Information Commissioner's Opinion:

Who's Under Investigation?

The processing of victims' personal data in rape and serious sexual offence investigations

31 May 2022

Information Commissioner's Office

Foreword

This report reveals a distressing picture of how victims of rape and sexual assault feel treated by police and the legal system.

Victims are being told to consent to hand over extraordinary amounts of information about their lives, in the immediate aftermath of a life changing attack.

Victims are being asked to allow access to medical records, school reports, social service records and the contents of their mobile phones as a precondition to accessing justice.

Victims are being treated as suspects.

This is not about data protection or data processing. This is about people feeling revictimised by a system they are entitled to expect support from.

It is no surprise that growing evidence suggests these intrusive practices are contributing to victims withdrawing from the legal process and thereby the derisory conviction rates in relation to serious sexual offences. More than 80% of sexual offences are believed to go unreported to police. A 2019 study in London looked at 501 allegations of rape taken to police. Just 36 led to someone being charged. Only 14 ended in a conviction.

And we know too that this burden is not shared equally. Victims of rape are more likely to be female, more likely to have a disability and more likely to identify as gay, lesbian or bisexual.[1]

Change is required. We hope that this report contributes to the rebuilding of trust that will enable more victims to seek the justice to which they're entitled.

The changes we are recommending are supported across the criminal justice sector, and indeed we have seen positive steps already from the Attorney General's office[2]. And now those changes must happen. That is what the law requires. It is what my office will continue to push for. And it is what people affected by these crimes have a right to expect.

John Edwards
Information Commissioner

[1] rape-review-equality-statement.pdf (publishing.service.gov.uk)
[2] Attorney General's Guidelines on Disclosure - GOV.UK (www.gov.uk)

Contents

Executive summary

It is important that victims across all UK jurisdictions have trust and confidence in the way their personal information is handled throughout the criminal justice system. It is also crucial that the many other 'third party' organisations involved in it can do so confidently, proportionately and safely. For example local authorities, social services, education providers and medical professionals who need to use and share data with the police in England and Wales, Scotland and Northern Ireland. In publishing this Opinion, the Information Commissioner aims to assist police, the wider criminal justice system and other organisations to understand their roles and mutual obligations to use victims' personal information respectfully and in compliance with data protection laws. The Commissioner hopes that this, in turn, should contribute to improving the confidence of victims, as well as the efficiency and effectiveness of the criminal justice system in investigating and prosecuting rape and serious sexual offences (RASSO).

Focussing on the victims, the Commissioner recognises the significant trauma that can be associated with RASSO cases. This can be further amplified if victims' personal information is used in distressing ways after an incident, during an investigation or further into the criminal justice system. This information could include a full download of their mobile phone, a trawl through historic medical and psychiatric records or even information dating back to childhood.

The ICO welcomed the very important issues raised directly by London's Victims' Commissioner Claire Waxman, alongside a number of other key organisations in the public and voluntary sectors across the UK. They raised deep concerns to us about the police and the wider criminal justice system's reliance on statements for victims' consent and about excessive collection of victims' personal information (including sensitive information).

> "Vulnerable victims are being told that in order for their case to progress they have to essentially, sign away their rights to privacy. Victims who decline to grant access having their cases dropped at alarming rates, despite robust evidence which supports otherwise."
>
> **Claire Waxman – London's Victims' Commissioner**

As part of our investigations, we have consulted with public organisations across the UK such as:

- Police Scotland and Police Service of Northern Ireland;
- the Public Prosecution Service Northern Ireland and the Department of Justice; and
- the Crown Office and Procurator Fiscal Service.

In particular, we have consulted with the:

- Home Office (looking into disclosures to police by 'third party' organisations);
- the Ministry of Justice (assisting with the development of a revised Victims' Code of Practice[3]); and
- the Crown Prosecution Service (in developing guidance for pre-trial therapy providers).

This work pointed towards a lack of clarity in understanding the rules set out in data protection law which are required for sharing victims' information fairly and lawfully.

There is a growing body of research analysing very low charge rates for RASSO cases. This suggests that the criminal justice system is failing to foster the trust and confidence of victims necessary to sustain their involvement in the process. For example, the Home Affairs Committee inquiry into the investigation and prosecution of rape[4] was published on 12 April 2022. It explored the key question of why rape prosecutions are so low, at a time when the number of police-recorded rapes are high.

Separately, many RASSO victims express concerns about the level of intrusion into their private lives during police investigations. This reportedly accounts, at least in part, for their withdrawal from the investigatory process.

Example

Person A's historic medical and psychiatric records are accessed to help inform the investigative stage after a serious sexual assault is reported. As these records go back many years, Person A is concerned that it is excessive and everything about them would be scrutinised. They have been victim to a sexual assault, but because of the amount of information requested they now feel like they are being treated as a suspect.

In practice, police and prosecution services are collecting intimate personal information about victims of RASSO cases, not just from victims themselves but also from others, such as their doctors and counsellors. In some circumstances, they are making judgements about the case based on information that is often unconnected with the assault in question. Much of this information is highly sensitive and investigators must handle it with appropriate safeguards, as set out in data protection law. Fundamentally, victims must be given a greater voice in the process and have their rights protected.

[3] https://www.gov.uk/government/publications/the-code-of-practice-for-victims-of-crime
[4] https://committees.parliament.uk/publications/9600/documents/162463/default/

The demands for such intimate information from victims are a cause for concern and can fall into particular categories. These can range from:

- unnecessary and excessive requests;
- excessive interrogation of information; and
- simplistic interpretation of information without offering the victim a chance to provide an explanation about the information before any decisions are made.

Examples of such information collection could include:

A victim is required to sign a statement and provide the police with a full download of their mobile phone (including contacts, call logs, messages, location data and web history) and social media account going back several years. This is even when the person is a victim of a stranger attack, and had not met their assailant prior to the event.

A victim's educational records and qualifications are requested as part of an investigation. Further historic school records are then also required that suggested the victim had been caught lying as a teenager.

An investigation requires sensitive medical records that detail a victim's medical history. However, the requested medical records also go back to the birth date of the victim.

Where victims have access to counselling services to deal with trauma, notes are often recorded. During an investigation discussion notes are requested by the police and potentially disclosed further to the defendant during the criminal justice process. The counsellor and the victim are both unaware of the potential for such onward sharing.

While the investigator must decide what is necessary and relevant to their investigation, the Commissioner finds these examples excessive and a disincentive for victims. It can cause victims to feel re-victimised. It can cause them to withdraw from the criminal justice process meaning offenders are not held to account. In such cases it appears victims can are subjected to a far greater level of scrutiny of their personal information than the suspects. This raises further issues of excessive information collection and discrimination.

Example

Person B is reluctant to provide a digital device to investigators as it could include texts, emails, pictures and potentially deleted data. They are also concerned that the device contains information about their friends and family including sensitive conversations. Person B feels intimidated about the possibility

of this information being collected without having a voice in the process, or any explanation why this information is needed.

The ICO has continued to work in this area following adoption of data protection laws for criminal law enforcement in 2018. We are aware of first hand concerns about how personal information is handled in such cases, and the negative impact this can have on a person's rights and freedoms, when done badly. This report, the third by the ICO in this area, concludes our initial examination of law enforcement data processing during investigations.

We've heard from victims and groups working with them. We have also heard from practitioners at various levels of the criminal justice system about the challenges they face in managing such volumes of data. We have produced this Opinion in response to that and to help provide clarity about our expectations. This should provide greater certainty about how the ICO will uphold and enforce victims' rights in this area.

At its core, is the Commissioner's concern that:

- the current approach is undermining trust and confidence in the criminal justice system across the UK; and
- victims should not have to subject themselves to intrusive investigations and information collection and use practices as a result of reporting a crime which has been perpetrated upon them.

Victims may be more inclined to continue with the criminal justice process if there is no unnecessary intrusion into their private lives and those of friends and family, and less pressure to provide unlimited access to information such as phone or digital device data.

Example

Person C is informed by the police that a full download of their mobile phone is required with pictures and messages on it that date back years. Person C is reluctant to provide all of this historic information, but they are told that the prosecutor would not compromise on a narrower timescale and may drop the case if the information is not provided. Person C therefore feels unfairly compelled to provide the information in order to progress the case.

It is therefore necessary to properly consider the data protection principles, particularly the data minimisation principle, and how they apply to the collection of victim's information in RASSO cases. It is important that data protection law is not perceived as a barrier to sharing information, where it is necessary and proportionate to support victims, and to ensure a fair trial for those suspected of perpetrating serious crime. However, the victim needs to be placed at the centre of the process. This means the practices need to be designed so that victims can

easily understand them and have confidence that they know what their information rights are and that those are being respected.

The ICO has produced further guidance on sharing personal data with law enforcement authorities within its data sharing guidance hub. This provides helpful checklists, tools and case studies to make it easier for police and organisations to request and share personal information with confidence.

This Opinion builds upon the Commissioner's investigations into the extraction of data from mobile phones. This is as well as complaints we have received and the ongoing work by the relevant stakeholders to address the recommendations made in the subsequent reports. It extends the principles developed through that work and sets out a framework within which police investigators might lawfully and fairly obtain personal data relating to victims from:

- victims themselves;
- their electronic devices; and
- other organisations that may hold their data.

It is implicit that the Commissioner is concerned that aspects of individual investigations involving victims data fall short of the requirements of the DPA and UK GDPR, and are therefore unlawful. This Opinion makes the Commissioner's expectations clear. Therefore, it is likely that the ICO will take enforcement action about practices not reaching these standards in the future.

