Regulatory Sandbox Final Report: Zamna

A summary of Zamna's participation in the ICO's Regulatory Sandbox

Date: November 2023

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. We assess these criteria via our application processes.

1.3 The Sandbox specifically seeks projects operating within challenging areas of data protection. Sandbox participants have the opportunity to engage with us, draw upon our expertise and receive our advice on mitigating risks and implementing data protection by design and default into their product or service. This helps ensure that appropriate protections and safeguards are implemented.

1.4 Airlines that rely on manual travel document verification have found it increasingly inefficient and time consuming to carry out these checks due to the rise in travel requirements and volume of passengers. Mistakes in travel document verification checks can lead to non-compliance with border control requirements and hefty fines for these airlines. It can also be difficult for passengers to work out which travel documents are needed as often there is no single source of travel requirements. Zamna's Verified Passport and Verified Health solutions seek to make it easier for passengers to understand their travel requirements and for an airline to verify this information. Zamna's products use novel cryptography and distributed ledger technology ('DLT') to deliver a data minimising solution for pre-airport checks. This innovative approach reduces friction, which is often encountered in the travel industry, whilst maintaining robust levels of passenger verification.

1.5 We accepted Zamna into the Sandbox on 2 December 2021. We determined that Zamna's product aligned with the ICO's anonymisation/pseudonymisation, distributed ledger technologies, and data sharing areas of focus at the time of its application.

1.6 The ICO and Zamna agreed to work on the following objectives as part of Zamna's bespoke plan:

- **Objective one:** To examine the processing of anonymous data by working through chapter two of the ICO guidance (in consultation at the time of entry) on anonymisation. In particular, to consider (i) the "reasonably likely" and (ii) "motivated intruder" tests in relation to the data processing and explore the applicability of the "in whose hands" principle for Zamna, the airlines, the health providers and external third parties.
- **Objective two:** To determine the role and responsibilities of Zamna as a controller, processor or neither under the UK General Data Protection Regulation ('UK GDPR'). We agreed to focus in particular on the purposes and means of processing, and ensuring that consideration was awarded to data subject rights in light of the distributed nature of the processing, the storage of the data and the novel use of distributed ledger technology.
- **Objective three:** To consider the products' compliance with the data protection principles, particularly the lawfulness and fairness of the processing, security and accountability.

1.7 The Sandbox work commenced after an initial discovery phase, during which the project's scope was reframed to only include a consideration of Zamna's Verified Passport product in August 2022. Although Zamna initially applied to the Sandbox in relation to both the Zamna Verified Passport and Verified Health solutions, once in the Sandbox the work moved to focus solely on the Verified Passport product. Zamna has confirmed that the underlying technical infrastructure that is considered in this report is the same across both products (ie signal generation and the components of the Zamna Client). Where the processing is the same, our advice will be relevant and can be applied to the Verified Health product. However, there are extra considerations for the Verified Health product relating to the processing of special category health data which were outside the scope of Zamna's participation in the Sandbox.

1.8 The final objective of Zamna's plan was completed in July 2023. This report summarises the work that was carried out during Zamna's time in the Sandbox.

2. Product description

2.1 Zamna's Verified Passport product aims to assist airlines with ensuring that their passengers are able to satisfy the various requirements associated with flights to different locations. These requirements may relate to:

- passport/travel ID document requirements (document type and time to expiry requirements);
- destination-specific permissions (eg visa requirements);
- passenger specific restrictions (eg travel bans, travel watchlists (Interpol etc.)).

2.2 The purpose of the product is to give airlines confidence in the consistency of passenger documentation and allows passengers to make sure that they have all the relevant documentation required for departure and arrival at the destination country. The Verified Passport confirms the consistency of the passenger's travel documentation with their other details. The product also confirms that the presented documentation is consistent with documentation previously relied upon for travel by the passenger and that previous airlines believe is valid. This verification is turned into a "Signal" and over time, the more times a passenger flies, the more airlines build trust in the "Signal" associated with that passenger.

2.3 To do this, Zamna's Verified Passport product involves two separate features, which are provided to airline clients:

- the ability to build checklists for passengers to identify pre-flight travel documentation requirements; and
- the optional ability to generate cryptographic signals to verify whether a passenger's travel document has been accepted for travel previously.

Key definitions

2.4 Zamna's Client App refers data to its software development kit, which is hosted locally and solely on the client's infrastructure. It can be hosted either on the premises or using a cloud provider of the clients' choice.

