# THE CHIEF CONSTABLE OF CLEVELAND

## Subject Access Requests

Internal audit report 3.20/21

Final

29 July 2020

# 1. EXECUTIVE SUMMARY

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit / assignment and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely. Based on the information provided by you, we have been able to sample test the control framework.

## Why we completed this audit

A review of Subject Access Requests (SARs) was undertaken as part of the approved internal audit plan for 2020/21. Our review was undertaken to ensure SARs have been processed in a timely manner by the Force and in accordance with Article 15 of the General Data Protection Regulation (GDPR).

Individuals have a right of access to their personal information held by organisations relating to them to help them understand how and why organisations are using their data and that they are doing so lawfully. The powers contained within Article 15 gives individuals the right to request a copy of any of their personal data which are being processed by data controllers. These requests are known as SARs. Following receipt of a SAR an organisation has one calendar month to respond. Failure to comply with these statutory deadlines can lead to fines and sanctions being imposed from the Information Commissioners Officer (ICO).

SARs for the Force are managed by the Information Management Department. The department is led by the Head of Information Management who is also the Force's allocated Data Protection Officer (DPO). The day-to-day receipting and management of SARs is handled by the Information Rights Officer who is supported by an Information Rights Apprentice.

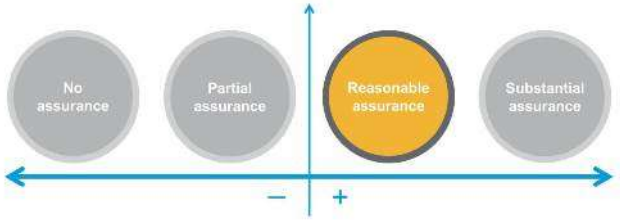
For the 2019 / 2020 financial year, the Force received a total of 354 SARs. Of the 354 requests, 52 (15 per cent) were submitted by either current or ex-staff members of the Force. As part of this review, a sample of 35 SARs have been selected and reviewed from the 2019 / 2020 financial year to ensure the requests have been processed in line with statutory guidelines and ICO guidance. Six of the requests selected as part of the audit sample related to existing staff members within the Force, two requests related to ex-staff members and the remaining 27 were external requests.

## Conclusion

There is an appropriate control framework in place for governing subject access requests. Our work confirmed that there are adequately designed controls in place, however, testing identified that the controls are not always consistently applied. From the sample of 35 SARs reviewed, 29 instances were noted where the requests had been processes within one calendar month. However, six instances were noted where requests had been processed and information disclosed outside of the set one calendar month period. Areas of improvements have been noted which has resulted in the agreement of **one high and four medium** priority management actions.

**Internal audit opinion:**

Taking account of the issues identified, the Chief Constable of Cleveland can take **reasonable assurance** that the controls in place to manage this area are suitably designed and consistently applied. However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk.




## Key findings

**We identified the following exceptions with the Force's established control framework resulting in one high and four medium priority actions:**

Through review of the Force's SAR Procedure it was noted that the document does not currently contain guidance around all the key processes involved within the SAR process such as response periods, extensions, complaints and conflicts of interest. It was also noted that the procedure does not contain a last review date and therefore it was not possible to confirm the procedure had been subject to regular review and approval. If the Force's SAR Procedure does not cover all key aspects of the SAR process and is not subject to regular review and approval, there is a risk that the Procedure may not be fit for purpose and reflective of current working practices. **(High)**

The Information Rights Officer who currently manages SARs joined the Force in September 2018. The officer was due to attend a Data Protection Intermediate Level Training Course delivered by the NPCC in March 2020. However, the course was cancelled due to the impacts of Covid-19 and is currently being rescheduled. If regular data protection training is not provided to individuals involved within the SAR process, there is a risk that staff members may not possess the necessary skills and knowledge to complete requests in line with statutory guidelines. **(Medium)**

