| Police Scotland logo | Freedom of Information Response Our reference: FOI 23-0597  Responded to: 27 March 2023 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

## 7. What percentage of your data is stored: (scaling percentage 0%, 0-10%, 10-25%, 25-50%, 50-75%, 75-100%, NA) a) On-premise b) Private Cloud c) Public Cloud

## 8. What percentage of your data is stored: (scaling percentage 0%, 0-10%, 10-25%, 25-50%, 50-75%, 75-100%, NA) a) With UK providers b) With USA providers c) With European providers d) Other

## 19. Do you outsource your open data service? (select all that apply) a) We outsource our open data service b) We use data.gov.uk c) We use a local company to host the data d) We use internal software

In response to the three questions above, in terms of Section 16 of the Freedom of Information (Scotland) Act 2002, I am refusing to provide you with the information sought. Section 16 requires Police Scotland when refusing to provide such information because it is exempt, to provide you with a notice which:

(a) states that it holds the information,

(b) states that it is claiming an exemption,

(c) specifies the exemption in question and

(d) states, if that would not be otherwise apparent, why the exemption applies.

The exemptions that I consider to be applicable to the information requested by you are:

Section 31(1) – National Security and Defence

Section 35(1)(a)&(b) – Law Enforcement

Section 39(1) – Health, safety and the environment

Section 31(1) – National Security and Defence

Information is exempt information if it is required for purpose of safeguarding national security.

Disclosure of this information could undermine any ongoing or future operations to protect the security or infrastructure of the United Kingdom and increase the risk of harm to the public.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

This is a non-absolute exemption and requires the application of the Public Interest Test.

Section 35(1)(a)&(b) – Law Enforcement

If the information was disclosed it could assist groups, organisations and those with hostile intent to identify, with some accuracy, Police Scotland’s technological capabilities and take steps to attack or hijack known vulnerabilities to Police systems directly or the supply chain. To provide the requested data could assist those with intent on doing harm with a tactical advantage when planning or perpetrating criminal plans and unlawful activities and maximise the impact of destruction, harm and disruption that may be caused.

Disclosure could have a negative effect on national security should the release of information be used and manipulated by criminal fraternities to try and attack politicians, public figures and other protected establishments and individuals.

Information is exempt information if its disclosure under this Act would, or would be likely to prejudice substantially the prevention or detection of crime and the apprehension or prosecution of offenders.

This is a non-absolute exemption and requires the application of the Public Interest Test.

Section 39(1) – Health, safety and the environment

The disclosure of the information requested may have the potential to increase the number of attacks on public figures, operational police officers and members of the public and the potential to present a risk to an individual’s personal safety.

Public Interest Test

I would suggest that public accountability may favour disclosure, given that the information concerns the efficient and effective use of resources by the Service. Likewise, disclosure of the information would also inform the public debate on the issue of policing and contribute to the accuracy of that debate.

However, any disclosure under FOI legislation is a disclosure to the world at large and any information identifying the focus of policing activity could be used to the advantage of criminals.

Consequently, in terms of the applicability of the exemptions listed above, the need to ensure the effective conduct of the service in relation to prevention and detection of crime and the public safety considerations involved in the delivery of operational policing clearly favour non-disclosure of the information requested.

It is important to note that the UK faces a serious and sustained threat from violent extremists and this threat is greater in scale and ambition than any terrorist threats in the past. The police service has a duty to promote the safety of all individuals, whether protected or not, and will not reveal any information that might jeopardise this goal. To provide details of resources allocated to their protection is likely to place individuals at serious and increased risk.

Accordingly, I would argue that the need to ensure the efficient and effective conduct of the service favours non-disclosure of the information requested and on balance is significantly in the public interest. I cannot identify any corresponding viewpoint in disclosing the requested information and therefore the exemptions are upheld.

I must advise you that it is doubtful it could ever be in the public interest to disclose information which would jeopardise the delivery of policing and the safety of individuals and prejudice the prevention or detection of crime.

## 9. Post brexit will your organisation store more data in the UK or less data in the UK? (select one) a) More b) No change c) Less

In response to this question, I must respond in terms of Section 17 of the Act, I can confirm that the information you seek is not held by Police Scotland.

By way of explanation, this information is not recorded.

## 1. Do you have a policy/strategy on how you use your data? (Outside of data protection and data privacy covered under general legislation)

## (select one) a) We have no strategy around data b) Our data strategy is covered by the IT strategy c) Our data strategy is an essential part of our IT strategy and clearly supporting our organization’s goals d) Our data strategy encompasses all of our departments and is aligned to our organization’s goals e) The data strategy is a key part of business model & company strategy f) Our data policy is covered by the trust or wider departmental organisation we belong to

## 2. (If yes) What considerations are included in your data policy/strategy? (scaled based on maturity - from Well established, Working on, No intent to include) Data sovereignty Data interoperability Data security Data skills Data availability Data ethics and responsibility Inter-departmental/agency collaboration Citizen outcomes / Tax payer value Data retention

## 3. Do you have a dedicated resource aligned to your data initiatives (excluding data protection)? (select one) a) There is no specific budget for data initiatives available b) Some data initiatives are covered by IT budgets c) Budgets for specific data initiatives are managed in the IT department with contributions from other departments d) There is a cross-departmental budget for our data strategy which is provided centrally e) The executive office decides on the data strategy for our whole organization, including strategic budget allocation

## 4. Do you have these roles within your organisation? (options - Yes, No, Partially, Plan to hire) a) Data analyst b) Data scientist c) Data engineer d) Machine Learning engineer

## 5. Do you outsource these roles? (options - Yes, No, Partially, Plan to outsource) a) Data analyst b) Data scientist c) Data engineer d) Machine Learning engineer

