SECRETARIAT / SECRÉTARIAT

SECRETARIAT OF THE COMMITTEE OF MINISTERS
SECRÉTARIAT DU COMITÉ DES MINISTRES

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contact: Ireneusz Kondak
Tel: 03.90.21.59.86

Date: 28/04/2025

DH-DD(2025)479

Meeting:	1531st meeting (June 2025) (DH)
Item reference:	Action Report (22/04/2025)

Communication from the United Kingdom concerning the case of Catt v. the United Kingdom (Application No. 43514/15) - *The appendices are available upon request to the Secretariat.*

* * * * * * * * * * * *

Réunion :	1531e réunion (juin 2025) (DH)
Référence du point :	Bilan d'action (22/04/2025)

Communication du Royaume-Uni concernant l'affaire Catt c. Royaume-Uni (requête n° 43514/15) ***(anglais uniquement)*** - *Les annexes en sont disponibles sur demande au Secrétariat.*

Execution of Judgments of the European Court of Human Rights
ACTION REPORT

CATT v THE UNITED KINGDOM
Application number 43514/15
Judgment final on 24 April 2019
Information submitted by the United Kingdom Government on 22 April 2025

INDEX OF CONTENTS

CASE SUMMARY

1. The applicant was a pacifist, over ninety years old, who participated in demonstrations including protests organised by a group called Smash EDO. Whilst he had no criminal record and was not considered a danger to anyone, the protests involved disorder and criminality, and information about the protests and members of Smash EDO was collected by the police and held on the database referred to in the proceedings as the domestic extremism database.

2. In 2010, the applicant requested that information relating to his attendance at demonstrations and events, mostly related to Smash EDO, between 2005 and 2009 be deleted from the database. The request was initially refused; however, following a review in 2012, records that referred primarily to him were deleted. Some entries that made incidental reference to him did, however, continue to be retained on the database. He challenged this, arguing that retaining the data was not necessary within the meaning of Article 8.

3. The European Court of Human Rights found a violation of the applicant's Article 8 rights. The Court accepted that there were good policing reasons why such data had to be collected, and in the case of the applicant it had been justified because Smash EDO's activities were known to be violent and potentially criminal. However, the Court expressed concerns about the continuing retention of the data, as it did not consider there to be a pressing need, after a time, to retain the data relating to him.

4. The Court considered that the continued retention of data in the applicant's case had been disproportionate because it revealed political opinions requiring enhanced protection. It had been accepted he did not pose a threat (taking account of his age) and there had been a lack of procedural safeguards, the only safeguard provided by the Management of Police Information[1] (MOPI) Code of Practice being that data would be held for a minimum of six years and then reviewed. The Court did not consider that this was applied in a meaningful way as the decision to retain the data did not take account of the heightened level of protection it attracted as data revealing a political opinion. The Court rejected the argument that it would be too burdensome to review and delete all entries on the database relating to the applicant; also, if this were accepted as a valid reason for non-compliance, that would create a route to allow violations of Article 8.

5. The applicant was awarded EUR 27,000 plus any tax that may be chargeable to the applicant, in respect of costs and expenses.

[1] https://www.college.police.uk/app/information-management/management-police-information

INDIVIDUAL MEASURES

Just satisfaction:

6. The just satisfaction award has been paid. Evidence of payment has been supplied separately.

Other measures:

7. The Government has taken the following individual measures in respect of the applicant.

   a. The police unit (National Domestic Extremism and Disorder Intelligence Unit) which held the standalone database containing the applicant's six data entries which were the subject of the judgment, has ceased to exist.

   b. The information held by this unit was transferred to the National Counter Terrorism Policing Operations Centre within the Metropolitan Police Service (MPS). A new national database, the National Common Intelligence Application (NCIA), supports the work of this Centre, and is detailed in the General Measures section below.

   c. Other police forces migrated their respective standalone databases to the NCIA. Searches were then conducted by the Compliance & Protective Monitoring Unit across the migrated databases for any references to the applicant. Any remaining references to the applicant that were identified were deleted by 4 October 2019.

   d. The same exercise was conducted in respect of any PDF records held and all references to the applicant were deleted from those records by 4 October 2019.

   e. The ongoing Undercover Policing Inquiry (www.ucpi.org.uk) requires that MPS data is adequately preserved for the purposes of the inquiry. The MPS have therefore maintained a copy of the standalone database referred to in paragraph 1, which contains references to the applicant. Access to this database is restricted to fewer than 20 individuals and it is preserved only for the purposes of the inquiry.

8. The Government considers that all necessary individual measures have been taken and no consequences of the violation suffered by the applicant persist.

GENERAL MEASURES

A) Introduction

9. There are 48 civilian police forces in the United Kingdom (UK): 43 territorial police forces in England and Wales, a national police force in Scotland (Police Scotland) and in Northern Ireland (Police Service of Northern Ireland (PSNI)), and three specialist police forces (the British Transport Police (BTP), the Civil Nuclear Constabulary (CNC) and the Ministry of Defence Police (MODP)).

10. Whilst policing is a devolved matter in Scotland and Northern Ireland, it is legislated for by the UK parliament in respect of England and Wales (for the 43 territorial police forces operating within England and Wales; BTP operating in England, Wales and Scotland; CNC operating in England and Scotland; and MODP across the UK). The Scottish Government and the Northern Ireland Executive are responsible for deciding how most police services are organised and

managed in their nations. Policing culture is very similar throughout the UK, and Police Scotland and the PSNI share many of the characteristics of English and Welsh forces.

11. Each of the three administrations produces guidance for police retention, review and disposal of information.

12. The College of Policing sets the standards, provides training and shares good practice for everyone who works for the police service in **England and Wales**. Police records management for England and Wales is governed by the College of Policing's Management of Police Information[2] (MOPI[3]) Authorised Professional Practice (APP) ("the MOPI APP"), the Police Information and Records Management (PIRM) 2023 Code of Practice[4] which is supported by the Archiving of records in the public interest APP[5] published by the College.

13. Chief Officers in England and Wales must have regard to the PIRM Code of Practice in discharging their duties and they should establish and maintain information and records management policies within their forces that comply with supporting national guidance and the principles of this Code. Chief Officers in the devolved administrations and other forces adhere to its principles.

