Faces, fingerprints and fines:
a practitioner's guide to staying compliant when using biometric and surveillance technologies

Simon Ridding, Barrister
33 Bedford Row

Simon Ridding, Barrister at 33 Bedford Row Chambers, distils recent UK biometric and surveillance enforcement, litigation and regulatory developments into a practical compliance framework, arguing that the decisive legal questions are no longer whether biometric technologies can be used, but whether organisations can demonstrate necessity, proportionality, governance, accuracy and accountability throughout the deployment lifecycle

According to its published enforcement and audit materials, between Winter 2024 and Spring 2026, the UK Information Commissioner's Office ('ICO') issued its first formal enforcement notice against an employer for biometric time and attendance scanning; published dedicated biometric recognition guidance; reprimanded a school for its deployment of cashless catering facial recognition; successfully appealed a tribunal decision involving a US-based facial recognition company's extra-territorial reach; and opened a rolling series of audits of police forces deploying facial recognition. Over the same period, the Home Office launched a consultation on a new statutory framework for law enforcement use of facial recognition, and (in an unlinked incident) a police force suspended its live deployments after bias and accuracy concerns came to light.

Taken together, these developments demonstrate how quickly the UK's biometric and surveillance landscape has evolved. While the resulting legal and regulatory framework can appear fragmented, recent enforcement action and case law provide increasingly clear signals as to where regulators and courts are prepared to draw the line. For organisations seeking to harness the efficiencies offered by biometric and surveillance technologies, and for practitioners advising them, understanding those boundaries is critical. This article examines where those lines currently sit and offers a practical framework for navigating them.

Five core questions

The practical message is straightforward: biometric and surveillance systems should be treated as high-risk infrastructure, not as ordinary IT procurement. Yet this distinction is often obscured by the way such technologies are marketed and deployed. A networked door access system with embedded facial recognition, for example, may be presented as little more than an access control solution. In reality, it is a biometric system, and organisations that fail to recognise that fact risk overlooking the additional legal, governance and accountability obligations that accompany its use.

Prior to the deployment of any tech that may be captured by the law, controllers should be able to answer five questions:

- why is this system necessary at all;
- what less intrusive alternatives were considered and why have they been rejected;
- what lawful basis under Article 6 UK GDPR, and which Article 9 condition (or, where applicable, Schedule 8 condition under Part 3 of the Data Protection Act 2018), are relied upon, and is the corresponding documentary basis (including any appropriate policy document) in place;
- how have equality, accuracy and false-positive risks been tested, and by whom; and
- what will happen, operationally and legally, when a data subject pushes back against the system?

The regulatory architecture in brief

Biometric data are defined by Article 4(14) UK GDPR as personal data resulting from specific technical processing relating to physical, physiological or behavioural characteristics which allow or confirm the unique identification of a natural person. Biometric data occupy a peculiar position in the overall data protection regime. Where biometric data are processed for the purpose of uniquely identifying a natural person, Article 9(1) UK GDPR treat them as special category data, engaging the heightened conditions of Article 9(2).

Contrary to some prevailing notions, the Data (Use and Access) Act 2025 ('DUAA') should not be interpreted as imparting a general relaxation of the standards applicable to biometric or surveillance processing

The ICO's Guidance on biometric recognition (dated 23rd February 2024) treats systems used to recognise, verify or identify individuals through biometric characteristics as generally engaging Article 9, because the processing is for the purpose of uniquely identifying a natural person. Controllers should nevertheless analyse the particular use case, as categorisation, detection or estimation systems that do not single out an individual may not cross the threshold. The author would caution against two common theoretical errors: first, the casual assumption that the system triggers Article 9 (which may obscure the lawful basis question), and second, the casual assumption that it does not (the more common and more dangerous mistake).

The lawful use of surveillance camera systems, which are not always biometric, is addressed in the ICO's Guidance on CCTV and video surveillance, and controllers should also consider the Surveillance Camera Code of Practice issued under section 30 of the Protection of Freedoms Act 2012.

