ico.
Information Commissioner's Office

Application to the Sandbox beta phase

Getting Started

Please submit all completed applications to applysandbox@ico.org.uk, no later than midday **24 May 2019.**

Please include all the information we need to assess your application within this Word document and mark up any sections that are confidential or commercially sensitive.

Please do not use web-links or signpost to further information.

By submitting this form you are certifying that the information you have provided is true and accurate and that you have the relevant authority to make this application.

Your organisation's details

What is the name of your organisation?	The Greater London Authority (GLA)
What is your registered address?	City Hall, The Queen's Walk, London, SE1 2AA
Where is the team developing your product	Not applicable – same as above

or service based (if different from above)?	
Who is your authorising senior manager?	Jeremy Skinner, Assistant Director Communities and Intelligence, City Intelligence Unit, Greater London Authority. Section 40 (2) Jeremy.Skinner@london.gov.uk
Who is your Sandbox Single Point Of Contact (SPOC)?	Sophie Deakin. Senior Strategic Crime Analyst. The City Intelligence Unit, Greater London Authority. Section 40 (2) Sophie.Deakin@london.gov.uk
What is your organisation's website URL?	www.london.gov.uk
What is your ICO registration number?	Z4760661
Have you reported any incidents, or had any enforcement action taken against you initiated by the ICO in the last two years? **If yes, please provide brief details, and if possible include the date the matter was reported and the ICO reference number.**	No reported incidents and no instances of enforcement action being taken against the GLA.
Are you a micro, small or medium-sized enterprise/organisation ?	The GLA is a large organisation >249 employees.

Do you employ or are you in anyway associated with former ICO staff? **If yes, please explain the role of the former ICO staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	No – not to our immediate knowledge. Although, GLA is a large Government organisation, so it is plausible that someone may be associated to an ICO staff member. There is no feasible means as to determine this though.
Do you employ any staff who are related to or are in anyway associated with an ICO staff member? **If yes, please explain the role of the staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	No – not to our immediate knowledge. Although, GLA is a large Government organisation, so it is plausible that someone may be associated to an ICO staff member. There is no feasible means as to determine this though.
Your product or service	
What product or service do you wish to	In order to reduce levels of violence in London, the Mayor has set up a Violence Reduction Unit (VRU) which is taking a public health approach to violence. As part of this work, the VRU needs to better understand how public health and social services can be managed to drive down crime. There is increasing interest from the VRU, the Mayor's Office of

participate in the ICO Regulatory Sandbox?	Policing and Crime (MOPAC) and the Greater London Authority (GLA), for health, social and crime data to be looked at in an integrated and collaborative way. Our proposed Sandbox inclusion aims to build on an existing service run by the GLA known as 'SafeStats' which brings together multi-agency emergency service data on violent incidents within the capital and makes this available to authorised analysts to support strategic planning, policy making and operations. Our proposed Sandbox inclusion aims to bring together a much more diverse range of public health, social service and crime data that we cannot currently access to improve the evidence base on the drivers of violence and provide an understanding of how the many different factors which influence it are related. This will allow us to map the key life-stages and pathways undertaken by different groups of children to understand how these result in violence, with the associated negative costs for their families and wider communities. To address the data sharing issues, our sandbox will use a progressive but cautious approach to data-sharing. There are three distinct stages to the product development, all of which have their own attributable output, and will contribute to the evidence-base for violence in London. 1. The first stage refers to taking the aggregate data to which we already have access, and obtaining it at a lower geographical level, specifically to Lower Super Output Area (LSOA). While we already have data at this level on levels and rates of crime, most of the public health data is at borough-level, which means that differences within boroughs cannot be observed, comparisons cannot be made between small areas similar in makeup, the narrative may be confused, and there may be issues trying to normalise or contextualise the data. Therefore, this stage of the product involves us working with several datasets at geographical level lower than we would ordinarily be able to access. This would also involve accessing and compiling LSOA level aggregate datasets on relevant Borough services that are not currently available on a London-wide basis. The main output from this stage will be a better mapping of the different services that are needed to prevent violence, and an understanding of changes in service levels are related to the later rates of violence observed by the emergency services. 2. The second stage refers to the acquisition of individual record-level data for a range of public health and emergency services datasets with common identifiers. These common identifiers could be demographics such as age, ethnic category and gender. The outputs from this stage will provide a better understand of the at-risk populations and the public health factors that pose the greatest protective and risk factors for susceptibility to violence, make comparisons across the different services, and evidence issues of increased vulnerability, disproportionality and over-representation amongst group of society that are a major feature of violence. This stage does not require uniquely identifying data outputs, such as names or NHS numbers.