This Opinion acknowledges the complexity of this subject area and the difficult decisions that investigators and prosecutors need to make. They have to assess what material is required to ensure an accused person is able to have a fair trial, whilst also recognising the impact of unnecessary intrusion into the private life of the victim. The Commissioner is thankful for the assistance his teams have had from those directly involved in these issues, from all perspectives across England and Wales, Scotland and Northern Ireland.

Summary of recommendations

The Commissioner makes a number of recommendations that are intended to lead to a consistent environment in each of the UK's jurisdictions, within which individual organisations can feel confident that they are complying with data protection law, and uphold the rights and protections of victims and third parties.

Recommendation 1

The National Police Chiefs' Council must mandate to all police force/service(s) throughout the UK that they must cease using statements or forms indicating general consent to obtain third party materials (also

known as Stafford statements – England and Wales). Data protection is not a barrier to fair and lawful sharing and acquisition, but data minimisation is key. Any personal data obtained relating to a victim must be adequate, relevant, not excessive and pertinent to an investigation.

Recommendation 2

The Crown Prosecution Service, the Public Prosecution Service Northern Ireland and the Crown Office and Procurator Fiscal Service should ensure that their prosecutors are fully aware of this Commissioner's Opinion. They should be properly equipped to act according to the principles he promotes to uphold the rights and protections of victims.

Recommendation 3

The National Police Chiefs' Council should work with the College of Policing and the Crown Prosecution Service to produce advice and supporting forms for police force/service(s) to use across England and Wales when requesting personal information from third party organisations.

The Police Service of Northern Ireland and Police Scotland should also work with the Public Prosecution Service Northern Ireland and the Crown Office and Procurator Fiscal Service respectively to produce similar documentation.

The forms should be consistent with the principles established in this Commissioner's Opinion. They should:

- give clear advice to third parties who will be in receipt of such requests;
- make clear whether the requests are voluntary or mandatory:
- explain the reason for seeking the information: and
- explain that information sought might end up being disclosed to a defendant.

Recommendation 4

The Commissioner makes further recommendations directly to the Chief Constables of forces across the UK, to ensure they are able to fully demonstrate compliance with data protection legislation when processing information relating to victims of rape and serious sexual offences (RASSO).

Given the impact of investigators' interactions with the victims of RASSO

cases, Chief Constables should update policy, guidance, training and other documentation to make it consistent with this Opinion. We expect this to cover at least the following areas:

- the circumstances under which it might be appropriate to seek access to material from (i) a victim's electronic devices, or (ii) other third party organisations. How they can use that information, who they can disclose it to, and how they can secure it;
- the formulation and documentation of appropriate parameters around material they are seeking;
- the nature of the contact with the victim and the information they should provide to them;
- the information they should provide to the third party organisation whom they are requesting material from; and
- how to deal with cases where a request for information is declined by a third party.

Recommendation 5

Chief Constables across the UK must have in place appropriate policy, guidance and training for the ongoing management and retention of personal information relating to victims. This should ensure that they are managing and fully safeguarding information, whether they:

- obtain it directly from the victim;
- extract it from their devices; or
- acquire it from third parties.

This is in accordance with this Opinion, the UK GDPR and the DPA 2018.

Next steps

The Commissioner will continue to work with organisations across the UK jurisdictions to assist them in interpreting this Opinion and implementing its recommendations; in particular those recommendations relating to training, tools for practitioners and updating policies.

In considering any regulatory action or use of enforcement powers, the Commissioner may refer to this Opinion as a guide to the interpretation and application of the law. Each case will be fully assessed on the basis of its facts and relevant laws.

The Commissioner may also update or revise this Opinion based on any material legal or practical developments in this evolving area, such as judicial decisions and case law, or further findings from regulatory work and practical experience.

Compliance with the key principles of UK GDPR and DPA 2018 is fundamental for good data protection practice. Breaches of the law, including excessive collection of victim's information, can leave organisations open to regulatory action. Alongside the Commissioner's statutory duty to respond to complaints, he intends to address and prioritise complaints arising from victims experiences of the system as they arise, and may take other measures such as targeted audits and assessments of individual forces as circumstances require.

Organisations processing for law enforcement purposes must also be aware of their general duties under Section 44 DPA 2018. This includes making victims aware of:

- the existence of their right to complain to the Information Commissioner; and
- the contact details of the Commissioner.

The Commissioner will also highlight this Opinion to victim support groups across the UK jurisdictions, so that they can draw attention to any ongoing practices that are inconsistent with his recommendations.

1. Introduction

1.1 Background

It is difficult to contemplate the significant, potentially life-long, impacts felt by a victim[5] of a rape or serious sexual offence (RASSO). Yet the UK Government's response to the independent *End-to-End Rape Review*[6], published in June 2021, admitted that rape victims in England and Wales are "nearly always" failed by the criminal justice system.

There is no doubt that the investigation and prosecution of RASSO cases is a complex process. However, there are some deeply concerning statistics and apparent high levels of underreporting. The MOPAC London Rape Review 2019 examined 501 allegations and found in 58% of cases the victim/survivor withdrew the allegation. In a further 29% the police decided to take no further action. Only 60 were submitted to the CPS, 36 were charged, 23 proceeded to trial and 14 ended in either a guilty plea or verdict - an overall conviction rate in the sample of 3%. There has also been a subsequent MOPAC review in 2021[7] that found that the picture of reported rape in London has remained largely unchanged. Further, to highlight the important statistics across the UK jurisdictions, during 2019/20, just under 13% of rape cases reported in Scotland resulted in someone being proceeded against[8] and, over the same period in Northern Ireland, 5% of cases resulted in charge[9].

There are of course circumstances where victims do not even report to the police what happened. We can speculate that anecdotal experiences of the investigation process or the experiences of friends or family may contribute to non-reporting. The House of Commons Home Affairs Committee report into the investigation and prosecution of rape[10] published 12 April 2022, detailed statistics about people that chose not to come forward after an incident. This report included latest estimates from the Crime Survey for England and Wales (CSEW). In the year ending March 2020, an estimated 1.8% of adults aged 16 to 74 years (773,000) experienced sexual assault (including attempts). Statistics showed that fewer than one in six female victims and fewer than one in five male victims of sexual assault since the age of 16 reported it to the police.

---

[5] The term 'victim' is used in the Opinion to refer to a person reporting a crime against them. The Commissioner recognises and respects that others may refer to them as a 'complainant' or 'survivor'.

[6] https://www.gov.uk/government/publications/end-to-end-rape-review-report-on-findings-and-actions

[7] https://www.london.gov.uk/sites/default/files/final_rr_victimtech_61221.pdf

[8] From Scottish Government Recorded Crime and Criminal Proceedings statistics 2019-20

[9] From Police Service of Northern Ireland Recorded Crime Statistics

[10] https://committees.parliament.uk/publications/9600/documents/162463/default/

We can therefore make a conclusion from these statistics, that the real overall conviction rate for RASSO cases is likely to be a fraction of the 3% demonstrated in the sample reviews.

Criminal justice processes involve many different organisations. They all play their part in an effort to progress an efficient and effective investigation on behalf of the victim which results in a fair trial for the accused. The reasons for this ecosystem failing the victim may be varied, and certainly are unlikely to be caused by a single factor. In response to the End-to-End Rape Review, the UK Government has set out a multi-agency action plan that aims to introduce a number of improvements to outcomes for victims.

1.2 The need for change

There is a growing body of evidence to demonstrate the impact on victims when they feel their privacy has been intruded on unnecessarily.

The Victims' Commissioner for England and Wales[11] analysed data compiled by Rape Crisis England & Wales[12] in which RASSO victims were asked to identify the reasons for withdrawing their complaint. She found[13] that one in five victims withdrew complaints, at least in part, due to disclosure and privacy concerns. Victims in 21% of complaints had concerns about their digital material being downloaded and the disclosure of their GP, hospital, school and employment records, along with a combination of negative press coverage and victim experiences. We have heard of similar experiences.

In 2020, the Victims' Commissioner surveyed[14] victims of rape about their experiences of the criminal justice process. The results showed that, for many, scrutiny of their private lives was instrumental in their decision not to report, and those that did report the crime found the scrutiny really traumatic. Only 33% agreed that the police clearly explained why any request to access mobile phone and other personal data were necessary. 22% said that the police explained how they would ensure that data would only be accessed if relevant and necessary. Victims had serious concerns that requests for their data were often unduly intrusive.

The ICO has previously investigated the extraction of data from mobile phones by the police.[15] We found inconsistencies in how police force/service(s) justified

[11] https://victimscommissioner.org.uk
[12] https://rapecrisis.org.uk
[13] https://victimscommissioner.org.uk/news/the-reasons-why-victims-of-rape-and-sexual-violence-withdraw-from-the-criminal-process-without-seeking-justice/
[14] https://victimscommissioner.org.uk/published-reviews/rape-survivors-and-the-criminal-justice-system/
[15] https://ico.org.uk/about-the-ico/what-we-do/ico-investigation-into-mobile-phone-data-extraction-by-police-in-the-uk/

acquiring highly sensitive personal information from devices belonging to victims and others involved in criminal investigations.

There are suggestions from external reviews and those leading RASSO investigations that the Crown Prosecution Service (CPS)[16] may be driving the police to process excessive amounts of data. HM Crown Prosecution Service Inspectorate (HMCPSI)[17] conducted a thematic review of rape cases[18]. This followed the high-profile collapse of the prosecution in a number of cases due to disclosure issues[19]. The review revealed the CPS sometimes requires the police to provide all possible digital material and third party material before it will consider a charge in a rape case. It reported that around 40% of CPS requests were not proportionate. A common issue was found to be

> "not setting out proper parameters for an action to get information from the complainant's digital devices, and making requests for third-party material (such as education, medical or Social Services records) that were not necessary."[20]

The End-to-End Rape Review[21] revealed differing views for the reasons behind the increase in the amount of victims' data sought by the CPS. The survey underpinning the review revealed the perceptions by the police that CPS requests had become 'standard', with lines of enquiry being too broad and resembling 'fishing expeditions'. The CPS, however, defended its approach saying that prosecutors were simply subjecting cases to more rigorous review when making charging decisions.