Contrary to some prevailing notions, the Data (Use and Access) Act 2025 ('DUAA') should not be interpreted as imparting a general relaxation of the standards applicable to biometric or surveillance processing. Readers are aware that the DUAA makes various key changes, including introducing a new 'recognised legitimate interests' basis; reform of the automated decision-making regime through new Articles 22A–22D UK GDPR; and the reconstitution of the regulator as the Information Commission. Practitioners should check the commencement dates for each relevant DUAA provision. Importantly for this article's purposes, Article 22B preserves heightened controls on solely automated significant decisions based wholly or partly on special category data, which covers most biometric-recognition processing. Again, the DUAA should not be read as materially relaxing the core safeguards applicable to biometric-recognition processing.

Controllers must also identify whether their processing falls under either the UK GDPR/Part 2 DPA 2018 regime or the law-enforcement regime in Part 3 DPA 2018. Where a competent authority processes biometric or surveillance data for law enforcement purposes, Part 3 applies different terminology and safeguards: sensitive processing is permitted only where either (1) the data subject has consented and an appropriate policy document is in place, or (2) the processing is strictly necessary for the law-enforcement purpose, meets a Schedule 8 condition, and is supported by an appropriate policy document. Local authorities should not assume they operate exclusively in the Part 2 arena, since counter-fraud, environmental and trading standards enforcement functions may engage Part 3.

Clearview: the extra-territorial trap for procurers

In *The Information Commissioner v Clearview AI Incorporated* [2025] UKUT 319 (AAC), the Upper Tribunal allowed the Commissioner's appeal after finding that the First-tier Tribunal ('FtT') had erred materially in law in finding that Clearview's processing was outside the material scope of "the GDPRs by operation of Article 2(2)(a)". The matter was remitted back to the FtT on the basis that the Commissioner had the jurisdiction to issue the notices. Clearview was, however, granted permission to appeal to the Court of Appeal, which is currently pending.

The Upper Tribunal held that:

- Clearview's scraping and processing of biometric facial templates derived from publicly accessible images of UK residents constituted processing 'related to' the monitoring of behaviour of UK data subjects within the meaning of Article 3(2)(b) UK GDPR;
- such processing was not removed from material scope under Article 2(2)(a) merely because Clearview's customers were foreign law enforcement or national security agencies; and
- the relevant 'related to' test is capable of capturing processing by one controller in support of monitoring carried out by a different controller.

Absent any successful appeal, the reach of this decision goes well beyond Clearview itself, applying to local authorities, private companies and police-adjacent bodies who consume biometric matching or analytic outputs from overseas vendors

Absent any successful appeal, the reach of this decision goes well beyond Clearview itself, applying to local authorities, private companies and police-adjacent bodies who consume biometric matching or analytic outputs from overseas vendors. It is not a direct ruling on every downstream procurement scenario, but it materially increases the compliance risk of relying on biometric products whose underlying database has been built through scraping. The fact that a vendor sits offshore and processes images of UK residents under a third-party contract immunises neither the vendor nor the controller/procurer.

Practically speaking, vendor due diligence has shifted in character. It is no longer sufficient to receive bland assurances that the provider is compliant in its home jurisdiction. A controller deploying a third-party facial-recognition product whose underlying database has been built through scraping must assess its own lawfulness, fairness, transparency, accuracy, transfer and accountability obligations, including whether reliance on the vendor's data or model outputs creates foreseeable risks to data subjects. In light of the decision, controllers are advised to demand a documented data provenance audit from any biometric vendor, and to treat the absence of one as a refusal to engage in compliance.

Serco: the lawful basis trap for employers and operators

The ICO's enforcement notices of 23rd February 2024 against Serco Leisure Operating Limited, Serco Jersey Limited and seven associated community leisure trusts provide useful guidance as to the deployment of biometric functions in the workplace. More than 2,000 employees across 38 leisure facilities had been required, from May 2017, to authenticate attendance using facial recognition and fingerprint scanning. The standard operating procedure was uncompromising - use the system or face disciplinary action.

