Regulatory Sandbox Final Report: Crisis UK

A summary of Crisis UK's participation in the ICO's Regulatory Sandbox

Date: July 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 Crisis UK ('Crisis') is the national charity for people experiencing homelessness, providing vital help so that people can rebuild their lives and are supported out of homelessness for good. Crisis uses research to determine strategies for enhancing its services and discovering solutions to combat homelessness.

1.4 Crisis entered the Sandbox as the lead organisation in a consortium with representatives from homelessness services in local authorities, working together as part of the Countrywide Homelessness Data Development Working Group. This group has a broad objective of developing and delivering county-wide data sharing to support the prevention and relief of homelessness.

1.5 Crisis believes that the creation of a By-Name-List ('BNL') would assist materially in meeting this objective. A BNL is a real-time list of all known people experiencing homelessness in a pre-defined geographical area. The BNL

method has been developed and used in the US, Canada, and Australia as part of the 'Built For Zero' model[1] for ending homelessness. Crisis intends to develop this model for a UK homelessness context.

1.6 Oxfordshire was selected as the use case for the BNL, and it served as the focus for the Sandbox work. Crisis led the work in the Sandbox as the organisation with the expertise in homelessness (and homelessness data), with the intention that the BNL would be a product and service owned and delivered by local authorities. The other parties involved in the Sandbox project included:

- Oxford City Council;
- Cherwell District Council;
- South Oxfordshire District Council;
- Vale of White Horse District Council;
- West Oxfordshire District Council;
- Oxfordshire County Council; and
- Oxfordshire Homelessness Alliance.

1.7 Crisis was accepted into the Sandbox on 13 January 2022, and a bespoke Sandbox plan was developed and signed off on 11 April 2022. The objectives agreed as part of the plan were as follows:

[1] 'Built For Zero' is a national change movement/initiative where local areas are invited to sign up to be part of a national network of communities committed to ending homelessness.

- **Objective 1** - Crisis will seek to establish the different roles and responsibilities under the UK GDPR for the organisations involved in the proposed processing. Crisis will also establish which lawful bases may be available for the proposed processing under Article 6 of the UK GDPR and will seek to identify appropriate conditions for processing special category data under Article 9 of the UK GDPR.
- **Objective 2** - Crisis will explore whether personal data can be 'pseudonymised' and/or 'anonymised' and used for research purposes.
- **Objective 3** - Crisis will explore the data protection risks posed by the data sharing and implement a 'data protection by design and default' approach.

1.8 During the Autumn of 2022, it was confirmed that due to capacity constraints, the Oxfordshire local authorities were unable to engage with the Sandbox on the BNL project at that time. As such, instead of reviewing a DPIA co-authored by Crisis and the Oxfordshire local authorities, we agreed to review template documentation, developed by Crisis, to support Crisis in reaching a position where it could advocate for the use of BNLs and support local authorities in delivering them in the future.

2. Product Description

2.1 The concept behind the BNL is to account for every person experiencing homelessness in an area by means of a real-time[2] list, thereby enabling insight into the inflow (those entering homelessness, either newly identified or from housing) and outflow (people housed or leaving the area) of homelessness. To populate the BNL, personal

[2] 'Real-time', in this context, means that the data will be regularly updated.

data is collected from a number of contributors, including from organisations acting within commissioned and non-commissioned services[3]. Contributors acquire data directly and indirectly from people in the course of performing their service.

2.2 Crisis explained that the BNL dataset is usually stored by a nominated local authority. This authority stores the data centrally and shares it with organisations involved in a data sharing partnership ('DSP'). Access to the data is controlled by the nominated local authority, through dedicated control mechanisms that consider the organisation's role and the necessary information for their specific purposes.

2.3 The BNL uses a unique identifier to ensure the accuracy of the data and allow deduplication across data provided by different contributors. The BNL aims to improve data reliability and engagement with homeless people, for example, by limiting the number of times a person experiencing homelessness provides the same information.