The review also found that in many cases there was a disproportionate examination of the life of the victim that was not mirrored in the treatment of the suspect. Victims may be more inclined to continue with the criminal justice process if there is no unnecessary intrusion into their private lives and less pressure to provide unlimited access to phone or digital device data.

Further, the time taken to access digital and third party material has been seen to cause investigative delays. This is further impacting the likelihood of a satisfactory conclusion of cases.

Finally, many victims have been encouraged to sign a 'Stafford statement' (after TB, R (on the application of) v The Combined Court At Stafford [2006] EWHC

---

16 https://www.cps.gov.uk
17 https://www.justiceinspectorates.gov.uk/hmcpsi/
18 https://www.justiceinspectorates.gov.uk/hmcpsi/wp-content/uploads/sites/3/2019/12/Rape-inspection-2019-1.pdf
19 See for example https://www.cps.gov.uk/publication/joint-review-disclosure-process-case-r-v-allan
20 Para 5.50 HMCPSI report
21 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994817/rape-review-research-report.pdf

1645 (Admin)[22]). This gives police and prosecutors 'blanket' consent to access their confidential information held by third party organisations without further justification. This includes historic education records and sensitive medical records. The ICO understands that this was not the intended use of these statements, nor is such use considered by the Information Commissioner to be lawful.

As the UK-wide regulator of data protection legislation, the Information Commissioner is keen to ensure that:

- the police and other organisations processing personal data about victims are clear about their obligations; and
- criminal justice processes in all of the UK's jurisdictions are able to run efficiently.

1.3 Building upon previous work

This Opinion builds upon the foundations established through the ICO investigation into mobile phone extraction (MPE)[23] undertaken by law enforcement agencies to extract data from electronic communication devices during the course of a criminal investigation.

The report called for significant changes to the ways that the police and others involved in criminal justice processes consider their requirements for highly sensitive data from digital devices belonging to victims, witnesses and suspects.

There was widespread agreement that improvements were needed across the criminal justice system in the UK. This was in order to respect privacy and information rights whilst allowing thorough investigations and robust prosecutions to be conducted that respect the right to a fair trial. This has led to some significant changes to guidance from the Attorney General's Office[24], the College of Policing[25] and the National Police Chiefs' Council[26].

The work the ICO established through the MPE investigation continued following the publication of its reports in June 2020 (regarding England and Wales) and June 2021 (regarding Northern Ireland and Scotland). The ICO assisted a range of agencies and organisations in interpreting the findings and responding to the recommendations. These same agencies were considering how to respond to the findings of the external reviews and reports described earlier in this chapter. This is in addition to improving compliance with data protection principles when accessing victims' digital data from their phones. The ICO were encouraged by

[22] https://www.bailii.org/ew/cases/EWHC/Admin/2006/1645.html
[23] https://ico.org.uk/about-the-ico/what-we-do/ico-investigation-into-mobile-phone-data-extraction-by-police-in-the-uk/
[24] https://www.gov.uk/government/organisations/attorney-generals-office
[25] https://www.college.police.uk
[26] https://www.npcc.police.uk

the responses from agencies, and their commitment to improvement. However, improving compliance in this area is ongoing and will require continued ICO support and monitoring.

Whilst MPE and victims' data processing are distinct areas of interest, there is a clear connection from a data protection compliance perspective. A person is classed as a victim when a crime is reported to the police and their personal details are first recorded. The police begin an investigative process with the aim of bringing an offender to justice, and this involves processing further sensitive information. Just as with MPE, criminal justice and data protection legislation govern how the police may lawfully and fairly process sensitive information about victims. This covers information that originates from the victim themselves, their digital devices or from third party organisations.

1.4 The call for this Opinion

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA)[27] allow the Information Commissioner to issue, on his own initiative or on request, opinions to Parliament, government, other institutions or bodies, and the public. They can cover any issue related to the protection of personal data.

This Opinion has already highlighted a number of reports demonstrating the impact that privacy intrusion can have on victims of RASSO. The ICO has consulted with:

- Police Scotland and Police Service of Northern Ireland;
- the Public Prosecution Service Northern Ireland and the Department of Justice; and
- the Crown Office and Procurator Fiscal Service.

In particular, the:

- Home Office[28] (looking into disclosures to police by 'third party' organisations);
- Ministry of Justice[29] (assisting with the development of a revised Victims' Code of Practice[30]); and
- Crown Prosecution Service (in developing guidance for pre-trial therapy providers).

This work all pointed towards a lack of clarity in understanding the rules set out in data protection legislation which are required for sharing victims' information

[27] https://www.legislation.gov.uk/ukpga/2018/12/contents
[28] https://www.gov.uk/government/organisations/home-office
[29] https://www.gov.uk/government/organisations/ministry-of-justice
[30] https://www.gov.uk/government/publications/the-code-of-practice-for-victims-of-crime

fairly and lawfully. Further ICO work with victims' groups across the UK reinforced the negative impact this lack of understanding has on victims themselves and the need for more clarity and certainty. A victim may feel that a focus on their intimate private life after a traumatic experience is unfair, disproportionate or even as a re-victimisation.

This Opinion therefore focuses on the examination of RASSO victims' private information by police in the course of criminal investigations and proceedings. The ICO's previous work on MPE explained:

- the conditions that must apply for the processing of personal data from digital devices; and
- the need for such processing to be fair and lawful under data protection legislation.

This Opinion now extends these concepts to apply to the collection and use of data held by other 'third party' organisations.[31] This third party information is often originally held for purposes other than law enforcement, but is then requested by the police to assist with an investigation. This material may be stored digitally or held on paper.

The legislation sets out a framework that can be used to assist law enforcement and other practitioners in assessing the appropriateness of seeking access to, or disclosing, personal and sensitive information relating to victims. The ambition is that this will go some way to:

- addressing the barriers met by RASSO victims;
- improve their confidence when seeking the assistance of police; and
- provide clarity through the criminal justice process.

Equally, organisation should use this Opinion as a reference so that they have the confidence to request and share data efficiently. This should give them further knowledge of the permissive gateways that allow sharing to take place. This, in turn, should lead to improvements in the speed of progressing cases and ultimately positively influence charging rates.

1.5 The structure of this Opinion

This section has provided the background to this Opinion and why it is required. It is clear from official reports of recent inquiries that there is a pressing need to clarify the circumstances under which investigators may process materials relating to victims in the course of their criminal investigations.

[31] Relevant 'third party' organisations might be heath care providers, local authorities, educational institutions, etc.

The remainder of this Opinion sets out the legislation that relates to the processing of personal information of victims for law enforcement purposes, and processing more generally. It then focuses on the necessary conditions set out in data protection legislation for this type of information to be shared by third parties fairly and lawfully with the police, in the course of criminal investigations. **Sections of this Opinion are intended as a practical guide for informed practitioners in this area to understand how they can comply with the law enforcement provisions and wider application of UK data protection laws.**

The Commissioner is in no way seeking to encroach on the investigative process or to define what constitutes a reasonable line of enquiry. When terms such as 'appropriate', 'proportionate' and 'necessary' are used in this Opinion, they are being used within the scope of data protection legislation. This should not be conflated with their meaning in the context of a criminal investigation.

The Commissioner notes these judgements are for law enforcement professionals to make in the circumstances of a particular RASSO investigation. However, organisations may be called to account for, and may be held to account by the Commissioner, for the manner in which those judgements are made in a particular case.

Finally, this Opinion makes recommendations for further work in this area. This is to provide greater reassurance to victims that their privacy is being preserved to the extent this is possible, and that their information rights are being respected.

2. Legislative framework

This chapter is an overview of the most significant legislation that applies to the processing of personal data relating to victims. It covers the areas of human rights, criminal justice and data protection. **It is also intended for informed practitioners to help them understand how they can comply with the law enforcement provisions and wider application of UK data protection laws.**

2.1 Human rights legislation

Article 8 of the European Convention on Human Rights (ECHR)[32] is the right to respect for private and family life, and states[33]:

> "1. everyone has the right to respect for his private and family life, his home and his correspondence; and
>
> 2. there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The ECHR has been given further effect in UK law by the Human Rights Act 1998.

In cases where a public authority is exercising a statutory power, this must still meet the ECHR "quality of law" test. This means the outcome must be foreseeable and applied only when "necessary in a democratic society". There must therefore be sufficient safeguards to prevent abuse and ensure the power is not exercised disproportionately. For example, policies and procedures that demonstrate appropriate consideration of necessity and authorisation.

If an interference with Article 8(1) rights (ie respect for private and family life, home and correspondence) is to be justified, it must meet the four-part test in Bank Mellat v Her Majesty's Treasury (No 2)[34], namely whether:

1. the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
2. it is rationally connected to the objective;

[32] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[33] Article 8 ECHR
[34] https://www.bailii.org/uk/cases/UKSC/2013/39.html

3. a less intrusive measure could have been used without unacceptably compromising the objective; and
4. having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the person and the interests of the community.

The High Court (England and Wales) made this clear in TB, R (on the application of) v The Combined Court At Stafford [2006] EWHC 1645 (Admin)[35] (the Stafford case). If the police requested the medical records of a witness (including the victim) from a third party - often through issuing a summons - the witness had the right to be informed and potentially raise objections. That right included a procedural right to be independently represented before the judge determining the summons application.