14. The MOPI APP, which is the guidance issued under the Code, requires forces to carry out scheduled reviews, based on crime type, of data held. Each force is responsible for its own compliance with the APP.

15. In terms of the retention of information, in **Northern Ireland** the PSNI Review, Retention and Disposal schedule identifies the disposal arrangements for records created or received by the PSNI irrespective of format. The schedule complies with the requirements of data protection legislation, the Public Records Act (Northern Ireland) 1923 and the Disposal of Documents Order (S.R. & O.1925 No 167).

16. Whilst governed by specific legislation as above, PSNI also liaise closely with colleagues in the College of Policing and monitor the guidance agreed in the MOPI APP in relation to the retention, review and disposal of police information.

17. Records Management for **Police Scotland** is governed by and defined in its master record set of Policies, Standard Operating Procedures (SOP) and Guidance. In terms of the retention of information, Police Scotland's Record Retention SOP[6] defines record retention and disposition arrangements. The SOP complies with the requirements of data protection legislation and the Public Records (Scotland) Act 2011.

---

[2] https://www.college.police.uk/app/information-management/management-police-information

[3] Under MOPI, data records are recorded under the following groups:

- Group 1 Data – Serious Offences and Public Protection Matters
- Group 2 Data – Other Sexual and Violent Offences
- Group 3 Data – All other offences

[4] https://www.college.police.uk/guidance/police-information-and-records-management-code-practice

[5] https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal#archiving-of-records-in-the-public-interest

[6] https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.docx

18. As explained under the Individual Measures, the information held in the database to which the *Catt* judgment refers was transferred to the National Crime Intelligence Application (NCIA), which is overseen by Counter-Terrorism Policing (a collaboration of UK police forces) who comply with the England and Wales Retention Review and Disposal regime and who have taken specific actions following the *Catt* judgment, which are also detailed at Sections C and D.

19. The Data Protection Act 2018 (DPA) and General Data Protection Regulations 2018 (GDPR) apply to all administrations.

20. With regards the national records deletion process (RDP) concerning the Police National[7] Computer (PNC); National Fingerprint Database (IDENT1) and the National DNA Database (NDNAD):

    a. A member of the public can apply for deletion of records on the national systems (PNC, IDENT1 and NDNAD) through the RDP.
    b. ACRO provides a triage process so that applications fit within the guidance criteria, before sending them to the relevant chief officer(s).
    c. When a chief officer receives an application, under the MOPI guidelines, this triggers a review of information held about the subject, which means that local records are also examined and considered for deletion.
    d. The attached statistics (document titled *RDP Figures – KP*) demonstrate that a high proportion of applications are either approved or partially approved, which may be indicative of the RDP working effectively.

21. This is relevant because although the National Police Coordination Centre (NPoCC)[8] coordinates the strategic national public order response, the vast majority of data on an "incident level" basis would be found within local records. As an example:

    - Anyone arrested for a public order offence at a protest would have this event recorded on PNC.
    - The local force would record on local systems whatever information was required to progress the investigation to an outcome (e.g. No Further Action), which would be recorded on PNC.
    - If a subject wanted their national PNC records erased, they would apply through the national RDP, which would follow the above steps a.-c.
    - Thus, if a non-convicted protester wanted their arrest and corresponding information deleted, there is an effective "pressure release valve" because they can apply at any time to have their records erased.

22. We are not aware of any cases of a similar nature to *Catt* having occurred since the 2019 judgment.

[7] Reference to 'National' refers to a function or service, and processes arising from those, available to all police forces throughout the United Kingdom, i.e. the 48 police forces referred to in paragraph 9.
[8] https://www.npcc.police.uk/our-work/national-police-coordination-centre-npocc/

B) The Data Protection Act 2018

England and Wales

Retention for no longer than necessary (section 39(1) DPA)

23. The DPA regulates the processing of personal data for, among other things, general purposes (under Part 2 DPA, which incorporates UK GDPR) and law enforcement purposes (under Part 3 DPA, which is derived from the Law Enforcement Directive[9]) more commonly referred to as policing purposes. Personal data processed under Part 3 or Part 2/GDPR, including special categories of personal data and criminal offence data are recorded and further processed on policing databases where it is necessary for policing purposes. The policing purposes include[10]:

- protecting life and property,
- preserving order,
- preventing the commission of offences,
- bringing offenders to justice, and
- any duty or responsibility of the police arising from common or statute law.

24. The retention, review and disposal process, detailed in the APP, is based on records of individuals (nominals) who have come to the notice of police as offenders, suspected offenders or whose details have been recorded for another policing purpose. As new information and intelligence is recorded it becomes part of the relevant nominal's record.

25. The nature of the information/intelligence is graded according to the nature of the crime. There are three groups 1-3, with the most serious crimes falling into Group 1 and the least serious Group 3. Records relating to people who are convicted, acquitted, charged, arrested, questioned or implicated for offending behaviour that does not fall within Group 1 or Group 2 are dealt with in Group 3.

26. The nominal record is categorised on the basis of the highest group for which information / intelligence is recorded against the individual. This will determine the frequency of reviews.

27. Reviews are conducted having regard to **all the personal data** held about the nominal, which helps to ensure that data is not retained for longer than is necessary, in accordance with the fifth data protection principle[11] (Section 39, DPA). This allows for the reviewer to consider the impact of retention or deletion on the data subject and the public in a comprehensive manner.

[9] https://www.legislation.gov.uk/eudr/2016/680/contents
[10] https://www.college.police.uk/guidance/police-information-and-records-management-code-practice
[11] (1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

Time limits for periodic review (section 39(2) DPA)

28. Reviews of the personal data are carried out on a scheduled basis as set out below. These are time-based, and dependent on risk posed by or to the individual or individuals, necessity and proportionality.

Group 3

29. A nominal which has Group 3 information/intelligence recorded against them will be reviewed after an initial 6-year clear period. The 'clock is reset' every time new information/intelligence is recorded against the individual.

30. In the case of Group 3 nominals, there is scope for forces to auto-delete the record after 6 years if there is no new information/intelligence. Such decisions are based on the controller having carried out a risk assessment.