The ICO found Serco in breach of Articles 5(1)(a), 6 and 9 UK GDPR. Three findings deserve highlighting:

- Article 9(2)(b), read with Schedule 1 paragraph 1 DPA 2018, was, on the facts, the incorrect condition: Serco relied on the employment, social security and social protection condition, asserting that working time, national minimum wage, right to work and tax obligations required attendance verification. The ICO rejected the proposition that those obligations made biometric attendance processing necessary. The Article 9(2)(b) route additionally requires a corresponding UK law basis in Schedule 1 of the DPA 2018 and an appropriate policy document; the condition does not run as broadly as employers tend to assume

- necessity is a comparator question: the ICO held that Serco had failed to evidence why fingerprint or facial scanning was necessary or proportionate where less intrusive alternatives, such as fobs, ID cards and verified manual sign-in, existed. Necessity in this context is not "necessary to operate the chosen system", it is "necessary to achieve the underlying purpose, having properly considered and excluded less intrusive alternatives"; and
- consent in an employment context is structurally suspect: even if Serco had offered an opt-out (it did not), the ICO recorded the imbalance of power between employer and employee as a vitiating factor. The same logic transposes to local authority service users dependent on a service, and to pupils dependent on a school.

The Serco enforcement action is best read not as a blanket prohibition on workplace biometrics, but rather as an illustration that their lawfulness may be balanced on a far narrower legal footing than most controllers presently contemplate. The obligation to evidence proportionality through a contemporaneous, comparator-rich Data Protection Impact Assessment ('DPIA') is the single most undervalued compliance step in the field.

Bridges: the proportionality and PSED twin track

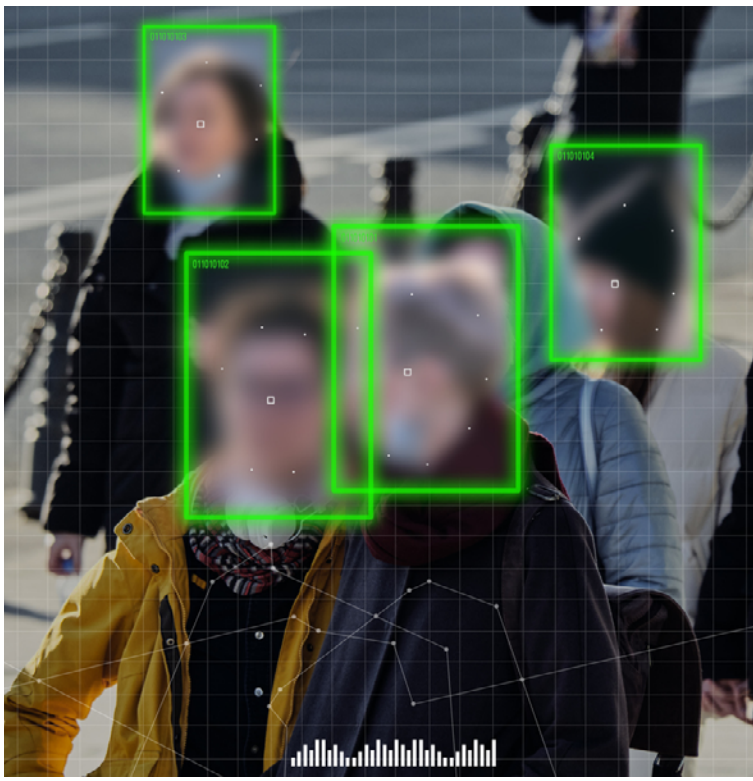
R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058 remains the foundational domestic authority on the use of live facial recognition ('LFR') by public authorities. The Court of Appeal held that:

- South Wales Police's use of LFR was not 'in accordance with the law' under Article 8(2) European Convention on Human Rights ('ECHR') because the legal framework left 'fundamental deficiencies' — in particular, excessive discretion as to (1) who could be included on a watchlist, and (2) where LFR could be deployed;
- the DPIA was inadequate, failing to address the rights and freedoms of the broader population scanned (not merely those who matched the watchlist); and
- South Wales Police had not complied with the Public Sector Equality Duty ('PSED') under section 149 of the Equality Act 2010, having failed to take reasonable steps to interrogate whether the algorithm itself produced differential outcomes on protected characteristics.