This resulted in witnesses being advised to attend summons hearings in numerous cases. In order to avoid unnecessary hearings, a 'Stafford statement' was introduced. This gives the witness the opportunity to confirm they had no objection to a summons being granted and did not seek to be present or represented at a hearing.

For contextual clarity, it is important to note that Stafford statements (England and Wales) subsequently came to be misused, in two ways:

- They were used by police in contexts much broader than might have otherwise been sought in a specific summons, such as identifiable medical records.
- They also requested consent to obtain unlimited amounts of unspecified personal information from third party organisations, incorrectly presenting this as representing a lawful basis for the processing.

2.2 Relevant criminal justice legislation

This section outlines those aspects of the law that place obligations on investigators to gather evidence. These vary slightly across the UK.

2.2.1 England, Wales and Northern Ireland

The Criminal Procedure and Investigations Act 1996 (CPIA)[36] and its code of practice set out how investigators in England, Wales and Northern Ireland should gather evidence. This covers how to record, retain and reveal to the prosecutor material obtained in a criminal investigation which may be relevant to the investigation.

[35] https://www.bailii.org/ew/cases/EWHC/Admin/2006/1645.html
[36] https://www.legislation.gov.uk/ukpga/1996/25/contents

Most significantly, the CPIA code for England and Wales[37] sets out the fundamental responsibility placed on investigators. An equivalent code of practice in Northern Ireland imposes the same obligations on investigators in that jurisdiction.

> "In conducting an investigation, the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances. It is a matter for the investigator, with the assistance of the prosecutor if required, to decide what constitutes a reasonable line of inquiry in each case."[38]

It also provides helpful definitions of terms describing information collected for criminal investigation purposes.

> "*Material* is material of any kind, including information and objects, which is obtained or inspected in the course of a criminal investigation and which may be relevant to the investigation. This includes not only material coming into the possession of the investigator (such as documents seized in the course of searching premises) but also material generated by them (such as interview records)" [39]
>
> "Material may be *relevant to an investigation* if it appears to an investigator, or to the officer in charge of an investigation, or to the disclosure officer, that it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case" [40]

Under the CPIA, investigators must retain material that may be relevant to an investigation for prescribed periods. The details of which are dependent on the outcome of the case.

2.2.2 Scotland

In Scotland, the Criminal Justice and Licensing (Scotland) Act 2010[41] and the code of practice[42] issued under Section 164 of that Act set out the obligations placed on the investigators and prosecutors.

---

[37] https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-1996-section-231-code-of-practice
[38] s3.5 CPIA Code
[39] s2.1(7) CPIA Code
[40] s2.1(8) CPIA Code
[41] https://www.legislation.gov.uk/asp/2010/13/contents
[42] http://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Guidelines_and_Policy/Code%20of%20Practice%20-%20Disclosure%20of%20Evidence%20in%20Criminal%20Proceedings.pdf

> "An essential element underpinning the duty of disclosure is the obligation on the police to pursue all reasonable lines of enquiry, including any line of enquiry that might point away from the accused as the perpetrator of the offence.
>
> A reasonable line of enquiry will include any line of enquiry that might:
>
> i) Exculpate or point away from the accused as the perpetrator of the offence; and/or
>
> ii) Mitigates the offence(s)
>
> The Crown has an obligation to ensure that all reasonable lines of enquiry are pursued and accordingly, may instruct the police to carry out particular lines of enquiry where this has not already been identified."[43]

2.3 Data protection legislation

UK citizens' information rights are enshrined in legislation, primarily through the UK GDPR and the DPA 2018[44].

This section outlines the main parts of the legislation that are relevant to the processing of data relating to victims.

The UK GDPR provides some key definitions at Articles 4(1) and (2) .

> "(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
>
> (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[45]

[43] ss15.1-15.3 Criminal Justice and Licensing (Scotland) Act 2010 (Section 164) Code
[44] http://www.legislation.gov.uk/ukpga/2018/12/contents
[45] Article 4 UK GDPR

It the context of this Opinion, personal data relating to a victim may be processed by:

- a policing organisation (from the time the incident is reported, throughout the investigation and beyond); or
- other non-policing organisations (either for reasons unconnected with them being a victim or because they are a victim).

The specific legislation governing this processing is dependent on a combination of the type of organisation undertaking it and the primary purposes for which it is taking place.

2.4 Data protection legislation: law enforcement processing

Part 3 of the DPA 2018 governs the processing of personal data for law enforcement purposes. Section 31 defines "the law enforcement purposes" to be:

> "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[46]

This part of the DPA 2018 contains specific provisions relating to "competent authorities" processing data for law enforcement purposes. As defined at Section 30, competent authority means:

> "(a) a person specified or described in Schedule 7, and
>
> (b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes."[47]

Chief constables and other policing bodies are amongst those specified in Schedule 7 of the DPA, and are therefore defined as a competent authority.

2.4.1 Principles

When undertaking law enforcement processing, the DPA 2018 makes organisations responsible for, and requires that they be able to demonstrate compliance with, the following principles[48]:

- First principle: The processing must be lawful and fair.

[46] s31 DPA
[47] s30 DPA
[48] ss35-40 DPA

- Second principle: The processing must be limited to a specified, explicit and legitimate purpose, and it must not be processed in a manner that is incompatible with the purpose for which it was collected.
- Third principle: The data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Fourth principle: The data must be accurate and, where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay. In addition, as far as possible, a clear distinction must be made between different categories of people – those suspected of an offence, those convicted, witnesses and complainants. Personal data based on fact must as far as possible be distinguished from personal data based on personal assessments.
- Fifth principle: Data should be stored for no longer than is necessary, and appropriate limits must be set for periodic review of the need for continued storage.
- Sixth principle: There must be adequate measures in place to ensure the appropriate security of data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

This Opinion focuses on the application of the first and third principles to the processing of data about victims. It must be lawful and fair, and fundamentally adequate, relevant and not excessive. The principle of data minimisation is a key thread that runs throughout this Opinion.

2.4.2 First principle: lawful and fair processing

At section 35 of the DPA 2018, the first principle underpins all processing for law enforcement purposes. It states that processing for law enforcement purposes can be lawful only if and to the extent that it is based on law and either:

> "(a) the data subject has given consent (within the meaning of data processing law) to the processing for that purpose; or
>
> (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority."[49]

For England, Wales and Northern Ireland, the "based on law" condition may be the CPIA. In Scotland, it may be the Criminal Justice and Licensing (Scotland) Act 2010, specifically **the obligation to pursue all reasonable lines of enquiry**, as set out in section 2.2 of this Opinion.

[49] s35(2) DPA

Regarding the use of "consent" or "necessity" conditions, the definition of consent as referenced in Part 3 of the DPA 2018 is derived from UK GDPR Article 4(11) which states that:

> "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[50]

The first ICO report into mobile phone extraction[51] explained in detail the difficulties in relying upon the consent of data subjects for lawful processing in the context of criminal investigations. The main factors making it difficult to achieve valid consent for victims' data include:

- the limited capacity of RASSO victims to make fully informed, freely given, rational decisions[52] during times of high trauma;
- the perceived power imbalance between the police and the victim being asked to provide access to their data, along with the perception that a refusal of consent may impact the ability of the case to continue (validated by the HMCPSI thematic review of rape cases[53]). This suggests that consent may not be freely given; and
- the absence of the ability to withdraw consent in any real sense due to the legal requirements on the police and investigators to retain materials relevant to the investigation.

The Commissioner believes that there is a more appropriate alternative condition to consent for processing victims' data. Namely that **the processing is necessary for the performance of a task carried out for the law enforcement purpose** by a competent authority.

It is also a more logical fit with the concepts of respecting victims' privacy and not seeking to process their data unless it is necessary for the progression of an investigation. This is in addition to overcoming the challenges in meeting the criteria for consent to be valid. When arriving at a lawful basis for processing, it is still important to consider overall fairness in the context of RASSO cases. A victim may perceive a focus on their intimate private life as unfair, disproportionate or as a re-victimisation. Especially if consent is not applied correctly or their personal information is obtained for necessary law enforcement purposes, but in far greater detail than those alleged to have committed a crime.

---

[50] Article 4(11) UK GDPR
[51] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf
[52] https://www.justice.gc.ca/eng/rp-pr/jr/trauma/index.html
[53] https://www.justiceinspectorates.gov.uk/hmcpsi/wp-content/uploads/sites/3/2019/12/Rape-inspection-2019-1.pdf

Where appropriate to the investigation, taking into account any possible prejudice, the police should inform all parties about how they will use their personal information throughout the investigative process. Also, they should tell them about the likelihood of the information being disclosed to others, such as a defendant.

2.4.3 Sensitive processing

In the context of law enforcement processing, there are further considerations for lawful and fair processing where the data is considered to be "sensitive".

"Sensitive processing" means:

> "(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
>
> (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
>
> (c) the processing of data concerning health;
>
> (d) the processing of data concerning an individual's sex life or sexual orientation."[54]

The nature of a criminal investigation into a RASSO case means it may involve processing some of these categories of data relating to the victim.

In such circumstances, the police must have an appropriate policy document[55] in place before the processing takes place, and:

- the data subject has given their consent of the data subject (as explained above); or
- the processing is strictly necessary for the law enforcement purpose and meets at least one of the conditions set out in Schedule 8 of the DPA.

The Schedule 8 conditions are:

- statutory purposes;
- administration of justice;
- protecting individual's vital interests;
- safeguarding of children and of individual's at risk;
- personal data already in the public domain;
- legal claims;
- judicial acts;

[54] s35(8) DPA
[55] https://ico.org.uk/media/for-organisations/documents/2616230/part-3-appropriate-policy-document.docx

- preventing fraud; and
- archiving.