	3. The third and final stage refers to actual record linkage between the various public health and emergency services datasets; facilitating an exploration of the unique journeys across time of those involved in violence. This enables us to look at the dynamics of the drivers and causes of crime, how they interact with one another and how they contribute to occurrence of violence. We currently have access to record-level data from the London Ambulance Service, the London Fire Brigade, the NHS (in the form of Accident and Emergency admissions for Assault), Transport for London, the British Transport Police, and the Metropolitan Police Service. However, we are currently unable to link the data records contained within the respective datasets, due to these being depersonalised and having an absence of common identifiers. The relevant public health factors often have cumulative effects, and to understand the impact that they have individually or collectively, the data needs to be looked at longitudinally. This is because the risk/protective factors can (and do) occur at different points of an individual's life, with the impacts/effects differing across an individual's life course. To enable an understanding of the impact that the individual risk/protective factors have on violence rates, we need to be able to control for other confounding factors – this can only be done through the utilisation of an all-encompassing record-level linked dataset. The output at this stage would be the creation of a number of pseudonymised datasets linking one or more datasets for analysis. Across each of these three stages of product development, we aspire to embed data science, specifically predictive analytics, decision support technologies, and probabilistic data linkage to better understand the relationships between different services and how their performance affects the violence in our communities. The benefits of this Sandbox will be that by bringing together data from a wide range of services across the city, we can better understand how they can work together to reduce violence. For this one-year project, we do not propose creating a linked dataset that can be shared operationally by service staff. If successful as an analytical project, we would work towards this as a longer-term goal.
What do you consider to be the lawful basis for the processing in your proposed innovation?	As part of the Police and Social Responsibility Act, in 2011, the Mayor of London was given a direct mandate for policing in London, being directly responsible for policing performance, setting strategic direction and allocating resources through the Police and Crime Plan. The priorities identified for London all align to Violence and the associated issues; violence against women and girls, keeping children and young people safe, and hate crime and intolerance. The high priority attributed to violence has led to the establishment of the London-based Violence Reduction Unit (VRU). This unit has resulted from extensive research around the public health approaches such as in Glasgow, which has evidenced large successes in reducing violent crime. The VRU is being staffed with specialists in health, police and local government to enable the delivery of a long-term public health approach to tackle the causes of violent crime. The primary focus will be on the delivery of early interventions to reduce the prevalence of violence; expanding on the

	Mayor's Knife Crime Strategy and other aligned work. The unit will increase the co-ordination between the Metropolitan Police, local authorities, youth services, health services, criminal justice agencies and City Hall as part of the new enhanced partnership. The purpose of this project is to contribute to the reduction and prevention of violence in London, through enhancing the shared understanding of violence by collectively analysing data from various sources. The aligned legal bases for the processing of the information in our product proposal are: - Section 17 of the Crime and Disorder Act 1998 provides that authorities subject to the Act (inclusive of the GLA and MOPAC) must do all they reasonably can to prevent crime and disorder in their area - Section 115 of the Crime and Disorder Act 1998, which legally justifies the sharing of information where it is necessary to prevent crime and disorder or for crime reduction purposes - Section 30 of the Greater London Authority Act 1999 (as amended) provides the Mayor with a general power to act on behalf of the GLA to do anything which he considers will further the promotion of social development in Greater London and to promote improvements in the health of persons in Greater London - Section 143 of the Anti-Social Behaviour Crime and Policing Act 2014 provides an express power for MOPAC, as a local policing body, to provide or commission services "intended by the local policing body to help victims or witnesses of, or other persons affected by, offences and anti-social behaviour." **Article 6 lawful basis** The lawful basis under Article 6(1)(e) applies to the processing of personal data under this project: - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Section 8(e) of the 2018 Act prescribes that the reference Article 6(1)(e) of the GDPR to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for the exercise of a function conferred on a person by an enactment or rule of law. Processing of the data is considered necessary to help support a reduction in crime and disorder in London, both of which are in the public interest and within the prescribed statutory duties of the Mayor of London – thus, we do not believe that any unreasonable or unwarranted interference on individuals' rights or freedoms is apparent.