2.5 Zamna Client refers to the combination of the software development kit, the Zamna API and the airline's Peer node on Zamna's DLT. These components form the entirety of the Zamna products provided to the airline on their systems.

2.6 The Zamna Cloud acts as the location for storage and retrieval of encrypted signals within the Zamna Network which allows data verifications to take place, whereby the airline can query the Zamna Cloud for previously generated Signals. It does not sit in the airline's infrastructure, it is hosted by both AWS and IBM Cloud and managed by Zamna.

2.7 Zamna's DLT is a permissioned DLT that stores the record of transaction for a cryptographic signal. The Zamna DLT acts as a Decentralised Public Key Infrastructure ('DPKI') which holds the registry of joined parties and their public credentials (eg public keys). Only a hash of the Signal is included in the transaction record. An airline verifies the authenticity of each Signal against the local DLT log and ensures the response is consistent and was not tampered with.

2.8 The Zamna Network is a permissioned Network, where each connected party running the Zamna Client, runs its own independent Node. The "Zamna Network" refers to the collection of nodes for each member of the Zamna DLT, including the node run by Zamna. Zamna's approach is that it allows an airline participating in the network to enable the secure matching of Verified Passport Signals generated by other airlines in the network. All participants in the Zamna Network are required to enter into Zamna's common set of contractual obligations which regulates the way participants must operate within the network.

Building a checklist for travel requirements

2.9 The process of building a checklist for passengers can be separated into several processing activities:

(i) Developing a template rules set for the Rules engine

The Zamna Verified Passport product consolidates and aggregates travel and immigration laws and regulations found in various formats from different jurisdictions and digitises them into a Rules Engine. This Rules Engine is hosted by Zamna using the Zamna Cloud. We understand the Rules Engine does not involve the processing of personal data – it is solely the creation and maintenance of a database holding digitised travel documentation requirements.

(ii) Application of the Rules Engine to create a "fit to fly" checklist for the passenger

This is the application of the Rules engine to a specific airline request for a destination. The Zamna Engine generates "rules sets" for specific destinations that identify the basic documentation requirements for travel to a specific destination. The Zamna Rules Engine generates a rules set for the destination country upon request by an airline, the rules set lists the travel requirements for that destination.

To create a checklist, the airline uses the Zamna Client App hosted locally and solely on the client's infrastructure. The Zamna Client App is integrated with the airline's systems and receives personal information from the passenger, such as passport information, booking information, and information relating to the relevant flight. The Client App sends the flight data (dates of the flight, the origin and destination, and whether there are any transfers/layovers) to the Zamna Cloud in order to retrieve the relevant rules set. This rules set identifies the travel requirements for the destination specified by the airline. No further information is provided by the airline or Client App to the Zamna Cloud, and Zamna does not have visibility over airline-specific passenger identifiers to generate the rules set. Airlines can use an operational filter that sits within the Client App to apply additional requirements to the checklist. Airlines can therefore set their own information requirements and collect more or fewer categories of personal information than the template rules set suggests.

The end product of the Client App is a "fit to fly checklist" for the passenger. This is a list of relevant requirements for the passenger's destination and those specified by the airline.

(iii) Completion of the "fit-to-fly" checklist by the passenger

The passenger provides personal data to the airline to complete the passenger-specific checklist within the Client App. On the airline's relevant passenger-facing application, the passenger may be presented with a green tick for completed requirements or an action required symbol for missing or inconsistent documentation. The airline may collect this personal information either at the airline's check-in desk at the airport, or online. Zamna states that the personal information collected by the airline for the purpose of completing a fit-to-fly checklist is processed and stored solely by the airline and not by Zamna. The Client App processes the passenger-provided information to confirm whether the presented documentation or information meets the relevant technical passport requirements. This ensures that the passenger is able to address any documentation issues before they arrive at the airport for the flight and prior to arrival at their destination.

The generation, persisting and retrieval of Signals to verify previous travel

2.10 The generation of cryptographic signals to verify whether a traveller's travel document has been accepted for travel previously is an optional further feature that an airline can offer to its passengers. As outlined above, the Client App verifies the consistency of passenger-asserted information with the technical requirements of the relevant travel document identified in the rules set as part of the checklist process. This verification of a document by the Client App can be turned into a Signal. This means that the airline can use the Client App to apply cryptographic processes to the passenger's personal data and the fact that its consistency has been verified by the Client App, and to store this encrypted data set (in the form of a Signal) in the Zamna Cloud.