In the case of sensitive processing, there must be a demonstration of **strict necessity**. This is the case if the police have set aside consent as an appropriate condition sufficient to justify processing for law enforcement purposes. The "statutory purposes" condition could be applied to the police exercising their duty in the interests of the public.

Organisations need to demonstrate that they have considered other, less privacy-intrusive means and have found that they do not meet the objective of the processing.

The right to the protection of personal data is not an absolute right. It must be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality.

Bridges, R (On Application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)[56] found that the test set out in Bank Mellat v Her Majesty's Treasury (No. 2) [2013] UKSC 39[57] (outlined in section 2.1 of this Opinion), is equally relevant in considering the strict necessity to undertake law enforcement processing. This takes into account any interference with Article 8(1) ECHR rights.

2.4.4 Third principle: adequate, relevant and not excessive processing

The third principle of Part 3 of the DPA (the data minimisation principle) states that:

> "personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed."[58]

In practice, law enforcement authorities must ensure that the personal data they are processing:

- is sufficient to properly fulfil their stated purpose;
- has a rational link to that purpose; and
- is limited to what is necessary.

They should also periodically review their processing to check that the personal data they hold is still relevant, and delete anything they no longer need. This is closely linked with the storage limitation principle.

[56] https://www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html
[57] https://www.bailii.org/uk/cases/UKSC/2013/39.html
[58] s37 DPA

In the context of RASSO cases, this means that any personal data generated or acquired by investigators should be sufficient for the progression of the investigation and discharging the investigators' duties. But must be limited to that which might be reasonably believed to be relevant. As mentioned, the data minimisation principle is a key thread that runs throughout this Opinion, and has strong relevance in RASSO cases.

Example

A victim's educational records and qualifications are requested as part of a RASSO investigation. Further historic school records are also required that suggested the victim had been caught lying as a teenager.

In this case, the victim may feel that the requested information is excessive, intrusive and the historic information unrelated to the investigation. This can add to the distress of the victim who is already subject to a traumatic process. A request for all data held about a person is less likely to be appropriate than one that is time bound (eg around the time of the incident) and limited to particular types of data.

2.5 Data protection legislation: general processing

The UK GDPR is the legislation that covers the information rights of people whose personal data is processed for "general purposes". In the context of this Opinion, this means the processing of victims' data for purposes other than those relating directly to law enforcement. This covers processing by policing organisations or more commonly, third party organisations.

2.5.1 Principles

Article 5 of the UK GDPR sets out the key principles that apply to processing personal data:

- First principle: It must be processed lawfully, fairly and in a transparent manner in relation to individuals ("lawfulness, fairness and transparency").
- Second principle: The data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation").
- Third principle: It must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation").
- Fourth principle: It must be accurate and, where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy").

- Fifth principle: Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation").
- Sixth principle: It must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

In addition, the "accountability"[59] principle requires organisations to be responsible for, and able to demonstrate compliance with, the above principles.

We use the term "organisation" in this Opinion, but under data protection legislation a "controller" means:

> "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[60]

This Opinion focuses on the first three principles.

2.5.2 First principle: lawful, fair and transparent processing

Under this UK GDPR principle, organisations must identify valid grounds (known as a "lawful basis") for processing personal data. In doing so, they must ensure they are not in breach of any other laws. They must not process the data in a way that is unduly detrimental, unexpected or misleading to the people concerned. They also must be clear, open and honest from the outset with people whose personal data they are processing.

There are several potential lawful bases available for general processing. At least one of which must apply if the processing is to be lawful:

> "(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

[59] Article 5(2) UK GDPR
[60] Article 4(7) UK GDPR

> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[61]

It is for organisations to determine the most appropriate lawful basis for the processing they carry out. This will depend upon the nature of their organisation and the specifics of the purposes of the processing.

They must carry out the processing in a transparent manner and provide, from the outset, information to individuals explaining how and for what purposes they are processing their information[62]. It is also very important that they advise people of their rights about the processing of their data.

Of significance in the context of processing victims' data is the right "to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her"[63]. This right applies when the processing is carried out under the lawful bases set out in Article 6(e) ("public interest") or (f) ("legitimate interests") of the UK GDPR.

If a victim exercises their right to object, the organisation is required to comply with this request unless it was able to demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms"[64] of the victim. The right to object is therefore not an absolute right under data protection legislation in some circumstances.

In addition, the "crime and taxation: general' exemption"[65] is set out in Schedule 2 of the DPA 2018. This allows an organisation to restrict one or more of the rights of individuals when processing data for the prevention and detection of crime, to the extent that complying with the provision is likely to prejudice that purpose. Organisations must consider each restriction on a case-by-case basis.

It is important to note that an objection to such processing under data protection legislation may sit alongside a separate objection in RASSO cases. Stafford statements seeking a person's consent are not an adequate lawful basis for data processing principles and law enforcement authorities must identify another lawful basis. However, the importance of a person's Article 8 rights, as

[61] Article 6(1) UK GDPR
[62] Article 13 UK GDPR
[63] Article 21 UK GDPR
[64] Article 21(1) UK GDPR
[65] See Part 1 Schedule 2 DPA

outlined in the Stafford case (England and Wales), still require specific and separate consideration. For that reason, even when data protection requirements are met, a person should be involved appropriately throughout the process. Where they raise an objection to the disclosure of their data, law enforcement authorities must identify and discuss their broader rights with them, along with an explanation of any options they may have.

2.5.3 Second principle: purpose limitation

Organisations need to be clear about their purposes for processing personal data. They also need to provide information that explains these purposes to individuals whose data they are processing.

The processing must be limited to the original purposes, and organisations must not use people's information in any way they would not expect.

Any processing for a different purpose may only take place if the new purpose is compatible with the original purpose, consent is obtained, or there is a clear obligation or function set out in law.

Again, where appropriate, organisations could apply the crime and taxation: general exemption. This means that they may process the data for a new purpose linked to the prevention or detection of crime.

2.5.4 Third principle: data minimisation

As with law enforcement processing, under the UK GDPR data minimisation principle, personal data must be adequate, relevant and not excessive. Organisations must ensure that:

- the data they are processing is sufficient to fulfil the stated purpose;
- the data is rationally linked to that purpose;
- they hold or process in any other way no more data than is required to fulfil the purpose; and
- they are able to demonstrate that they have appropriate processes in place to ensure that they only collect and hold the personal data that they require for their stated purpose.

2.5.5 Special category data

Article 9 of the UK GDPR states:

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning

> health or data concerning a natural person's sex life or sexual orientation shall be prohibited."[66]

However, there may be legitimate circumstances in which it is necessary to process some of this special category data relating to RASSO victims, especially relating to their health or sex life.

Organisations must be able to rely on one of the following conditions[67] before undertaking any such processing:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

When relying on conditions (b), (h), (i) or (j), organisations must meet a further associated condition set out in Part 1 of Schedule 1 of the DPA.

If relying on the Article 9(2)(g) substantial public interest condition, they must also meet one of further conditions set out in Part 2 of Schedule 1 of the DPA 2018.

In most cases, they must have an "appropriate policy document"[68] in place, unless otherwise stated in the legislation.

2.5.6 Criminal offence data

A further issue relating to the processing of information is the Article 10 UK GDPR requirement. This means that organisations need to pay special attention to data about offenders or suspected offenders in the context of criminal offences (including allegations, proceedings or convictions).

Public bodies, or private bodies who are given public sector tasks, may have 'official authority' laid down by law to process criminal offence data. Other organisations must meet one of the conditions set out in of Schedule 1 of the DPA.

In most cases, they must have an appropriate policy document[69] in place (to cover this and any special category data processing). The ICO has produced

[66] Article 9(1) UK GDPR
[67] Article 9(2) UK GDPR
[68] See Part 2 Schedule 1 DPA
[69] See Part 2 Schedule 1 DPA

further guidance outside this Opinion about processing criminal offence data under UK GDPR.

3. Processing victim data

This Opinion is concerned with the processing that takes place **as a result of** a person being a victim of a RASSO incident, rather than more general processing of information by organisations who are unaware a person is a victim. It covers:

- the requirement for police to process information they obtain directly from a victim;
- police requests for information from a victim's digital devices; and
- police requests to a third party organisation that may be holding information about a victim.

It is not for the data protection regulator to dictate how investigations and prosecutions are conducted. However, under Part 3 of the DPA 2018 the "processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law"[70]. Therefore, it is necessary for the ICO to consider the extent to which different investigative actions have a valid basis in law. Police and prosecutors across the UK are answerable and accountable to the ICO for how they meet their data protection obligations as they undertake their investigations and prosecutions.

3.1 Obtaining personal data from a victim

Once a victim has made a complaint, it is common that a police force/service need to record personal details relating to them. These include the basic identification details of the person and their account of what had taken place. Given the traumatic nature of RASSO cases, the processing is inherently sensitive.

Victims must be assured that the personal information they reveal to the police will be handled appropriately, in accordance with all aspects of Part 3 of the DPA 2018. They are, however, ultimately in control of what they choose to divulge directly to investigators. How they exercise that control depends on the quality of information they are given by the investigators about:

- the need for collecting certain information;
- how the investigators will be use it; and
- who the investigators will disclose it to.

For example, if investigators will disclose information to defendants further along the process. It is therefore very important that investigators are open and honest with victims from the start.

[70] s35(2) DPA

3.2 Acquiring data from victims' electronic devices

As reported in the End-to-End Rape Review and other reports, the examination of digital materials generated by and stored on electronic devices is an increasingly common feature of RASSO investigations. Much of this relates to communications between the victim and other persons.