## 6. Who is responsible for setting your data strategy? (Understanding how senior the ownership is within the organisation)

## (select one) a) Level 1: CEO b) Level 2: CDIO, CIO, CTO, CxO c) Level 3: Senior Manager (Director/VP) d) Level 4: Delegated to departmental/line managers without organization-wide responsibility e) Level 5: Implicit throughout the organization

## 10. When developing your data storage strategies what are your main considerations? (Scale on importance) a) Data sovereignty b) Data gravity c) Data security d) Storage latency

## 11. What is the maximum period you would hold data for? (If there are varying period for different types of data, please provide more information)

## 12. What is the process for identifying obsolete data in your organisation?

## 13. How mature is your architecture in managing your data end-to-end, from ingestion / generation to final consumption? (\*\*Need a descriptor to define mature)

## (select one) a) Our data is only available in the respective application b) We capture and share data from multiple applications through data warehouses c) A central data lake holds all of our data at rest d) A central data hub connects data producers and consumers for both analytics and operational use cases, and holds both real-time data and data at rest

## e) We have a central data hub which also includes external data sources f) We put everything into a data lake and then classify into data warehouses

## 14. At what level does data add value to your organisation? (select one) a) Application b) Team c) Departmental d) Organisational e) Cross-organisational

## 15. What level of analytics methodologies do you master and support? (two boxed answer – currently use, currently master) a) Spreadsheet-based analytics b) Business intelligence/canned reporting c) Statistical analytics and machine/deep learning on big data at rest d) Statistical analytics and machine/deep learning with real-time data

## 

## 16. How far does your analytics architecture span across your organization? (select one) a) Our analytics remains local and/or within application boundaries b) Our analytics use cases can include data from multiple applications c) Our analytics use cases can consume data sources from all relevant applications d) In addition to consuming data sources from all relevant applications, our analytics use cases also consume real-time data

## e) Our analytics use cases consume data from data warehouses/data lakes, f) In addition to consuming real-time data, our analytics use cases also leverage external data

## 17. What are the biggest obstacles in your organization to creating value from data and implementing a data-centric strategy?

## (select all that apply)

## Our top management does not see data value creation as a strategic priority

## b) There are cultural barriers to adopting a data-centric approach c) We don’t have enough budget d) We don’t have the required skills e) There is no clear accountability for data strategy, governance and processes f) We don’t have access to the required technologies, tools and platforms g) We struggle to access external data in an efficient and trustful way h) Regulatory uncertainties with regards to data ownership and data privacy i) We don’t have enough data j) Our data quality is too low k) Our data is buried in silos l) We have no operating model for managing AI solutions in production

## 18. Do you have a policy for open data or transparency data (select one)

## a) Only an open data strategy b) Only a transparency data policy c) Both d) Neither - do not have any e) Under an existing IT or data strategy e) In the implementation process or drawing up a strategy

## 19. Do you outsource your open data service? (select all that apply) a) We outsource our open data service b) We use data.gov.uk c) We use a local company to host the data d) We use internal software

## 22. Do you have definitive protocols for managing your data in terms of… (select all that apply) a) Lineage b) Provenance c) Heritage d) Not sure

In response to the other questions above, I can advise that Police Scotland has an explicitly defined Data Strategy at a corporate level, and hence covers all use of data and information covering structured data, unstructured electronic, and hard copy data.

The data strategy recognises that data is an organisational asset, and must be managed as such, and also highlights the role that data plays in keeping people safe, preventing and detecting crime, keeping officers safe, enabling partnerships, maintaining a sustainable organisation, and also ensuring legislative compliance.

The data strategy covers the entire data lifecycle, from planning what data is important, to acquiring data, to storing and sharing data, to using data, and finally retiring data. Focus has been on establishing core foundational data capabilities that enable us to manage data through that entire data lifecycle, and hence covers capabilities such as data governance (e.g. data ownership, data quality, data standards, metadata, data lineage), information assurance (e.g. data protection, information sharing, records management and information security), master data management, analytics, data literacy, and data ethics. Future areas of focus will include an open data strategy.

Police Scotland have an established Chief Data Office (CDO), led by our Chief Data Officer. The CDO function is responsible for maximising the value of data for Police Scotland, and defines relevant data policies, standard, procedures to ensure the integrity and availability of our data across the entire data lifecycle.

The Data Strategy is owned and lead by the Chief Data Officer, and the CDO function.

There are a number of core data roles across Police Scotland, both in the CDO function and wider. These include industry standard roles such as Data Governance analysts, Information Compliance Officers, Information Security Officers, Record Management Officer, Data Ethics analysts, Data analysts, Data Scientists, and Data Engineers.

Like many Police Forces, and public sector organisations, Police Scotland has a complex data landscape, with is predominantly stored on premise, whilst ensuring that our data meets legislative compliance with Data Protection laws and security obligations.

Ensuring that Police Scotland comply with records retention legal obligations is an organisational priority. Therefore, we have Records Management operational procedures which specify the retention periods for various different record types. Each retention period, for each record type, is driven by a combination of legal and operational requirements. Operational processes exists to identify and retire records which have reached the end of their specific retention period. This includes a combination of automated and manual processes.

Like most organisations, Police Scotland have a wide range of operational systems. Therefore, we have a number of technology solutions which ensure that data from disparate operational systems are harmonised for wider corporate analytical consumption, including data lakes, data warehousing, data virtualisation, and tactical operational analytical solutions. Similarly, we have a number of end-user reporting solutions ranging from standard office tools, to modern Business Intelligence visualisation tools, to statistical solutions.

If you require any further assistance please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by [email](mailto:foi@scotland.police.uk) or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by [email](mailto:enquiries@itspublicknowledge.info) or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.