2.11 This process involves several steps, which we summarise here:

- The airline creates a Blinded Distributed Data Identifier ('BDDI') – this involves using the Client App to blind the passenger's passport data with a large random factor, creating partial signatures, and aggregating the partial signatures.
- The airline creates a digital signature of the relevant personal data using the BDDI corresponding to the relevant individual passenger and additional meta-data, and encrypts the digital signature using the Client App. The airline sends the BDDI and

encrypted Signal to the Zamna Cloud.

- The Zamna Cloud slices and stores pieces of this Signal across its distributed database management system, we refer to this as persisting the signal. No single data record is stored in its entirety on any single database node. The BDDI value is used to locate the matching storage buckets for a given passenger in the Zamna Cloud. Multiple Signals can be associated with the same BDDI but stored in different buckets on the Zamna Cloud.
- In parallel, the supporting transaction for each generation of a Signal is written into the Zamna's decentralised permission ledger ('the Zamna DLT'), which acts as a verifying timestamp. The Zamna DLT contains a single hash of the combined BDDI and the Signal.

2.12 We understand that Zamna intends for each persisted Signal and each reading of the Signal to require passenger consent. Zamna has stated that airlines can currently only receive the information that passengers have consented for them to retrieve. Consideration of the consent and the format of this consent is outside the scope of Zamna's participation with the ICO Sandbox and we have not considered consent as a lawful basis.

2.13 To generate, persist and retrieve verification information from a Signal, an airline must process the passenger's passport information using the Client App in order to generate the BDDI key. Once created and persisted on the Zamna Cloud a Signal can be retrieved by participating airlines for subsequent flights taken by that individual. This means the same airline that originally generated the Signal, or other participating airlines in the Zamna Network can use the passenger's passport information to generate the BDDI and retrieve the Signal to verify whether the personal data provided by the passenger was accepted for travel and was consistent with technical requirements for the previous airline. In subsequent flights, the DLT can be queried by an airline to verify that the Zamna Cloud has returned all related Signals with a "Match", "Mistake", or "Unknown" response in relation to the passenger.

2.14 Airlines can also access meta-data about how the verification happened, once the airline has decrypted the corresponding Signal using the Client App on their infrastructure. This meta-data indicates whether the verification originated from within a secure environment (such as an airport) or from a secure mechanism (such as data extraction from a passport chip). This

enables subsequent airlines to determine the nature of verification suitable for their needs by the airline, for example, to insist on a certain number of verifications to have happened for them to trust the passenger's information. The meta-data also gives the date and time of the verification event. We understand that Zamna cannot and does not access this metadata.

3. Key data protection considerations

3.1 Zamna and the Sandbox addressed a number of key data protection considerations to Zamna's travel verification solution, these are outlined below.

Joint Controllership

3.2 One Sandbox objective was to help Zamna determine whether it was acting as a controller, processor or neither in relation to the processing activities involved in the Zamna solution. Further to this, we looked to understand whether, if it was acting as a controller, it acted jointly with the airlines. To assess Zamna's role in the processing accurately it was necessary to break down the overall processing into two distinct activities, as Zamna's relationship to the processing was different in respect of each activity:

- The application of the Rules engine to create a fit to fly checklist for a passenger
- Processing where signals are persisted for subsequent flights and other airlines

The application of the Rules to create a fit to fly checklist for a passenger

3.3 To determine whether Zamna was a controller or processor in regard to this information, the first step was to determine whether personal information was being processed in this activity. In the first instance, Zamna does not receive or process any personal information when it is digitising travel requirements to build a Rules Engine. Secondly, we determined that the flight information used to generate rules for a passenger checklist is unlikely to identify an individual directly and as such

would not be personal information in Zamna's hands. The identity of the passenger is not considered by Zamna when producing the rules set because the rules relate to a specific destination, not to an individual. On the other hand, flight information is likely to be personal information in the hands of the airlines in Zamna's network as they have additional information about the passenger. Lastly, Zamna does not collect personal information from passengers for the completion of the fit-to-fly checklist by the passenger. These operations are conducted solely by the airline within the Client App on its' own systems. As a consequence, Zamna cannot act as a processor nor a controller as it does not process personal data in connection with the creation of the Rules Engine, or the airline's specific customer checklist.

