South West Region - Draft Rights of Access consultation points

- **Page 17 – (Extending a request)** Talks in detail about the circumstances in which we can extend requests by a further two months, however this is restricted to processing under GDPR, not the DPA'18, where there is no such extension for law enforcement processing. Whilst the ICO can only provide guidance on current legislation, and there is work ongoing with the home office, this point should still be highlighted in the guidance.

- **Page 18 – (Complex requests)** *'Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual has requested a large amount of information'.* For the police service, the fact that there is a large volume of data ***is*** a contributing factor due to the amount of third party data, contained within. Many of the documents / emails / systems, which contain the data subjects personal data are littered / intertwined with a plethora of third party data, which has to be reviewed. This is a complex process where each line has to be carefully perused to ensure that the data controller has regard for:

  - the type of information that would be disclosed, e.g. warning markers and flag from Police National Computer
  - any duty of confidentiality owed to the other individual,
  - any steps taken by the controller with a view to seeking the consent of the other individual,
  - whether the other individual is capable of giving consent, and
  - any express refusal of consent by the other individual.

- All South West Region forces will have examples of SAR's taking several days to complete due to their **volume and complexity**. There has to be a cut-off point otherwise, we are looking at an undefined time period, which, if followed to its natural conclusion could take years to complete.

- **Page 19 (can we charge a fee?)** - Whilst we can charge for postage the ICO needs to be more explicit on the circumstances in which the data controller can decline posting; for example, other secure data transfer (Egress) is available, or the Data Subject can attend a local office or location agreeable to both parties.

- **Page 22 – (how we should deal with bulk requests)** Whilst we are purpose blind we are often explicitly told why the request is being made; particularly when it is received via a solicitor in order to defend a claim, or the data subject states 'I need it for court next week'. Whilst we appreciate that there is no such term as an 'abuse of process' the ICO needs to be more explicit in what type of requests could be considered as 'unlawful' Rights of Access. The guiding principle of this 'right' is to allow the data subject to ensure that their personal data is being processed lawfully; for example that it is accurate, up to data, and is not being processed for longer than is necessary. It is our position that this right should not be used as a way of circumventing other recognised disclosure routes. Wiltshire Police give the example where they were recently criticised by an Employment Tribunal Judge who commented that pre-disclosure, via the RoA route was unhelpful, as it muddied the water when considered against the actual formal disclosure received via the correct route. As the ICO is aware, the RoA is to one's own personal data, it does not extend to the provision of documents per se, therefore disclosures made under the RoA sometime appear disjointed and out of context. Additionally, the RoA does not routinely disclose third party data, which

many applicants are requiring. Over the past few years and particularly post May 2018, forces in the South West Region have seen a rise in RoA requests. Many of these request are for civil litigation, whether this is for personal injury, neighbourhood disputes or disclosure to the family law court. The latter is actively encouraged when connected to private law hearings despite our representation that this will only provide a one sided view of the facts.

- **Page 23 (What efforts should we make to find information?)** – Wiltshire police have conducted research to indentify any bespoke redaction software, which does not involve human intervention, without success. All of the redactions of documents / extraction of personal data in the police service is completed by hand as mentioned in the page 18 comment above. We will reiterate the point again that many of the documents 'in scope' are littered with third party data, police tactics, as well as preserving the integrity of ongoing investigations. All of these actions have to be conducted verbally with the officers involved in the case. Additionally disclosure officers have to manually assess what information is already known to the data subject; this can take several hours.

- **Page 23** – (**Can we clarify the request?)** The guidance suggests that we are still obliged to respond to the applicant within one calendar month, even if we do not receive confirmation of the information requested, or the processing activities their request relates to. Whilst there is the option to extend the time limit by two months if the request is complex, this does not extend to Law Enforcement processing. Could the guidance clarify what Law enforcement organisations should do in such scenarios? Could the guidance clarify what organisations should do if no clarification is received? The very reason confirmation is requested is to be able to respond.