The challenges associated with acquiring and examining mobile phones (especially those used by victims) were examined in detail in the ICO reports[71] following its investigation into this practice. The key elements are summarised in this section.

The England and Wales Court of Appeal (Criminal Division) judgment in relation to Bater-James & Anor v R [2020] EWCA Crim 790[72] established a number of principles about the examination of a victim's devices.

The Court considered four issues of principle, the first of which was:

> "The First Issue of Principle: Identifying the circumstances when it is necessary for investigators to seek details of a witness's[73] digital communications. These are usually, but by no means always, electronic exchanges conducted by way of multiple platforms on smart mobile telephones, tablets or computers. These platforms are so numerous that it is pointless to attempt to list examples. In essence, the question in this context is when does it become necessary to attempt to review a witness's digitally stored communications? The linked question is when is it necessary to disclose digital communications to which the investigators have access?"

The Court found that there is "no obligation on investigators to seek to review a witness's digital material without good cause"[74]. The judgment also said there must be a proper basis, usually based on a reasonable line of enquiry, that it would reveal relevant material. 'Fishing expeditions' are not appropriate.

It found that there is "no presumption that a complainant's mobile telephone or other devices should be inspected, retained or downloaded, any more than there is a presumption that investigators will attempt to look through material held in hard copy."[75]

---

[71] https://ico.org.uk/about-the-ico/what-we-do/ico-investigation-into-mobile-phone-data-extraction-by-police-in-the-uk/
[72] http://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html
[73] The judgment uses the term "witness" to also refer to complainants (and therefore victims).
[74] Para 67 Bater-James & Anor v R [2020] EWCA Crim 790
[75] Para 77 Bater-James & Anor v R [2020] EWCA Crim 790

The judgment reiterates the point that victims do not automatically waive their right to privacy under Article 8 of the ECHR. Therefore, it is only necessary to disclose that material which is reasonably capable of undermining or assisting the case for the accused.

The second issue the Court considered was:

> "The Second Issue of Principle: When it is necessary, how should the review of the witness's electronic communications be conducted?"

The Court of Appeal found that police force/service(s) must consider whether it is actually necessary to obtain the material required from a victim's device. If it is, they also need to:

- consider whether it is sufficient simply to view limited areas (eg particular messages or images);
- wherever possible, use alternatives to data extraction without taking possession of the device (eg taking screenshots or making some other record);
- if more extensive enquiries are necessary, examine the device and extract the data with the minimum of inconvenience to the victim;
- return the device without unnecessary delay. This point has been developed by the UK Government in its response to the End-to-End Rape Review with its ambition to have all rape victims' devices returned to them within 24 hours (or, exceptionally, a replacement provided);
- use incremental searching where there are large volumes of data, and the defendant should participate in this process; and
- avoid revealing irrelevant personal information by making appropriate redactions to any disclosed material.

The third issue the Court considered was:

> "The Third Issue of Principle: What reassurance should be provided to the complainant as to ambit of the review and the circumstances of any disclosure of material that is relevant to the case?"

The judgment set a range of things that the police should tell the victim, including that:

- they will be kept informed about disclosure decisions, including:
    - how long the investigators keep the device;
    - what the police plan to extract from it; and
    - what the police examine with a view to disclosure;

- the police will only copy or inspect any content within the device if there is no other appropriate method of discharging the prosecution's disclosure obligations; and
- the police will only provide material to the defence if it meets the strict test for disclosure. They will serve it in a suitably redacted form so they do not unnecessarily reveal personal details or other irrelevant information (eg photographs, addresses or full telephone numbers).

The fourth issue the Court considered was:

> "The Fourth Issue of Principle: What is the consequence if the complainant refuses to permit access to a potentially relevant device, either by way of "downloading" the contents (in reality, copying) or permitting an officer to view parts of the device (including, *inter alia*, copying some material, for instance by taking "screen shots")? Similarly, what are the consequences if the complainant deletes relevant material?"

It is a matter for the court to consider the circumstances relating to, and implications of, a victim refusing access to digital materials or deliberately deleting them. However, it is important that investigators explain to victims the procedure that the investigation follows (as above). They should also make them aware of the consequences of any decision not to allow access to the requested digital materials.

The judgment states:

> "It is important to note that a refusal by a complainant or a witness to divulge the contents of a mobile telephone or similar device clearly does not, without more, constitute bad faith or misbehaviour on the part of the police or the prosecutor."[76]

It asserts the importance of understanding any reasons for such a refusal and consideration, by the court, of the adequacy of the trial process in the absence of the material from the device.

The first ICO report[77] on MPE explained that the processing of data from a mobile device is likely to amount to sensitive processing. This is equally likely to be the case for other electronic devices used for communications.

[76] Para 96 Bater-James & Anor v R [2020] EWCA Crim 790
[77] https://ico.org.uk/media/about-the-ico/documents/2620093/ico-investigation-mpe-england-wales-202106.pdf

Therefore, in order to comply with data protection legislation, investigators need to be confident before requesting access to a victim's electronic devices that:

- they are following a **reasonable line of enquiry**; and
- their proposed processing is **strictly necessary**.

Investigators should consider:

- ☐ We have considered in the circumstances of the investigation, if the proposed line of enquiry is reasonable and necessary.
- ☐ We have considered if there are specific devices which we believe store relevant material.
- ☐ We have considered if there is a reasonable and legitimate means of acquiring the device(s) if needed.
- ☐ We have explored if there are means of fulfilling the line of enquiry without resorting to extracting and examining digital data.
- ☐ We have considered if the public interest benefits outweigh any privacy concerns of the person or victim.
- ☐ We have made contact with the device user where appropriate and only acquired the minimum amount of data which is strictly necessary.

3.3 Acquiring data from other organisations

In addition to examining electronic devices, investigators often seek access to victims' personal information held by other third party organisations.

The England and Wales Court of Appeal (Criminal Division) judgment in Alibhai & Ors, R v [2004] EWCA Crim 681[78] provides guidance about what to consider. It found that there is no absolute obligation to obtain information relating to victims that are held by third parties. There must be a "margin of consideration" as to what is required in each case.

This means that it is difficult to justify, from a data protection perspective, the acquisition of vast quantities of material just because they exist. Investigator's requests to third parties need to be targeted and, to the greatest extent possible, specific.

As stated in Bater-James & Anor v R [2020] EWCA Crim 790[79], it "is not a 'reasonable' line of inquiry if the investigator pursues fanciful or inherently

[78] https://www.bailii.org/ew/cases/EWCA/Crim/2004/681.html
[79] https://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html

speculative researches. Instead, there needs to be an identifiable basis that justifies taking steps in this context."[80]Therefore, in order for a request to be valid, investigators should make it sufficiently precise.

Example

A RASSO investigation requires sensitive medical records that detail a victim's medical history. However, the requested medical records also go back to the birth date of the victim.

In this circumstance, the victim may view this request as speculative, excessive and distressing. Acquiring vast quantities of material just because it exists, would be difficult to justify unless there was a compelling reason. It is for investigators to make an informed decision about what information they need in a particular case. But they need to make targeted and specific requests to third parties for relevant information.

3.3.1 Formulating the request

Where a police force/service identifies potentially relevant information held by a third party organisation, they must clearly explain their reason for obtaining it. Police force/service(s) also need to consider the appropriateness of such a request, following Bater-James & Anor v R [2020] EWCA Crim 790 and Alibhai & Ors, R v [2004] EWCA Crim 681. Forces in other UK jurisdictions (Scotland and Northern Ireland) should also take such case law into consideration when formulating a request.

Taking those principles into account, investigators need to demonstrate before they request access to a victim's information from a third party that:

- they are pursuing a **reasonable line of enquiry**; and
- it is **necessary**.

If they are proposing to seek access to materials that meet the criteria for sensitive processing (eg medical records), then they need to meet the further conditions associated with **strict necessity**.

This Opinion has explained that to rely upon the consent of the victim in justifying processing of their data in these circumstances is unlikely to comply with data protection legislation. However, the Stafford case sets out the requirement for investigators to work with and consult victims in the process. It is therefore appropriate for an investigator to discuss with a victim where relevant material may be held and to seek their views about the police gaining access to it. This should assist the investigator in first balancing the public interest in obtaining the material against the consequential impact on the

[80] Para 70 Bater-James & Anor v R [2020] EWCA Crim 790

victim's privacy. Then, if appropriate, the investigator can make a proportionate request to the third party with sufficient specificity.

The investigator should consider:

- ☐ We have considered in the circumstances of the investigation, if the proposed line of enquiry is reasonable and necessary.
- ☐ We have explored if there are means of fulfilling the line of enquiry without requesting material about the person or victim held by other organisations.
- ☐ We have considered if the material is likely to meet the relevance and disclosure tests.
- ☐ We have made the person or victim aware of their information rights and broader rights, and considered if they have raised an objection to the material being sought.
- ☐ We have considered if the public interest benefits outweigh any privacy concerns of the person or victim.

Any request to a third party organisation must take into account the obligations that organisation has under data protection law. This is in addition to considering the privacy rights of the victim. Therefore, investigators should make the request sufficiently detailed and specific that the third party organisation is able to assess its validity and be confident in volunteering the information.

Further, investigators should clearly explain to the third party organisation that any information they provide could be disclosed further to the defendant. The disclosure remains voluntary even when the victim consents to the disclosure.

