Regulatory Sandbox Final Report: CDD Services Ltd

A summary of CDD Services' participation in the ICO's Regulatory Sandbox

Date: September 2022

Information Commissioner's Office

Contents

1. Introduction

1.1 The ICO introduced the Regulatory Sandbox ("Sandbox") service to support organisations who are developing products or services that use personal data in innovative and safe ways and where such products or services deliver a potential public benefit.

1.2 Organisations who are selected for participation in the Sandbox have the opportunity to engage with us; draw upon our expertise and receive our advice on mitigating risks and implementing 'data protection by design' into their product or service, whilst ensuring that appropriate protections and safeguards are in place.

1.3 CDD Services is a private limited company that provides digital compliance solutions to organisations. CDD Services entered the Sandbox to explore specific data protection related matters regarding their SafeGuarden platform ("SafeGuarden"). CDD Services intended to pilot SafeGuarden in the Hull4Heroes 'Veterans Village' which provides transitional housing, employment, training and support for ex-service people and their families. In brief, SafeGuarden would allow people to prove their identity and grant permission to share their personal data with different parties or organisations ("Service Providers") in order to access their services.

1.4 CDD Services is the holding company for several entities, specifically;

- CDD Software Services (CSS) Ltd,
- CDD Management Services (CMS) Ltd and
- SafeGuarden Ltd.

1.5 SafeGuarden Data CIC[1], ("SafeGuarden Data"), the entity responsible for storing personal data in respect of SafeGuarden, is not a subsidiary of CDD Services. However currently the board comprises of representatives from the CDD Services' management team. This report details the roles and responsibilities in respect of the proposed processing of personal data.

1.6 The ICO accepted CDD Services into the Sandbox on 23 November 2020.

1.7 As part of CDD Services' Sandbox plan, the ICO and CDD Services agreed to work on the following set objectives:

- **Objective 1 – Establish the different roles and responsibilities under the UK GDPR of each of the organisations involved in the Hull4Heroes pilot.**

This would involve the creation of a detailed data map to understand the lifecycle of people's personal data, including the Article 6 lawful bases and Article 9 special category data conditions relied upon for the proposed processing. CDD Services and the Sandbox would also consider the role of SafeGuarden and whether it would be considered a 'data trust'[2].

- **Objective 2 – Establish the appropriate Article 6 lawful bases and Article 9 special category data processing conditions**.

With support from the Sandbox, CDD Services would establish the appropriate lawful bases and special category

[1] Community Interest Company.
[2] A high-level definition of a data trust can be briefly set out as; a formal structure that supports ethical data usage, management, and sharing. Unlike a single data sharing agreement between two parties, the processing and sharing will occur through an independent data stewardship with a fiduciary obligation (an impartial, legal and ethical responsibility regarding the use of the data) to data subjects, through a repeatable framework that can be accessed potentially by large numbers of controllers for a variety of purposes. Please note, this understanding could be subject to change as the research in this area evolves, as the ICO understands the notion of data stewardship is in its infancy.

data processing conditions, where necessary, that would be relied upon for the specific processes required for the pilot for each of the Service Providers involved.

- **Objective 3** – **Implement 'data protection by design and default' into CDD Services' software application, including the user journey and back-end system used by Hull4Heroes and the Service Providers in the pilot.**

The Sandbox would provide steers in relation to data minimisation and purpose limitation. CDD Services would also develop applicable documentation, such as privacy information for users, collaboratively with the Service Providers involved and develop a Data Protection Impact Assessment (DPIA) to identify and mitigate risks of the proposed processing. The controller is responsible for carrying out a DPIA and so if CDD Services or SafeGuarden were not defined as a controller then instead they would input into the DPIA. The ICO Sandbox would review and feedback on this documentation.

- **Objective 4 – Conceptually explore potential blockchain functionality, including the challenges that this component may pose to the data protection compliance of the pilot technology.**

- **Objective 5** - **The Sandbox would provide ad hoc compliance support to CDD Services whilst user testing of the technology was underway.**

The Sandbox would provide steers to mitigate emerging risks identified during testing.

Sandbox work focused around objectives one to three. Objective four was not completed and user testing did not take place within the Sandbox. The Hull4Heroes project was temporarily paused and as a result there was insufficient information for a specific 'use case' to fully explore the data protection considerations for SafeGuarden. CDD Services also re-evaluated their priorities and following the Home Office, Department of Culture, Media and

Sport's (DCMS) and the Disclosure & Barring Services' announcement to introduce permanent digital 'right to work' and 'right to rent' checks decided to realign their product in respect of the Digital Trust Framework currently under development by DCMS.