The Home Office's consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies (which ran between 4th December 2025 and 12th February 2026) is the legislative attempt to address the type of deficiencies identified in *Bridges*. Notably, it reaches beyond facial recognition to other similar technologies such as object, action and emotion detection, signalling the likely scope of future regulation. At the time of writing, the government's response paper has not been published, though the Biometrics and Surveillance Camera Commissioner published his own response on 24th February 2026. In the law enforcement sphere, until a framework is enacted, the College of Policing's authorised professional practice is the operational rulebook for police forces.

In the meantime, the most significant development for practitioners to be aware of is that the ICO has converted the *Bridges* principles into an active supervisory programme, conducting since 2025 a rolling series of data protection audits of forces deploying facial recognition (South Wales, Gwent, Essex and Leicestershire), with a cross-force outcomes report expected later in 2026. Two points matter to every controller, not only the police:

- the ICO now expects routine testing for bias and discriminatory outcomes, whether arising from a system's design, its training data or its watchlist composition - a direct application of the *Bridges* PSED finding; and
- its working proposition is that governance comes first, i.e. a controller that cannot demonstrate sound governance of a biometric system is unlikely to be operating it lawfully. The Home Office's own December 2025 disclosure of historic bias in the retrospective facial recognition algorithm used against the Police National Database confirms that accuracy and bias risk attach to retrospective as well as live systems.



The Essex Police episode offers a cautionary example. The force paused its live deployments after independent evaluation and before the ICO's March 2026 audit identified accuracy and bias risks. The instructive detail lies in the cause of the issue: Essex Police had applied a match-confidence threshold developed for one vendor's facial recognition algorithm to a different system. The episode illustrates the risks of treating biometric technologies as interchangeable, and the importance of validating performance settings against the specific system being deployed. Field testing conducted by the University of Cambridge found the system correctly identified only around half of those on the watchlist, with a statistically significant disparity in identification rates between demographic groups. However, it is important to note that the National Physical Laboratory found no such bias, the latter apparently stemming from the use of different methodologies and standards.

The lesson for any controller is that accuracy is not a figure to be lifted from a vendor brochure, and a confidence threshold is system specific. Further, it must be validated against the deployed model, the target population and must be re-tested on material change. Litigation exposure has widened too, with the Equality and Human Rights Commission being granted permission in August 2025 (in *R(Thompson and Carlo) v Commissioner of Police of the Metropolis*) to intervene in a judicial review of the Metropolitan Police's LFR use, although that challenge failed in April 2026.

Although *Bridges* concerned police use of LFR, it is relevant to all public authorities, who must address the Article 8, data protection and PSED dimensions directly. As an example, although the case was dismissed, the grounds asserted in *R (Thompson and Carlo) v Commissioner of Police of the Metropolis* related to breaches of Articles 8, 10 and 11 which clearly demonstrates an inclination to move beyond the standard data protection causes of action.

Generally, private sector controllers will not usually owe the PSED, but should still address equivalent risks through UK GDPR fairness, necessity and proportionality analysis, equality law risk assessment, contractual governance and DPIA evidence. For local authorities, the PSED point is acute: a council deploying facial-recognition CCTV in a town centre scheme without a properly evidenced PSED assessment runs a serious risk of public law unlawfulness, irrespective of whether its data protection paperwork is otherwise in order.

Generally, private sector controllers will not usually owe the PSED, but should still address equivalent risks through UK GDPR fairness, necessity and proportionality analysis, equality law risk assessment, contractual governance and DPIA evidence.