2.4 We understand that the BNL dataset may include data such as:

- unique identifier;
- given name or nickname;
- physical description of a person;
- geographic location(s) where a person has been seen;
- their current housing situation;

[3] 'Commissioned', in this context, means that the organisation has been funded by a council to provide homelessness services, whereas 'non-commissioned' means that the organisation provides homelessness services, but has not been funded by a council to do so.

- which organisation is working directly with them;
- their date of birth/age;
- gender;
- whether someone identifies as LGBTQ+;
- ethnicity;
- total time spent homeless; and
- number of times homeless previously.

2.5 The possible sources of personal data that will be used to populate the BNL with this information are as follows:

- Personal data sourced from and shared between organisations who form a DSP ('Shared Data').
- Personal data sourced from and submitted directly to the BNL by organisations outside the DSP.

The DSP

2.6 Crisis envisages that the BNL dataset would only be shared with (ie be made accessible to) the organisations which make up a DSP. We understand that the DSP is likely to consist of a lead nominated local authority, other local authorities, and some commissioned non-profit organisations including charities. These organisations will engage directly with people experiencing homelessness through services and outreach work. These organisations may hold records of people that they are already supporting, which may include personal data beyond the scope of the BNL dataset as set out above. These records may also form part of the Shared Data.

Outside the DSP

2.7 It is our understanding that organisations outside the DSP may also share personal data with members of the DSP for the purpose of adding personal data to the BNL. We understand these organisations may include those with a 'Duty to Refer' under the Homelessness Reduction Act 2017[4]. These include prisons, young offender institutions, secure training centres and colleges, probation services, jobcentres in England, adult and children social services, emergency departments, hospitals providing inpatient care and the Secretary of State for Defence in relation to members of the regular armed forces.

2.8 Other organisations outside the DSP, but without a statutory Duty to Refer, may also share personal data with members of the DSP to help the operation of the BNL. These organisations may include non-commissioned non-profit organisations, charities (eg drug and alcohol charities), housing associations and family services. It is envisaged that local businesses, religious and community groups, and members of the public may also share personal data with members of the DSP via StreetLink[5], so that it can form part of the BNL dataset.

2.9 Different services will have different permissions and access to the dataset, based on their role, ie some will be able to add people to the BNL, whereas others will be able to update information on people already on the BNL. It is our understanding that members of the DSP will have full access to the BNL dataset, and organisations outside the DSP will not be able to access or view the BNL dataset.

[4] A guide to the duty to refer - GOV.UK (www.gov.uk).
[5] The 'StreetLink' project enables members of the public to connect people experiencing homelessness with local services that can support them. We did not provide feedback relating to the StreetLink project or its role with the BNL.

3. Key Data Protection Considerations

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

Data Mapping

3.2 We understand that the processing for the purposes of the BNL is likely to build on the existing processing carried out by local authorities in the fulfilment of their statutory functions to reduce homelessness.

3.3 As such, in order to address Objective 1 of Crisis' Sandbox plan, to establish the roles of the organisations involved and to understand the lawful bases and conditions for processing, we asked Crisis to undertake a data mapping exercise which illustrated the existing ways relevant personal data is processed by local authorities expected to form a DSP. In addition, we asked Crisis to examine how the processing for the BNL would differ from current arrangements.

3.4 Following our request, Crisis submitted a data map to us outlining the flows of personal data for the different organisations involved and a 'data dictionary' which described the categories of personal data for both the existing and proposed processing. These documents were developed with the input of Oxfordshire County Council and included an analysis of the lawful bases that could be appropriate for the BNL processing.

3.5 Crisis considered that the members of a DSP would act as joint controllers for the BNL dataset processed via the DSP because of their shared purpose and objective of addressing and reducing homelessness. All members of the DSP would also have access to the BNL dataset.

3.6 Crisis determined that organisations outside of the DSP, sharing data with the DSP for the purposes of the BNL, would act as independent controllers in relation to personal data that they processed for their own purposes.

