

Acknowledgements

openDemocracy is an independent global media platform that seeks to challenge power and encourage democratic debate.

This report (published in 2024) was researched and written by Jenna Corderoy and edited by Martin Williams, Ramzy Alwakeel and Indra Warnes.

Thanks also to Duncan Lewis Solicitors, John Pring, Emily Apple, Jessica Upton, Network for Police Monitoring, Nicola Burgess, Andrew Frederick, Andrew Lownie and Jon Baines.

Cover image: Alexander Spatari / Getty Images / Composition by James Battershill for openDemocracy.

Introduction

Data protection laws provide a vital legal resource in the UK. The UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 gives people the right to request a copy of any personal information an organisation holds about them.¹ This is known as a Subject Access Request (SAR).

SAR is an extremely powerful right, covering public authorities as well as private companies, charities, political parties and other organisations. Over the years, SARs have been responsible for exposing injustices, supporting legal claims and revealing the extent of surveillance.

For instance, they have revealed how an MP was secretly flagged by a government disinformation unit after criticising ministers;² shown why a journalist was banned from covering a UK arms fair;³ revealed how the Home Office confused an asylum seeker with at least three other refugees while trying to deport him;⁴ and found that the Department for Education kept files on teaching staff⁵ and education experts⁶ who had criticised government policy. And last year, Nigel Farage sparked a surge in requests to banking institutions after he used an SAR to support his claim that Coutts private bank had shut down his account because of his political views.⁷

The rules say that SARs should usually be responded to within one month. In complex cases, this deadline can be extended to a further two months.⁸ But that is all. And in instances where the request is directed at police and law enforcement authorities, no such extensions apply.

But long and unjustified delays – sometimes lasting several months – are increasingly commonplace and can have real-life impacts. Documented by openDemocracy for the first time here, these delays are depriving citizens of their personal information and undermining their legal and human rights.

For instance, we found that an asylum application made by a victim of human trafficking had been put on hold due to the government delays in responding to an SAR. In another case, an individual's claim for false imprisonment cannot currently proceed because of the failure to comply with requests on time.

¹ Organisations tend to ask for proof of identity when an individual requests a copy of their personal information.

² <https://www.theguardian.com/politics/2023/jun/18/caroline-lucas-flagged-by-disinformation-unit-over-covid-criticism>

³ <https://www.middleeasteye.net/news/exclusive-why-ian-cobain-was-actually-banned-covering-uk-arms-fair>

⁴

<https://www.theguardian.com/uk-news/2023/sep/27/uk-home-office-in-mistaken-identity-row-over-plans-to-deport-indian-asylum-seeker>

⁵ <https://www.theguardian.com/politics/2023/oct/21/uk-government-keeping-files-on-teaching-assistants-and-librarians-internet-activity>

⁶ <https://www.theguardian.com/education/2023/sep/30/revealed-uk-government-keeping-files-on-education-critics-social-media-activity>

⁷ <https://www.bbc.co.uk/news/business-66272594>

⁸ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access/> It is important to note that when police forces process SARs in relation to law enforcement, they cannot extend the deadline. They have to respond within the 30-day deadline.

Such impacts were also reflected in the Report of the Independent Inquiry into Child Sexual Abuse in 2022, which said victims and survivors had “faced difficulties” when requesting their records from institutions.⁹ The report stated: “Issues may include long delays, procedural hurdles, and poor communication and explanations from the institutions. The Inquiry also received evidence that some institutions did not respond appropriately to requests for access to records. For some complainants, the search for records and the lack of communication and explanation was difficult and upsetting.”

In many cases, it can take months or even years to receive a response. And when requesters do receive their responses, sometimes the disclosures are missing key information that they need – for instance, to support asylum applications. In some cases, lawyers are forced to apply for court orders to compel government departments to release personal data to their clients in full.

SAR compliance is meant to be upheld by the Information Commissioner’s Office (ICO), but we found that formal action is vanishingly rare. Although it tracks and monitors complaints, the ICO almost always gives organisations a free pass to ignore the rules.

Meanwhile, it is ironically extremely difficult to obtain and monitor transparency records in the UK. Although a few public authorities do publish some basic statistics about SARs on their websites, the vast majority do not.

Often, the only way to obtain the relevant data is by using the Freedom of Information (FOI) Act to make specific requests. But this is only possible with public authorities. And even then – as we found out – many authorities either refuse to provide detailed information, or do so in a format that is not comparable with other authorities, rendering them almost meaningless.

Meanwhile, millions of companies and other private organisations who receive SARs are not subject to the FOI Act, so there is no requirement whatsoever for them to disclose details of how promptly they respond to SARs.

For this report, we focused on three groups of public authorities: police forces, central government departments, and London borough councils. These authorities are likely to regularly receive requests that relate to serious legal proceedings, from criminal court cases and asylum applications, to adoption records and custody battles. Therefore, the prompt and fair handling of these requests is not only important for the sake of the individual’s legal rights, it also has wider legal and justice implications.

