Regulatory Sandbox Final Report: Thames Valley Police

A summary of Thames Valley Police's participation in the ICO's Regulatory Sandbox

Date: November 2023

ico.
Information Commissioner's Office

Contents

1. Introduction

1.1 The Regulatory Sandbox ('the Sandbox') is a service the ICO provides to support organisations that are developing products or services which use personal data in innovative and safe ways, and will deliver a potential public benefit.

1.2 The Sandbox is a free, professional service that is available to organisations of all sizes who meet our entry criteria and specified areas of focus, and who are operating within challenging areas of data protection. During 2021 – 2022, the Sandbox considered applications from organisations developing products or services involving complex personal data sharing, and/or projects exploring the use and deployment of innovative technologies.

1.3 Thames Valley Police ('TVP') entered the Sandbox as the lead organisation in a data sharing partnership, known as 'Thames Valley Together' ('TVT'). TVT is a multi-agency project tasked with delivering on the objectives of the Serious Violence Duty ('the Duty'), which was legislated for as part of the Police, Crime, Sentencing and Courts Act 2022 ('PCSC 2022').

1.4 The Duty's origins can be traced back to the UK Government's Serious Violence Strategy of 2018[1], which marked a shift in approach to tackling violent crime by endorsing a public health approach. Recognising that serious violence is a complex social issue with multiple underlying factors, the strategy proposed adopting a public health approach that treats violence prevention much like a disease prevention model. This approach focuses on identifying the risk and protective factors associated with violence, analysing patterns and trends, and

[1] Home Office – Serious Violence Strategy, April 2018

implementing evidence-based interventions to address the root causes and mitigate the impact of violent incidents.

1.5 Following a consultation on this public health approach in 2019, the UK Government enshrined a new legal duty in law in 2022. The Duty mandates specified authorities to collaborate in implementing a public health approach to tackle serious violence in their locality. By doing so, local partners are required to share relevant information, utilise data-driven insights, and develop targeted strategies that address risk factors and promote protective factors within communities.

1.6 TVT stands as an early example of a partnership aimed at operationalising the Duty. While TVT only applies to the Thames Valley region (Berkshire, Buckinghamshire and Oxfordshire), the expectation is that similar partnerships will emerge across England and Wales to fulfil the requirements of the Duty. Some of following organisations ('TVT Partners') are involved in the TVT project:

- Thames Valley Police (the project lead);
- Ten local councils and social care organisations, including Bracknell Forest Council, Brighter Futures for Children, Buckinghamshire Council, Milton Keynes Council, Oxfordshire County Council, Reading Borough Council, Royal Borough Windsor & Maidenhead Council, Slough Borough Council, West Berkshire Council and Wokingham Borough Council;
- Regional Fire and Rescue Services;
- Regional Youth Offending Services; and
- HM Prison and Probation Service.

1.7 TVP was accepted into the Sandbox on 19 May 2022, and a bespoke Sandbox plan was developed and signed off on 27 September 2022. The objectives agreed as part of the plan were as follows:

- **Objective One** – TVP will complete a data mapping exercise to help inform early considerations of the different roles and responsibilities under the UK General Data Protection Regulation ('UK GDPR') and the Data Protection Act 2018 ('DPA 2018') for the organisations involved in the TVT project.
- **Objective Two** – TVP will assess the necessity and proportionality of the various personal data processing activities that form part of the TVT project, ensuring compliance with Article 5(1)(b) 'purpose limitation', Article 5(1)(c) 'data minimisation' and Article 5(1)(e) 'storage limitation' of the UK GDPR.
- **Objective Three** – TVP will produce a Data Protection Impact Assessment ('DPIA') ahead of the commencement of any live processing of personal data for the Sandbox to review.

1.8 The Home Office, as the UK Government department responsible for the PCSC 2022 and policing in England and Wales, attended some of the meetings between the Sandbox and TVP to explore the practical application of the Duty and discuss where the Serious Violence Duty Guidance[2] could be further developed in relation to data protection requirements.