3.7 Upon reviewing Crisis' documentation, we identified several key questions and considerations that aimed to facilitate more granular discussions on the development of the BNL processing with Oxfordshire County Council ('OCC') and the Countrywide Homelessness Data Development Working Group. These considerations focused on how personal data is collected from people experiencing homelessness, how people exercised their rights, how data is shared and the nature of the privacy information.

Compliance Documentation

3.8 In order to address Objective 3, to assess the data protection risks posed by the BNL, Crisis, in partnership with Oxfordshire County Council, submitted a Data Protection Impact Assessment ('DPIA') to us on 3 May 2022 for our review.

3.9 We provided recommendations on the DPIA template OCC used, advising on improvements that could be made for the purposes of the BNL. This advice included providing greater detail on the data protection principles, joint governance arrangements, data subject rights, and any public consultation work carried out in relation to new projects.

3.10 Furthermore, we recognised that the DPIA suggested minor changes to a system ('OxTHINK') already in use by OCC, whereas the data maps appeared to present a systemic change in the way local authorities and other organisations would tackle homelessness. We recommended that any disconnections between the documents were addressed.

3.11 As a result of OCC taking a step back from the BNL project in the Autumn of 2022, Crisis decided to concentrate on how local authorities could implement the BNL processing on a more conceptual basis. Crisis would then be able to support local authorities that it works with on how to deliver their own BNLs in the future.

3.12 Crisis submitted a number of template documents to the ICO for review. These were: a data sharing framework, template privacy notices for organisations inside and outside the DSP, a template consent statement for adding personal information to the BNL, a template information sharing agreement, a template purpose compatibility assessment for adding Shared Data to the BNL, and a template data protection impact assessment.

3.13 As the submitted documentation was in template form, reflecting conceptual processing activities, there was, understandably, a certain amount of specificity lacking in the documents. We advised Crisis that we were unable to confirm or provide assurance that the use of the templates would, in practice, discharge a local authority's controller obligations under the UK GDPR. As such, we provided general recommendations in relation to the documentation and explained that, should a local authority use the templates created by Crisis, they would need to be tailored to suit the specific circumstances of that local authority.

3.14 We also explained that the local authorities and organisations participating in a BNL would be under no obligation to use the templates developed by Crisis, and could seek to comply with UK GDPR requirements as they found appropriate, in accordance with their own legal advice and the wider data processing activities they engaged in.

Privacy Notices

3.15 The UK GDPR requires controllers to be transparent with people about what they do with their personal data. Articles 13 and 14 of the UK GDPR specify the information that needs to be provided ('privacy information'). Crisis provided two template privacy notices for us to review. One was intended for use by organisations *within* a DSP to provide to people from whom they collect personal data that will be added to the BNL. The other privacy notice

was developed for use by organisations *outside* of a DSP to provide to people from whom they collect personal data that will be shared with the DSP, for the purposes of the BNL.

3.16 We did not comment on compliance with the specific requirements of the UK GDPR, as the privacy information was in template form (and not linked to particular data processing activities). However, we suggested areas in which further clarity and detail would assist. Some of these areas are set out below.

3.17 In relation to the privacy information that would be provided by the organisations within the DSP, we advised that the explanations of the purposes of processing were likely to be unclear to people. Privacy information should provide specific information about how personal data will be used. We noted that Article 6(1)(e) 'public task' was suggested as a possible lawful basis. Although we did not consider whether 'public task' would be appropriate for the purposes of the BNL, we advised that, where 'public task' is relied upon, the applicable tasks, functions, powers, or basis in law under the homelessness legislation would need to be set out by the relevant controller.

3.18 We also advised on Article 12 of the UK GDPR, which specifies the requirements around how privacy information should be communicated to people. In the context of the BNL processing, it may be appropriate for privacy information to be provided verbally in some circumstances. Crisis indicated that, where required, they would work with relevant controllers to develop scripts appropriate to their planned processing activities.