	Article 9 Considerations The processing of data concerning the health of an individual meets the requirement in Article 9(2)(g) of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 or 2 of Schedule 1 of the 2018 Data Protection Act. The following condition of Schedule 1 of the 2018 Act will apply to our processing of data relating to the health of an individual: - Paragraph 6: processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest. **Special Category Data -** For the inclusion of special category data in this project, the special category condition for processing under Article 9(2) are: - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; - processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. **Criminal Convictions and Offence Data -** For the inclusion of criminal convictions and offence data in this project, the separate condition for processing this data complies with Article 10. "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."
What are the specific data protection issues you are dealing with that mean your product	The Data Protection challenges immediately relevant to our proposed product are: - Complex data sharing at several different levels; both internally and externally

needs to enter the Sandbox?	- Building good user experience and public trust by ensuring transparency, clarity and explainability of our proposed data use - Clarification and guidance around how GDPR/DPA18 relate to our proposed use of data science - The utilising of existing data for new purposes such as for record linkage - Ensuring the security of data and identifying data breaches in complex and innovative environments. - Culturally different approaches to data and potential sharing across the public sector - Perceptions outside of the GLA that GDPR means data cannot be shared, rather than GDPR supporting and facilitating lawful sharing.
Will your product or service process personal data within the UK?	Yes
Will your product or service process special category data? If yes, please specify.	Yes – inclusive of race and ethnic origin, health data, and offending/conviction histories.
Does your product or service involve any form of international data transfer? If yes, please specify.	No
Is your product or service likely to result in a high risk to the rights and freedoms of individuals? If yes, please specify.	The main of the risks to the data subjects concerned are standard data protection risks found when handling personal data. The high-risk element is derived from: - the processing of both special category and criminal offence data - data from several different sources being combining and potentially matched/linked - the personal data being collected from a source other than the individual data subjects, so they will not be explicitly provided with a GLA privacy notice ('invisible processing') - the data processing includes data on vulnerable individuals and groups of individuals. As a precautionary measure, we will be completing a thorough Data Protection Impact Assessment (DPIA) prior to any data processing. Should the nature, scope, context, or purposes of the data processing change, an updated DPIA will be produced.

How is your product or service innovative?	[redacted]
How and to what extent will your product or service benefit the public?	

	Violent crime has a complex relationship with health; known to negatively affect both people's physical and mental health. Through creating an established and strong evidence-base for the predictors of violence, these risks can be mitigated, and the impacts minimised. Health inequality is a pertinent issue for public health and for crime reduction. The victims and perpetrators of violence are consistently reported to have higher health needs, and worse health outcomes across a range of measures compared to the rest of society. Through a better understanding of these health needs, the right health provisions can be provided at the right time to those that need them most; reducing health inequality and increasing the overall health and wellbeing of society. **Better public services** The proposed project will assist in the intelligence- and evidence-led allocation of funding and resources to both the geographical locations most in need, and to the most vulnerable and needing groups within society. The optimisation of scarce resource deployment thus results in a more efficient use of public funds, better service user experiences, and more effective and successful public services.
Does your product or service require any other form of regulatory authorisation to proceed? Or are there any other regulatory implications that we need to be aware of? **If yes, provide information on its current status and/or what these implications are.**	In current form, all involved parties have approved the application to the ICO, namely the GLA, MOPAC and the VRU. All data being utilised in current form meets the MOUs and data sharing agreements drawn up with the GLA City Intelligence Unit (SafeStats), namely, using the data for the prevention and reduction of crime, under the legal framework of the Crime and Disorder Act. Throughout the three stages of the product development, further authorisation will be sought from data providers for more disclosive and/or additional data to be supplied, inclusive of the London Ambulance Service, NHS, Metropolitan Police Service, and the Department of Education. It will also be necessary to notify data providers of our intentions to undertake record linkage between the various data sources and our proposed use of data science, to seek their individual authority to progress these.
Your proposed Sandbox plan	
What activity do you want to undertake in the ICO Sandbox?	The GLA along with MOPAC on behalf of the VRU would like to undertake a combination of informal advisory mechanisms, adaptive mechanisms, and anticipatory mechanisms. These include: - informal supervision of our product testing