3.4 However, we advised Zamna that they should carry out and document an identifiability assessment to evidence that an individual cannot be identified directly or indirectly from the flight data provided by the airline. Where Zamna does in fact process personal data for the activities specified above, even if this was not intended or the primary objective, it will act as a processor if it does not determine the purposes or means of this processing and is acting solely under the instructions of the airline. This will depend on the specific circumstances of each processing activity where they have established that they are able to identify an individual from the flight data received by the airline.

3.5 During the participation, we also considered whether Zamna exercised enough influence over the purpose of the creation of the fit to fly checklist to amount to joint controllership. Our view was that although Zamna has developed the Client App for the particular purpose that airlines can use it to generate the checklist for passengers and that Zamna provides a template rules set for each passenger destination, Zamna does not become a joint controller for this activity. Though Zamna provides the client airline with the rules sets, the Client App, and certain tools to help integrate the Client App in the airline's infrastructure, it does not determine exactly how the rules set or Client App is operationalised by the airline. The airlines make the ultimate decision as to which categories of personal data to collect and how to apply these rules sets. The airlines request the rules sets for particular journeys and make the ultimate decision as to how to apply the rules sets. For example, it could generate checklists based on these rules sets for all passengers and destinations, or for only certain passengers or certain destinations, or for only certain objectives such as generating a checklist for VISA requirements alone. Though Zamna creates template rules sets which the airlines use to identify suggested documentation requirements, each airline can decide to collect more or fewer categories of personal information based on its own operational filters and according to

their own internal requirements. As a result, Zamna cannot be said to be a controller jointly with the airlines for the processing of personal information to generate the fit to fly passenger checklists as it does not determine the essential means of processing nor the purpose for which the checklist will be used by each individual airline.

Processing where signals are persisted for subsequent flights and other airlines

3.6 We consider that Zamna acts as a joint controller along with the airlines in the Zamna Network when persisting a Signal in Zamna's Cloud and recording the transaction on Zamna's DLT. In contrast to processing flight data to generate and provide rules sets to airlines (which is a distinct processing activity, and does not involve the processing of personal data by Zamna), Zamna and the client airlines jointly determine the purpose and means of processing personal data in generating and persisting Signals which contain pseudonymised passenger information.

3.7 Upon entry to the Sandbox, Zamna's view was that they were not joint controllers as their purpose for persisting signals in the Zamna Cloud was different to the airlines' overall purpose for using the Zamna solution. However, we advised Zamna that joint controllership can exist even if parties do not share or pursue exactly the same purpose of processing if the purposes of processing are closely linked or complementary. In the Zamna solution, a joint controllership relationship arises due to the close link between Zamna's purpose of building a commercially viable ledger of Signals (for commercial use by current and future participating airlines), and the airlines' purpose of generating and retrieving Signals to verify passenger data using Signals that were originally generated by other participating airlines.

3.8 For joint controllership to exist, all parties must have a tangible impact on the purposes and means of the processing of personal data in such a way that the processing would not be possible without both parties' participation. In Zamna's case, the processing would not be possible without the airline collecting passengers' personal information to which each Signal relates and the airlines' use of the Client App and Zamna Cloud which Zamna provides.

3.9 We helped Zamna to think more broadly about how purpose for processing may be defined as, while the airlines' purpose was clear, Zamna had not identified the mutual benefit to both parties that would help to identify Zamna's purpose of processing. The airlines generate, persist and retrieve Signals in order to provide a more efficient passenger experience and

to obtain greater confidence in the reliability and veracity of the travel documents presented by a passenger which helps them to reduce the risk of repatriation fines in the event the travel documents are incorrect, incomplete or out of date.

3.10 Zamna's purpose for processing goes beyond remuneration as Zamna's purpose of persisting encrypted Signals in the Zamna Cloud and the corresponding transaction in the Zamna DLT enables it to provide a commercial service to airlines and adds commercial value to their solution. Zamna places controls on the way that airlines interact with the Zamna Cloud and Zamna DLT to ensure this commercial viability as the more signals that are available in the Zamna solution, the more attractive it is to future airline customers (see 3.12). This commercial interest is sufficient to show that Zamna has influence over the purpose of processing.