3.19 In relation to the privacy information that would be provided to people by the organisations outside of the DSP, Crisis identified two possible lawful bases that could be relied on by these services, Article 6(1)(a) 'consent'[6] and Article (6)(1)(f) 'legitimate interests'. Where organisations intend to rely on legitimate interests, they should

[6] The challenge of using Article 6(1)(a) 'consent' as a lawful basis in the context of the BNL processing is outlined in detail at 3.34 of this report.

conduct a 'legitimate interests assessment' which should establish the necessity of the processing and balance the interests of the organisation against those of the individual.

3.20 We advised that it would be important for the organisations utilising the templates to tailor the information to their particular circumstances, and to ensure they reflect the relevant processing activities adequately and appropriately.

Information Sharing Agreement ('ISA')

3.21 Crisis drafted a template ISA to assist with the development of a more complex data sharing agreement between the members of a DSP (joint controllers) and the organisations outside a DSP (independent controllers).

3.22 We advised that the template agreement should be used as a starting point, and any data sharing agreement which is entered into in connection with the BNL would need to be tailored to the specific circumstances, with specific legal advice sought by each of the parties to ensure that the agreement is accurate.

Data Protection Impact Assessment ('DPIA')

3.23 Crisis shared a template DPIA with us on 16 September 2022, which they intend for members of the DSP to populate in relation to the creation and use of a BNL. As the DPIA was provided in template form, we advised that it would need to be amended to reflect the specific policies and governance processes of the relevant controller(s) carrying out the assessment. Although it would be the responsibility of the members of a DSP to ensure that their DPIA is populated with sufficient granular detail and the relevant context of individual processes, there were a number of additions that we recommended to improve the template. Some of these recommendations are set out below.

3.24 The template outlined why there is a requirement for a DPIA (ie sharing special category data, and processing data concerning people who need extra support to protect themselves). As per the list of processing operations published by the ICO in accordance with Article 35(4) UK GDPR, a DPIA should also be carried out where there is an intention for data to be combined, compared and matched from different databases. As such, we advised Crisis and the other controllers to consider how they can engage in the matching of data from multiple sources in a way that is necessary and proportionate.

3.25 The DPIA template stated that: *'The DSP will be processing Shared Data to discharge statutory functions and the lawful basis is Public Task.'* We explained to Crisis that, as the DSP is not a separately constituted entity, it cannot act as a controller. Instead, each member of the DSP would act as a joint controller with the other parties that make up the partnership. Consequently, Crisis was advised that the template should clarify that any lawful basis and statutory functions relate to each controller, rather than the DSP as a whole.

3.26 The template lacked information about the role and purpose of a BNL. Additionally, a description of how assets would be relied on for any processing and storage of data was absent (eg the document management system used by the DSP members or if cloud storage would be used), as well as an absence of any recommended technical measures to be employed to mitigate security and confidentiality risks. We also recommended the addition of specific deployment elements within the template DPIA, such as the scope of the processing, geographic area, number of people likely involved, and the definition of 'real-time'. Whilst Crisis may not have prior knowledge of these areas ahead of working with a specific local authority, we recommended the inclusion of these fields within the template DPIA to prompt controllers to include this information.

3.27 Crisis was also advised to amend the template to allow data controllers to include further information about whose data will be collected and how. Controllers are expected to consider whether the data they collect is from a demographic at need of support and assess whether this restricts their ability to object or freely consent to the

processing of their data. One way to assess this is by conducting a risk assessment which includes a process that enables people to exercise their rights under data protection law. The template DPIA should clearly reference this risk assessment.

3.28 We recommended expanding the space within the template DPIA to allow for a more detailed assessment of the necessity and proportionality of the BNL processing. We considered that participant organisations should outline the benefits of the processing for the people experiencing homelessness, the organisations themselves and the public/society as a whole. Organisations should also include a description of any alternative, less intrusive methods that have been attempted to address the problem they are looking to solve, along with an explanation of why these methods did not fulfil the intended purpose. Furthermore, we advised that the template DPIA should provide additional clarification on the specific items of personal data that are deemed necessary for the purpose of the processing. It should also evaluate whether it would be proportionate to share all of the proposed data fields with all parties involved, taking into account the data minimisation principle.