	- processing 'walkthroughs' – step by step analysis of proposed processing activity, leading to informal advice; - workshops with design and development teams at an early stage to inform early planning - workshops with data providers to work through and create compliant sharing, and discuss record linkage in relation to GDPR/DPA 2018 - advice around applications to data suppliers for record level data - informal steers on risk mitigation and privacy by design/default - letters of negative assurance on exit - guidance around the innovative technology usage in our project, in terms of compliance around data protection and future regulatory provision. Acknowledgement that the above activities would need to be made more project specific after initial discussions with the ICO.
Do you want to undertake any form of testing involving 'live' personal data as part of your sandbox participation? **If yes, provide details and how you will control any risks to data subjects.**	No – we will be testing on dummy data to minimise the risks to data subjects.
What is your proposed timeline and the key milestones of your proposed participation in the Sandbox?	July 2019 – introductory meeting with an ICO sandbox team member July 2019 – commence planning with ICO sandbox assistance September 2019 – sandbox plan to be signed off September 2019 – sandbox exercise for current product September 2019 – complete DPIA October 2019 – make approaches to the various data agencies and organisations for data October 2019 – write the necessary DSAs for the newly anticipated data sources November 2019 – internal evaluation to assess progress, and feedback session with the ICO regarding what has occurred thus far December 2019 – first official sandbox review and feedback meeting

	March 2020 – second official sandbox review and feedback meeting May 2020 – sandbox exercise for new/enhanced product June 2020 – third official sandbox review and feedback meeting September 2020 – final meeting to evaluate the process, provide feedback to the ICO, and inform the sandbox exit report.
What are the key risks to data subjects of your involvement in the sandbox?	The potential key risks for the data subjects due to our sandbox involvement are: - The use of personal data for purposes that differ from that originally stipulated at the point of collection; - The unintentional/intentional identification of the data subjects; - Unauthorised access to, or use of, personal data; - The loss, disclosure or corruption of personal data; - The inappropriate or unauthorised sharing of personal data; - The retention of personal data for longer than necessary for the specified purpose; and - A failure to uphold data protection principles or information rights. It should be appreciated that the above risks to the data subjects, could occur due to human errors during the data processing and are not necessarily the result of malicious intentions. While all reasonable precautions will be undertaken to manage and mitigate the occurrence of these documented risks, they remain as potential risks during our Sandbox involvement. As we handle and process personal data daily in other aspects of our work, such as through access to the National Pupil Database, and GP Registrations, as well as through our own SafeStats data platform, we are fully sighted on the risks and compliant with all governing legislation.
What control mechanisms will you use to prevent harm to data subjects?	There are numerous control mechanisms which will be implemented to prevent harm to the data subjects; some of which are GLA standard policy and procedures such as the Data Protection Controls, and others that will be introduced specifically for the project in question. GLA standard: - The GLA has a well-defined and comprehensive data protection management structure, which includes an incident management structure that notifies incidents to the Senior Information Risk Officer and a designated Data Protection Officer - The existence and strict adherence to an up-to-date Data Protection Policy - The GLA undertakes system privacy/specification testing