2. Product Description

2.1 TVT is a cloud-based environment where specified authorities in the Thames Valley region can share relevant information to facilitate a public health approach that identifies the causes of serious violence and develops

[2] Serious Violence Duty Guidance – GOV.UK

targeted products designed to tackle them. A key characteristic of a public health approach is its population-level coverage. This means that a project or intervention aims to encompass and address the entire population, rather than targeting only specific groups. In the TVT context, population-level coverage is defined as including everyone who comes to the attention of a TVT Partner due to the indication of a serious violence risk factor(s). This approach recognises that focusing solely on people already associated with serious violence would be insufficient for effective intervention and prevention. By adopting a population-level strategy, the goal is to increase the chances of early identification and support, acknowledging that addressing underlying risk factors before people become victims or offenders is crucial in reducing serious violence.

2.2 The Home Office's Serious Violence Duty Guidance indicates some of the risk and protective factors associated with serious violence, drawing on research carried out by the World Health Organisation. This includes, but is not limited to, child abuse, learning disabilities, poor parental supervision and substance abuse. The TVT cloud-based environment serves as the mechanism to consolidate such data on risk and protective factors, which is spread across the various TVT Partners, into a centralised platform. Microsoft Azure ('Azure') was selected by the TVT Partners as the provider for the cloud-based environment.

2.3 TVP explained that the data sharing and product creation process would operate under the following framework: Each TVT Partner maintains a secure staging area accessible solely by them to share relevant data into the Azure cloud environment. TVT Partners will only share personal data from their respective agencies of people exposed to risk factors within the past six years. Each TVT Partner is responsible for identifying people involved in events indicating a risk factor and the data items relevant for sharing. Upon transferring data to the cloud environment, the data will be immediately deleted from the TVT Partner's staging area.

2.4 The TVT project team primarily consists of employees from TVP and vetted partners. The TVT project team have three distinct roles – 'developer', 'viewer' or 'researcher'. These are described below:

- Developer – The developer will use data ingested into the data environment, including some personal data, to create products designed to identify the causes of serious violence and tackle them. The developer role necessitates an elevated level of access within the cloud environment. As such, this role is subject to thorough vetting procedures and continuous monitoring of their activity.
- Viewer – The viewer will only see products created by a developer. Only viewers that have been vetted to a high level will have sight of products which contain personal data.
- Researcher – The researcher will carry out research into risk and protective factors. Their primary aim is not to build a product, rather to determine the effectiveness of the categories of data ingested into the cloud environment. The researcher will be subject to heightened supervision and auditing, particularly in cases where researchers are external to the TVT partnership or have access to personal data.

TVP explained that the TVT project is guided by the principle that as the volume of personal data increases, the total number of people with access to the data falls. This approach serves to minimise the potential risks associated with unauthorised access and unnecessary data retention. In alignment with this principle, any research undertaken aims to use the lowest necessary level of data to effectively address research inquiries. By default, research is conducted by the TVT project team. If this is not feasible, researchers are provided with synthetic data to work with, enabling them to produce code. The TVT project team will then run the code and share the outputs with the researchers at an aggregate level, thus maintaining strict control over access to personal data.

2.5 The primary purpose of the TVT project is to develop products that identify the underlying causes of serious violence and combat it with targeted interventions. Products are categorised at three Levels, as outlined below:

- Level One – information used to inform Strategic Needs Assessments ('SNAs') in order to understand local issues;

- Level Two – information used to identify hotspot locations and support a targeted approach;
- Level Three – information used to identify individuals at risk for high-intensive support programmes.

2.6 Level One products will aggregate risk and protective factors into geographical regions. Such views of the data are valuable for strategic planning, particularly aiding specified authorities in producing an SNA, which is a legal requirement under the Duty. A serious violence SNA is a process where local partner organisations work together to identify people who are at risk of experiencing serious violence, either as a victim or an offender. The insights gained from an SNA inform decision-making, enabling partners to agree on priorities and allocate resources. A Level One product may be included within some SNAs as supporting evidence.

2.7 The data within Level One products is anonymous and does not constitute personal data. Steps will be taken to prevent the possibility of identifying people. For example, TVP explained that in cases where counts of a specific risk or protective factor are low within a geographic area, the data will be supressed to a range of 1-10 rather than displaying the actual count.