3.29 The template DPIA included references to 'criminal offence data'. It was unclear what data shared with members of the DSP would be considered criminal offence data. We understand that such data would not be specific, but a person's offending background could be inferred from referrals to the DSP from prisons or the probation service (or other organisations outside of the DSP which are involved in the criminal justice system). In order to assess the risk further in the DPIA, we advised that the controller(s) analyse the nature and content of such referrals. The controllers should also consider whether they have official authority to process criminal offence data. If they do not, they would need to identify a specific condition for processing in Schedule 1 of the DPA 2018 and, if they cannot, this information should not be shared with members of the DSP. Crisis was advised to update the template to reflect this.

3.30 Crisis identified 12 generic sources of risk within the template, but there was no assessment of the likelihood or severity of these risks. We acknowledged that it would be the responsibility of the controllers to amend and add to the risk assessment, depending on their specific processes, the technology and assets they use, and the data protection maturity of the organisation. We advised that Crisis could provide additional guidance or a worked example (clearly marked as guidance) to demonstrate the level of detail expected. We also recommended that the risk assessment should place more emphasis on the individual harm that could result from the processing, given the potential vulnerability of the people that would be involved. For example, an inappropriate disclosure or loss of information about a person who has become homeless due to escaping an abusive living situation could potentially result in significant physical or emotional harm.

Purpose Compatibility Assessment

3.31 Crisis developed this template to assist members of a DSP who already hold and share personal data, to establish whether their existing purposes were compatible with further processing as part of a BNL. Essentially, the template explored whether personal data collected for a separate specified purpose could be legitimately included within a BNL.

3.32 The 'purpose limitation principle', under Article 5(1)(b) of the UK GDPR states that "*personal data must be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes…*". We advised Crisis that personal data may be used for a new purpose where: the purpose that it is originally collected for is compatible with the new purpose; an individual consents to the new processing; or where there is a new clear legal provision allowing for the new processing in the public interest.

3.33 We found that the template purpose compatibility assessment followed the format of the ICO's template legitimate interests assessment, which helps to assess compatibility. However, we were not able to provide specific feedback on the assessment in the abstract, given that each assessment would always be fact dependent.

The Challenge of 'Consent'

3.34 Crisis indicated that some organisations outside of a DSP were likely to prefer relying on consent for the collection of personal data from people due to a number of factors, including the notion that consent was the only appropriate means of sharing personal data. We flagged with Crisis that consent was not always the most appropriate lawful basis to rely on. As a result, we agreed to provide a steer to Crisis outlining some of the possible challenges for these organisations in obtaining and managing consent as a lawful basis under UK GDPR.

3.35 As we do not have visibility over the underlying processing activities involved in creating and maintaining the BNL, the steer provided was intended to provide high-level commentary and highlight some general considerations and challenges that controllers should take into account when assessing whether consent is an appropriate lawful basis (or, if explicit consent, special condition) for the processing of personal data for the purpose of establishing and maintaining the BNL.

3.36 Article 4(11) of the UK GDPR describes 'consent' as "*any freely given, specific, informed and unambiguous indication of a 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*". Article 7 specifies additional conditions when relying on consent as a lawful basis under Article 6, or explicit consent as a special condition under Article 9. This includes a controller demonstrating that the person has consented to the relevant processing activities, eg by way of an audit trail and maintaining records, that consent to one processing activity is clearly distinguishable from other matters, and that consent can be easily withdrawn.

3.37 Where consent is difficult to obtain or maintain, there may be an alternative lawful basis that is more appropriate for a controller's purposes. Consent is only likely to be the most appropriate lawful basis if the controller wishes to, and in practice can, provide genuine choice and control to the person in relation to how their personal data is

processed. We posed a number of questions to Crisis to guide their discussions about consent in relation to the BNL processing:

- Does consent provide genuine control to the individuals?
- Is the personal data subsequently processed under an alternative lawful basis (other than consent)?
- Will personal data still be processed, even if a person withdraws their consent?
- Can controllers build trust and provide transparency without obtaining consent? (Through the provision of comprehensive privacy information)
- Is consent genuinely required? Is the consent "freely given"? How is consent withdrawn?
- Is the consent "specific and informed"? Is the consent unambiguous? Is the consent explicit?