In view of these product changes, the temporary pause of the Hull4Heroes project, and the limited information available regarding a specific 'use case', the ICO provided limited informal steers to CDD Services during their Sandbox participation, which are summarised below. Please note, the steers did not consider CDD Services' product alignment with the DCMS trust framework, as this decision was taken after CDD Services participation in the Sandbox.

1.8 The ICO provided recommendations for CDD Services to consider further following their exit from the ICO Sandbox to ensure the proposed processing complies with the data protection legislation. These recommendations are summarised below.

1.9 This report reflects the work that has been undertaken during CDD Services' Sandbox participation which came to an end in March 2022. Since its exit from the Sandbox, CDD Services has carried out additional work, most notably on the DPIA as a result of the ICO's feedback. This work is summarised at 3.15 and 4.4.

2. Product description[3]

2.1 SafeGuarden is a digital-ID centred online platform, which uses CDD Services' Spotlite Compliance Platform ("Spotlite"), an existing product which has been re-designed to support the SafeGuarden business model and the Hull4Heroes 'Veterans Village' use case. This product will enable ex-service personnel to prove their identity and grant permission to share their personal data with Service Providers who will then provide support to them and their families in relation to housing, employment and training, based on permissions set by the individual.

2.2 The ICO understands there are intended to be 86 Service Providers in the Hull4Heroes project overall; 34 Service Providers in East Riding and 52 Service Providers in Hull. When scoping initial Sandbox work, CDD Services identified a small number of parties to focus on for the purpose of the Sandbox work, namely; Hull4Heroes, Veterans Hub, and NHS Veterans Mental Health Services.

2.3 Service Providers intend to have their own Client Portal, a web portal used to manage their applicants, teams, and workflows. SafeGuarden will allow Service Providers, to create and host their own Communities of Practice (CoPs), which they can set policies, control standards and workflows for. For the Hull4Heroes use case, there are four different schemes representing different communities of practice to support individuals, including:

[3] The product description and data protection steers reflect the ICO's understanding of CDD Services' SafeGuarden proposal based on the information CDD Services provided. It should be noted that since exiting the ICO Sandbox, CDD Services have further developed their product somewhat. See paragraph 1.7 for more.

- SafeGuarden ID and Attribute Sharing Scheme
- Hull 4 Heroes Scheme covering the Veterans Village
- Veterans Hub Scheme covering Veteran's engagement with local council services
- A Scheme covering health assessments and access to health services

2.4 A 'Scheme' is comprised of a group of different organisations. A 'Scheme Owner' is the lead organisation that creates, runs and sets the rules of a scheme. The Scheme Owner is responsible for determining the data items required within a given Scheme. The 'Service Providers', agree to follow a specific set of rules around the use of digital identities or data. When the Scheme is set up, a Scheme Owner will create a template 'Wallet' for each Service Provider. The data items in the Wallet will be those necessary for the Service Provider to fulfil their purposes. A Service Provider will be able to access or download personal data from a specific Wallet linked to an individual. Service Providers and individuals can belong to more than one CoP and those within a CoP can collaborate and provide services to each other.

2.5 Individuals will register for a RealMeID Account ("account") on SafeGuarden via Spotlite. SafeGuarden will offer identity assurance and verification levels for an individual's account on the basis of their consent. Their identity could be verified using their smart phone, or by scanning and uploading different forms of identity evidence eg passport. This account will collate all the documents and data for an individual into a Wallet within a single SafeGuarden Data Store. Where this is not possible, for example, due to accessibility issues, an individual can

also register for an account via a Service Provider which will collect the individual's personal data and create a SafeGuarden account on behalf of that individual.

2.6 Service Providers may refer individuals to other Service Providers based on their need to access specific support. However, other than referrals, a Service Provider cannot transfer a person's data to another Service Provider. Only the data subject themselves can grant access to their data, and a Service Provider has to request this directly from the individual. In terms of referrals between different service providers, only certain categories of information can be shared, such as: name, residential address, email address(es), phone number(s) and social media tags (where applicable). A Service Provider may also be able to retain a snap-shot view access depending on their legal purposes, such as for records of engagement or for audit trail purposes.

2.7 From an individual's point of view, SafeGuarden provides a data vault within which, there are four separate data accounts, one for each scheme.[4] Within each scheme, an individual has a Wallet for each Service Provider. Access to that data is cross referenced by Scheme and Wallet, and the individual controls which data is available in which Scheme or Wallet.

[4] See 2.4 for further information.

3. Key data protection considerations

3.1 Below is a summary of the informal advice provided by the ICO during CDD Services Sandbox participation. As explained above, it should be noted that CDD Services' product has somewhat developed since the delivery of these informal steers.