2.8 Level Two products utilise the same data as Level One, but at a more granular level, such as postcodes and/or allowing unsuppressed counts of a particular risk or protective factor. As such, the data within Level Two products cannot be considered anonymous. Level Two products are primarily intended for professional consumption by specified authorities, aiding them in identifying and resolving risk factors at a location-based level, rather than at a person level.

2.9 TVP explained that they would not apply methods to suppress low counts of a risk or protective factor due to the perceived low risk of a person being identified. TVP acknowledged the theoretical possibility of re-identification if a person had access to an alternative source system (such as police or social care systems). For example, a Level Two product might present the crime details within a hotspot location, including the age band of the person

suspected of committing the offence. While this product on its own is unlikely to enable the person to be identified, a social care professional could use this information to carry out searches within their own system, potentially revealing more details. TVP explained, however, that the TVT product would not allow a person to identify any information they were not already entitled to access through their own source system.

2.10 Level Three products will include personal data to identify people who require targeted support or intervention, whether as potential victims or offenders of serious violence. TVP explained that the inclusion of personal data is required to match multiple records belonging to a person, providing a comprehensive and accurate depiction of the data, thus avoiding misleading insights or potential delays to intervention that could arise from using anonymised data. TVP clarified that access to personal data will be restricted to a small number of vetted developers during the development phase. Subsequently, access will be granted only to vetted professionals when the product is actively deployed to ensure the provision of high intensity support programmes.

2.11 One governance measure of the TVT project is the creation of its Data Ethics Committee, comprising legal and ethical experts from UK-based universities, Thames Valley community representatives, TVP's Independent Advisory Group, and subject matter experts on topics, including data protection, cloud computing and machine learning. The Committee's key function is to oversee and review products before they are deployed live, ensuring ethical considerations and legal compliance are upheld throughout a product's implementation.

2.12 In addition, the TVT project has a Programme Board which supports TVT Partners in fulfilling their responsibilities as joint data controllers. The Programme Board consists of representatives from all TVT Partners and also includes representatives from organisations in the process of joining TVT. At the Programme Board, products are tracked through all stages of the product lifecycle, and discussions are held regarding requests to alter a product's status. Decisions are formulised by means of amending the Information Sharing Agreement ('ISA') and the joint data controller agreement, which are signed by an authorised party from each TVT Partner.

3. Key Data Protection Considerations

3.1 TVP and the Sandbox considered a number of key data protection themes in relation to the development of TVT. Some of those key areas of consideration are outlined below.

Data Mapping

3.2 We understand that the processing for the purposes of TVT is likely to build on the existing processing carried out by specified authorities in the course of performing their services and functions as public sector organisations.

3.3 As such, in order to address Objective One of TVP's Sandbox plan (to establish the roles and responsibilities of the organisations involved under the UK GDPR and DPA 2018), we asked TVP to undertake a data mapping exercise which illustrated the lifecycle of the data, starting from its ingestion into the data environment to the development of products containing personal data. We provided TVP with advice on identifying the lawfulness of the processing and the importance of ensuring fairness and transparency. While the Duty permits the new processing from a conceptual standpoint, we queried whether people understood the practical implications. To address this, we emphasised the importance of TVT explaining the purpose of the new processing (to fulfil and operationalise the objectives of the Duty) to the public, the specific data required to fulfil the new purpose, and the parties involved in the data sharing at each stage.

3.4 Moreover, we emphasised the necessity of explaining how personal data would be utilised in creating products and which products themselves contained personal data. The description provided would need to be sufficiently detailed and granular to help people understand this complex data sharing project. Ensuring transparency is crucial in building trust and ensuring personal data is processed in line with data protection law.

3.5 Following our request, TVP submitted its Record of Processing Activity ('RoPA') to us which outlined the data flows for the TVT project. The RoPA also detailed the categories of personal data, the lawful basis and the special category data conditions for the processing, and indicated what personal data would be used for product creation and in the products themselves. The RoPA proved to be a valuable starting point, enabling us to identify several key questions and considerations. These insights served to facilitate more granular discussions on the development of TVT, which are explored below.

Roles and Responsibilities

3.6 There are a number of parties involved in the TVT project and it is important that each TVT Partner understands its role prior to the project commencing the processing of personal data.