3.38 In the context of the BNL, there may exist an imbalance of power between the organisations collecting personal data and providing a much-needed service on the one hand, and the people relying on these services to secure safe accommodation/housing on the other. Where people feel unable to consent without detriment (eg losing access to housing services), the consent is unlikely to be valid as it will not be considered freely given.

3.39 Although it is our understanding that the organisations involved in the BNL processing are eager to maintain trust with the people they are obtaining the personal data of, consent may not, in practice, provide the person with a greater degree of control over the processing. In addition, reliance on consent does not automatically mean the controller discharges its transparency obligations more effectively. It is important to remember that controllers remain subject to general transparency obligations to inform people in relation to all processing activities,

regardless of lawful basis. Organisations can still build trust with people without seeking to obtain consent, for example, through providing clear and effective privacy information.

3.40 Crisis developed a template consent statement for the organisations outside of a DSP to use and to provide to people where they choose to rely on their consent to process and share their personal data with members of the DSP for the purposes of the BNL. It should be noted that this consent form would be optional, and organisations could choose to comply with the conditions of UK GDPR consent in their own way.

3.41 We advised that the template lacked sufficient detail on what the person would be consenting to and the purposes of the processing. Consent requests as a minimum should include: the name of the organisation requesting consent and other controllers relying on this consent, the purposes for processing, details of processing activities and the option for people to withdraw their consent at any time, including the process to do this. Controllers must find a balance between ensuring that the detail for a person to consent is specific enough, whilst also ensuring the request is as concise and easy to understand as possible.

3.42 Crisis explained to us that some organisations outside of the DSP are likely to seek consent from people in order to share their contact details with members of the DSP. Subsequently, the DSP members would rely on the 'public task' lawful basis to process the personal data (ie to include the personal data in the BNL). We advised that a person subject to this data sharing practice would have limited control over their personal data once it formed part of the BNL. For example, if a person chose to withdraw the consent they provided to a non-DSP organisation, they could only do so to the extent that their personal data had not already been shared with members of the DSP. If their personal data had already been shared with members of the DSP (and incorporated into the BNL), the person's withdrawal of consent would be, in practice, ineffective. We advised that it was likely to be misleading to seek consent from a person in these circumstances.

Explicit Consent

3.43 Crisis also intended for a BNL to include 'special category data'. We were informed that many of the organisations, including local authorities that are part of a DSP, may choose to rely on Article 9(2)(a) 'explicit consent' to process this information. This would mean that data items such as ethnicity and LGBTQ+ status would be optional data fields for a person to provide. Crisis explained that the likely purpose behind processing this data would be for monitoring the diversity and inclusivity of the services used by people experiencing homelessness. We advised that, where the collection of special category data is based on explicit consent, this must be confirmed with a clear statement of affirmative action, specifying the nature of the data being collected, and it must be separate from other forms of consent that the organisation requested. We recommended that the template consent statement be modified to include an additional consent request, such as a separate opt-in tick box. This would indicate to people that the collection of special category data is distinct from other data being collected by the organisation for separate purposes. We also recommended that Crisis consider whether the collection of this information was necessary, and, if so, whether alternative special conditions for processing were available to the relevant organisations.

3.44 We advised Crisis that where organisations choose to rely on certain Article 9 special conditions other than explicit consent, such as 'employment, social security and social protection' or 'reasons of substantial public interest', they are also required to meet an associated condition in UK law, set out in Part 1, Schedule 1 of the DPA 2018. We noted that 'safeguarding of children and individuals at risk' is one such Schedule 1 condition. We advised Crisis that, where organisations choose to rely on a Schedule 1 condition for the processing of special category data, they would need to establish whether they fulfil the requirements of these conditions. The development of an 'appropriate policy document' ('APD') is a requirement where data is being processed under specified Schedule 1 conditions. This document should demonstrate that an organisation's processing of special category (and criminal

offence data where applicable) is compliant with the data protection principles. We recommended that Crisis adapted their template to indicate this.