Group 2

31. For nominals in Group 2 the review periods are every 10 clear years (for not coming to the notice of the criminal justice system).

Group 1

32. Group 1 nominal data is reviewed every 10 years for accuracy and necessity until the nominal is deemed to be 100 years of age.

National Retention Assessment Criteria (NRAC)

33. Reviews are based on the risk the individual may present using national retention assessment criteria (NRAC). All forces have a Review, Retention and Disposal function and they are trained and resourced accordingly.

34. NRAC asks a series of questions focused on potential risk factors in an effort to draw reasonable conclusions about the risk of harm presented by nominals. Wherever a record is assessed as being necessary and proportionate to the purpose it serves, it can be retained. These questions are as follows:

- Is there evidence of a capacity to inflict serious harm?
- Are there any concerns in relation to children or vulnerable adults? (Where 'concerns' refer to concerns for safety)
- Did the behaviour involve a breach of trust?
- Is there evidence of established links or associations which might increase the risk of harm?
- Are there concerns in relation to substance misuse?
- Are there concerns that an individual's mental state might exacerbate risk?
- Are there any other issues that impact on the level of risk the individual presents?
- Could this individual be of interest to ongoing public inquiries?

35. Where the answer to any of the questions is 'yes', the characteristics of the nominal and their fundamental rights must be fully considered and balanced against any risk identified during the completion of the NRAC. If, having carried out the balancing exercise, the information relating

to the nominal being assessed should be retained, it must be reviewed again at intervals designated by the review schedule, ensuring that:

- records remain adequate and up to date;
- records meet national quality standards;
- new information can be considered; and
- risks are still current.

36. A completed copy of this assessment template should be kept on file as a record that the review has taken place and to support the subsequent decision.

37. Political opinions are only recorded if relevant to the threat/risk posed by the individual and thus will be retained, if required following the NRAC review, to maintain the integrity and value of the record. Age will be recorded routinely on most records to aid identification and also assess threat/risk. Again, the age will be retained, following an NRAC review, to maintain the integrity and value of the record.

Requests for erasure (section 47 DPA)

38. The APP makes it clear that when carrying out reviews, the review should consider the obligations imposed by key legislation such as the DPA, Children Act 2004[12], and Equality Act 2010[13] requirements.

39. Pursuant to the DPA, nominals have a number of individual rights, including those of erasure and rectification, which they can exercise against the police for any data held on police systems. This right is made clear in College of Police issued guidance and is made available to the public in the Force Privacy Notice published on their web pages which includes information on making a complaint should an individual have concerns about use of their personal information, see paragraph 13 at the following link: https://www.college.police.uk/privacy.

Review of adherence to police management information regulatory framework

40. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS)[14] is the independent public body which assesses police forces and fire & rescue services across England, Wales and Northern Ireland for their effectiveness, efficiency, and legitimacy (PEEL). It undertakes inspections of police forces on a cyclical basis and its PEEL assessments are published on its website: https://hmicfrs.justiceinspectorates.gov.uk/peel-reports-year/2023-25/

41. HMICFRS regularly consults on its inspection programmes and frameworks and the Home Office will work with it to actively consider whether the adherence to the current police guidance on information management and record-keeping published by the College of Policing on July 2023 can be examined through future PEEL inspections, or through other inspection activity.

[12] Duty to ensure functions are discharged having regards to the need to safeguard and promote the welfare of children
[13] The Public Sector Equality Duty requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations when carrying out their activities.
[14] https://hmicfrs.justiceinspectorates.gov.uk/

42. On this basis, the Government considers that the systems and processes employed in England and Wales comply with the requirements of the *Catt* judgment.

Northern Ireland (PSNI)

Retention for no longer than necessary (section 39(1) DPA)

43. The DPA is applicable in Northern Ireland and PSNI regularly process data under Part 3 (Law Enforcement Processing). Mandatory training is undertaken by each member of staff to ensure they are aware of their obligations under this Act. PSNI require all staff and officers to complete mandatory E-Learning on Data Protection every 2 years. The training materials are not an exact mirror of the APP but designed to cover all elements of compliance.

44. PSNI provide guidance for all officers and staff for sensitive processing under both parts 2 and 3 of DPA. This guidance aligns with PSNI's existing SI0518 Data Protection Service Instruction and reflects the Home Office Appropriate Policy Document (APD) and is produced in accordance with our obligations under sections 35(4) and 35(5) of Part 3 of the DPA.

45. The guides apply to sensitive processing – as defined in section 35(8) DPA – undertaken by the PSNI in accordance with Part 3 of the DPA. PSNI processing of special category data for general purposes is covered in a separate document APD for sensitive processing, UK GDPR/Part 2.

46. The PSNI Review, Retention and Disposal (RRD) Schedule assists PSNI in complying with its statutory obligations in relation to data protection, by identifying what records it holds, how long it needs to keep these and subsequently what should happen to these records at the end of their life cycle. The Schedule applies to all records created or received by the PSNI, irrespective of format.

47. The Schedule complies with the requirements in the Public Records Act (NI) 1923 and the Disposal of Documents Order (S.R. & O.1925 No 167) and assists PSNI in meeting its legislative compliance in relation to both the DPA and GDPR. Adherence to the Schedule will ensure records are processed in line with data protection principles with records being managed; accurately, effectively, in line with a specific business purpose, and only held for as long as is necessary.

48. PSNI will review and assess records in line with this Schedule and any reviews that result in a decision to extend the minimum retention of records must be recorded on a National Retention Assessment Criteria (NRAC) Form. This form provides extra assurance that records are only retained when necessary to do so.

49. PSNI will keep information only for as long as is necessary; therefore, to ensure compliance with the fifth data protection principle, during the compilation of the schedule the Records Manager liaises with Information Asset Owners across the Service in relation to:

- their assets
- description/example of record within the assets

- retention (minimum period) for which a review must be undertaken
- rationale or legislation dictating the retention
- final action to be performed on the record.

50. In considering the above, PSNI takes into account:
    - the College of Policing APP
    - specific National Archives guidance
    - local Public Record Office of Northern Ireland (PRONI) advice and guidance
    - specific legislation, Regulations, National Guidance, and PSNI business need. Some examples of this include, Police (Northern Ireland) Act 2000, Regulation of Investigatory Powers Act 2000, Police and Criminal Evidence (NI) Order 1989, The National Archives guidance and National Police Chiefs' Council (NPCC) RRD Schedule.