	- The physical server is located within the TfL Data Centre, which has suitable access controls and CCTV coverage. GLA rent space within this secure environment. The location and aligned arrangements for this server all meet the necessary security requirements of both TfL and GLA. The server is only accessible from City Hall - Appropriate security is applied to all external routes in to the organisation; including internet firewalls and remoted access solutions - The GLA has a security standard to personal data proportion to the Government Security Policy Framework, which includes the destruction of personal data once it is no longer required; the use of personal data sharing and processing agreements; the maintenance of a corporate risk register; the maintenance of a personal data asset register; the incorporation of privacy by design recommendations into system and project developments; and the use of data protection impact assessments to ensure that controls are appropriate to privacy risk - The relevant security policy (including details on password length and complexity) is overseen and approved by the GLA Security Board - The GLA has control measures in place to regularly review the people, processes and technology risks that may impact upon arrangements for secure data handling. There are processes in place to conduct periodic reviews of the technological security for all major systems. There are also sporadic audits undertaken on the GLA IT security by the GLA's internal audit department - The GLA regularly monitors and audits all access to the GLA computer systems and network. Specifically, GLA system access is monitored through an Intrusion Detection System. There is also the monitoring and alerting service (OSSSI) that GLA use, which sends an email alert to the Senior GLA Engineers when an account is locked - Although, the GLA is not specifically ISO27001 certified, the GLA information security policy is aligned to this standard; with periodic audits of the relevant GLA information security policies undertaken using the ISO27001 as the default benchmark - Access to all corporate GLA security policies can be provided to the ICO upon request. Project specific: - Only staff with current Data Protection training and awareness will be allowed access and/or sight of the data - No raw data files received as part of this project will be disclosed without prior consent from the relevant data controller

	- Data will not be transferred outside the European Union at any point and the data; with all relevant data servers based in the EU - At the end of the specified retention period(s), all sensitive electronic records will be destroyed to current NCSC standards, as defined at www.ncsc.gov.uk/guidance, and the NHS Records Management Code of Practice for Health and Social Care 2016 - All data subject names, NHS numbers and other identifying numbers will be subject to pseudonymisation - All data received will either be by secure encrypted online file transfer, or via a password-protected Excel or flat-file format to a dedicated mail box (whereby the password is supplied separately) - All data received as part of this project will be securely stored, processed and manipulated within a secure GLA server held within the GLA environment - A specific, password-protected folder will be created in the GLA server for the purposed of storing the data supplied under this project - All electronic access to the relevant secure GLA server has a two-stage system access control. Firstly, using personal login credentials to the standard internal-GLA server. Then, secondly, using an authentication login procedure on a further remote connection in to a secure server via a Remote Desktop Connection from a computer terminal within City Hall - The data will be accessed through the software applications of R/RStudio and FME via a direct folder share from the secure server to designated, restricted high-performance GLA computer terminals. The folder shares will only be established with specific, nominated individuals. Access will remain on a need to know basis - The data will not be copied or moved in to any other locations outside of this secure server environment - There will be no hard copies of any of the received personal data reproduced - All uses of the personal data for analytics and reporting shall be subject to appropriate review to ensure that risks of data subject re-identification are minimised - All additional data and information requests will have the principles of data minimisation applied – making sure that the data is adequate, relevant and limited to what is necessary; limiting the proposed collection, storage and usage of the personally-identifiable information to minimise the level of potential identification of the data subjects - The data will not be retained for longer than is deemed necessary for the project – individual retention periods will be agreed and ratified as part of the Data Sharing Agreements with the data supplying agencies.
What actions will you take in the event of a control mechanism	The GLA takes the security of data and the rights of data subjects extremely seriously; having rigorous internal policies and technical measures in place to safeguard information and data. The GLA has procedures in place to monitor access and to identify unauthorised and/or unlawful access and use of personal data, such as the accidental loss or damage to the information, the damage or loss of the information by means of malicious software/hacking, and the deliberate