3.7 TVP explained that the data environment processing is subject to a joint controllership arrangement, with TVP as the lead organisation. Each TVT Partner would maintain controllership over the data it processes whilst performing its service or function as a public body. However, when sharing the data with the Azure data environment, it would fall under the joint controllership arrangement.

3.8 It is important to note that most data sharing is covered by the general processing provisions under the UK GDPR and Part 2 of the DPA 2018. However, data sharing by a 'competent authority' (as defined in Schedule 7 of the DPA 2018) for specific law enforcement purposes is subject to a different data protection regime under Part 3 of the DPA 2018. Competent authorities are also likely to process personal data for general purposes under the UK GDPR/Part 2 DPA 2018, eg for Human Resources matters or other non-law enforcement purposes.

3.9 We recommended that TVP differentiated the processing under UK GDPR/Part 2 DPA 2018 and processing under Part 3 DPA 2018. We explained that as the UK GDPR/Part 2 DPA 2018 does not apply to the processing of personal data by a competent authority for any of the law enforcement purposes, UK GDPR/Part 2 DPA 2018 joint

controllership agreements do not apply to Part 3 DPA 2018 processing. Similarly, Part 3 DPA 2018 joint controllership arrangements apply only where "*two or more competent authorities jointly determine the purposes and means of processing personal data*". This means that an organisation that is not a competent authority, or does not process personal data under Part 3 DPA 2018, cannot be designated a joint controller for law enforcement processing.

3.10 TVP clarified in their second DPIA[3], sent to us on 11 July 2023, that the joint controllership arrangement only applies to the UK GDPR/Part 2 DPA 2018 processing within the data environment. No equivalent arrangement exists, or needs to exist, to satisfy Part 3 DPA 2018 for two reasons. Firstly, TVP explained that no Part 3 DPA 2018 processing occurs in the data environment. While some specified authorities under the Duty are also designated as competent authorities under Schedule 7 of the DPA 2018 (eg TVP), and will share data into the data environment originally processed under UK GDPR/Part 2 DPA 2018 **and** Part 3 DPA 2018, any Part 3 DPA 2018 data is repurposed to become UK GDPR/Part 2 DPA 2018 data when it is shared with the data environment. Further information on repurposing data between the two data protection regimes can be found in our data sharing code of practice hub.

3.11 Secondly, TVP explained that once a TVT Partner has received a product, they will then go on to deliver interventions and services as a sole controller under the appropriate data protection regime for their public function. TVP acknowledged that in some limited cases Level 3 products may constitute, or result in, policing interventions which require the processing to occur under Part 3 DPA 2018. But this would happen outside the TVT project and would be limited to circumstances where the personal data indicates a risk to a person that

[3] TVP submitted its first DPIA for the TVT project to us on 31 January 2023. Following our review of the first DPIA, we agreed to review a second iteration of the DPIA. This second review further considered the joint controllership arrangement and the data protection regime to which it applied.

requires an immediate intervention to avoid serious harm. Following TVP's explanation, we agreed with the designation of the TVT Partners as joint controllers only under UK GDPR/Part 2 DPA 2018.

Necessity and Proportionality

3.12 Objective Two of the Sandbox plan required TVP to consider data minimisation in relation to the personal data that is expected to be processed by the TVT project. The data minimisation principle is set out in Article 5(1)(c) of the UK GDPR. It states that "*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)*". Accordingly, as set out in our guidance, TVP must ensure that the personal data the TVT project processes is:

- adequate – sufficient to properly fulfil TVT's stated purposes;
- relevant – it should have a rational link to those purposes; and
- limited to what is necessary – TVT should not process more personal data than it needs for its purposes.

3.13 The UK GDPR does not define the terms adequate, relevant and limited to what is necessary. These must be assessed on a case-by-case basis, taking into account the relevant circumstances. Therefore, we advised TVP that they would need to fully understand the context within which TVT is intended to operate. TVP will also need to explain the reasons why personal data will be processed and how this links to its purposes for processing to ensure TVT is only processing the personal data it actually needs in that context.