9

<https://www.iicsa.org.uk/reports-recommendations/publications/inquiry/final-report/ii-inquirys-conclusions-and-recommendations-change/part-h-supporting-victims-and-survivors/h5-access-records.html#:~:text=Under%20the%20Data%20Protection%20Act,access%20or%20subject%20access%20request>

Executive summary

Our investigation found:

- Long delays to SARs are undermining people's legal and human rights. For instance, we found that an asylum application made by a victim of human trafficking had been put on hold due to the government delays in responding to an SAR. In another case, an individual's claim for false imprisonment is currently unable to proceed because of the government's failure to comply with requests on time. Civil claims and complaints against the police are also being delayed as a result of poor SAR performance.
- Delays in dealing with these requests have also impacted victims of the Windrush Scandal, many of whom needed to obtain copies of their immigration records in order to claim compensation.
- Lawyers believe that certain government departments regularly omit paper documents from SAR responses, and refuse to cooperate when complaints are made.
- Public authorities' compliance with SARs is often shrouded in secrecy; several government departments, police forces and councils refused to provide us with performance data.
- The Foreign, Commonwealth & Development Office (FCDO) stands out for its astonishingly bad record for handling SARs. Last year, it responded to just one in five requests within the standard one-month deadline. Lawyers also complained about the performance of the Metropolitan Police.
- There is almost no enforcement of SAR compliance, creating a 'Wild West' for personal data. The Information Commissioner's Office very rarely takes direct action against organisations, even when there are clear breaches to the law. The watchdog itself admits it doesn't "punish an organisation for breaking the law" apart from in the "most serious cases", and encourages ordinary citizens to pursue cases themselves through the courts. However, given how expensive this can be, most people will be left at the mercy of individual organisations, with little to no ability to enforce the law.

Personal data in Whitehall

Central government departments often deal with SARs from the most marginalised people in society. These include asylum cases, where people at risk of being removed from the UK often need to access their records to prove their immigration history.

But in recent years, several government departments have been reprimanded by the ICO over their handling of SARs. This includes the Ministry of Defence, which had a huge backlog of requests,¹⁰ and the Home Office, which missed the deadline for some 20,000 SARs during part of 2021.¹¹

To assess SAR compliance in Whitehall, we sent FOI requests to every government department, asking for details of their compliance record between 2021 and 2023. Specifically, we asked:

1. How many SARs were responded to within one month;
2. How many were responded to after one month but with a permitted extension;
3. How many were responded to after one month but without a permitted extension;
4. How many were responded to after three months and six months?

Several departments failed or refused to provide these figures. Out of 20 departments, only 12 provided the full data that we asked for,¹² while three provided partial data that was often of limited use.¹³

Others (including the Ministry of Justice and the Department for Work and Pensions) said it would cost too much to answer the questions. Without the data from these major departments, it is impossible to conclusively assess SAR compliance levels in Whitehall, although the figures we did manage to obtain nevertheless shed some light.

They reveal an astonishingly poor record by the Foreign, Commonwealth & Development Office (FCDO) last year, responding to just a fifth of requests within the month deadline.

¹⁰ <https://ico.org.uk/media/about-the-ico/documents/4021724/mod-reprimand-letter.pdf>

¹¹ <https://ico.org.uk/media/about-the-ico/documents/4021721/home-office-reprimand-letter.pdf>

¹² These were: Attorney General's Office, Department for Business and Trade, Department for Energy Security & Net Zero, Department for Environment, Food & Rural Affairs, Department for Science, Innovation & Technology, Department for Transport, Department of Health and Social Care, Foreign, Commonwealth & Development Office, Home Office, Northern Ireland Office, Scotland Office, Wales Office

¹³ These were: Department for Culture, Media & Sport, Department for Education, HM Treasury

The percentage of SARs responded to within a month broken down by year:¹⁴

Department	2021	2022	2023
Attorney General's Office	100%	100%	86%
Department for Business & Trade (established 2023)	Unavailable	Unavailable	53%
Department for Culture, Media & Sport	65%	94%	96%
Department for Education	Unavailable	Unavailable	82%
Department for Energy Security & Net Zero (established 2023)	Unavailable	Unavailable	100%
Department for Environment, Food & Rural Affairs	77%	76%	91%
Department for Science, Innovation & Technology (established 2023)	Unavailable	Unavailable	92%
Department for Transport	87%	37%	62%
Department of Health & Social Care	68%	77%	77%
Foreign, Commonwealth & Development Office	21%	24%	21%
Northern Ireland Office	88%	100%	33%
Scotland Office	100%	Did not receive SARs	100%
Wales Office	100%	Did not receive SARs	100%

Source: FOI

Additional to this data is the Home Office, which has three separate teams that deal with SARs. Of these, the unit responsible for immigration records receives by far the most requests – with close to 44,000 SARs last year alone – but responded to the fewest within a month.

¹⁴ There are caveats to the data above, however. In its release, the Department for Education said that some SARs that were received were closed as “no response was received from the requester following a request for identification”. This may apply to other departments too, and the Department for Business and Trade said that some requests were not “valid”. Also, some departments receive relatively low numbers of SARs each year; the Northern Ireland Office, Scotland Office and Wales Office typically receive requests in the single digits, if any, meaning a small number of delays or timely responses can have a misleading impact on their overall compliance rates.

The percentage of SARs sent to the Home Office that were responded to within a month, broken down by year:¹⁵

Home Office Unit	2021	2022	2023
Subject Access Request Unit (SARU) (immigration records)	32%	28%	64%
HM Passport Office	74%	99%	99%
Information Rights Team (IRT) (other Home Office SARs)	64%	74%	78%

Source: FOI

SAR requests are still classified as being dealt with “in time” when government departments extend the deadline by up to two months. For example, in 2022 the Department for Transport said that 37% of its SARs were processed within one calendar month, but a further 34% were answered beyond the month deadline with permitted extensions. These responses are considered on time under data protection law.

The Foreign, Commonwealth & Development Office (FCDO) stands out as being consistently late with responses. In 2023, it received 159 SARs, of which 49% were responded to late (after the one-month deadline, without a permitted extension). And 16% took more than six months.