Data stewardship

3.2 A high-level definition of a data trust is a formal structure that supports ethical data usage, management, and sharing. Unlike a single data sharing agreement between two parties, the processing and sharing will occur through an independent data stewardship with a 'fiduciary obligation' to data subjects through a repeatable framework that can be accessed potentially by large numbers of controllers for a variety of purposes. A 'fiduciary obligation' in the context of data trusts means a controller must steward data with impartiality and transparency.

3.3 Based on the information provided by CDD Services, the ICO's view was that it was unlikely that SafeGuarden Data is a data trust, as SafeGuarden was not intended to hold a fiduciary obligation to data subjects. However, the ICO advised CDD Services that data trusts are not recognised in the data protection legislation as it currently stands, and the ICO's thinking around data trusts is in its infancy. Subsequently, it was agreed by both parties on 17 August 2021 to progress with the other tasks in CDD Services' Sandbox plan and CDD Services would explore this further outside of the Sandbox process.

Controllership

3.4 SafeGuarden provides a means for individuals to upload, verify and share their personal data with the organisations that they choose. SafeGuarden also enables more seamless business-to-business sharing of personal data in respect of referrals from one service to another.

3.5 In any data sharing venture, it is important to understand what the respective data protection roles and responsibilities are for each organisation involved. These will change depending on whether an organisation is processing personal data as a controller, a processor or if one or more organisations are joint controllers. These roles should be determined prior to the commencement of any data sharing initiative. When determining controller and processor relationships, it is necessary to examine the role and type of relationship each party has in relation to the actual processing activity that is taking place and to determine their respective status as a controller, joint controller (where they act together with either another or other controllers in order to decide the manner and purposes of processing), or a processor.

3.6 In order for CDD Services to begin to examine the roles of each of the organisations involved, a list of preliminary data mapping questions were provided by the ICO Sandbox on 23 March 2021. These questions were divided into three areas of focus:

1) the data processing carried out by the Service Providers at present,

2) the proposed 'User Journey': the expected data flows supported by the SafeGuarden product from collection of personal data through to deletion, and

3) the role of SafeGuarden and CDD Services in relation to the data processing.

Exploring these kinds of questions is a helpful way for organisations developing products using personal data to examine the life cycle of the data. It also helps to examine what the prospective roles and responsibilities of the involved organisations will be in regard to the personal data under the UK GDPR.

3.7 The ICO Sandbox attended and observed a meeting with one potential Service Provider, a mental health service, on 8 June 2021. During this meeting the Service Provider explained how they currently process ex-service personnel personal data, and provided some insight into the customer journey and the technology currently in use. It appeared that the SafeGuarden product could help overcome some of the challenges that the organisation currently faces in respect of supporting and referring individuals to other services. This meeting was beneficial to both CDD Services and the ICO Sandbox in understanding how existing processes could fit with CDD Services' proposed innovation and how the SafeGuarden product could streamline these processes. These discussions provided CDD Services with an opportunity to examine the proposed roles and responsibilities for one of the prospective organisations involved in the pilot.

3.8 On 17 December 2021, the ICO Sandbox provided CDD Services with an informal steer on controllership in respect of Objective 1 of the Sandbox plan. This steer outlined the considerations CDD Services should take into account to help ensure that its proposed data sharing model could comply with UK data protection law. The ICO steer also included a summary of the key facts as understood by the ICO and several recommendations for CDD Services to consider and implement prior to moving forward with the proposal. Due to delays experienced in the Hull4Heroes pilot, the informal steer provided by the ICO related more generally to the operation of SafeGuarden, using the Hull4Heroes pilot as an example where appropriate.

3.9 Key points from the steer are as follows:

- The UK GDPR does not apply to the processing of personal data in the course of a purely personal or household activity, with no connection to a professional or commercial activity. A data subject cannot be considered a controller of their own personal data where the personal data is processed for the individual's own 'domestic purposes'.
- SafeGuarden Data are likely to be acting as a processor on behalf of the Service Provider(s):
    - **if** an individual signs up to SafeGuarden and completes identity or due diligence checks specifically in order to share information with one or more Service Providers,
    - **and** SafeGuarden Data are collecting and processing personal data purely pursuant to the requirements of the Service Provider(s),
    - **and** the Service Provider(s) in question is determining the means and purposes for processing (rather than SafeGuarden Data).
- If a Service Provider creates a SafeGuarden account for an individual, SafeGuarden Data are also likely to be acting as a processor on behalf of the Service Provider.
- If SafeGuarden Data makes the decision to collect and process certain personal data, then they may be a joint controller with the relevant Service Provider. However, in this scenario, consideration would need to be given to the purposes of processing and whether SafeGuarden's purposes align with those of the other joint controller(s). If SafeGuarden Data have different purposes for processing the personal data as a controller, then SafeGuarden Data are likely to be a controller in their own right in relation to such processing.
- If an individual signs up to SafeGuarden and completes identity or due diligence checks solely in order to store their personal data, without the involvement of a Service Provider, it's likely SafeGuarden Data would

be acting as a controller of this personal data.