3.3.2 Responding to the request

The CPS legal guidance "Rape and Sexual Offences - Chapter 3: Case Building"[81] says:

> "In the context of a RASSO investigation, third party material that is commonly encountered includes:
>
> - Social services departments
> - Forensic Physicians
> - Counsellors/therapists
> - Schools

[81] https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-3-case-building

- Medical Practitioners
- Hospitals
- Family Court
- Owners of CCTV"

This is a diverse range of organisational types that will have collected data from people for different purposes under different lawful bases under the UK GDPR. In some cases, organisations have a statutory duty to proactively bring matters to the attention of the police. Such circumstances are beyond the scope of this Opinion. The focus here is to assist organisations in understanding their obligations when they receive a request from a police force/service to provide information in the course of a criminal investigation.

It is recognised that these organisations may not have a detailed insight into the conduct of criminal investigations. Nor is it always appropriate for the police to reveal to them the full details of the investigation. However, organisations must be confident that they are respecting the information rights of their service users before disclosing their personal information. In particular, in circumstances when the person (who has become a victim of crime – in this case RASSO) would have otherwise expected their information to be kept private. This is especially important in medical or therapeutic settings in which special category data is routinely held.

Example

A victim uses a counselling service after an incident, and during the discussions notes are recorded. During an active RASSO investigation, the police request the discussion notes from the service. The service must respect the rights of the victim when considering disclosure. Especially if there is a particular expectation of privacy and confidentiality attached to the service or information. The service should primarily consider the consent of the victim, any privileged information within the notes, and if disclosure is in the best interests of the victim.

This is particularly important to the victim if there is potential for the information to be disclosed further to the defendant during the criminal justice process. This could be very damaging to the victim in some cases.

To comply with the data minimisation principle, the service should only provide as much information as is adequate, relevant and limited to the purpose of sharing with a law enforcement authority.

Regardless of whether they receive a request for material from the police, organisations must ensure they are complying with the UK GDPR. This includes meeting any conditions required if they process special category or criminal offence data (see sections 2.5.5 and 2.5.6 of this Opinion).

An organisation should treat sharing personal information with the police as a separate processing operation with its own purpose and associated lawful basis. It is not always simply a continuation or extension of the original processing.

The "crime and taxation: general exemption" at Paragraph 2 of Schedule 2 of the DPA 2018 is available when sharing personal data with a law enforcement authority. An organisation may apply this to justify the new purpose. However, there is still an obligation for the organisation to consider the lawful basis for sharing information with the police. This is for the organisation to determine but, in the context of a criminal investigation, this is likely to be Article 6(f) ("legitimate interests").

There is a three-part test to consider in order to determine whether the requirements of Article 6(1)(f) of the UK GDPR are met. In other words, whether it is appropriate to respond to a police request for information. It covers:

- Purpose test: is the organisation (third party) pursuing a legitimate interest?
- Necessity test: is the processing necessary for that purpose?
- Balancing test: do the person's interests override the legitimate interest?

Additional considerations apply if the response to the request involves disclosing special category (eg medical records) or criminal offence data.

For special category data, the Article 9(2)(g) "substantial public interest" condition may be appropriate.

Before sharing special category or criminal offence data, the organisation must identify an appropriate condition in Schedule 1 of the DPA. It may be able to rely on the paragraph 10 condition. This permits such sharing where it is necessary for the prevention or detection of unlawful acts, and where asking for consent would prejudice that purpose. Again, organisations must consider applying such a condition on a case-by-case basis.

The ICO has produced further guidance on sharing personal data with law enforcement authorities within our data sharing guidance hub. This provides helpful checklists, tools and case studies to make it easier for police and organisations to request and share personal data with confidence.

Taking all these factors into account, before undertaking the new processing (ie providing the victim's personal data to the police), the third party organisation needs to consider:

☐ We are satisfied, on the basis of the details provided by the police, that they have a legitimate reason for requesting information from our organisation.

- ☐ We have considered if it is necessary to disclose the requested information in order to assist the police's investigation.
- ☐ We have confirmed (either by directly engaging with the person or victim or through the police request) that they are aware of their broader rights and have not objected to the disclosure, separate to any right to object under data protection legislation.
- ☐ We have made clear to the person or victim where appropriate, that information provided to the police may be disclosed further, such as to a defendant.
- ☐ We have identified where appropriate, an alternative authority that allows us to provide the information without the person or victim agreeing.
- ☐ We have considered if the reasons provided by the police and the needs of the investigation outweigh the interests, rights and freedoms of the person or victim.

The organisation looking to disclose information should record the legitimate interests assessment (LIA) they have conducted. This will assist them in demonstrating that they are complying with their data protection obligations.

In assessing the necessity of the processing, the organisation should apply the data minimisation principle to assess whether the request is proportionate. For example, a request for all information held about a person is less likely to be appropriate than one that is time bound (eg around the time of the incident) and limited to particular types of information. In respecting victims' information rights, organisations must resist the temptation to invite police to browse everything they hold about a person and extract what they feel is relevant. The police request should be as specific as possible. This will assist the organisation to decide the necessity and extent of information the police require.

As stated in section 2.5.2 of this Opinion, the victim has the right to object to this type of processing under UK GDPR. However, this is not an absolute right in these circumstances. Further, an objection to such processing under data protection legislation may sit alongside a separate objection in RASSO cases. Stafford statements seeking an person's consent are not an adequate lawful basis for data processing principles – and another lawful basis for data processing must be identified. However, the importance of a person's Article 8 rights, as outlined in the Stafford case, still require specific and separate consideration. For that reason, even when data protection requirements are met, a person should be involved appropriately throughout the process. Where they raise an objection to the disclosure of their information, the police must discuss their broader rights with them, along with an explanation of any options they may have.

It is appropriate to decline the request and talk further with the investigator if an organisation is not clear whether:

- the victim has been made aware of their right to object; or
- if the victim's wishes are unclear.

The police may be able to provide clarification, contact the victim or alternatively provide advice about how the organisation can communicate directly with the victim, if this will not compromise the purpose of seeking the material. If this contact does not provide sufficient reassurance to the organisation, then in some cases an order from an appropriate court could be sought by the police.

4. Conclusions and recommendations

Following a number of reviews into inefficiencies in the criminal justice system relating to RASSO cases, a significant amount of work is being undertaken UK-wide. This includes the UK Government's Tackling Violence Against Women and Girls Strategy[82] and its response to the End-to-End Rape Review. The issues being addressed are complex and interlinked, and no single measure will resolve them.

It has been reported through a number of independent reviews that the victim's lack of confidence in the system contributes to the very low charging rate in RASSO cases. This, at least in part, is attributed to victims being concerned about unnecessary intrusions into their privacy and to delays in acquiring all the material requested by investigators and prosecutors.

This Opinion explains that compliance with data protection legislation ought not to be a barrier to effective and efficient sharing of data. That is where it is necessary and proportionate to do so, in the interests of conducting a thorough investigation and fair trial. However, police and other organisations need to do further work to demonstrate to victims and to others that they are processing data fairly and lawfully in compliance with data protection law.

Data protection principles, properly understood and applied, should not be an:

- excessive block on requesting or sharing relevant information, nor
- overly permissive gateway to obtaining and processing irrelevant information.

It is primarily for an investigator to determine what material they should obtain when carrying out an criminal investigation. They should do this by applying the guidance from Bater-James & Anor v R [2020] EWCA Crim 790[83]. The work of the Commissioner in explaining the data protection principles, with particular focus on data minimisation, should not be viewed as significantly affecting how investigators apply that guidance in practice. Equally, whilst not necessarily a data protection issue, it is acknowledged that there is a risk of not obtaining sufficient information to allow a fair trial to take place. Investigators have to strike a difficult balance when investigating RASSO cases.

In this section of the Opinion, the Commissioner makes recommendations that call for collaboration between a number of agencies and organisations across the UK. These are not trivial to address. The ICO remains committed to working with

[82] https://www.gov.uk/government/publications/tackling-violence-against-women-and-girls-strategy
[83] http://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html

all interested stakeholders and, in particular, assisting UK organisations in understanding and implementing the recommendations.

4.1 Enabling system-wide change

The Commissioner makes a number of recommendations that are intended to lead to consistency in each of the UK's jurisdictions. This means individual organisations feel confident that they are complying with data protection law, in both requesting and providing personal data.

4.1.1 Ceasing the invalid use of 'consent' broadly, using Stafford statements

We have discussed the challenges associated with the use of consent (as defined by data protection law) as a lawful basis for acquiring and further processing materials of relevance to criminal investigations.

The conditions required for consent to be a sufficient justification for processing, including it being freely given and specific, are unlikely to be met. This is due to the context of a victim being asked to provide access to a wide range of unspecified materials. Rather, the materials must be:

- rooted in an identifiable investigative requirement (ie a reasonable line of enquiry); and
- specific in scope.

Recommendation 1

The National Police Chiefs' Council must mandate to all police force/service(s) throughout the UK that they must cease using statements or forms indicating general consent to obtain third party materials (also known as Stafford statements – England and Wales). Data protection is not a barrier to fair and lawful sharing and acquisition, but data minimisation is key. Any personal data obtained relating to a victim must be adequate, relevant, not excessive and pertinent to an investigation.

4.1.2 Harmonising the prosecution approach

We heard consistently through our work that investigators may be inclined to be risk averse and seek to obtain as much material as possible from a range of third party sources. This is in anticipation of prosecutors requiring it prior to making a charging decision. At its worst, this blanket approach can be interpreted as a speculative attempt to identify evidence of the victim's 'bad character' or previous history which may impact their credibility at trial. Not only is this practice contrary to data protection law; but at its best represents a misunderstanding. With the increasing volumes of personal data being

generated, this approach is unlikely to be sustainable. It places a significant and unnecessary burden on the police to review the material in order to comply with their disclosure obligations.