3.14 Discussions with the Home Office confirmed that it would be the responsibility of local partnerships to determine the personal data that would be necessary to achieve the objectives of the Duty. In light of this, the Sandbox and TVP worked together to determine the categories of data necessary for identifying and mitigating risk factors associated with serious violence. For example, we emphasised to TVP the importance of granularity; ie

interrogating the necessity and effectiveness of each data item's contribution. We also recommended that ingested data should undergo regular reviews to ensure its ongoing relevance and that special consideration was awarded to the inclusion of data relating to victims and children.

3.15 TVP submitted its first DPIA for the TVT project to us on 31 January 2023. Considered alongside the RoPA, these documents detailed a large data sharing project with an approach of reducing excess data items over time when they are shown to be unnecessary. In our written steer, provided on 3 May 2023, we advised that a 'process all and scale back' approach was likely to run contrary to the data minimisation principle. Our guidance on the principle emphasises that controllers must not collect personal data on the off chance that it might be useful in the future. As such, we recommended that TVP carried out further analysis on the categories of personal data to be ingested into the Azure cloud environment.

3.16 TVP carried out this further analysis to find that only 30% of data items were useful for inclusion within TVT and the development of its products. As a result, TVP's second DPIA stated that the remaining 70% of data items originally proposed for inclusion were removed from the TVT project altogether. We advised TVP to continue regularly reviewing the categories of data and ensure its RoPA is updated to reflect any amendments.

3.17 TVP advised that it was necessary to process the data of victims and children because a comprehensive and accurate picture of the risk factors could not be obtained without their data. When assessing the necessity of children's data in particular, which requires additional protection and justification for use under the UK GDPR, TVP highlighted that the Serious Violence Strategy indicates that the majority of the known risk factors for involvement in serious violence affect people during childhood. Factors such as imprisonment of a parent or growing up in a community affected by violence can have significant impacts during childhood and persist into adulthood. TVP explained that the inclusion of such data would enable TVT to develop effective interventions and preventative measures. We agreed with TVP's assessment that the data of victims and children is likely to be

necessary for inclusion in the TVT project. However, we emphasised the importance of implementing appropriate controls on all personal data in the data environment.

3.18 TVP acknowledged and accepted the recommendations we provided in respect to data minimisation. Notably, TVP agreed to reduce the originally proposed annual reviews of data items into the data environment to six-monthly reviews. This increased frequency will enhance the project's ability to assess data relevancy and eliminate any unnecessary data. Additionally, it will help the project to demonstrate compliance with the storage limitation principle. The Sandbox believes that our collaboration with TVP has contributed to minimising potential data protection risks, whilst not compromising the development and objectives of the TVT project.

3.19 On a related point, we asked TVP to clarify the rationale behind the six-year retention period for personal data within the TVT project and advised them to avoid blanket retention schedules. TVP indicated that the decision to retain data for six years was aligned with a policing industry standard – Management of Police Information ('MoPI'). According to MoPI, certain types of offences (eg non-violent and non-sexual) require a retention period of six years[4]. However, as MoPI does not apply to all organisations within the TVT project, we recommended that TVP carried out additional work to justify the necessity of TVT's proposed retention period.

3.20 TVP has since explained that it will design functionality to deliver a more granular approach to data deletion, so that all personal data is retained for no longer than necessary. In particular, the design will optimise opportunities to delete children's data at the earliest opportunity.

3.21 Notwithstanding the Duty mandating specified authorities to develop strategies that reduce serious violence, we asked TVP to assess whether the TVT processing would be compatible with TVT Partners' original processing

[4] Review, retention and disposal ('MoPI') – College of Policing

purposes. TVP conducted an assessment, explaining that the secondary processing aims to analyse risk and protective factors related to serious violence. By aggregating data, products could be created that would enable earlier identification of potential issues, ultimately improving the health of communities within the Thames Valley region. TVP determined that the secondary processing was compatible because it built on the original and existing processing practices of TVT Partners, which include providing outreach services, supporting children in school and improving community facilities.

Transparency

3.22 The UK GDPR requires controllers to be transparent with individuals about what they do with their personal data. Articles 13 and 14 specify the types of information that need to be provided to individuals ('privacy information'). Article 12 specifies how the privacy information detailed in Articles 13 and 14 is communicated to data subjects.