Chelmer Valley and the children dimension

A reprimand issued by the ICO to Chelmer Valley High School on 22nd July 2024 for its processing of the biometric data of approximately 1,200 pupils through a cashless-catering facial-recognition system, is, on its face, a DPIA failure. The school did not conduct a DPIA before deployment in March 2023 and it relied on parental opt-out rather than affirmative consent. It also failed to properly analyse whose consent was required and whether consent was validly obtained. It also failed to consult its Data Protection Officer.

The deeper lesson here concerns the personal data of children. The ICO's Age-Appropriate Design Code and the heightened expectations under Recital 38 of the UK GDPR mean that any controller, schools, leisure trusts, local authority services, etc. should treat children's biometric processing as among the most sensitive operations in the regime. In a school context, controllers should not assume parental opt-out is sufficient and they must consider the child's own rights and capacity. Further, they also need to consider the requirements for valid UK GDPR consent, and the education-specific provisions in the Protection of Freedoms Act 2012 which sit alongside, rather than displace the UK GDPR and the DPA 2018. The requirement of necessity in this context closely mirrors the Article 8(2) ECHR test. As schools can readily achieve the same objective through less intrusive means,

such as card, fob or PIN-based payment systems, it is likely to be difficult to demonstrate that facial recognition is a necessary and proportionate solution.

A practitioner's checklist

Drawn from the cases above and from practice, below is a non-exhaustive set of practical recommendations, grouped by the stage of the deployment lifecycle. Several depart from the usual checklist and reflect what is, in the author's view, the gap between published guidance and enforcement priorities.

Before procurement:

- conduct a 'reverse' DPIA: document the non-biometric alternatives first and articulate, by reference to evidence, why each is insufficient, so that the chosen system emerges as the least intrusive option capable of meeting the purpose rather than as an apologia. This being the antidote to the Serco failure;
- put biometric-specific controls in the contract: procurement is now a core compliance control. Contracts should address controller/processor (or joint controller) status; Article 28 UK GDPR processor terms; sub-processing and audit rights; model and dataset provenance warranties; demographic performance testing; retention, deletion and security standards; incident notification; transfer mechanisms; and explicit restrictions on vendor reuse of customer images, templates or telemetry for product improvement or model training unless expressly assessed and authorised;
- treat international transfers as a front-end issue: if images, templates, watchlists, logs or support access data leave the UK, identify the transfer mechanism, conduct any required transfer risk assessment, and ensure the vendor cannot route support, hosting, analytics or model training data through unassessed jurisdictions, the obvious risk being cloud-based vendors and the less obvious one being on-premises systems with offshore support; and
- commission demographic differential testing: the PSED (Public Sector Equality Duty) in section 149 of the Equality Act 2010 requires public authorities to evidence due regard to equality impacts. In the private sector, equivalent testing is often essential to defend indirect discrimination risk. Demand the vendor's testing report; its absence is itself a red flag for the DPIA. Ensure the testing is specific to the model and population actually deployed, the Essex Police suspension having turned in part on a threshold calibrated for a different vendor's algorithm. Generic accuracy figures do not discharge the obligation.

Before deployment:

- treat the supplier's DPIA as a starting point, not a finished product: vendors routinely supply template DPIAs that omit the controller's specific operational context, but the ICO has been clear that DPIA responsibility is non-delegable - a controller cannot outsource the assessment of risks to its own data subjects;
- prepare an appropriate policy document where required: many DPA 2018 Schedule 1 conditions likely to be relied on for biometric processing, including the employment condition in paragraph 1 and most substantial public interest conditions in Part 2, require an appropriate policy document, and competent authorities processing for law-enforcement purposes must separately address the Part 3 sensitive processing safeguards. The appropriate policy document is among the most frequently overlooked steps; in the recent enforcement actions, its absence is often the first contravention identified;
- audit watchlist composition: for any LFR-style deployment the watchlist is the central locus of controller decision-making, and Bridges identified watchlist discretion as the principal deficiency, so the controller should record, for every individual: (1) the lawful basis for inclusion; (2) the source of the underlying image; (3) the date of inclusion; and (4) the trigger for removal;
- address the automated decision-making regime explicitly: where a biometric output is used to make a significant decision based solely on automated processing - one producing legal or similarly significant effects, with no meaningful human involvement - the UK GDPR automated decision-making provisions, as amended by DUAA (Articles 22A–22D), may be engaged. Under the new Article 22B, a significant decision based entirely or partly on Article 9(1) special category data may not be taken solely by automated means unless either (i) it is based entirely on personal data for which the data subject has given explicit consent, or (ii) it is necessary for entering into or performing a contract between the data subject and controller, or is required or authorised by law, and Article 9(2)(g) applies (substantial public interest, on a domestic law basis, with suitable safeguards). Controllers should ensure human involvement is real, timely and capable of changing the outcome, not a token rubber-stamp;
- build a real right to object - and a practical non-biometric alternative - into the operational design: in employment, education and service-provision contexts the data subject should be able to refuse the biometric route without disadvantage: 'use the fingerprint scanner or use the manual book' works, 'use the fingerprint