failure and in particular in case of any breach?	or knowing disclosure of information to a person not entitled to receive it. It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the GLA's internal disciplinary procedures. If misuse is found there is a robust and defined mechanism to facilitate an investigation, including the initiation of criminal proceedings where necessary. The current GLA Procedure for Incident Management is as follows: - All incidents of unauthorised access to GLA systems are recorded on the GLA Service Desk System - An Incident Manager is appointed by the Head of IT or the Head of IT Operations. They will record all the details of the incident - If the incident has resulted in any financial loss to the GLA the Head of Financial Services will be notified as will the Police - All incidents are reported to the GLA Information Security Board - A report on what action is being undertaken to prevent a repetition of the incident will be presented to the GLA Information Security Board While adhering to the above GLA Procedure for Incident Management, additional, specific actions to be taken in the event of a control mechanism failure or breach include: - The designated Single Point of Contact (SPOC) for this project is responsible for notifying the data supplier(s) in the event of loss or unauthorised disclosures of data within 72 hours of the event - The project SPOC will also be responsible for notifying the relevant internal department, namely the GLA Data Protection Officer - Upon reporting any security incidents relating to the personal data subject to this project, the GLA will fully cooperate with the relevant data provider(s) incident investigation requirements - If required, audits of personal email transmission, printer reprographics, and scan and send jobs as well as server logins and folder access incidences can all be obtained through the GLA Technology Group - If a reportable breach occurs during the project, it will also be reported to the ICO within 72 hours of the breach occurring, in line with the GDPR requirement. All GLA staff have a responsibility to help in protecting the assets of the GLA from loss, danger or harm. Anyone who identifies a potential security weakness or threat should contact the appropriate part of the GLA.

What is your proposed exit plan if it is unsuccessful (i.e. there is a technological failure)?	Should the suggested project be un-successful, and require an early termination, the primary focus of the exit strategy should be to minimise the detriment to the data subjects, while managing expectations and curtailing any reputational detriment. It is vital that key timescales for the exit should be drawn up and abided by. The exit strategy requires several things taken in to consideration: - A thorough assessment of the critical risks and issues that culminated in the required early termination of the project, with resolves and future mitigations highlighted where able - If feasible, make plans to move the project forward at a later stage without the highlighted issues resurfacing - A potential re-design of the project looking at the structure and processes, where these have been relevant to the failing of the current Sandbox project - Accountability mechanisms to be implemented - Procedures for conflict resolution to be initiated - Sanctions to be imposed if deemed appropriate and necessary - Internalisation of the issues and share learning from the experience - A comprehensive feedback session with the ICO – a critical appraisal of what went right and what went wrong during the project - Ensure transparency around the exit and communicate with the key stakeholders around the issues experienced - Identify the sustainability of successful features of the project - Look at progression routes for alternative options - Identify which areas of the project need to be sustained as a business as usual function – absolve back in to daily functioning - Consideration to (depending on reason for early exit): (1) Phasing Down – what activities/functions can be gradually phased down, (2) Phasing Out – what activities do we need to withdraw from, and (3) Phasing Over – can any activities be transferred to another organisation, so the activity can continue? Attention to be paid to which elements of the project are dependent on others. In terms of the data sharing and processing undertaken as part of the project, it is paramount to protect the personal data that has been received, stored and and processed; with additional requirements in the event of a premature project conclusion: - If deemed appropriate or requested by any of the data suppliers, all personal data received will be securely destructed by a member of the GLA Technology Group (TG) utilising MS SDelete (and other appropriate erasure tools) to recognised and accepted government standards

	- If required, the returning of all personal data electronic files to the data suppliers via secure transfer - If relevant, notify all data suppliers so that any data sharing is put on hold - Cease all data processing on the personal data until further instruction - No further analysis, or record linking to be undertaken unless still permitted to do so.

ico.
Information Commissioner's Office

Application to the Sandbox beta phase

Getting Started

Please submit all completed applications to applySandbox@ico.org.uk, no later than midday **24 May 2019.**

Please include all the information we need to assess your application within this Word document and mark up any sections that are confidential or commercially sensitive.