- For the collection of personal data as it is added to Wallets in SafeGuarden, the entity or entities which determine the means and purposes for processing the personal data will be the controller(s), either in isolation or jointly with others. For example, when a Wallet is created by a Service Provider uniquely for their own use, the Service Provider is likely to be a controller. When a Wallet is created by a Service Provider for the use of a CoP, all Service Providers involved in that specific CoP may be considered joint controllers in relation to the personal data, if they share the same purposes for processing. If SafeGuarden Data is not involved in making any of the decisions regarding the purposes and means of the processing, SafeGuarden Data are considered likely to be acting as a processor.
- CMS, who manage the Spotlite system, may be a sub-processor to SafeGuarden Data for the purpose of conducting identity or due diligence checks if such checks are conducted pursuant to an agreement with SafeGuarden Data. The ICO Sandbox indicated that it would, however, need more information about the relationship between CMS and SafeGuarden in this context and see any contracts between the parties, in order to advise more specifically on the relationship between the parties.
- If a Service Provider edits or add personal data into SafeGuarden that only they (ie, the specific Service Provider) can see, the Service Provider in question would be doing so in their capacity as a controller.
- Where the personal data is shared, eg where a referral is made from one Service Provider to another, this

would constitute a sharing of personal data between controllers.[5]

- If Service Providers reuse personal data obtained via SafeGuarden for a different purpose than it was originally intended, they are likely to be a controller for this processing. Service Providers will need to complete a purpose compatibility assessment to consider the compatibility of their processing against the purpose for which that data was originally collected.
- SafeGuarden Data are likely to be the controller of the derived data (Applicant [data subject] ID, Service Provider ID, Reason for Interaction, Date and Time) generated by interactions between data subjects and Service Providers on SafeGuarden if they are the only ones who can access and use the data. If SafeGuarden Data intend to repurpose it, they will need to complete a purpose compatibility assessment and consider whether they should refer to this processing in their privacy notice to individuals.

3.10 The ICO provided several recommendations to CDD Services as part of the informal steer. In particular, the ICO advised CDD Services to complete a more comprehensive data mapping exercise to ensure it is clear what processing activities are intended to take place in the SafeGuarden platform, what personal data will be processed, the purpose(s) for processing this personal data, and the data flows. The ICO also recommended that CDD Services revisit the ICO guidance on controllership to ensure CDD Services have fully considered whether SafeGuarden Data will be involved in making decisions regarding the purposes and means of the processing. This was in order to determine whether SafeGuarden Data would be a controller of any of the processing activities they have identified. The informal steer also stated that, if SafeGuarden Data are acting as both a controller and

[5] Following the delivery of the 'controllership steer', CDD Services informed the ICO that CDD Services considered the only sharing of data between controllers would be the contact information required to complete referrals. Other than this, CDD Services considered that the proposal itself does not involve the sharing of personal data between controllers, but if an individual grants permission to a Service Provider, that organisation could gain specific access to specific data attributes within the data vault itself.

processor for any of intended processing, SafeGuarden Data must ensure their systems and procedures distinguish between the personal data they are processing in their capacity as controller and what they process as a processor on another controller's behalf.

Data Protection Impact Assessment

3.11 On 14 March 2022, CDD Services submitted a data protection impact assessment ('DPIA') for CDD Services in respect of the SafeGuarden platform to the ICO Sandbox. This early draft DPIA was shared with the ICO with the purpose of exploring further compliance discussions. The ICO provided an informal steer on this document to CDD Services on 26 April 2022, in line with Objective 3 of the Sandbox plan.

3.12 A DPIA is a process to help organisations analyse, identify, and minimise the data protection risks of a project or plan as set out in Article 35 of the UK GDPR. A DPIA can cover a single processing operation, or a group of similar processing operations. It is a key part of the accountability obligations under the UK GDPR, and when completed effectively can help organisations assess and demonstrate compliance with its data protection obligations.