Time limits for periodic review (section 39(2) DPA)

51. PSNI will keep information only for as long as is necessary, and built into the PSNI Review, Retention and Disposal Schedule are review and retention periods for each information asset.

52. PSNI also adhere to the MOPI principles and relevant records are reviewed according to their MOPI group. This includes 10-year reviews for MOPI 1 and MOPI 2 groups. PSNI adhere to the MOPI APP and assign MOPI codes to offences as per the MOPI table included within this APP. MOPI 1 offences are the most serious offences, posing the most risk, and include public protection matters. These records are retained until the subject is aged 100 years with 10-year reviews. MOPI 2 offences include other sexual and violent offences; these records are held initially for a 10-year clear period and are then reviewed every 10 years. Any offence not included within MOPI 1 or MOPI 2 are classified as MOPI 3 records and are retained for 6 years with, where relevant, 5-year reviews. These MOPI groupings are included as information assets within the PSNI RRD Schedule. As indicated above, PSNI also use a NRAC form, in the same manner as the England and Wales response above, to justify the retention of records to ensure that records are not held excessively.

53. Once the PSNI RRD Schedule is compiled and signed off by the Service's Senior Information Risk Officer (SIRO), it is presented to the Public Records Office Northern Ireland (PRONI) for onward transmission to the library of the Northern Ireland Legislative Assembly where it sits for 10 plenary sessions, thus enabling local members of the legislative assembly to challenge any aspect. Once it has proceeded through this process (and any queries resolved) it is adopted as the current Service Review, Retention and Disposal (RRD) schedule. While there is no mandated time period for the lifetime of a schedule, PRONI consider 3 years an acceptable period. During the review and updating of the Schedule at the 3-year juncture, each information asset on the Schedule is reviewed in consultation across PSNI and against the NPCC National Retention Schedule. This ensures that the arrangements against each asset are still relevant and up to date in terms of review/retention periods, the rationale for applying these timeframes and that the final action attached to each asset is still appropriate. This review ensures PSNI are only holding the data for as long as is necessary and in line with data protection principles. The PSNI RRD Schedule is found at the footnoted link.[15]

[15] https://www.psni.police.uk/sites/default/files/2022-07/Police%20Service%20of%20Northern%20Ireland%20-%20Review%2C%20Retention%20and%20Disposal%20Schedule%20V0.3.pdf

54. When a nominal record is reviewed, PSNI practice would reflect that of national guidelines considering threat, risk, intent and capability, using NRAC. As part of this assessment, all categories of data are considered. Political opinions are only recorded if relevant to the threat/risk posed by the individual and thus will be retained, if required following the NRAC review, to maintain the integrity and value of the record. Age will be recorded routinely on most records to aid identification and assess threat/risk. Where appropriate, age will be a factor which the RRD Reviewer takes into consideration when deciding whether to delete or retain a record. Data (including that relating to age) may be retained, following an NRAC review, to maintain the integrity and value of the record, having regard to all the underlying material.

55. Record Reviewers, are nominated individuals from within the respective area, trained to review records once the minimum retention timeframe (as set out in the PSNI RRD Schedule) has expired, and make recommendations regarding final action, subject to the assessment of risk in line with national guidelines and / or a justifiable continuing business need, for consideration and sign-off by the respective Information Asset Owner (IAO).

Requests for erasure (section 47 DPA)

56. In compliance with data protection legislation PSNI operate a process for Subject Access requests where members of the public can request to see a copy of the information that PSNI hold on them. In addition to the right of access, individuals have the right to request that a number of other rights, enshrined in data protection legislation, are actioned, including the right to rectification, right to restriction and the right to erasure. Once a request has been submitted to PSNI, a specialist Panel will review the request and respond within one month. If the Panel decline the request the requestor is informed in writing and advised if they disagree with the decision they have the right to complain to the Information Commissioner's Office. Further information can be located at the footnoted link.[16]

Ongoing measures

57. PSNI submitted the RRD Schedule to Public Records Office Northern Ireland (PRONI) in March 2024, and responded promptly to a series of queries from PRONI in June and September, returning a further amended RRD Schedule in November 2024. To date, PSNI's understanding is that this has not been laid before the NI Assembly by PRONI but will be in the near future. The current RRD Schedule will continue to apply until this approval process is concluded.

58. Any additions or amendments to the College of Policing APP will be reflected within PSNI policies and procedures.

59. PSNI's Record Review follows national protocols, framed by MOPI and College of Policing guidelines, using the NRAC process to assess risk. No cases of a similar nature have occurred in Northern Ireland since the 2019 judgment.

60. In addition, but in broader terms, PSNI's Data Governance structures have been strengthened significantly, and there has been extensive work undertaken on education and awareness across

[16] https://www.psni.police.uk/request/information-about-yourself/enacting-other-rights-under-data-protection-legislation

the service relating to Information Management. Its Information Asset Owners (IAOs) hold accountability and responsibility for Information Management in their respective business areas, and further education and awareness events for IAOs are scheduled to prioritise, energise and capitalise on the importance of this work.

61. It is acknowledged that members of the public can apply under GDPR for the right to erasure, and processes are in place to manage such requests.

Scotland (Police Scotland)

Retention for no longer than necessary (section 39(1) DPA)

62. The DPA regulates the processing of personal data for, among other things, general purposes (under Part 2 DPA, which incorporates UK GDPR) and law enforcement purposes (under Part 3 DPA, which is derived from the Law Enforcement Directive[17]). Personal data, including special categories of personal data and criminal offence data are recorded and further processed by Police Scotland where it is necessary for policing purposes. The policing purposes include:
    - the prevention and detection of crime,
    - preventing harm/risk of harm to an individual(s),
    - legal proceedings,
    - the discharging of statutory functions, including but not limited to that included in the Police and Fire Reform (Scotland) Act 2012 which states that "the main purpose of policing is to improve the safety and well-being of persons, localities and communities in Scotland"[18].