Through testing a sample of 35 SARs it was noted that six of the requests reviewed were in relation to existing staff members within the Force. Through review of supporting documentation for the six requests it was noted that three of these were in relation to information regarding staff sickness and performance issues. Due to the nature of these requests, it was noted that the information required should be readily available to the relevant staff members and not have to be obtained through the SAR process. If existing staff members within the Force are submitting SARs for information which should be readily available to them, there is a risk of the Information Management Department receiving large amounts of inappropriate SARs, resulting in inefficient practices. **(Medium)**

A sample of 35 SARs were selected and tested. Six instances were identified where requests had been processed and information disclosed outside of the set one calendar month period. We confirmed that the Force had not applied any extensions to the six requests. One of the instances related to a total processing period of 118 days and a further instance was also noted which amounted to 74 days. If SARs are not processed within one calendar month, or extensions applied where appropriate, there is a risk that the Force may be in breach of GDPR statutory guidelines. **(Medium)**

Through review of agenda documents for all Information Security Board (ISB) meetings held in the current financial year, we confirmed that 'GDPR' is a standing agenda item for each meeting. However, it was noted that monitoring or compliance statistics in relation to SARs are not currently reported to the Board. As a result, the Board are not currently made aware of any SAR exceptions which have surpassed their set disclosure deadlines. There is a risk that staff in senior position are unaware of issues with compliance resulting in a lack of oversight of issues, which could result in potential for ICO investigation. **(Medium)**

**Our audit review identified that the following controls are suitably designed, consistently applied and are operating effectively:**

Roles and responsibilities regarding the receipt and actioning of SARs have been clearly defined and documented. The Information Management Department is currently undergoing a restructure (this was placed on hold due to Covid-19). As part of the restructure, officers within the department are to be trained on actioning SARs and Freedom of Information Requests (FOIs). Therefore, once training has been completed there will be three members of staff in place who will be able to action both SARs and FOIs.

The Force has a data retention schedule in place which details the duration for which SAR supporting documentation should be maintained such as ID verification.

All SAR related documentation is currently documented and stored within a local shared drive. The Force is currently in the process of implementing a dedicated case management system for SARs which will allow for centralised data management and efficient resolution of cases. The dedicated system will allow for easier management of new, on-going and archived cases as well as functionality for data analysis and reporting.

Appropriate ID checks are completed in line with ICO guidance by the Force for all SARs. Where a request has been made by a third-party, the Force will obtain evidence to verify that the requestor has relevant authority to act on behalf of the subject.

Any documentation which is disclosed as part of a SAR which contains information outside of the scope of the original request or which does not directly relate to the requestor is redacted prior to being disclosed.

The Force will refuse any SARs which are manifestly unfounded or deemed excessive. Where a SAR is denied, the requestor is notified within one calendar month of receiving the original request along with the following information:

- Why the Force believes the request is manifestly unfounded or excessive;
- That the requestor has the right to escalate the issue to the ICO; and
- That the requestor is entitled to seek to enforce the right of access via the courts.

The Force does not currently charge any fees for dealing with SARs. Should a request be deemed manifestly unfounded or excessive then the request is rejected. As per ICO guidance, the Force is not required to charge a fee in such circumstances and reserves the right to simply refuse such requests.

The Information Rights Officer compiles and records SAR compliance statistics on a monthly basis. The statistics include any open and closed requests as well as any requests which have surpassed their set disclosure deadline. The compliance statistics are sent to the Central Records Unit at the National Police Chief's Council (NPCC) on a monthly basis who subsequently report the figures to the ICO.

# 2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

| **Risk: SR22 – Failure to meet compliance with the UK Data Protection Bill** | | | |
|---|---|---|---|
| **Control** | The Force has a SAR Procedure in place which documents the process for obtaining documentation to fulfil a SAR. The Procedure covers electronic systems, e-mails as well as manual files as part of the Force's search criteria. The procedure is subject to regular review and is located on the Force's local intranet. The Force has letter templates in place for correspondence with requestors. | **Assessment:** | |
| | | **Design** | ✓ |
| | | **Compliance** | × |
| **Findings / Implications** | The Force's SAR Procedure was obtained and reviewed. The procedure is located on the Force's local intranet and is easily accessible by relevant staff members within the Information Management Department.<br><br>The procedure was found to contain the following key information regarding the actioning of SARs:<br>• Encryption process for data disks;<br>• Manifestly unfounded request letter template;<br>• Guidance letter to request ID;<br>• Fingerprint request process;<br>• Master opening process;<br>• CCTV disclosure process; and<br>• Photograph disclosure process.<br><br>However, it was noted that the procedure is not comprehensive and does not include key SAR process information such as:<br>• Verbal requests;<br>• Third-party requests;<br>• Response periods;<br>• Extension periods;<br>• Excessive requests;<br>• Appeals and complaints. | | |