3.45 Crisis was also asked to consider whether collecting personal data relating to a person's 'physical description' could reveal or concern special category data, such as data relating to their health or their racial or ethnic origin. Whilst this may be vital information to homelessness outreach teams when trying to identify and locate people, it is also information likely to be collected ahead of a person consenting to the processing of their personal data. We recommended that Crisis and the organisations involved in the processing considered alternative special category conditions (other than explicit consent) for this processing.

3.46 As a result of the consent steer, Crisis informed us that they intend to carry out a wider educational piece internally and externally to ensure organisations and their staff understand UK GDPR consent, how it can be used, and its challenges. Crisis also informed us that they are in the process of recruiting a Data Lead role for Built for Zero, who will work on the development of BNLs to support this training need.

Identifiability of Personal Data

3.47 Originally Crisis' Objective 2 was to 'explore whether personal data can be 'pseudonymised' and/or 'anonymised' and used for research purposes.' However, Crisis decided that it only wished to receive 'monthly figures' from each of the future DSPs to track the success of the BNL and whether it had made a difference to overall homelessness figures. Crisis do not need to receive personal data for these purposes and will ask lead organisations to transfer anonymised data to them monthly.

3.48 Crisis requested our advice in ensuring that the data they will be provided with would be truly anonymous. Crisis outlined the following categories of data they would receive:

- number of new entries on BNL;
- numbers in each 'list status' – New, Returner, Actively Homeless, Housed, Dormant;
- numbers in each list status broken down by – age bracket, gender, LGBTQ+, ethnicity;
- average number of times homeless for all on BNL; and,
- average time from added to BNL list to Housed.

3.49 We advised Crisis to conduct an identifiability assessment to consider the means that could be reasonably and likely used to reidentify the information, considering the data and its environment, the context, the scope and purposes of the processing, and the technical and organisational measures applied to secure the data. Crisis should consider whether their staff have access to any other data they could use to piece together with the categories above to identify people. If taking all these factors into account, and identifiability is more than likely, then the information would be considered personal data and should be treated as such. We recommend that Crisis familiarise itself with our draft anonymisation guidance, particularly the draft guidance on identifiability[7].

3.50 In the case of lower counts, Crisis should consider small cohort suppression and instruct leading authorities to suppress figures with lower counts. For example, if a count on a category is lower than five, the authority should report this as <10 or another appropriately suppressed score, so Crisis are never receiving single counts of any categories which would make identification easier.

[7] Our anonymisation guidance is to be published at some time after the publication of this Sandbox exit report. Readers should be mindful of any potential changes to the draft guidance.

3.51 As new categories are introduced, Crisis will need to carry out additional identifiability assessments based on that new category. Whether data remains anonymous over time should be periodically reviewed, eg new technological developments or changes to public availability of certain records may render the data identifiable within a few years.

3.52 The risk of identifiability will depend on whether it is likely that a person can be identified from the data. Reducing the identifiability of data down to less than remote will render it effectively anonymous. There must be a balance between managing the risk whilst maintaining the utility of the data.

4. Ending Statement

4.1 Crisis' participation in the Sandbox has allowed the ICO to further consider the challenges that may occur in complex data sharing initiatives involving a number of parties. The effective mapping of the data lifecycle can be an extremely useful exercise for organisations to begin with when starting out on such a venture. This can help identify the challenges to effective data sharing and the risks that can be posed to a person's rights and freedoms, particularly in the context of processing data about people experiencing homelessness.

4.2 Crisis has found that participation in the Sandbox has deepened its understanding of the complex data sharing issues which arise in the context of their aspiration to produce and advocate for BNLs, and the multi-agency approach that involves. Sandbox participation has allowed Crisis to refine and improve the support it can offer to communities who have an aspiration to introduce BNLs. The involvement in the Sandbox has allowed Crisis to work in more depth on its guidance templates, thereby providing a stronger foundation upon which to build further trust and understanding of the BNL project.