63. In line with the DPA fifth data protection principle, and the requirements of element 5 of the Records Management Plan[19] (required by the Public Records (Scotland) Act 2011 s1), Police Scotland details and publishes its instructions on how long records are retained and when they are deleted in the 'Records Retention Standard Operating Procedure'[20] (SOP). This is supplemented by detailed Guidance and Instructions specific to systems and processes.

Time limits for periodic review (section 39(2) DPA)

64. Retention periods for 'crime records', which are those records and data that relate to the investigation of crimes and incidents are transitioning from an event-triggered model to a model based on nominals. In the new nominal model, the information is graded 'low', 'medium' or 'high' according to the nature of the crime/incident and will be retained for 10, 20 or 100 years. The most serious crimes, generally Scottish Government Justice Directorate (SGJD) Group 1-2 are considered high risk and SGJD groups thereafter classified either medium or low on a pre-defined matrix.

65. The nominals associated with the most serious crimes and/or patterns of serial behaviour will be held for the longest period to address risk, harm and public safety.

[17] https://www.legislation.gov.uk/eudr/2016/680/contents
[18] https://www.legislation.gov.uk/asp/2012/8/section/32
[19] https://webarchive.nrscotland.gov.uk/20240926193359mp_/https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/keepers-assessment-report-police-scotland-august-2022.pdf
[20] https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.docx

- Where a nominal has a low crime/incident associated to them and no other information is added, it will automatically delete after a period of 10 years.
- Where a nominal has a medium crime/incident associated to them and no other information is added, it will automatically delete after a period of 20 years.
- Where a nominal has a high crime/incident associated to them and no other information is added, it will automatically delete after a period of 100 years.
- Where a nominal has a low crime/incident associated to them and other information is added within the defined time spans, the low crime incident will adopt the retention policy of the latest information; for example, a low crime/incident followed by a low crime/incident 3 years later will all be retained until 10 years has passed from the date of the last crime/incident.
- Where a nominal has a high crime/incident associated to them, any low or medium crime/incident records to which they are already associated will also be retained for the maximum time.

66. Manual review requirements have been limited to apply a consistent approach and reduce subjectivity.

67. Police Scotland, in common with other UK forces, utilises the CT Policing Network for processing information in relation to counter-terrorism activities, this includes RRD activities which are undertaken on its behalf by CTPHQ (further documented at section (C) of this document. Police Scotland does not maintain separate domestic extremism databases.

68. Intelligence on all policing matters is triaged at the point of electronic capture on the Scottish Intelligence Database (SID) by specialist intelligence officers to ensure that it meets one of the standard grounds for collection and retention and has been properly evaluated and where applicable sanitised, prior to any dissemination (known as 'sanitisation'). At this point specialist intelligence officers with additional mandatory training and following documented Guidance undertake reviews and select an appropriate deletion date based on predefined principles. A delete date of 1, 6 or 12 years is applied which is wholly dependent on the contents of the intelligence (including the level of criminality involved and threat posed) and balanced against principles of proportionality and necessity of retention.

69. On reaching the delete date, the intelligence will again be evaluated by a trained individual to check if grounds for retention remain, in which case a further deleting period is selected or, if grounds no longer exist, the intelligence is removed from the system permanently.

70. The training course for the Scottish Intelligence Course requires pre-reading of certain materials, notified to students as part of a formal process. The pre-reading material includes the attached document titled *Scottish Intelligence Database (SID) Review Retention and Weeding* [Deleting] *of Intel Material - Guidance Document* which at paragraph 4.6 states:

> 'This list of situations [grounds] is not exhaustive and it is imperative that the LIO [Local Intelligence Officer] in every case consider **all relevant** information that may influence their decision to retain or delete intelligence and never assess the intelligence in isolation.'

71. Such situations would include age and political opinion.

72. Where the last piece of intelligence linked to a nominal (individual) is deleted then that nominal record will be deleted entirely. The nominals associated with the most serious crimes and/or patterns of behaviour will be held for the longest period to address risk, harm and protect public safety:
    - A retention period of 12 years will be considered where existing intelligence indicates that a person is a "core nominal" for example, they are a leading member of an organised crime group, or intelligence indicates that they have committed a Group 1- Non-sexual Crime(s) of Violence or a Group 2- Sexual crime
    - A retention period of 6 years will be considered where intelligence indicates that a person has committed a crime in certain defined categories, including Group 3- Crimes of Dishonesty, Group 4- Damage and Reckless Behaviour or Group 5- Crimes against Society, that on conviction, a person could be expected to be imprisoned for a term of 3 years or more if they are over the age of 21 years of age or expected to be detained for the same period if under the age of 21 years of age. (Crime Groups are defined as per the Scottish Crime Recording Standards)
    - A retention period of 1 year will be considered where intelligence indicates that a person is involved in any form of criminality, other than those for which the punishment is imprisonment, for example Road Traffic Offences, Vandalism, Anti-Social and Disorder.

73. Evidence is provided in the table below to demonstrate that the SID sanitisation, review and deleting processes have been routinely undertaken in line with the processes described during 2024.

	Total No. of Logs on SID **A**	**Total No. of Logs Sanitised** **B**	**Total No. of Logs Reviewed** **C**	**Logs Set to Auto-delete** **D**	**Total No. of Logs Deleted** **E**
2024					
March	2339819	26023	30825	527	15082
April	2350074	28547	41322	240	17813
May	2355840	29097	31787	125	23496
June	2365923	26299	29469	452	17090
July	2373556	27394	31561	93	19223
August	2387946	27490	25137	70	12960
September	2402534	27884	25171	720	12720
October	2416008	29030	22299	82	15254
November	2432353	27803	19791	72	12534

74. Column C indicates the total number of logs subject to a manual review each month by a trained intelligence officer. At the end of the review, a log will either be retained and a new delete date added, as per the deleting rules, or it will be deleted as indicated in Column E.

75. Column E indicates the total number of logs that auto-deleted. When a trained intelligence officer decides a log does not meet retention criteria for an extended retention, they can either change the delete date to that day and it will delete that night, or they can set to auto-delete and it will delete on its original delete date with no more notifications.