scanner or use the manual book' works, 'use the fingerprint scanner or face disciplinary action' does not, and the Serco enforcement turned in significant part on the absence of a workable alternative; and

- make transparency operational, not documentary: this means layered notices, visible signage, online deployment information where appropriate, and clear explanations of purpose, lawful basis, data categories, retention, data-sharing, rights routes and whether biometric matching or automated decision-making is involved, and for LFR deployments the watchlist purpose and the consequences of a possible match, subject to legitimate operational constraints.

During operation:

- maintain a biometric estate register: every camera, terminal, template store and matching server should be itemised, with retention period, Article 6 lawful basis, Article 9 condition (or Schedule 8 condition) and DPIA review date recorded, cross-referring to the controller's Article 30 record, DPIA, appropriate policy document, privacy notice, contract and retention schedule. It is likely to be among the first documents a regulator asks to see;
- architect for matched-image-only retention and template discipline: distinguish between raw images, biometric templates, match candidates, audit logs and watchlist images, each with a separate retention justification, and configure the matching engine so that non-match images and templates are deleted within seconds; and
- write the false-positive protocol before go-live: accuracy is not merely a vendor metric. Define the confidence threshold, false-positive process, escalation route, human review standard, staff training and record-keeping. The threshold should be derived from and validated against the specific algorithm deployed, not borrowed from another system - the precise failure that led Essex Police to suspend its deployments in 2026. The operational question is not whether the algorithm is accurate in the abstract, but what staff are instructed to do when it is wrong.

On change and review:

- re-DPIA on every material change: a DPIA is not a one-time artefact. *Bridges* emphasised that each LFR deployment must be reassessed for its specific time, place and watchlist. The same principle applies to any biometric system following a change in scope, vendor, retention period or purpose. Controllers are advised to undertake a fixed annual review in any event, recorded on the estate register.

The direction of travel

The Data (Use and Access) Act 2025 has not, despite some commentary, softened the regulatory standard for biometric and surveillance processing. The Home Office's now closed consultation on a statutory framework for law enforcement facial recognition; the ICO's rolling audits of police forces and its insistence that governance and bias-testing come first; the Essex Police suspension; the European Court of Human Rights intervention in the Metropolitan Police litigation; the ICO's enforcement-led approach to workplace biometrics; the Upper Tribunal's restoration of the Clearview penalty; and the steady accretion of school, council, and employer facing enforcement, all point in the same direction. Biometric and surveillance technologies will be deployed lawfully, or they will be deployed unlawfully. There is little middle ground, and rather less judicial sympathy for the controller who treats the DPIA as paperwork.

For both public and private sector organisations, the solution is not avoidance but discipline. Biometric systems can be deployed lawfully where there is a properly articulated necessity, a thoroughly tested algorithm, a diligently documented DPIA, a properly composed watchlist (where relevant), a comprehensively evidenced PSED assessment (where applicable), an operational transparency regime, contractual controls on the vendor, and an available alternative for the data subject. Where any one of those is absent, the controller should expect the regulator's attention, and increasingly, the data subject's lawyers.

Simon Ridding
33 Bedford Row
sr@33br.co.uk