- **Page 23 (narrowing the scope of their request)** - This approach, without any tangible ICO guidance is totally unmanageable, in a number of cases. For example, a prolific offender with hundreds of separate occurrences, combined with multiple Professional Standards complaints and years of internal / external email correspondence can and does take weeks to:

    - redact third party data
    - identity what is already known to the data subject
    - establish know tactical capabilities
    - avoid prejudicing ongoing investigations

The ICO needs to provide some parameters for organisations to work with. This guidance does not take into account the complexities of Law Enforcement data, which, by its very nature is quite often strewn with third party data; most of it not known to the data subject.

Page 30 – (In what format should we provide the information?) ***Data subjects are not required to perform an action as a requirement to receive disclosure.*** As a data controller, you are responsible for the security of personal data and should take all reasonable steps to ensure that it is protected from loss; therefore, it does not follow that the data subject should ***not*** have to take action to receive the information (e.g. by collecting it from our premises) unless they agree to do so. For example Wiltshire police send over 95% of their disclosures via secure data transfer; this requires the data subject to download a software application, which is an action. This guidance is suggesting that the data subject

can essentially refuse on more secure transfer methods and opt for unsecure postage. By following this guidance, organisations will be at odds with their security obligations.

Page 35 – (What does manifestly unfounded mean?)

In General – It is strongly argued that there should be a 'time taken' parameter / consideration applied to this exemption. As it stands an application could, and South West Region forces have numerous examples of, requests taking several days/weeks. This interpretation of the act is particularly concerning when coupled with the comments on page 23 vis-à-vis the fact that the requester is not obliged to narrow the search criteria.

These two sections were openly accepted as the perfect opportunity to address the perennial issue / interpretation of 'disproportionate effort' that organisations grappled with in the '98 act. The ICOs stance, quite rightly, was that 'disproportionate effort' was concerned with the communication of the personal data, not the status of the actual request per se. Therefore, data protection practitioners, in the police service were hopeful this guidance would finally address the problem of dealing with requests involving *very large* volumes of data.

By way of example, organisations such as the police service receive high volumes of requests whereby the applicant will ask for *all* of their personal data. Due to the nature of police processing an individual's personal data is often mixed in with other third party data, which has to be located / assessed / redacted; this can take disclosure officers several weeks / months, to process. It would be helpful if this guidance included some indication as to the lengths vis-à-vis, how long an organisation is expected to spend furnishing a request. To simply leave this issue 'hanging' is not helpful to practitioners.

Since the removal of the £10 charge the police service has seen a significant increase in requests relating to 'obvious' legal proceedings (including prospective legal proceedings), obtaining legal advice, or for the purposes of establishing, exercising or defending legal rights. All police forces will have had several cases whereby individuals will use the Right of Access process to pursue, reinvestigate complaints against the police service. This is despite a full independent investigation having already been completed by our complaints department. These type of disclosures usually involve the processing of hundreds of documents and a duplication of effort on already limited police resources.

I note that this guidance does not address the processing of personal data contained in CCTV or Body Worn Video footage. The personal data processed by such means, is, by its very nature, accurate and up to date, therefore how can this be regarded as a legitimate request under Data Protection legislation. Such requests, which we term an 'abuse of the process' cause delays in processing those 'legitimate' rights of access requests.

We wish t suggest that the ICO gives consideration to adding a forms of words such as:

'A request is likely to be excessive if there is another route to obtain the information and the Act is being used to circumvent that'.

This would allow individual forces and the ICO to determine if the Right of Access is being abused, and used as a way of furnishing disclosure where other, more appropriate, long established routes are available. Comments to page 22, articulate this point where Wiltshire

Police were criticised by an ET Judge for furnishing disclosure for Employment Tribunal purposes via the Right of Access route. Going forward this particular scenario would be viewed as targeting a particular employee (as below) against whom the applicant has some personal grudge.

Targeting an individual – A request may be manifestly unfounded if:

'the individual is targeting a particular employee against whom they have some personal grudge;'

This point needs to be articulated further as many requests received by the police service, particularly from internal members of staff are related to a grievance. This type of request is, by its very nature 'Targeting an individual'. Could this be clarified as the servicing of such requests normally involve the perusing of reams and reams of documents and emails.

The police service also receive several requests a month for Body Worn Video footage to use as evidence against an officer. This is not only an abuse of process as articulated above but also targeting an employee.