Requests for erasure (section 47 DPA)

76. There remains the right of individuals to engage their statutory rights under data protection legislation based on their individual circumstances which can lead to a decision to reduce the retention period for certain data based on those circumstances. Police Scotland has a team in place to deal with any requests and publishes information required of it by the DPA to enable individuals to engage their data subjects' rights, including but not limited to the right to request deletion of data[21]. When each applicant is informed of the outcome of their request, they are also informed that they have the right to lodge a complaint with the Information Commissioner's Office (ICO) if they are not satisfied with the way that their request has been handled. Contact details for the ICO are provided directly to the applicant with each response. This procedure is also outlined on the same page of the Police Scotland website.

Ongoing measures

77. Police Scotland transitioned its crime retention policy, implemented in 2024, and will review the new policy to coincide with its statutory requirement to resubmit a Records Management Plan in 2027.

78. Police Scotland will consider whether any further assessment of retention of special category data in DPIAs is required as part of an ongoing review of DPIA creation.

79. Police Scotland will work with National Counter-Terrorism Police Headquarter colleagues to ensure that RRD which is being undertaken on behalf of Police Scotland is being done taking consideration of the *Catt* judgment. In addition, Police Scotland will update its Record Retention SOP as this work progresses.

C) The National Common Intelligence Application in UK Counter-Terrorism Policing

Introduction

80. The Counter-Terrorism Policing (CTP) Network operates as a collaboration of UK police forces working with the UK intelligence community to help protect the public and UK national security by preventing, deterring, and investigating terrorist activity. The Network is coordinated by the CTP Headquarters (CTPHQ) which has a number of functions, including providing policy and guidance on the use of data. The CTP Retention, Review and Disposal (RRD) Policy is one of these policies.

81. It should be noted that since the *Catt* judgment, CTP no longer has primacy for Strategic Protest. This area of policing business now sits with the National Police Chiefs' Council, including compliance with data protection principles. However, due to a public inquiry into Undercover Policing (Undercover Policing Inquiry: Official Website (ucpi.org.uk)) the records belonging to the now defunct National Policing Domestic Extremism Unit have been retained on NCIA. These records are retained in accordance with a legal obligation as set out in s.35(3) Inquiries Act 2005, which stipulates:

[21] https://www.scotland.police.uk/access-to-information/data-protection/

‘(3) A person is guilty of an offence if during the course of an inquiry—

(a) he intentionally suppresses or conceals a document that is, and that he knows or believes to be, a relevant document, or

(b) he intentionally alters or destroys any such document.

For the purposes of this subsection a document is a “relevant document” if it is likely that the inquiry panel would (if aware of its existence) wish to be provided with it.’

82. As a consequence, these records are retained for the purposes of the UCPI and not general users. There are no records related to the applicant contained within this [NCIA] dataset.

National Common Intelligence Application

83. The NCIA is the national secure intelligence database for the CTP Network. Prior to its implementation, Counter Terrorism (CT) and extremism-focused policing units used different instances of the National Special Branch Information System (NSBIS). This led to approximately 60 unnetworked NSBIS databases across the UK. This resulted in duplicate information being migrated into the NCIA, as often the same information was disseminated to different CT units across the UK. Since the implementation of the NCIA, CTP has invested heavily in removing duplicate intelligence and reviewing nominal records, a process which continues today and is expected to be completed by December 2025.

RRD Activity

84. Operating on one national database has enabled better compliance oversight. A robust governance structure is in place and the senior RRD lead for the NCIA is required to report progress against their RRD targets, each quarter.

85. A new unit of 45 members of staff is being recruited to review overdue records by December 2025 and a technical solution to merge duplicate records has been implemented. This ensures that the NCIA will only contain records that have a continuing policing purpose and are not duplicated.

86. The RRD staff have all undertaken a robust 10-day training course to ensure that the balance between protecting the public and the rights of the individual is appropriately applied to all cases. The decision to retain and dispose of records are subject to a multi-tiered assurance process that ensure consistency in decision making. The first level is by a reviewer’s line manager and the second level is undertaken by an independent RRD assurance reviewer.

87. The Terminology and Threshold Matrix lays out the definitions and thresholds which are to be applied in an effort to determine whether information and intelligence to which this CTP Relevance Test applies should be passed to a more appropriate unit for assessment and further action if appropriate.

88. The matrix is used to determine if intelligence received is relevant to CT Policing. Below are some examples to highlight how the matrix is used, albeit the exact definitions are sensitive due to operational considerations.

- Example 1*:* If a white supremacist was handing out leaflets stridently promoting their cause which fall just beneath the criminal threshold, this would typically be regarded as High Level Aggravated Activism. This is because, whilst the activity is (short of criminality) 'low', the ideology being espoused in the leaflets seeks the subjugation of a specific group/proportion of the population. Applying the matrix, a practitioner may regard the intelligence as being CT relevant and could ultimately become a contributing radicalising factor for a self-initiated terrorist.

- Example 2: If environmental protesters were to hand out leaflets promoting their cause that fall just beneath the criminal threshold, this would typically be regarded as Lawful Activism and would not be CT relevant. This is because the combination of ideological outcome and activity are unlikely to influence possible terrorist activity.

- Example 3: An individual leaves a pipe-bomb next to an animal testing centre with the phrase "death to animal murderers" attached to it. Whilst the ideological outcome may be 'Low' or 'Moderate' (depending on the case), their activity would meet the TACT threshold therefore would meet the CTP threshold. This is because all activity which is assessed as 'Severe' (meets definition of S.1 Terrorism Act 2000 and offences under TACT 2000 & 2006) is CTP relevant regardless of the 'Ideological Outcome'.

- Example 4: A group undertake a protest about a new road being built glue themselves to plant machinery. In this instance, the ideological outcome would be 'Low' and the activity (depending on the exact details) may extend up to 'Moderate'; this being reflective of the need to consider human rights points around lawful protest. From a CT perspective, this matter would not be CT relevant and would fall within the Low-Level Activism space.

89. In the case of Mr Catt, the ideological outcome i.e. lawful protest to bring about change, would be **low** and not relevant to CT policing.