| Risk: SR22 – Failure to meet compliance with the UK Data Protection Bill | | | | |
|---|---|---|---|---|
| | Additionally, the procedure does not currently provide any guidance regarding conflict of interests which may arise for the Data Protection Officer when exercising their statutory duties. Instances of such conflicts include where a SAR relates to the DPO and a review request is received or a complaint which has resulted in ICO involvement. In these instances, the DPO would not be able to effectively carry out a second-tier review of the relevant SAR without a conflict of interest arising.<br><br>Where such a conflict of interest arises, it is recommended that the request is reviewed by the Data Controller and an appropriate course of action decided, which may involve outsourcing the request to an external party or a DPO from another force.<br><br>We also noted that the procedure does not contain a last review date and therefore it was not possible to confirm the procedure had been subject to regular review and maintained up to date.<br><br>If the Force's SAR Procedure does not cover all key aspects of the SAR process and is not subject to regular review, there is a risk that the Procedure may not be fit for purpose and reflective of current working practices. | | | |
| **Management Action 1** | A review will be undertaken of the Force's SAR Procedure to ensure coverage is in place for all key aspects of the SAR process including conflicts of interest. | **Responsible Owner:**<br>Head of Information Management / Data Protection Officer | **Date:**<br>31 August 2020 | **Priority:**<br>High |

| Risk: SR22 – Failure to meet compliance with the UK Data Protection Bill | | | |
|---|---|---|---|
| **Control** | Staff members involved within the SAR process have been provided with appropriate training to ensure requests are dealt with effectively and in line with legislative guidelines. | **Assessment:** | |
| | | **Design** | ✓ |
| | | **Compliance** | × |

| | | | | |
|---|---|---|---|---|
| **Findings / Implications** | Through discussions with the Head of Information Management we confirmed that the Force does not currently have any in-house data protection training provision in place for Information Rights Officers who deal with SARs. Data protection training is currently provided via external training providers.<br><br>The Information Rights Officer who currently manages SARs joined the Force in September 2018. The Officer was due to attend a Data Protection Intermediate Level Training Course delivered by the NPCC in March 2020. However, the course was cancelled due to the impacts of Covid-19 and is currently being rescheduled.<br><br>The DPO is currently acting as a single point of contact for any queries from the Information Rights Officer in regard to SARs and therefore it is imperative that sufficient training provisions are in place to avoid any processing delays in the DPO's absence.<br><br>If regular data protection training is not provided to individuals involved within the SAR process, there is a risk that staff members may not possess the necessary skills and knowledge to complete requests in line with statutory guidelines. | | | |
| **Management Action 2** | The NPCC Data Protection Training Course will be rescheduled and attended by the Information Rights Officer. | **Responsible Owner:**<br>Head of Information Management / Data Protection Officer | **Date:**<br>31 December 2020 | **Priority:**<br>Medium |

| **Risk: SR22 – Failure to meet compliance with the UK Data Protection Bill** | | | |
|---|---|---|---|
| **Control** | The Force's website contains a dedicated section which details the procedure and various channels in place for individuals to submit a SAR. A SAR Form is in place which must be completed by the requestor in order for a request to be processed. | **Assessment:** | |
| | | **Design** | ✓ |
| | | **Compliance** | × |
| **Findings / Implications** | A sample of 35 SARs (10 per cent of the total population for the 2019/20 financial year) were selected and tested.<br><br>Six of the SARs reviewed were in relation to existing staff members within the Force. Through review of supporting documentation for the six requests it was noted that three of these were in relation to information regarding staff sickness and performance issues. Due to the nature of these requests, it was noted that the information required should be readily available to the relevant staff members and not have to be obtained through the SAR process.<br><br>If existing staff members within the Force are submitting SARs for information which should be readily available to them, there is a risk of the Information Management Department receiving large amounts of inappropriate SARs, subsequently resulting in inefficient practices. | | |