3.11 Zamna exercises control as they can prevent a particular airline, upon termination of the airline's participation and use of the Zamna Verified Passport, from deleting all the Signals persisted by that airline within the Zamna Cloud. This means that the Signals remain available to Zamna's other airline clients. Therefore, Zamna retains control over the Signals and the purpose for processing even when the original airline that generated the Signal no longer uses Zamna's Verified Passport and can no longer access the Signals.

3.12 Though Zamna and the respective airline have distinct purposes, the processing for these separate purposes is inextricably linked; this gives rise to a joint controllership. Even though airlines have other existing methods available to verify passenger information, it is important to differentiate between the general 'activity' of verifying previous travel and the specific processing in question that is being carried out. The processing of the generation and hosting of signals requires the involvement of both the airlines and Zamna. Inextricably linked means that the specific processing in question would not be possible without the participation of both parties because both parties have a tangible impact on the determination of the purposes and means of that processing.

3.13 Another key consideration in the Sandbox was whether joint controllership would be affected by the fact that the personal information that a Signal relates to is in practice unintelligible by Zamna (the data is pseudonymised and Zamna cannot generate or access the pseudonymisation key to identify the underlying individuals; see 3.27 - 32). The outcome in the Sandbox was that Zamna's lack of access to this personal information did not prevent a joint controllership arising as Zamna

exercises influence over both the purposes and means of processing the personal data to generate and persist a Signal. The fact that Zamna is a joint controller with the airlines also means that it is not possible to carry out an anonymisation assessment solely from Zamna's perspective. If the passenger information stored in the Zamna Cloud is personal information in the hands of an airline, as the processing of that data in the Zamna Cloud would not be possible without the participation of Zamna, Zamna will be a joint controller in respect of that processing regardless of whether Zamna can actually access that information in its unencrypted form.

3.14 As well as the purpose of processing, Zamna does exercise influence over some of the means of processing. The ICO's guidance on controllership provides examples of decisions that are taken by controllers, such as to whom data is disclosed. Zamna decides who will have access to the signals by introducing them into the Zamna Network in a protocol that is designed by Zamna, and each airline is bound by Zamna's contractual agreement. The addition of more legitimate airlines to the system is going to be in the best interests of both the collective group and Zamna's commercial interest to increase the available signals. These are examples of essential means of processing and as such, when considered with Zamna's role in determining the purpose of processing, makes Zamna a joint controller.

3.15 At the same time, airlines decide to use the additional feature of Zamna's solution in their infrastructure in order to generate and persist Signals. Airlines therefore decide to use Zamna's solution to process personal data, and in doing so also define the means of processing such as the data subjects and the categories of personal data included in the Signal. As a result, airlines jointly participate in determining the means of processing.

3.16 We helped Zamna to apply general principles of joint controllership to their complex processing ecosystem and as a result determined that Zamna was a joint controller. This enabled Zamna to begin to address how controllership obligations should be discharged between the parties, which was considered during their participation in the Sandbox and is discussed below.

Roles and responsibilities

3.17 Zamna wanted to understand what the roles and responsibilities of the airlines and Zamna respectively would be under a joint controllership arrangement. This was especially important given their concerns related to having to rely on contractual obligations entered into with the airline in order to ensure any of the responsibilities of a controller could be discharged due to their lack of access to the personal data.

3.18 We established that a key requirement of joint controllership, under Article 26 UK GDPR, is to have a transparent arrangement in place that sets out the agreed roles and responsibilities for complying with the UK GDPR. The main points of this arrangement should be made available to individuals, and we recommended that Zamna include these in the privacy notice available on their website. The transparent arrangement would be helpful to Zamna as they would rely on the airlines to carry out most of the data controller obligations given their direct relationship with passengers and access to the data. We advised Zamna that this transparent arrangement could be a standard document for all airlines upon entry to the Zamna Network, this would support their existing processes for developing agreements with new airline partners.

3.19 A primary concern in the finding of a joint controllership arrangement was determining what actions Zamna could take given that they could offer no assistance in actioning individual rights requests and Zamna would have no ability to actually ensure that airlines are complying with such requests. We discussed possible solutions with Zamna, for example specifying the airlines as a point of contact for individual rights requests in the privacy information on their website and at the instance where a passenger opts in to have their signals persisted. In addition, should an individual exercise their rights directly to Zamna as a joint controller, Zamna should have a process in place to direct these requests to the appropriate airline for that request to be actioned. The obligation of airlines to action these requests should be documented in the transparent arrangement.