3.13 The feedback and recommendations contained in the informal steer for the DPIA can be summarised as follows:

- In its current form, the DPIA fails to comply with the minimum requirements provided by Article 35(7) UK GDPR.
- At the time of its submission, it was not clear from the DPIA, which CDD Services Group entity or entities were considered to be the controller(s) for each of the processing operations covered by the DPIA, or whether certain CDD Services Group entities would be considered as processors for some aspects of the processing. Further consideration of the respective roles of the CDD Services Group entities should be undertaken and documented in the DPIA. The informal steer on controllership provided during participation

in the Sandbox should help CDD Services with this process.[6]

- The DPIA in its current form focussed on the functionalities and societal benefits of SafeGuarden and trust services generally, as opposed to describing and assessing the risks of the relevant processing operations. The DPIA requires clearer descriptions of the data flows eg how and why personal data is processed. This description should be granular and detailed.
- Although the DPIA considers the risks associated with the confidentiality, integrity, and availability of personal data, it should also identify and assess other risks to the rights and freedoms of individuals that could arise from the data processing. Such risks may include, for example, an individual's inability to access services or opportunities. The DPIA should consider whether (and how) these risks could be mitigated.
- In order to assess the necessity and proportionality of the processing covered by the DPIA, it should include a more detailed explanation of the appropriate lawful bases (and where applicable the special category data processing conditions) for each processing purpose or processing activity. The DPIA should also detail how these lawful bases and conditions apply. For example, where CDD Services' legitimate interests are relied upon there should be an explanation of, or reference to, an assessment of CDD Services' interests against the data subject's interests.
- The DPIA should include further details as to which data subjects' rights will be applicable and under what circumstances.

[6] See paragraph 3.4

3.14 The ICO also reminded CDD Services that when revising its DPIA, if there are any high risks identified that cannot be mitigated, it must consult the ICO before starting the processing via the official ICO prior consultation process.

3.15 Following CDD Services' Sandbox participation, CDD engaged a professional Data Protection Officer in April 2022 to support and enhance its considerations of data protection. A DPIA was redrafted substantially taking into account all of the ICO's recommenations and this analysis did not identify residual high risks to individuals. The ICO did not review or provide feedback on this document.

Additional considerations

3.16 In addition to the above, the ICO provided CDD Services with some information regarding data sharing agreements in respect of the individuals' contact information that is likely to be shared between the intended Service Providers. Where personal data is shared between controllers, it is best practice to have data sharing agreements in place (which is separate to identifying a lawful basis for processing) in line with the ICO's accountability framework. This framework outlines ways in which organisations can demonstrate their data protection compliance.

3.17 On 29 March 2022, the ICO Sandbox also provided CDD Services with information on how to register with the ICO if SafeGuarden Data is processing personal data as a controller. Controllers should register with the ICO before any processing of personal data commences. The ICO's registration self-assessment can help with determining whether a fee needs to be paid. Regardless of whether organisations are exempt from paying a fee, all organisations processing personal data still need to comply with the other data protection obligations.

4. Ending statement

4.1 CDD Services' participation in the Sandbox has allowed the ICO to further consider the issues that can arise in the context of complex data sharing activities involving several parties. The ICO's work with CDD Services has also highlighted the importance and usefulness for organisations in identifying a specific 'use case', in order to consider and mitigate data protection risks fully before live processing of personal data commences.

4.2 Through engaging with the Sandbox service, CDD Services has had the opportunity to explore in more depth the data governance and compliance issues concerning the sharing of personal data using digital wallets and digital IDs. Specifically, participation in the Sandbox has offered CDD Services the opportunity to consider the following compliance requirements in more depth:

- Accountability: The Sandbox has provided CDD Services with recommendations for how data protection by design and default may be embedded into SafeGuarden's systems and processes;
- Governance: The Sandbox has provided CDD Services with support in how to identify the roles and responsibilities in regards to the personal data processed eg who is a controller, processor and sub-processor(s).
- Risk Frameworks: the Sandbox has provided CDD Services with the opportunity to consider what fair and proportionate controls to reduce the risk of harm and digital exclusion may look like; and
- Purpose limitation: the Sandbox has allowed CDD Services to understand the importance of clear governance segregation between personal data sharing and those activities that may be used for marketing and other purposes outside of a Scheme.

4.3 It is hoped that the insights CDD Services have gained will inform its ongoing research and development of the SafeGuarden products and services.

4.4 Upon their exit from the Sandbox, CDD Services was advised to consider addressing and developing the areas outlined in the informal steers, to ensure that the proposed processing complies with the UK data protection legislation. The Sandbox recognises that CDD Services has undertaken additional work following its exit from the Sandbox including engaging a professional Data Protection Officer and redrafting its DPIA taking into account the ICO's steers provided during participation.