90. Before becoming an intelligence assessor, individuals must complete the National Standards of Intelligence Management (NSIM) Assessor training course, and therefore all should be trained in the standards of intelligence, including the Terminology and Threshold Matrix. The Matrix has formed part of the CT Intelligence Assessor course from 2021. The numbers of attendees on the course between 2021 and 2024 is provided in the attached document titled *20241210 NSIM Assessor Course 21-24 – Terminology and Thresholds Matrix*.

91. Further information on the Terminology and Threshold Matrix and its application was provided in response to a request under the Freedom of Information Act 2000 on 8 November 2022 which included three documents:

i. The Terminology and Thresholds Matrix Power Point Presentation
ii. Definitions: Activity in furtherance of ideology
iii. Matrix definitions

92. The response and these three documents are also attached.

93. Further, CTP have adopted a more proactive use of triggered reviews. During day-to-day business, if a record no longer has a policing purpose, it can be triggered for a review, without having to wait until the scheduled review period ends. This ensures that records on individuals that are found not to be involved in terrorism are removed from NCIA as soon as possible. Each region has Information Management Units that make assessments as to whether information should be retained on the system or triggered for review based on the continuing CT policing purpose to retain the information.

Details of the revised review, retention and disposal policy that supports the assessor team working with the National Common Intelligence Application database

Criteria for retention or deletion

94. Personal information is only retained on the NCIA where it has been assessed as counter terrorism relevant during the assessment process. Anything that is entered on NCIA and is found not to be CT relevant, is disseminated to a relevant crime unit, if necessary and triggered for disposal. As stated above, the CTP Network no longer collects intelligence on protests.

95. The very nature of CT Policing requires special category data to be collected routinely. This includes political opinions.

The Terrorism Act 2000 defines terrorism, both in and outside of the UK, as the use or threat of one or more of the actions listed below, and where they are designed to influence the government, or an international governmental organisation or to intimidate the public. The use or threat must also be for the purpose of advancing a political, religious, racial or ideological cause.

The specific actions included are:
- *serious violence against a person;*
- *serious damage to property;*
- *endangering a person's life (other than that of the person committing the action);*
- *creating a serious risk to the health or safety of the public or a section of the public; and*
- *action designed to seriously interfere with or seriously to disrupt an electronic system.*

Source: *Crown Prosecution Service (https://www.cps.gov.uk/crime-info/terrorism)*

96. The impact on the privacy of the individual is considered throughout the information lifecycle and it is only retained when there is an identifiable threat and risk to members of the public in the UK and abroad. If it is assessed that there is a continuing policing purpose to continue to retain the information, the information will be retained for a further 10 or 6 years, depending on the MOPI group. There is no 7-year review.

97. The RRD Reviewers have regard to all the special categories of data when reviewing cases. The nature of CT's mission means that political opinions are often highly relevant to the policing purposes being exercised. The reviewers are trained to take into consideration Article 8 of the European Convention on Human Rights and various pieces of legislation, including DPA, the Equality Act 2010 and the Criminal Procedure and Investigations Act 1996. A National Retention Assessment Criteria (NRAC) review is carried out under an Article 8/DPA

lens. NCIA is sophisticated enough to allow for data to be deleted where it no longer has a policing purpose, including political opinions.

98. Age is a relevant factor for reviewers, who will, among other things, take into consideration the age of the nominal at the time the data was recorded and at the date of the review. This is in recognition of the fact that people often mature with age and may not necessarily continue to pose a risk or be at risk when they are adults, having previously had their data recorded when they were children.

Maximum time limits

99. The maximum time limits for retention are in accordance with the MOPI groups (detailed above) which are documented on the College of Policing website.[22]

100. The time limit for retention for groups 2 and 3 is for so long as there is an ongoing policing purpose (as per the High Court of England and Wales judgment in R(II) v MPS [2020] EWHC 2528).

101. In CTP the onus is on the RRD Reviewer to justify why the material should be retained. The rationale is recorded in the NCIA and subject to an assurance regime to ensure consistency. Due to the potential harm caused by act of terrorism, MOPI 3 data in CTP is manually reviewed every 6 years.

102. When a nominal record is reviewed, the NCIA RRD Reviewer considers threat, risk, intent and capability, using NRAC. As part of this assessment, all categories of data are considered. Political opinions are only recorded if relevant to the threat/risk posed by the individual and thus will be retained, if required following the NRAC review, to maintain the integrity and value of the record. Age will be recorded routinely on most records to aid identification and assess threat/risk. Age will be a factor which the NCIA RRD Reviewer takes into consideration when deciding whether to delete or retain a record. Data (including that relating to age) may be retained, following an NRAC review, to maintain the integrity and value of the record, having regard to all the underlying material.

Categorisation

103. Much of the information stored on the NCIA is categorised as MOPI group 1, due to the serious nature of terrorism. If intelligence is found to be incorrect or relates to crime, it is triggered for review and disposed of from the NCIA. MOPI group 3 is used for material that CTP cannot be immediately linked to a terrorism offence. This category is also used for intelligence relating to the safeguarding of vulnerable people, including children.

104. The NCIA has the functionality where a member of staff can trigger a review outside of the scheduled review periods. This is used when it has been identified that there is no longer a policing purpose to retain the information; for example, when intelligence is found to be incorrect following an investigation.

[22] https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal

Periodic review

105. Since the introduction of the NCIA and the project set up to recruit 45 RRD staff, CTP's RRD response has significantly improved. Whereas prior to the implementation of the NCIA, there was little oversight of RRD activity on the different instances of NSBIS (predecessor to NCIA), CTP now has a robust governance and assurance structure that ensures RRD is being undertaken in a meaningful way. RRD performance is monitored at the CTP Digital Data and Technology Board, chaired by CTP's Data Director, who reports to the highest executive board in CTP. There is a backlog of cases that the RRD Team is working to eliminate by December 2025. Much of the backlog was caused by duplicate records being migrated from 60+ NSBIS systems into the NCIA.

106. The business-as-usual process is that records will be presented to the RRD Reviewer every 10 or 6 years, depending on the MOPI group. If the subject no longer presents a risk to the public and there is no longer a CT policing purpose to retain the information, it will be disposed of. If the data is retained, a rational is entered into the NCIA system and the scheduled review data is set to either 10 or 6 years hence, depending on the MOPI group.