3.20 During the Sandbox engagement, we also determined that to the extent that personal information, including pseudonymised data in the Signals, is held under Zamna's control and access to such data is only possible through Zamna's technical infrastructure, Zamna should have primary responsibility for the security on that database. The responsibility is to comply with the controller obligation to implement appropriate technical and organisational security measures to ensure the security of personal data. For more information, please read our guidance on security.

3.21 As a joint controller, Zamna will be responsible for compliance with the data protection principles. This means that Zamna will need to identify an appropriate lawful basis under Article 6 of the UK GDPR for its processing activity. If Zamna is relying upon the consent that is collected by the airline to persist a Signal, they will need to ensure that this consent identifies Zamna as a joint controller and the nature of the processing that Zamna will carry out. Zamna will need to consider this as part of their arrangement with the airlines. On the other hand, we advised that if Zamna is relying on legitimate interests they will need to carry out their own legitimate interests assessment and that they will not be able to rely on the lawful basis identified by the airlines as they may have different obligations for collecting the personal information used in the processing.

3.22 During their participation, Zamna raised the issue of liability that arises from joint controllership. This was due to Zamna needing to rely on contractual obligations entered into with the airline in order to ensure certain controller obligations were carried out and this would require them to supervise the activities of the airlines. We advised that although Zamna would be liable for any damage resulting from an infringement of the UK GDPR as a result of their processing activity, they would not be liable for damage resulting from a breach of the UK GDPR if they could prove that they were not in any way responsible for the event giving rise to the damage. Our advice confirmed to Zamna that the existence of joint liability does not necessarily imply equal responsibility between Zamna and the airlines. Each controller may be involved at different stages of the processing activity and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the processing activity and what is possible for each party. The allocation of responsibilities should accurately reflect where responsibility for compliance lies between the joint controllers i.e. the responsibility for responding to individual rights sits with the party with the ability to provide the response requested, and the responsibility for security of data lies with the controller in a position to ensure that security.

3.23 Depending on the circumstances, joint controllers can have a certain degree of flexibility when allocating obligations so long as the parties can ensure compliance with UK GDPR in relation to the respective processing. We provided Zamna with a matrix of the different controller obligations as a starting point for Zamna to develop their transparent arrangement, and to use the matrix to build suggestions as to how each joint controller might be able to fulfil their obligations. The development of these processes was outside the scope of Zamna's participation in the Sandbox.

Pseudonymisation and anonymisation

3.24 The ICO and Zamna worked together during Zamna's participation to determine whether the signals hosted in Zamna's Cloud were personal information. This assessment was critical to determining whether the discussions relating to joint controllership and responsibilities were applicable to Zamna and subject to UK GDPR requirements. The outcome of this work determined that Signals amounted to pseudonymised personal information.

3.25 Signals are hosted on Zamna's Cloud in an encrypted format which Zamna cannot decrypt without additional information held by the airlines. In order to retrieve the Signal, Zamna can identify and aggregate the sliced pieces of a Signal in the Zamna Cloud using the BDDI key provided by the airline. Participating airlines can retrieve a Signal and access the personal information on their systems using this BDDI key which is derived from a passenger's travel identity documentation when it is presented to the airline at check in. The querying airline independently verifies the Zamna Cloud response with the Zamna DLT. Using the decryption key (crypto artefact) which they hold, the airlines can then decrypt the Signals in Zamna's Cloud to access personal information in its unencrypted format. The Signals amount to pseudonymous information, and the decryption key held by the airlines is the additional information required to attribute the Signal information to a specific passenger. As Zamna is a joint controller for processing activities related to the generation and persisting of these signals, the personal information contained in a Signal remains pseudonymised personal data in Zamna's hands.

3.26 The BDDI acts as an identifier, which is used to single out or distinguish the exact set of encrypted pieces of a Signal held in the Zamna Cloud for a single individual and reconstruct them into a single encrypted record. Although Zamna's initial position was that the Signals, whilst in Zamna's hands, were simply a mathematical equation made up of random numbers, we have emphasised that the BDDI allows data relating to an individual to be correctly matched and returned to Zamna. Therefore, these numbers can relate to an individual within the matching process. The Signal alone does not directly identify an individual to whom it relates unless additional information is available. However, the Zamna system is used to generate the exact additional information (the BDDI) that is required to identify and retrieve the Signals relating to an individual for the purposes of verifying that their travel documentation has been used before. It is this additional information which is sent to the Zamna Cloud that sits outside of the airlines' technical infrastructure and is hosted by Zamna. If a living individual can

be identified, even indirectly by reference to an identifier, ie additional information that allows for identification, then the data being processed will be personal information. This processing therefore qualifies as pseudonymisation under Article 4(5) of the UK GDPR.