There needs to be a common understanding of data protection law and disclosure requirements that underpin the lawfulness of requests for material from third party organisations. This Opinion sets out the Commissioner's expectation for lawful and safe data sharing, highlighting good practice and core principles.

Recommendation 2

The Crown Prosecution Service, the Public Prosecution Service Northern Ireland and the Crown Office and Procurator Fiscal Service should ensure that their prosecutors are fully aware of this Commissioner's Opinion. They should be properly equipped to act according to the principles he promotes to uphold the rights and protections of victims.

4.1.3 Providing operational guidance

The analysis of the intersection of criminal justice and data protection legislation presented in this Opinion is complex. It may be open to interpretation in different ways between the large number of territorial police force/service(s) of the UK.

It is important that the principles established in this Opinion are reflected in operational practice if they are to have the intended positive effect on criminal justice outcomes.

The National Police Chiefs' Council has issued forms to complement the College of Policing Authorised Professional Practice about the extraction of material from mobile devices. Constructing similar forms for investigators to use when obtaining materials from third party organisations could assist them in complying with data protection law, especially in RASSO cases.

The diversity of organisations that investigators seek materials from means that it is difficult to provide operational guidance directly to practitioners. It is therefore prudent to accompany any request for third party material with advice about what the organisation should consider when formulating its response.

Recommendation 3

The National Police Chiefs' Council should work with the College of Policing and the Crown Prosecution Service to produce advice and supporting forms

for police force/service(s) to use across England and Wales when requesting personal information from third party organisations.

The Police Service of Northern Ireland and Police Scotland should also work with the Public Prosecution Service Northern Ireland and the Crown Office and Procurator Fiscal Service respectively to produce similar documentation.

The forms should be consistent with the principles established in this Commissioner's Opinion. They should:

- give clear advice to third parties who will be in receipt of such requests;
- make clear whether the requests are voluntary or mandatory:
- explain the reason for seeking the information: and
- explain that information sought might end up being disclosed to a defendant.

4.2 Implementing change

Chief Constables are individually accountable, as a competent authority, for processing personal data for law enforcement purposes within their respective organisations. The Commissioner therefore makes recommendations to them in order that they are able to demonstrate they are complying with data protection legislation in their processing of information relating to victims of rape and serious sexual offences (RASSO).

4.2.1 Engaging with victims and acquiring their data

It has been established that the way investigators interact with RASSO victims can have a significant impact on the victim themselves and whether they continue to participate with the investigatory process. This Opinion sets out the minimum conditions necessary for the processing of information about victims to be lawful. These need to be fully understood by all relevant staff and to be reflected in operational practice.

Recommendation 4

The Commissioner makes further recommendations directly to the Chief Constables of forces across the UK, to ensure they are able to fully demonstrate compliance with data protection legislation when processing information relating to victims of rape and serious sexual offences (RASSO).

Given the impact of investigators' interactions with the victims of RASSO cases, Chief Constables should update policy, guidance, training and other documentation to make it consistent with this Opinion. We expect this to

cover at least the following areas:

- the circumstances under which it might be appropriate to seek access to material from (i) a victim's electronic devices, or (ii) other third party organisations. How they can use that information, who they can disclose it to, and how they can secure it;
- the formulation and documentation of appropriate parameters around material they are seeking;
- the nature of the contact with the victim and the information they should provide to them;
- the information they should provide to the third party organisation whom they are requesting material from; and
- how to deal with cases where a request for information is declined by a third party.

4.2.2 Managing victim data

This Opinion focuses on the acquisition by the police of materials containing victims' personal data from victims themselves, from their devices and from third party organisations. However, the ICO investigation into the extraction of mobile phone data revealed concerns about the ongoing management of digital materials, including the regular review and ultimate deletion required under the DPA. It is important that RASSO victims feel confident that their most sensitive information will be handled appropriately. This includes it being kept secure and retained no longer than necessary, in accordance with the law.

Recommendation 5

Chief Constables across the UK must have in place appropriate policy, guidance and training for the ongoing management and retention of personal information relating to victims. This should ensure that they are managing and fully safeguarding information, whether they:

- obtain it directly from the victim;
- extract it from their devices; or
- acquire it from third parties.

This is in accordance with this Opinion, the UK GDPR and the DPA 2018.

4.3 Further work by the Commissioner

As with our earlier work, the Commissioner will continue to work with organisations across the UK jurisdictions to assist them in interpreting this

Opinion and implementing his recommendations; in particular those recommendations relating to training, tools for practitioners and updating policies.

In considering any regulatory action or use of enforcement powers, the Commissioner may refer to this Opinion as a guide to the interpretation and application of the law. Each case will be fully assessed on the basis of its facts and relevant laws.

The Commissioner may also update or revise this Opinion based on any material legal or practical developments in this evolving area, such as judicial decisions and case law, or further findings from regulatory work and practical experience.

Compliance with the key principles of UK GDPR and DPA 2018 is fundamental for good data protection practice. Breaches of the law, including excessive collection of victim's information, can leave organisations open to regulatory action. Alongside the Commissioner's statutory duty to respond to complaints, he intends to address and prioritise complaints arising from victims experiences of the system as they arise, and may take other measures such as targeted audits and assessments of individual forces as circumstances require.

As described in this Opinion, organisations processing for law enforcement purposes must also be aware of their general duties under Section 44 DPA 2018. This includes making victims aware of:

- the existence of their right to complain to the Information Commissioner; and
- the contact details of the Commissioner.

The Commissioner will also highlight this Opinion to victim support groups across the UK jurisdictions, so that they can draw attention to any ongoing practices that are inconsistent with his recommendations.

Further reading

End-to-End Rape Review report:
https://www.gov.uk/government/publications/end-to-end-rape-review-report-on-findings-and-actions

ICO investigation into mobile phone data extraction by police in the UK:
https://ico.org.uk/about-the-ico/what-we-do/ico-investigation-into-mobile-phone-data-extraction-by-police-in-the-uk/

ICO data sharing information hub:
https://ico.org.uk/for-organisations/data-sharing-information-hub/

ICO guidance on sharing personal data with law enforcement authorities:
https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/

Attorney General's Office (AGO) (Annual Guidelines on Disclosure):
https://www.gov.uk/government/publications/attorney-generals-guidelines-on-disclosure

The National Police Chiefs Council (NPCC):
https://www.npcc.police.uk/

List of abbreviations

RASSO.....Rape and Serious Sexual Offences

CPIA ..... Criminal Procedure and Investigations Act 1996

CPS..... Crown Prosecution Service

DPA ..... Data Protection Act 2018

ECHR .....European Convention on Human Rights

UK GDPR .....UK General Data Protection Regulation

HMCPSI .....HM Crown Prosecution Service Inspectorate

ICO..... Information Commissioner's Office

MPE ..... Mobile phone (data) extraction

NPCC .....National Police Chiefs' Council

S ..... Section (when referring to a section number within an Act)

Annex

The Information Commissioner understands it can be challenging and daunting for a third party organisation to receive a request from the police. As with other forms of data sharing, we have heard that fear of ICO intervention could be a source of concern and this may lead to some third parties not engaging in the process. The Commissioner can confirm that the ICO is unlikely to take regulatory action against a third party sharing data with the police, in the belief that they were acting lawfully and the sharing is necessary, proportionate and justified. This is in line with our Regulatory Action Policy.

Organisations are allowed to share personal data with law enforcement authorities that need to process personal data for the law enforcement purposes. This is under the framework provided by the UK GDPR and Part 3 DPA 2018. However, organisations must consider each case on its own merits. A blanket approach is not likely to be acceptable in all cases.

It is fundamental that the third party understands the:

- necessity for sharing the information; and
- quality of the initial request from the police.

This means they can consider the request quickly, efficiently and respond appropriately.

Checklist for third party organisations (disclosing to the police)

☐ We are satisfied, on the basis of the details provided by the police, that they have a legitimate reason for requesting information from our organisation.

☐ We have considered if it is necessary to disclose the requested information in order to assist the police's investigation.

☐ We have confirmed (either by directly engaging with the person or victim or through the police request) that they are aware of their broader rights and have not objected to the disclosure, separate to any right to object under data protection legislation.

☐ We have made clear to the person or victim where appropriate, that information provided to the police may be disclosed further, such as to a defendant.

☐ We have identified where appropriate, an alternative authority that allows us to provide the information without the person or victim agreeing.

- ☐ We have considered if the reasons provided by the police and the needs of the investigation outweigh the interests, rights and freedoms of the person or victim.

Checklist for police officers and investigators (RASSO cases)

Law enforcement requests for data held on a mobile devices

- ☐ We have considered in the circumstances of the investigation, if the proposed line of enquiry is reasonable and necessary.
- ☐ We have considered if there are specific devices which we believe store relevant material.
- ☐ We have considered if there is a reasonable and legitimate means of acquiring the device(s) if needed.
- ☐ We have explored if there are means of fulfilling the line of enquiry without resorting to extracting and examining digital data.
- ☐ We have considered if the public interest benefits outweigh any privacy concerns of the person or victim.
- ☐ We have made contact with the device user where appropriate and only acquired the minimum amount of data which is strictly necessary.

Law enforcement requests for data held by a third party organisation

- ☐ We have considered in the circumstances of the investigation, if the proposed line of enquiry is reasonable and necessary.
- ☐ We have explored if there are means of fulfilling the line of enquiry without requesting material about the person or victim held by other organisations.
- ☐ We have considered if the material is likely to meet the relevance and disclosure tests.
- ☐ We have made the person or victim aware of their information rights and broader rights, and considered if they have raised an objection to the material being sought.
- ☐ We have considered if the public interest benefits outweigh any privacy concerns of the person or victim.