| | | | | |
|---|---|---|---|---|
| **Management Action 3** | The Force will carry out an analysis regarding the number of SARs received from existing staff members to identify any trends. Following this analysis, the Force will implement an action plan to remodel existing processes in place to improve transparency and subsequently reduce the number of requests from existing staff members. | **Responsible Owner:**<br>Strategic HR Manager | **Date:**<br>31 December 2020 | **Priority:**<br>Medium |

| **Risk: SR22 – Failure to meet compliance with the UK Data Protection Bill** | | | |
|---|---|---|---|
| **Control** | The Force completes all SARs within one calendar month from the day they receive the original request. Requested information is disclosed with an accompanying disclosure letter.<br><br>Where a SAR is complex or contains multiple requests, the Force will apply an extension of up to an additional two calendar months. Where an extension is applicable, the original requestor will be notified within 30 days from the point the original request was made. | **Assessment:**<br><br>**Design**<br>**Compliance** | <br><br>✓<br>× |
| **Findings / Implications** | A sample of 35 SARs (10 per cent of the total population for the 2019/20 financial year) were selected and tested. We confirmed the following:<br><br>• In 34 instances it was confirmed that the Force had issued a disclosure letter to requestors with the relevant accompanying information upon completion of the requests.<br>• One instance was noted where a request was refused, and it was confirmed that the requestor was issued a refusal letter within one calendar month of the request being made.<br>• 29 instances were noted where requests had been processed within one calendar month of the original request date or from the point ID or additional required information was provided.<br>• However, six instances were noted where requests had been processed and information disclosed outside of the set one calendar month period. We confirmed that the Force had not applied any extensions to the six requests. One of the instances related to a total processing period of 118 days and a further instance was also noted which amounted to 74 days.<br><br>If SARs are not processed within one calendar month, or extensions applied where appropriate, there is a risk that the Force may be in breach of GDPR statutory guidelines. | | |

| | | | | |
|---|---|---|---|---|
| **Management Action 4** | Closer monitoring of SARs will be undertaken to ensure they are being processed in a timely manner and in line with statutory guidelines. | **Responsible Owner:**<br>Head of Information Management / Data Protection Officer | **Date:**<br>31 August 2020 | **Priority:**<br>Medium |

| Risk: SR22 – Failure to meet compliance with the UK Data Protection Bill | | | | |
|---|---|---|---|---|
| **Control** | Missing Control - Compliance statistics relating to SARs are periodically reported to the ISB. | **Assessment:** | | |
| | | **Design** | × | |
| | | **Compliance** | - | |
| **Findings / Implications** | Through review of agenda documents for all ISB meetings held in the current financial year, we confirmed that 'GDPR' is a standing agenda item for each meeting. The meetings are not currently minuted however a running action log is in place which is reviewed and updated after each meeting.<br><br>Through discussions with the Head of Information Management we confirmed that SARs are covered on an ad-hoc basis within the 'GDPR' section of the meetings, and any on-going complex requests are discussed.<br><br>However, it was noted that monitoring or compliance statistics in relation to SARs are not currently reported to the Board. As a result, the Board are not currently made aware of any SAR exceptions which have surpassed their set disclosure deadlines. Between January and June 2020, the Force has received a total of 164 SARs, 151 (92 per cent) of the requests were processed and completed within the set one calendar month deadline. Nine requests (five per cent) were closed after the set one calendar month deadline and had therefore surpassed the SAR statutory time limit as an extension had not been applied. The remaining four requests (three per cent) were still on-going at the time of audit, of which three have had an extension applied and one being currently overdue.<br><br>Additionally, it is recommended that due to the high number of SARs received from existing staff members within the Force, an analysis is conducted on the effects on workload for the Information Management Department. The results of this analysis should subsequently be reported to the ISB.<br><br>There is a risk that staff in senior position are unaware of issues with compliance resulting in lack of oversight of issues, which could carry potential for ICO investigation. | | | |
| **Management Action 5** | Compliance statistics relating to SARs will be periodically reported to the ISB.<br>Additionally, an analysis will be undertaken regarding the number of SARs received from existing staff members and the resulting effects on workload. Results of this analysis will be reported to the ISB. | **Responsible Owner:**<br>Head of Information Management / Data Protection Officer | **Date:**<br>31 August 2020 | **Priority:**<br>Medium |