The poor performance of many departments has led some MPs to use parliamentary questions to force the government to disclose information about the delays. One question prompted the Ministry of Defence to highlight how deadlines can be “legally extended”. In response to another parliamentary question, the FCDO revealed a “dip in performance” for the third quarter of the 2022/23 financial year, due to a number of factors including “an upsurge in Subject Access Requests... relating to Sanctions”.¹⁶

Alongside these figures, we also analysed the number of data protection complaints about central government departments that the ICO closed (“completed”) in the first half of 2023/24. We note that the departments receiving the most complaints are often the same ones that refused to disclose compliance data to us.

¹⁵ The Home Office said the total number of SARs received by SARU may include non-valid SARs (where either proof of identity or proof of authority were not supplied), and would therefore not have been processed within the statutory deadlines. We do not know how many of these requests were invalid. Also, the IRT does not record data by year, so the figures are in 12 month periods starting April 2020-March 2021.

¹⁶ <https://questions-statements.parliament.uk/written-questions/detail/2023-09-01/196810>

Department	Complaints completed	Complaints completed that were in connection to right of access
Ministry of Justice	243	139
Department for Work & Pensions	168	70
Ministry of Defence	36	26
Home Office	53	24
Cabinet Office	12	8

Source: ICO

Responding to our finding, a government spokesperson told openDemocracy: “We take our obligations under the Data Protection Act 2018 and UK General Data Protection Regulation very seriously, and we are working hard to remove delays to Subject Access Requests identified by the Information Commissioner’s Office.”

Impact on asylum cases

In 2017, former NHS nurse Dean Ablakwa was deported to Ghana, despite being born in the UK and having no criminal record. But he was unable to challenge the Home Office's decision because it failed to respond to his SAR.¹⁷

Speaking from the Ghanaian capital, Accra, at the time, he told The Independent that he felt like he was in prison. "My mental health is really bad. I can't sleep at night," he said. "I had plans, things to look forward to. But my life has been put on hold."

The delays were partly due to the Home Office complaining that the request should have been written "in blue ink". At the time, the Home Office said that SAR delays were sometimes inevitable due to the "complexities of some cases". While it is no doubt true that some cases are more complex than others, the department has shown no sign of improvements.

Lawyers at Duncan Lewis Solicitors told openDemocracy that these delays have impacted their clients' legal cases. Even when disclosures are made, they are sometimes missing important documents. For instance, they may include electronic records, but omit scans of hardcopy documents. But lawyers say that when they complain, the Home Office often refuses to engage with them and insists they have provided everything.

In one case last year, a client with physical and mental health diagnoses was detained at an Immigration Removal Centre. The individual was released after two months, but is now pursuing a claim for false imprisonment. For that claim to have any chance of success, lawyers needed internal Home Office documents with details of their detention, so an SAR was submitted in November 2023. The department provided a disclosure almost two months later, but it was full of unexplained redactions. Lawyers believe it was also missing key original documents from the time of the individual's detention. They complained but, at the time of writing, the lawyers have still not heard back from the Home Office.

Another case involved a human trafficking victim who was brought to the UK. They claimed asylum upon arrival, while still under the control of their traffickers. But before the asylum application was approved, they were taken to an unknown location, held against their will and sexually exploited by the traffickers. The Home Office accused the person of absconding and withdrew their asylum claim. Last summer, a unit within the department eventually accepted that the individual was a victim of trafficking and modern slavery.

The victim's lawyers asked for the asylum claim to be reinstated – but, in order to do this, they needed to fully understand why it was withdrawn in the first place. So an SAR was submitted for documents in the autumn of 2023. But lengthy delays meant they had no choice but to progress

¹⁷

<https://www.independent.co.uk/news/uk/home-news/home-office-justice-vital-information-sar-personal-data-immigration-history-a8983361.html>

the asylum case without them. A full disclosure did not come until February 2024. The very next day, lawyers were told that their client's asylum claim would be reinstated.

It's a similar story for victims of the Windrush Scandal, many of whom needed to submit SARs to the Home Office to access their full immigration records. These documents are essential to show the person's immigration history, which is often key to establishing their entitlement to compensation.

Nicola Burgess, a solicitor at Greater Manchester Immigration Aid Unit (GMIAU), supports Windrush survivors and helps them to submit SARs. However she says that, in the majority of cases, the disclosures are incomplete. Despite asking for copies of all documents held by the Home Office, the department only provides computer records, omitting older paper documents. GMIAU then has to write back and again request a full disclosure.

Burgess believes this is a tactic "designed to help the Home Office meet its targets and to reduce delays... But in our cases the computer records will never be sufficient as our client's entry to the UK will always pre-date the introduction of their computerised system."

Burgess currently has four active cases where the Home Office claimed to have made a full disclosure, but actually held more documents. "One is particularly egregious as a document has been relied on to refuse our client compensation but this has never been disclosed to us despite numerous specific requests. This puts our clients at a real disadvantage, not having sight of the full case against her or a real opportunity to respond."

Outside Windrush, GMIAU's other clients are also finding it difficult to obtain full SAR disclosures. In one case, the organisation had to make an application for a court order to compel the Home Office to provide missing information. "This is a step which wouldn't be required if full and frank disclosure was provided at the first possible opportunity in line with the DPA," added Burgess.

She continued: "The human impact of these failures is huge as it results in decisions being made about a person's life – whether it be the right to compensation for historic injustice, or the fair determination of a person's right to remain in the UK – and the individual simply doesn't have access to all the relevant information being considered or any reliable means of obtaining it. This perpetuates the inequality of arms in these cases where it is the individual against the state."