Please do not use web-links or signpost to further information.

By submitting this form you are certifying that the information you have provided is true and accurate and that you have the relevant authority to make this application.

Your organisation's details

What is the name of your organisation?	Please provide the full name of your organisation (and any relevant trading or legal entity names relevant to this application) and any unique identifier such as your Companies House number or Charity Registration number, where relevant. Novartis Pharmaceuticals UK Limited Company registration number 00119006
What is your registered address?	[redacted]

Where is the team developing your product or service based (if different from above)?	Please provide the address. [redacted]
Who is your authorising senior manager?	This is the person who has authorised your organisation to make this application. They must have appropriate decision making powers within your organisation. This may be your DPO, SIRO, CEO or relevant Director with responsibility for the product/service. Please provide their full name(s), job title and contact details. [redacted]
Who is your Sandbox Single Point Of Contact (SPOC)?	This is the person you want all correspondence regarding your application to be directed to. Please provide their full name(s), job title and contact details including email address. [redacted]
What is your organisation's website URL?	www.novartis.co.uk
What is your ICO registration number?	'This number should start with a 'Z', 'W' or 'A' Z6641953
Have you reported any incidents, or had any enforcement action taken against you initiated by the ICO in the last two years?	Having enforcement action or reported incidents taken against your organisation is not a bar to entry to the Sandbox. However we will need to consider the severity of the action or incidents, and the relevance of the issue to this application. [redacted]

If yes, please provide brief details, and if possible include the date the matter was reported and the ICO reference number.	[redacted]
Are you a micro, small, medium-sized or large enterprise/organisation ?	Please use the following guide: micro = 1-9 employees; small = 10-49 employees; medium = 50-249 employees; large = 250+ employees. We have 250+ employees.
Do you employ or are you in anyway associated with former ICO staff? **If yes, please explain the role of the former ICO staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	For example spouses, partners, children and parents, business partners, employers, managers, directors as per the terms and conditions. [redacted]

Do you employ any staff who are related to or are in anyway associated with an ICO staff member? **If yes, please explain the role of the staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	For example spouses, partners, children and parents, business partners, employers, managers, directors as per the terms and conditions. [redacted]

Your product or service	
What product or service do you wish to participate in the ICO Regulatory Sandbox?	Please include a full description of the personal data your product or service uses. As far as possible, please explain your product or service in plain English, without the use of unexplained jargon or industry-specific acronyms. The Novartis Voice Enabled Solutions (VES) project was commissioned to explore and develop voice technology within the healthcare sector. Our aim is 'making great patient care easier with voice enabled solutions'. [redacted]

[redacted]

What do you consider to be the lawful basis for the processing in your proposed innovation?	Please reference Article 6 and Article 9 (if required) of the GDPR in your response. And refer to our guidance as necessary. [redacted]

	[redacted]
What are the specific data protection issues you are dealing with that mean your product needs to enter the Sandbox?	If possible please refer to the specific provisions of GDPR/Data Protection Act 2018 that are relevant and indicate if any of the following DP challenges are relevant: • Use of personal data in emergent or developing technology such as biometrics, internet of things, facial recognition, wearable tech, big data, cloud-based products. • Complex data sharing at any and all levels. • Building good user experience and public trust by ensuring transparency, clarity and explainability of data use. • Perceived limitations, or lack of understanding of GDPR/DPA18 provisions on automated decision making, big data, machine learning or AI. • Utilising existing data (often at scale and in linking data) for new purposes or for longer retention periods.