107. The RRD staff have all undertaken a robust 10-day training course to ensure that the balance between protecting the public and the rights of the individual is appropriately applied to all cases. The decision to retain and dispose of records are subject to a multi-tiered assurance process that ensure consistency in decision making. Reviewers are aware that to retain data on an ongoing basis it must be for a legitimate aim, be lawful, and necessary and proportionate within the meaning of Article 8 of the Convention.

D) Overview of Review, Retention and Disposal in Counter-Terrorism Policing

108. The CTP RRD Policy aligns to the College of Policing guidance published on information management[23] but these are discrete documents. It seeks to balance the risk of terrorism to members of the public and the rights of the individual. In accordance with the MOPI, the NCIA has the functionality to create nominal records that can be categorised into the three MOPI Groups[24].

109. Upon the receipt of new intelligence, a trained Assessor assesses the MOPI Group of the nominal, considering both the current and new information and checks the accuracy of the data. This is relayed to a specialist unit that assigns the MOPI Group, indexes the information and creates the required links in the database. The Assessment of new information is key to maintaining public safety while balancing the rights of the subject. The Assessors attend a four-day course to undertake this role, part of which is assigning the correct MOPI group based on the information being assessed. Many CTP subjects of interest are categorised as MOPI 1 – Public Protection Matters but, where there is not a clear link to terrorism or the subject is a juvenile, the MOPI 3 category is used.

[23] https://www.college.police.uk/app/information-management
[24] See footnote 3.

110. The following are examples of the type of data recorded under each MOPI category:

- MOPI 1 category includes offences described in UK terrorism legislation and/or whether there is information that would help protect the public and our national security by preventing, deterring, and investigating terrorist activity.

- MOPI 2 category would be used for terrorism subjects of interest involved in offences of a sexual nature. In CTP this is rarely used, as the reason for recording and retaining information on NCIA is for terrorism purposes.

- MOPI 3 material is used for material that does not fit into the above categories. Generally, this is material that CTP cannot be immediately linked to a terrorist offence. This category is also used for intelligence relating to the safeguarding of vulnerable people, including children.

111. In accordance with MOPI, Group 1 records are reviewed every 10 years; Group 2 is reviewed following a 10-year clear period and Group 3, initially after 6 clear years and then every 5 clear years thereafter. The maximum time limit for MOPI 1 data is until the subject reaches 100 years (subject to accuracy and necessity, as it is acknowledged that not all information will be needed or is required to be kept for the full tariff); MOPI 2 is until the subject no longer poses a high risk of harm; MOPI 3 when the subject is no longer involved in terrorism-related activity. At the point of review, the onus is on the reviewing officer to make a case for retention and they must provide a rational explaining the policing purpose for retention.

112. By the very nature of the CT policing, special category data, including age and political opinions, are collected and processed by CTP across different IT platforms, in order to achieve its statutory obligations. A policy document is in place that explains the need to do this to keep people safe from terrorism. This data is reviewed and disposed of in accordance with the CTP RRD Policy and MOPI review periods above.

113. When a nominal record is reviewed, the NCIA RRD Practitioner considers threat, risk, intent and capability, using NRAC. Political opinions are only recorded if relevant to the threat/risk posed by the individual and thus will be retained, if required following the NRAC review, to maintain the integrity and value of the record. Age will be recorded routinely on most records to aid identification and also assess threat/risk. Again the age will be retained, following an NRAC review, to maintain the integrity and value of the record.

114. The new Code of Practice will not impact this because the details of retention, review and disposal practices are included in the Authorised Professional Practice.

E) Publication:

115. The judgment has been published on the database of the *British and Irish Legal Information Institute*:

- https://www.bailii.org/eu/cases/ECHR/2019/76.html

116. It was also summarised on a number of legal and general websites, including:

- *The Times* newspaper (Law Reports), 29 January 2019 https://www.thetimes.co.uk/article/domestic-extremism-database-lacks-appropriate-safeguards-cn9k3l39x

- *UK Police Law Blog* https://www.ukpolicelawblog.com/the-catt-that-got-the-cream/

- *UK Human Rights Blog* https://ukhumanrightsblog.com/2019/01/30/privacy-and-the-peace-protestor-an-extended-look/

F) Dissemination:

117. The UK Government disseminated the judgment to the police and other law enforcement agencies at the Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board meeting held on 6 March 2019. Membership of the board includes police force representatives, Government departments and representatives from the Devolved Governments. The meeting was also attended by representatives from the Information Commissioner's Office, the Investigatory Powers Commissioner's Office, the Office of the Biometrics Commissioner, the National Law Enforcement Data Service, the Surveillance Camera Commissioner, the Forensic Science Regulator's Office and the Police and Crime Commissioner for Surrey. Minutes of the meeting are publicly available at:

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808240/Facial_Images_and_New_Biometrics_Oversight_and_Advisory_Board_Mar_19_Minutes.pdf

118. Further, the UK Government disseminated the judgment to members of the joint National Police Chiefs' Council and Home Office FIND (Forensics Information Databases) Strategy Board, which oversees the police use of DNA and fingerprints.

119. The Devolved Governments have also disseminated the judgment to PSNI and Police Scotland, which have provided the information set out under the General Measures above.

G) State of execution of judgment:

120. The distinctive arrangement and organisation of policing in the United Kingdom is summarised in paragraphs 9-11 of this document, as are the discrete but aligned and concomitant guidance documents for each governmental administration (England and Wales, Scotland and Northern Ireland) concerning the retention, review and disposal of information by respective police forces at paragraphs 12-17. Legislation such as the Data Protection Act 2018 (DPA) and General Data Protection Regulations 2018 (GDPR) also applies to all administrations (paragraph 19).

121. As evidenced in sections A-D of the General Measures element of this document, the policing bodies for those administrations and Counter-Terrorism Policing have taken appropriate actions following the *Catt* judgment. In addition, all necessary individual measures have been taken and no consequences of the violation suffered by the applicant persist. Furthermore, we are not aware of any cases of a similar nature to *Catt* having occurred since the judgment in 2019. As a result, the Government considers that these measures collectively demonstrate a comprehensive, equitable and conclusive response to the judgment, that all necessary individual and general measures have been taken, and that the Committee's supervision of the case should be closed.