3.23 TVP acknowledged that people may not expect their personal data to be shared with the TVT project. As people have a specific 'right to be informed' about what is happening with their personal data, the Sandbox and TVP worked together to explore what communication strategies could be deployed to ensure that people are aware of the TVT processing. We recommended that communication strategies extended beyond a single privacy notice for TVT, as a single notice would not be likely to reach all data subjects. Given the nature and scale of the data sharing involved, we advised adopting a multi-faceted approach in providing privacy information. We also expressed that particular attention and consideration should be afforded to providing privacy information to children.

3.24 Given that a substantial portion of the personal data processed in the TVT project is anticipated to come from organisations, rather than from the person whom the personal data concerns[5], we highlighted an important consideration relating to the use of the disproportionate effort exception, as found in Article 14(5)(b). This exception allows controllers to be exempted from providing privacy information to people when it is deemed impossible to do so. As a general rule, disproportionate effort should not form a blanket approach. We recommended that TVP carried out further work on this, specifically exploring an approach where each TVT Partner takes responsibility for informing people with whom they have a direct relationship about the TVT processing. Where TVP and their partners consider that informing people about the processing would involve genuine disproportionate effort, the rationale behind this decision should be documented and efforts must still be made to inform people via indirect means.

3.25 Following our recommendations, TVP agreed that TVT Partners would implement the following:

- Regularly update the TVT privacy notice;
- Refer to the TVT processing in their organisation's existing privacy notices;
- Make information available about the TVT project to the people that use their service by increasing messaging and touch points;
- Hold public engagement events with target audiences, particularly children;
- Publish news items periodically and promote work on local television and radio; and
- In cases where Level 3 products are developed, inform the person about how their personal data was

[5] Article 14 of the UK GDPR relates to the provision of privacy information where personal data has not been obtained from the data subject.

obtained, what personal data was used and why.

3.26 TVP considered that the above actions would likely reach a significant proportion of the Thames Valley population. TVP added that where disproportionate effort did genuinely occur, TVT Partners would document their rationale.

Data Protection Impact Assessment ('DPIA')

3.27 In order to address Objective Three, TVP submitted its first iteration of its TVT DPIA on 31 January 2023. A DPIA must be carried out when the processing of personal data is "*likely to result in a high risk to the rights and freedoms of natural persons*" and it must be carried out before that processing begins. As part of this objective, we provided verbal steers to help TVP develop its DPIA, particularly in relation to data minimisation, purpose limitation and storage limitation. We provided written feedback on the DPIA on 3 May 2023. TVP submitted its second, updated DPIA on 11 July 2023. Below are some of the additional areas where we provided support to TVP.

Governance

3.28 We considered that the first DPIA was not sufficiently detailed when describing the governance processes. One recommendation we made was for each TVT Partner to include an addendum to the main TVT DPIA. While we recognised that a central DPIA could cover the processing activities under the joint controllership arrangement, we suggested that each specified authority should include a reference to their own processing activities. For example, they should outline their approach in determining which personal data items should be shared with the data environment, the measures taken to ensure accuracy, how access to the staging area is decided and controlled within their organisation, and their plans for sharing privacy information with people.

3.29 Additionally, we recommended updating the first DPIA to include the role and responsibilities of Microsoft Azure. This update should include reference to a data processing agreement, details about security measures, and use of privacy-enhancing technologies ('PETs') that are in place. In the second DPIA, we also observed the inclusion of the Ordnance Survey and the Office for National Statistics as suppliers of data to the Azure cloud environment. We advised that their roles should be outlined in greater detail, especially if the data they supplied constituted personal data or could contribute to identifying a person.

3.30 On a related point, we highlighted the importance of providing greater explanation of the access controls within the TVT project. This includes accounting for which employees have access to personal data, expanding on the vetting processes involved, and clearly outlining the procedures for handling access when employees of specified authorities join and leave the project.

3.31 TVP has since explained that they have conducted a further review of their governance processes and documentation. As a result, TVP has streamlined the TVT governance documentation by consolidating TVT's ISA, joint data controller agreement and DPIA into a single information package. TVP explained that this consolidation is designed to improve the support provided to individuals responsible for making decisions regarding the use of personal data within the TVT project.