# APPENDIX A: CATEGORISATION OF FINDINGS

| Categorisation of internal audit findings | |
|---|---|
| **Priority** | **Definition** |
| Low | There is scope for enhancing control or improving efficiency and quality. |
| Medium | Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media. |
| High | Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines. |

The following table highlights the number and categories of management actions made as a result of this audit.

| Risk | Control design not effective* | | Non Compliance with controls* | | Agreed management actions | | |
|---|---|---|---|---|---|---|---|
| | | | | | Low | Medium | High |
| SR22 – Failure to meet compliance with the UK Data Protection Bill | 1 | (12) | 4 | (12) | 0 | 4 | 1 |
| **Total** | | | | | **0** | **4** | **1** |

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

# APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

## Scope of the review

The internal audit assignment has been scoped to provide assurance on how the Chief Constable of Cleveland manages the following risk:

| Objective of the area under review | Risks relevant to the scope of the review | Source |
|---|---|---|
| To ensure subject access requests have been processed in a timely manner and in accordance with article 15 of GDPR. | SR22 – Failure to meet compliance with the UK Data Protection Bill | Risk Register |

## Scope of the review

When planning the audit, the following areas for consideration and limitations were agreed:

**Areas for consideration:**

Under article 15 of GDPR an individual has the right to obtain from a data controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. As such our review will consider the following areas:

- Policies and procedures are in place, reflecting current operating practices.
- Subject access requests have been acted upon within at least 30 days of receipt.
- Appropriate ID - and authority where making the request on behalf of another - has been provided by the individual making the request.
- Refusal of requests are appropriate and clearly communicated to the individual.
- When requests are manifestly unfounded or excessive a reasonable charge for the administrative costs of complying with the request has been applied.
- Extension of time to respond to requests are justified due to the complexity or a number of requests have been received from the individual. We will confirm that the individual has been made aware of the extension within one month of receiving the request.

- Applications on behalf of any other person (third party) are supported by an authorisation letter and proof of identification documents.
- The reporting of compliance statistics within the organisation, and action plans put in place to address underperformance where applicable.

Our testing will focus on requests made by external stakeholders and employed (internal) staff.

**The following limitations apply to the scope of our work:**

- This review will focus on subject access requests only.
- Testing will be undertaken on a sample basis, so we will not confirm all subject access requests have been processed appropriately.
- Our review will not guarantee the outcome of a review undertaken by the ICO.
- We will not review the actions put in place to improve performance but only confirm performance is reported through the organisation's governance structure.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

| | |
|---|---|
| **Debrief held** | 8 July 2020 |
| **Draft report issued** | 24 July 2020 |
| **Revised Draft report issued** | 29 July 2020 |
| **Responses received** | 29 July 2020 |
| **Final report issued** | 29 July 2020 |

| | |
|---|---|
| **Internal audit Contacts** | Dan Harris, Head of Internal Audit |
| | Angela Ward, Senior Manager |
| | Philip Church, Client Manager |
| | Kishan Patel, Lead Auditor |
| **Client sponsor** | Chief Finance Officer – Chief Constable |
| | Head of Information Management / Data Protection Officer |
| **Distribution** | Chief Finance Officer – Chief Constable |
| | Head of Information Management / Data Protection Officer |

**rsmuk.com**

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **The Chief Constable of Cleveland**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.