Case study:

John Pring

The Department for Work and Pensions (DWP) was one of the five government departments to refuse our FOI request. But a previous disclosure showed that in October 2022, it had some 2,678 SAR cases open. Almost half of these had been open beyond the one-month deadline, and a further 691 SARs were awaiting clarification.

In one case, the editor and founder of Disability News Service, John Pring, had to wait two-and-a-half years to obtain personal information held by the Department for Work and Pensions.¹⁸ He first submitted his request at the start of 2020, in an attempt to see how the department viewed his coverage of disability issues.¹⁹ But despite the ICO saying in March and October 2020 the DWP had clearly breached data protection rules, the department still did not respond.²⁰

The following year, law firm Mishcon de Reya stepped in, acting pro bono for Pring.²¹ Commenting at the time, the firm's senior data protection specialist, Jon Baines, said the ICO had "simply stood back and refused to take any meaningful action". Even with the support of a leading law firm, it wasn't until June 2022 that the DWP finally responded – and disclosed 90 pages of emails they had about Pring.

Among other things, these emails appear to support the accuracy of a story Disability News Service published in 2019, which revealed that a disability assessor had lied to the DWP about a woman's mental health. The original story reported how civil servants had dismissed the woman's allegations. They reportedly told her that disability assessors have "nothing to gain by fabricating evidence or suppressing information". However, emails obtained through Pring's SAR showed that, behind closed doors, the DWP had acknowledged the assessment had been "contradictory". The emails add that a "quality assurance team" had "identified a number of issues with the report and the decision-making".

Pring now claims that a "policy of delaying the release of potentially embarrassing information, often for years, has gradually become ingrained within DWP" – leading to a culture of cover-up, secrecy, delay and denial.

He added: "The department's legal duty was to release that information within a month. In fact, it took them two-and-a-half years, and even then they only did so after I managed to get pro bono support from the brilliant data protection specialist Jon Baines at Mishcon de Reya. How many disabled people are going to be able to access that kind of expertise?"

¹⁸ <https://www.disabilitynewsservice.com/dwp-finally-admits-defeat-in-information-battle-with-dns-after-two-and-a-half-years/>

¹⁹ <https://www.disabilitynewsservice.com/dwp-repeatedly-failed-to-provide-data-requested-by-dns-and-others-says-regulator/>

²⁰ <https://www.disabilitynewsservice.com/dwp-repeatedly-failed-to-provide-data-requested-by-dns-and-others-says-regulator/>

²¹ <https://www.mishcon.com/news/mishcon-acts-for-editor-of-disability-news-service-in-data-protection-matter>

Police forces

SARs represent one of the few tools that ordinary citizens have to hold the police accountable. In recent years, successful SARs have revealed concerning abuses of power – including monitoring peaceful protesters²² and placing journalists on the domestic extremist database.²³ Police forces reported an increase in SARs in March 2021 following the murder of Sarah Everard by an off-duty police officer.²⁴ At the time, police forces were coming under greater scrutiny about their officer vetting processes and their handling of the vigils and protests held in the aftermath of Everard's death.

But campaigners and lawyers told openDemocracy they faced significant difficulties in getting full disclosures on time, sometimes with real-world consequences.

Posing the same questions that we did to government departments, we asked every UK police force to provide details about their SAR compliance record.²⁵ But again, many refused or ignored our requests. Out of 48 police forces, only 14 provided the statistics in full²⁶, while 18 provided partial data.²⁷ The request was ignored by two forces²⁸ and refused by 14 others²⁹, who claimed it would cost too much to compile the data. Several of the biggest police forces, such as London's Metropolitan Police Service and Greater Manchester Police, were among those to refuse the request.

Based on the data we obtained, Devon & Cornwall Police and Dorset Police stood out as the two worst-performing forces by some margin. These forces joined together in a "strategic alliance" in 2015 to "improve delivery, resilience and flexibility, as well as save money" in areas including data protection. But their track record for handling SARs is shocking. Between 2021 and 2023, around a third of SARs submitted to the two police forces took more than six months to answer.

In response to openDemocracy's findings, a spokesperson for the two forces said the number of SARs they deal with has "increased each year" since 2018. They said that improving compliance is a "priority", but acknowledged that "we must undertake further work to make the improvements that are needed".

²² <https://www.theguardian.com/uk/2011/apr/11/domestic-extremist-police-databases>

²³ <https://www.theguardian.com/commentisfree/2014/nov/21/police-snoop-journalists-freedom-data-protection-act>

²⁴ <https://ico.org.uk/media/action-weve-taken/reports/4019584/timeliness-of-responses-by-police-forces-follow-up.pdf>

²⁵ It is important to note that when police forces process SARs in relation to law enforcement, they cannot extend the deadline. They have to respond within the 30-day deadline.

²⁶ These were: Cheshire Constabulary, Cumbria Constabulary, Devon & Cornwall Police, Dorset Police, Essex Police, Gloucestershire Constabulary, Merseyside Police, Northamptonshire Police, Surrey Police, Warwickshire Police, West Mercia Police, West Midlands Police, Gwent Police, Ministry of Defence Police

²⁷ These were: Bedfordshire Police, Cambridgeshire Constabulary, Hertfordshire Constabulary, Cleveland Police, Derbyshire Police, Durham Constabulary, Kent Police, Lancashire Constabulary, Norfolk Constabulary, North Yorkshire Police, South Yorkshire Police, Staffordshire Police, Suffolk Constabulary, Wiltshire Police, North Wales Police, Police Scotland, British Transport Police, Civil Nuclear Constabulary

²⁸ These were: Humberside Police, Police Service of Northern Ireland

²⁹ These were: Avon and Somerset Constabulary, City of London Police, Greater Manchester Police, Hampshire Constabulary, Leicestershire Police, Lincolnshire Police, Metropolitan Police Service, Northumbria Police, Nottinghamshire Police, Sussex Police, Thames Valley Police, West Yorkshire Police, Dyfed-Powys Police

In February 2024, shortly before the publication of this report, both forces were reprimanded by the ICO, after it learned that they had hundreds of overdue SARs.^{30 31} But for the hundreds of individuals who faced delays, this action may be seen as too little, too late. Statistics show that the forces' SAR delays were at their worst in 2021, where more than half of requesters were made to wait over six months. By the time the ICO finally issued its enforcement notices, the backlog was already improving.