3.27 Zamna has designed the technical infrastructure for the Signals so that the design of the system ensures that the passenger information contained in a Signal and held in the Zamna Cloud cannot be attributed to an individual without the use of the BDDI key. Zamna has stated that it is unable to identify individuals from the encrypted data in its system (ie the cryptographic Signal persisted to the Zamna Cloud and the record of the transaction persisted in Zamna's DLT) and would still be unable to access the data even if provided with an individual's passport which was used to generate the BDDI key in the airline's hands.

3.28 The ICO views the pseudonymisation process implemented by Zamna and the airlines in the generation and persisting of Signals as a technical and organisational measure that represents a good example of data protection by design and default under Article 25 UK GDPR. This pseudonymisation also helps Zamna and the airlines, as joint controllers, to fulfil certain obligations under the security principle in Article 5(1)(f) and Article 32 UK GDPR. However, the measures do not make the data anonymous or mean that Zamna is processing anonymised data, in respect of which the UK GDPR requirements would not apply. As the information is personal information in the hands of the airlines (who can decrypt it), and as Zamna is a joint controller with the airlines, the information cannot be anonymous in the hands of Zamna. This is because Zamna is jointly determining the purpose and means of the processing of this pseudonymised information with the airlines. The technical and organisational measures in place on the Zamna Cloud are privacy enhancing techniques that provide an enhanced level of confidentiality and security to passengers' travel information.

3.29 During their Sandbox participation, Zamna presented documentation to demonstrate that this pseudonymisation process would significantly reduce the likelihood of unauthorised re-identification of personal information. The documentation asserts that breaking into Zamna Cloud to access the Signals would not allow the identification of an individual as this is only computationally possible with the relevant and correlated BDDI for each Signal persisted. Zamna's linkability assessment concludes that an encrypted Signal will only ever respond to a specific and exact combination of personal information

(provided to the airline by the individual) that must be queried through the Client App software. Even if an individual were to possess the passport data used to create the BDDI and seeks (intentionally or unintentionally) to piece together different records to identify the data subject, they would still require access to the Client App in order to generate the relevant BDDI and BDDI decryption key. As such, Zamna asserts that it is not possible to combine several different data sets together to identify a particular data subject. Zamna notes that it has implemented technical and organisational controls such as self-policing rules in the Zamna Network to address the risk of unauthorised intrusion. Zamna's motivated intruder assessment concluded that such an intruder would lack the ability to complete any of the tasks required to decrypt the data and has carried out independent penetration tests (which the ICO has not seen or reviewed) which found that with current computational power, it would take anywhere between 1 to 10 million years to decrypt. As this was outside the scope of Zamna's Sandbox participation, the ICO has not conducted a technical or organisational audit in relation to Zamna's controls and cannot confirm whether the data security assessments summarised above reflect the processing in practice.

4. Ending statement

4.1 Zamna's participation in Sandbox has been a useful exploration of the application of joint controllership principles to complex processing ecosystems such as decentralised networks, and their impact on roles and responsibilities where one of the joint controllers does not have access to the personal information. Our application of these principles enabled us to help Zamna determine that they were joint controllers with the airlines for the specific processing activity of persisting signals for subsequent flights and other airlines. Working through these challenges has given Zamna the tools to inform their data protection and security strategies as appropriate to their designation when complying with data protection principles such as the lawfulness, fairness, security, and accountability of their processing.

4.2 The ICO and the Sandbox have also been able to apply the ICO's draft guidance on pseudonymisation to Zamna's joint processing to differentiate between anonymisation and pseudonymisation. We identified that Zamna was processing pseudonymised personal information and this has highlighted the value of pseudonymisation as a technical and

organisational measure for greater security of personal information. As a result, this has given Zamna confidence that their deployment of pseudonymisation techniques reveals a commitment to security and data protection by design.

4.3 Going forward, Zamna will continue to consider how they will use the ICO's advice to properly assign joint controller obligations between parties involved in the processing. They will also need to apply learnings from the Sandbox participation to their other products such as Zamna Verified Health, where they find the processing to be the same.