override a reporting, recall, disclosure, or safety obligation, and they do not permit use of the mark on a nonconforming product. A brand with a specific legal exposure should structure privileged work through its own counsel. See [For legal & QA](#) for how the certification record behaves under challenge.