Kent Police also received a reprimand from the ICO in late 2022.³² The ICO discovered that only 60% of the SARs it received between April 2020 and April 2021 were responded to within the statutory timescales. In the first half of 2022, that figure dropped to 22%.

Gloucestershire Police also stands out as having a particularly poor record for SARs, with nearly 14% of all requests taking more than six months to process over the last three years. But no enforcement notices against Gloucestershire Police are currently listed on the ICO's website.

The percentage of SARs responded to within a month, broken down by year³³:

	2021	2022	2023
Bedfordshire Police	85%	84%	78%
Cambridgeshire Constabulary	91%	83%	81%
Cheshire Constabulary	97%	95%	94%
Cleveland Police	65%	66%	72%
Cumbria Constabulary	63%	82%	85%
Derbyshire Constabulary	95%	65%	71%
Devon & Cornwall Police	37%	40%	28%
Dorset Police	38%	31%	29%
Durham Constabulary	77%	91%	77%

³⁰ <https://ico.org.uk/media/action-weve-taken/reprimands/4028177/devon-and-cornwall-police-final-reprimand.pdf>

³¹ <https://ico.org.uk/media/action-weve-taken/enforcement/chief-constable-dorset-police/>

³² <https://ico.org.uk/media/about-the-ico/documents/4021722/kent-police-reprimand.pdf>

³³ There are caveats to the data. Some police forces informed us that a few requesters withdrew their SARs prior to receiving a response. It is also quite possible that SARs were received towards the end of 2023, and were still being processed at the time the police forces received our FOI requests (and that the one calendar month deadline had not concluded).

Essex Police	46%	43%	75%
Gloucestershire Constabulary	69%	75%	78%
Hertfordshire Constabulary	83%	83%	79%
Kent Police	61%	23%	85%
Merseyside Police	98%	97%	98%
North Yorkshire Police	55%	59%	71%
Northamptonshire Police	71%	90%	60%
Surrey Police	94%	97%	96%
Warwickshire Police	92%	85%	92%
West Mercia Police	68%	71%	64%
West Midlands Police	5%	39%	74%
Wiltshire Police	82%	79%	69%
Gwent Police	75%	76%	50%
North Wales Police	98%	97%	94%
South Wales Police	59%	69%	58%
British Transport Police	88%	Unavailable	98%
Ministry of Defence Police	100%	100%	90%

Source: openDemocracy FOI requests

Rather than answering the questions openDemocracy put to them, several police forces claimed the information was already in the public domain and pointed us towards the National Police Chief's Council (NPCC)'s collation of SAR statistics. In reality, the NPCC data is very limited and does not answer openDemocracy's questions in full (for instance, it does not show when extensions have been applied, or how many requests were more than six months late) .

We analysed the most recent NPCC data available at the time of our research, which covered the 12 months up until August 2023. This further evidences that non-compliance with SARs is widespread. Across 31 police forces, on average, more than one in ten SARs were not responded

to within the one-month deadline. And six forces were “out of time” in more than half of the cases they dealt with.

Police force	Average percentage of SAR responses that were ‘out of time’ over previous 12 months
Dorset	75%
Devon & Cornwall	71%
West Midlands	63%
Nottinghamshire	61%
Sussex	53%
Dyfed-Powys	53%

Source: NPCC, August 2023

It may be easy to dismiss these delays as a purely bureaucratic issue, but in many cases they lead vulnerable people to suffer. For instance, SARs may be useful in historic child sexual abuse cases, where victims need to obtain documents and witness statements that can be used for potential damages claims against the institutions that failed them. Delays may therefore be distressing and disruptive to this process.

Likewise, video footage of stop-and-searches or arrests is often needed for evidence when people bring civil claims and complaints against the police. But lawyers told us they have struggled to obtain officers’ body-worn camera footage via SARs for their clients. Andrew Frederick, a solicitor at Scott-Moncrieff & Associates, said it can take months for the Metropolitan Police to respond to SARs, which adds months to his clients’ legal claims and has forced him to make complaints to the ICO.

“I would estimate that it is six to seven months on average to get it,” Frederick said. “I can’t think of one case that I’ve dealt with where they’ve complied with the one-month calendar deadline for providing body-worn video.”

Although some forces have improved their SAR compliance, the overall picture is concerning – especially as awareness of information rights increases and more people submit requests. The Metropolitan Police, for instance, has seen a steady rise in the number of SARs it has received, with more than 20,000 last year alone. As of 31 January 2024, the force had 2,612 open SARs, almost 2,000 of which were more than 60 days old.³⁴ When asked for details of its SAR performance by openDemocracy, the Metropolitan Police rejected our request.