Identifiability

3.32 In our early discussions with TVP, Level 2 products were initially considered by them to include anonymous data and therefore not regarded as personal data. However, based on the feedback provided in both verbal and written reviews, we recommended that Level 2 products should be treated as personal data. This decision was driven by the fact that low counts of the data would not be suppressed to numerical ranges, as seen in Level 1 products. Furthermore, we flagged that theoretically the data could be cross-referenced with alternative source systems

available to employees of specified authorities, thus potentially leading to the identification of a person. Following our feedback, TVP updated its DPIA and determined that Level 2 products were within the scope of the UK GDPR.

3.33 We also asked TVP to provide use cases and diagrams of Level 1, 2 and 3 products to visually represent how these products would work in practice. We understand that most of the products are still in development, but TVP was able to produce diagrams and use cases of Level 1 and Level 3 products in their updated DPIA. These examples serve as useful illustrations of the data processing journey; encompassing data collection, sharing, matching, analysis, and the development of products with the ultimate goal of reducing serious violence. Therefore, we recommend that once Level 2 products are developed, similar use cases and diagrams are added to the DPIA.

Accuracy

3.34 We advised TVP to provide more detailed information on how ingested data would be accurately matched within the data environment, with a particular focus on ensuring records are up-to-date and free from duplication. To address the data quality point, TVP implemented a new process to handle duplicate data, which involves reporting the issue to the TVT Partner that supplied the duplicated data. Additionally, TVP explained that TVT Partners would share data daily to ensure the most up-to-date data was being used. With the combination of a more frequent review period (six-monthly), TVP considered that risk of data inaccuracies, and consequently any delays in interventions aimed at those with greatest need, would be low.

Risk Assessment

3.35 We recommended that the first DPIA set out a more comprehensive identification of risks. This included further consideration of risks linked to storage limitation, purpose limitation, accuracy and identifiability. We also advised TVP to utilise a risk scoring matrix, as it is a valuable tool for evaluating and mitigating risk. A matrix acts as a

visual aid and can assist TVP in explaining the risks to its partner agencies. We understood that the absence of a risk matrix resulted in some anomalies within the first DPIA's risk assessment. An example of a risk matrix can be found in our DPIA support page.

3.36 In addition to identifying additional risks, we provided feedback on the risks TVP had already identified and suggested further mitigations. These included implementing robust governance arrangements, enhancing the delivery of privacy information, and ensuring data minimisation measures were in place.

3.37 It is important to highlight that the feedback we provided regarding the risk assessment was not exhaustive. As is the case with all DPIAs, they should not be viewed as one-off exercises because new risks may emerge as a project evolves. We also informed TVP that after the implementation of mitigations, should any processing which would result in high risks remain, they must consult us before any processing of personal data begins.

4. Ending Statement

4.1 TVP's participation in the Sandbox has been instrumental in understanding the challenges faced by organisations tasked with delivering complex data sharing projects. Through this engagement, we have witnessed the benefits of implementing 'data protection by design and by default' during a project's conceptual phase. By collaborating with the Sandbox, TVP had the opportunity to assess the balance between ensuring necessity and proportionality of the processing on the one hand, and delivering on the objectives of the Duty on the other. Together, we identified and addressed risks associated with the TVT processing to minimise its impact on people, and developed communication strategies to inform people about the processing. Sharing personal data responsibly and transparently is vital in building public trust.

4.2 Describing the Sandbox as a 'critical friend', TVP expressed the value they found in engaging with the Sandbox. TVP highlighted that our engagement enabled them to confidently address the more complex aspects of the TVT project and to ultimately design the project in a way which is privacy-friendly. TVP acknowledged that without the support from the Sandbox, significant changes might not have been implemented as swiftly, and these changes have notably enhanced the project. TVP believe that the insights gained from our collaboration will serve as valuable lessons for its future work and also emphasised that these lessons will help other partnerships to fulfil their obligations under the Duty.

4.3 Likewise, the Sandbox hopes that other local partnerships tasked with delivering on the objectives of the Duty will find the lessons from TVP's participation in the Sandbox useful. We also wish TVP and their partners success in the implementation and delivery of TVT, and hope that it will go on to achieve the aim of reducing serious violence.