Data published by the ICO covers all types of data protection complaints, including issues unrelated to SARs. For instance, people may complain about misuse of personal data, or

³⁴ <https://www.met.police.uk/sd/stats-and-data/met/right-of-access-performance-dashboard/>

inaccurate personal data. However, we have been able to filter these figures to show complaints “in connection to right of access”, which we believe will be almost entirely cases about SARs. We are also able to filter the results to show only complaints made about police forces.

The figures represent complaints that have been resolved by the ICO during the first half 2023/24. The top ten forces were as follows:

Council	Complaints completed	Complaints completed that were in connection to right of access
Metropolitan Police Service	177	141
Greater Manchester Police	63	53
Sussex Police	53	48
Police Scotland	54	37
Devon & Cornwall Police	30	22
Kent Police	24	17
Northumbria Police	25	17
Thames Valley Police	27	17
West Midlands Police	25	15
Northamptonshire Police	16	13
South Wales Police	19	13

Source: ICO

Case study:

Emily Apple

Emily Apple is acutely aware of the importance of SARs, having previously found out that police had monitored her due to her involvement in peaceful protests.

Apple works for Campaign Against the Arms Trade, as well as the Network for Police Monitoring (Netpol), and has been on the radar of police forces for years. She was violently arrested in 2008 after attempting to challenge police officers for not displaying their badge numbers.³⁵ She also discovered her name had been added to the Metropolitan Police's "domestic extremist" database.³⁶

Apple believes that SARs are needed so people can see how data is being recorded on protesters. "No one should be on a police database for exercising their democratic rights, but we know this is what happens," she told openDemocracy. "It's really important to know how and why the police are monitoring protests and the extent to which they're monitoring protesters."

"I want to make sure that there is accountability for the amount of surveillance that happens to me as a protester, and to be able to hold those systems to account, to be able to campaign on them politically. We have to have access to that data that is being collected on us."

But in her efforts to access personal information, she has faced repeated delays. This includes a response from Devon and Cornwall Police in 2023 that took around six months, which Apple said was "unsatisfactory", with documents missing. The records she did manage to obtain revealed the police knew her phone number and current email address. But the "intelligence trail", showing why they had obtained it, was not included in the disclosure. Phone calls and messages that she received from a police liaison officer while protesting the Bibby Stockholm, a boat used by the government to house asylum seekers, were also not included. "They've been selective as to what they've picked out and how they've done it," said Apple. "It's incredibly incomplete."

In the past, Apple has received successful SAR responses from the Metropolitan Police and been given reams of personal data. But in June 2023, the force rejected a new request outright, claiming that disclosure would likely prejudice the prevention or detection of crime. Apple thought this was odd, since she hasn't been arrested since 2019 and was not aware of any active investigations against her. She appealed against the decision straight away, but never heard back from the Metropolitan Police. Apple then referred the case to the ICO, which upheld her complaint, but – at the time of writing – she has still not heard back from the police and her messages have been ignored.

³⁵ <https://netpol.org/domestic-extremism/key-cases/emily-apple/>

³⁶ <https://www.theguardian.com/commentisfree/libertycentral/2009/oct/27/police-domestic-extremists>

Case study:

Jessica Upton

Jessica Upton joined Extinction Rebellion in 2019 and has since been arrested numerous times as a result of her protests. She has also joined other climate groups like Just Stop Oil.

But when she submitted an SAR to the Metropolitan Police last year, it sparked a bizarre and troubling exchange that has still not been resolved. More than two months after filing her request, she was informed that it was still waiting to be allocated to a caseworker for processing. This was later followed by a claim that the police force did not hold any information about her. Over the following months, Upton wrote to the police repeatedly to request a review of the case, as she was certain the response was wrong. Eventually – almost a year after she first made the request – she received an email from the police asking her to “bear with us” and saying the ICO was “aware of the situation”. At the time of writing, she has still not had a response.

Speaking to openDemocracy, Upton said: “I’m very anxious to know what details the police hold about me. I’m a veterinary surgeon and foster carer and so have DBS checks done regularly. I obviously keep my employers fully informed about my activism – protest is a right and it’s something to be proud of – but sadly I’ve known the police to be plain wrong and so I need to be aware of what is being recorded about me.

“For example, in October 2022 I was arrested for wilful obstruction of the highway and kept overnight to go straight to court the next day – partly because the desk sergeant was informed I’d previously been arrested for ABH [assault occasioning actual bodily harm] and was breaking bail conditions. Neither of these things were correct and understandably deeply distressed me as I am strictly non-violent and hadn’t ever had ABH mentioned to me at arrest.

“It took me 16 months of pursuing a complaint to be informed that I was correct and that the officer who’d reported the ABH had mixed me up with someone else. To be able to defend myself against such false allegations I need to know what the police have recorded about me.”

In response to openDemocracy, a spokesperson for the Metropolitan Police Service cited the “high demand” for SAR disclosures compared to other forces. “We ensure regular contact is maintained with the applicant and we appreciate the impact that delays have on individuals,” they said, adding: “We have commissioned a specific piece of work to redesign and further improve service development in this area.”

London councils

Local councils hold huge amounts of vital information, from adoption records to financial documents. People have even submitted SARs to councils in order to prove cases of mistaken identity.^{37 38} But as with other authorities, councils can present requesters with significant problems in the form of delays and inadequate responses.

In recent years, councils have received more reprimands by the ICO over poor SAR compliance than any other type of organisation – although the vast majority are still let off the hook. Last year, the London Borough of Lewisham was reprimanded over the frequency of delays, which the ICO said “has had a significant impact on the data subjects”.³⁹ The council blamed these delays on remote-working during the pandemic, as some requests related to paper documents. In 2022, the ICO also reprimanded Lambeth, Hackney and Croydon Councils over delays.^{40 41 42}

We sent FOIs to all London councils, posing the same questions as we did to police forces and government departments. But once again, many refused or failed to respond. Of the 33 councils, only nine provided the complete set of statistics we requested.⁴³ Twenty disclosed partial data, with varying degrees of usefulness.⁴⁴ Havering Council completely refused our FOI request on cost grounds, and Hackney and Enfield Councils hadn’t responded to our request at the time of writing.

This lack of transparency makes it impossible to tell whether compliance is improving or getting worse in councils like Hackney, which completely ignored our request.

³⁷

<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/action-taken-against-seven-organisations-who-failed-in-their-duty-to-respond-to-information-access-requests/>

³⁸ <https://www.bbc.co.uk/news/uk-england-birmingham-68144996>

³⁹ <https://ico.org.uk/media/action-weve-taken/reprimands/4026219/lewisham-reprimand-20230816.pdf>

⁴⁰ <https://ico.org.uk/media/action-weve-taken/reprimands/4025202/lambeth-reprimand-letter.pdf>

⁴¹ <https://ico.org.uk/action-weve-taken/enforcement/london-borough-of-hackney/>

⁴² <https://ico.org.uk/action-weve-taken/enforcement/london-borough-of-croydon/>

⁴³ These were: Barking & Dagenham, Bromley, Hammersmith & Fulham, Kensington & Chelsea, Lambeth, Lewisham, Merton, Waltham Forest, City of London

⁴⁴ These were: Barnet, Bexley, Brent, Camden, Croydon, Ealing, Greenwich, Haringey, Harrow, Hillingdon, Hounslow, Islington, Kingston Upon Thames, Newham, Redbridge, Richmond upon Thames, Southwark, Sutton, Tower Hamlets, Westminster

The percentage of SARs responded to within one month - breakdown by year:⁴⁵

	2021	2022	2023
Barking and Dagenham	89%	78%	81%
Bexley	67%	72%	71%
Bromley	35%	65%	57%
Croydon	7%	37%	63%
Ealing	48%	67%	59%
Greenwich	35%	46%	47%
Hammersmith & Fulham	34%	47%	43%
Harrow	53%	44%	64%
Kensington & Chelsea	63%	72%	85%
Kingston Upon Thames	88%	86%	57%
Lambeth	58%	68%	37%
Lewisham	71%	68%	57%
Merton	41%	54%	50%
Newham	84%	88%	76%
Redbridge	76%	74%	67%
Richmond Upon Thames	77%	89%	Unavailable
Sutton	89%	96%	79%
Waltham Forest	48%	69%	58%
Wandsworth	76%	65%	Unavailable
City of London	68%	75%	80%

Source: FOI

⁴⁵ There are caveats to this data, just as with the data collected for police forces and central government departments. Some people withdraw their SARs soon after making them. Bromley Council said that, for 2021, it could only provide data for 1 August to 31 December. When we received a response from Merton Council in early January, it informed us that the figures for 2023 are subject to change as some requests received at the end of December may still be within the original month deadline and some requests may be subject to extensions. Richmond upon Thames Council informed us that some SARs were not processed as they received no ID confirmation. It's likely that this may apply to other councils as well. And with some councils like Westminster, we had to exclude them altogether as they did not provide the total amount of SARs they had received by year.

It is important to note that, as with government departments, councils can apply for a two-month extension to respond to SARs, meaning these would still be classified as “in time”. But only 13 councils provided us with data about this, with some councils applying for extensions for up to one in five cases they deal with.

It appears that Lambeth and Lewisham Councils are still failing to respond on time, despite being reprimanded by the ICO. Last year, just 57% of cases in Lewisham were processed within one month – a significant dip compared to the years before. Croydon Council, however, appears to have made a big improvement since it was reprimanded, suggesting that intervention can result in a positive outcome.

The data openDemocracy has collected gives an idea about compliance levels among councils, and strengthens the call for councils to collate accurate, in-depth statistics on their SAR performance and publish them for wider scrutiny.

We also analysed the number of data protection complaints about London councils that the ICO “completed” in the first half of 2023/24. It is worth noting that Hackney and Enfield Councils – neither of which responded to our FOI request – are both in the ten most complained-about councils, along with Lambeth and Lewisham.

In response to our findings, a Lewisham Council spokesperson said: “We apologise for delays in our handling of Subject Access Requests and recognise that our past performance in this regard hasn’t been good enough. The council has agreed an improvement plan with the ICO and continues to work closely with them. This has already seen a steady improvement in response times.”

Lambeth Council blamed the “large number” of requests it receives, and claimed it has made “improvements to this service”.

The ten most complained-about London councils in relation to data protection:

Council	ICO complaints completed	ICO complaints completed that were in connection to right of access
Lambeth	28	19
Hackney	20	15
Hillingdon	18	14
Croydon	17	13
Camden	9	8
Enfield	11	8
Lewisham	14	8
Waltham Forest	14	7
Greenwich	9	6
Newham	13	6
Southwark	11	6

Source: ICO

SAR complaints to the ICO

According to the ICO website, when people are unhappy with how their SARs have been handled, the first step should be to complain directly to the organisation concerned. If the person is still unhappy with that organisation's response, they can register a complaint with the ICO. But even if it's clear that rules have been breached, this will not normally result in a reprimand or enforcement notice. Instead, the ICO will simply "give them advice and ask them to solve the problem".

The watchdog makes it clear that it does not "punish an organisation for breaking the law (apart from in the most serious cases)".⁴⁶ It adds: "We do not normally take regulatory action for individual complaints as we want organisations to comply with the law without us using our formal powers. It is therefore unlikely we will take regulatory action as a result of your complaint."

The ICO goes on to say: "You can also seek to enforce your rights through the courts. If you decide to do this, we strongly advise you to seek independent legal advice first."

However, pursuing cases through the courts can be prohibitively expensive. This means that in the vast majority of cases, ordinary people seeking to exercise the legal right to access personal information are left at the mercy of individual organisations, with little to no ability to enforce the law.

The ICO regularly publishes the number of data protection complaints it has received, which includes complaints about SARs.⁴⁷ In its 2022/23 annual report, the ICO said it had "completed" almost 35,000 data protection complaints, of which "a significant proportion" were from people who felt they had not been given access to the personal information an organisation holds about them.⁴⁸

Yet despite receiving so many complaints, it is extremely rare for the ICO to issue reprimands and enforcement notices. Just three reprimands were issued in relation to SAR compliance last year, all of which were directed at councils.^{49 50 51}

This situation is compounded by the ICO's high caseload, which saw the regulator receive more than 14,000 complaints about SARs last financial year. In an email to one complainant, an ICO staffer wrote: "We are currently dealing with a large number of cases, which has meant that we have been unable to deal with incoming complaints as promptly as we would like."

⁴⁶

<https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data/what-to-do-if-the-organisation-does-not-respond-or-you-are-dissatisfied-with-the-outcome/>

⁴⁷ <https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/data-protection-complaints/>

⁴⁸ <https://ico.org.uk/media/about-the-ico/documents/4025864/annual-report-2022-23.pdf>

⁴⁹ <https://ico.org.uk/action-weve-taken/enforcement/london-borough-of-lewisham-reprimand/>

⁵⁰ <https://ico.org.uk/action-weve-taken/enforcement/norfolk-county-council/>

⁵¹ <https://ico.org.uk/action-weve-taken/enforcement/plymouth-city-council/>

Analysis of more than 16,000 complaints that were completed in the first half of 2023/24 reveals a mix of public and private institutions receiving the most complaints.

The ten most complained about organisations in relation to data protection for quarters one and two of 2023/24:

Most complained about organisations	Number of data protection complaints	Complaints relating to SARs
Ministry of Justice (MoJ)	243	139
OVO Energy Limited	182	118
Chief Constable Commissioner for the Metropolis (Metropolitan Police Service)	177	141
Department for Work and Pensions (DWP)	168	70
Meta Platforms Technologies UK Ltd (formerly Facebook UK Limited)	115	70
Google UK Limited	112	6
Virgin Media Limited	97	37
Barclays Bank PLC	94	32
British Gas Trading Limited	84	49
HM Revenue and Customs (HMRC)	81	38

Source: ICO

Case study:

Andrew Lownie

For many years, historian Andrew Lownie fought for the disclosure of the diaries and correspondence of Lord Mountbatten, an influential and controversial member of the royal family.

The diaries were purchased by Southampton University for millions of pounds in 2011, with the promise they would be made accessible to the public.⁵² But when Lownie put in a request to view them, it was rejected; the university cited a Cabinet Office power of veto.⁵³ This led to a lengthy and complex legal battle, which cost Lownie hundreds of thousands of pounds.

Lownie submitted SARs to various institutions caught up in the scandal, but many provided information late and with key documents missing.

He told openDemocracy: “For six years I had been trying to obtain information from Southampton on their withholding of the personal diaries and letters of Dickie and Edwina Mountbatten, some 33,000 pages which had been bought with public monies to be open. This had culminated in an ICO Decision Notice for Southampton to release them which they then appealed.

“I concluded there must be extensive correspondence about me, given the size of the legal files, and my SAR was to discover more about what had happened behind the scenes. But Southampton simply produced my call slips ordering other Mountbatten documents in the collection.”

Believing there were many important documents missing from the response, Lownie complained to the ICO but was told that no further action would be taken. When he asked for this decision to be reviewed, the ICO simply recommended that the university should respond to Subject Access Requests within the statutory timeframe, but again said it would not take any further action.

An ICO caseworker told him: “If the university has confirmed that it has provided you with all the personal information you are entitled to receive, we have no choice but to accept these assurances in the absence of evidence to the contrary.”

They explained that since the ICO had now reviewed its initial decision, Lownie had exhausted the ICO’s complaints process.

⁵² <https://www.crowdjustice.com/case/andrew-lownies-case/>

⁵³ <https://www.theguardian.com/uk-news/2021/may/15/cabinet-office-blocks-publication-of-lord-mountbattens-diaries>

Recommendations

For organisations (including any public and private institutions that handle SARs):

1. Collate accurate and detailed data about SAR performance and publish these statistics on a regular basis.
2. Rapidly clear any SAR backlogs. And where SAR performance is consistently bad, increase support and increase the number of staff that deal with them.
3. Apply legal extensions to SAR responses sparingly and only in the most complex of cases.
4. Ensure that information searches for SARs include paper documentation when appropriate.

For the ICO:

1. Issue more reprimands and enforcement notices against public authorities and private companies that consistently fail to respond to SARs on time. This should include intervention on individual SAR cases where there has been a clear breach of data protection laws, instead of only taking action about an organisation's overall compliance levels.
2. Devote more resources to ensuring that cases are dealt with swiftly and are not allowed to pile up.
3. Devise strategies to meaningfully and effectively deal with cases where individuals believe they have not been provided with all the information they requested, including legal intervention if necessary.
4. Issue regular press releases to name and shame organisations that have poor SAR compliance – for instance, an annual list of organisations receiving the most complaints.