	• Building privacy by design into product development taking account of cost issues and difficulties of doing this until testing has been undertaken. • Ensuring the security of data and identifying data breaches in complex and innovative environments. [redacted]

Will your product or service process personal data within the UK?	[redacted]
Will your product or service process special category data? If yes, please specify.	[redacted]
Does your product or service involve any form of international data transfer? If yes, please specify.	[redacted]
Is your product or service likely to result in a high risk to the rights and freedoms of individuals? If yes, please specify.	Please ensure you refer to ICO guidance about Data Protection Impact Assessments, when answering this question. We will expect you to be undertaking a DPIA if you are developing a product or service of this nature. [redacted]

How is your product or service innovative?	We will interpret innovation broadly as any new idea, device or method, including new approaches to achieving existing objectives. Use any qualitative or quantitative measures as appropriate Pay particular attention to explaining in what way the idea, device or method is sufficiently different to previous approaches to be considered innovative. [redacted]

How and to what extent will your product or service benefit the public?	We will interpret public benefit broadly to encompass any demonstrable positive benefit to the public with no form of benefit being more valued than any other (e.g. health and wellbeing or financial). We also consider public benefit to cover business benefit in terms of 'back-office' solutions; however care needs to be taken to ensure that the ultimate benefit to the public is articulated (e.g. in efficiency savings). In assessing public benefit we will consider the potential depth (the amount of benefit experienced) and breadth (the volume of people benefiting) of your product or service using the criteria indicators provided alongside the other criteria and factors listed. Please use any qualitative or quantitative measures as appropriate. Particular attention should be given to explaining the extent of benefit realised 1) as a direct result of Sandbox participation or 2) should the product/service be successful post-Sandbox. Products/services need not be both broad and deep in their benefit to be considered. [redacted]

	[redacted]
Does your product or service require any other form of regulatory authorisation to proceed? Or are there any other regulatory implications that we need to be aware of? **If yes, provide information on its**	You remain responsible for complying with any other legal and regulatory obligations [redacted]

current status and/or what these implications are.	
Your proposed Sandbox plan	
What activity do you want to undertake in the ICO Sandbox?	Please describe what specific activity you want to undertake in the Sandbox, referring to both advisory assistance and adaptive mechanisms (e.g. statement of regulatory comfort upon exit). We will design and agree further Sandbox mechanisms with you, if you are successful, in your bespoke Sandbox plan. [redacted]

	[redacted]
Do you want to undertake any form of testing involving 'live' personal data as part of your Sandbox participation? **If yes, provide details and how you will control any risks to data subjects.**	If you wish to include live testing in your Sandbox participation we will require you to provide assurance to us that you have mitigated risks before processing can start. Please read the ICO's guidance regarding Data Protection Impact Assessments for further information. Live testing will only be considered in relation to data subjects based in the UK. [redacted]

What is your proposed timeline and the key milestones of your proposed participation in the Sandbox?	Although the Sandbox beta phase ends in September 2020, there is no requirement for your participation to last up until this date. We are equally interested in short engagements. [redacted]

	[redacted]
What are the key risks to data subjects of your involvement in the Sandbox?	[redacted]

What control mechanisms will you use to prevent harm to data subjects?	[redacted]
What actions will you take in the event of a control mechanism failure and in particular in case of any breach?	[redacted]

What is your proposed exit plan if it is unsuccessful (i.e. there is a technological failure)?	Please describe how you will end your participation, if needed. [redacted]

ico.
Information Commissioner's Office

Please submit all completed applications to applysandbox@ico.org.uk, no later than midday **24 May 2019.**

Please include all the information we need to assess your application within this Word document and mark up any sections that are confidential or commercially sensitive.

Please do not use web-links or signpost to further information.

By submitting this form, you are certifying that the information you have provided is true and accurate and that you have the relevant authority to make this application.

What is the name of your organisation?	Please provide the full name of your organisation (and any relevant trading or legal entity names relevant to this application) and any unique identifier such as your Companies House number or Charity Registration number, where relevant. TrustElevate Limited, **08046357** - Incorporated on 26 April 2012
What is your registered address?	75 Kenton Street, London, United Kingdom, WC1N 1NN
Where is the team developing your	Please provide the address.

product or service based (if different from above)?	Telefonica, Wayra accelerator programme – 20 Air Street, London W1B 5AN
Who is your authorising senior manager?	This is the person who has authorised your organisation to make this application. They must have appropriate decision making powers within your organisation. This may be your DPO, SIRO, CEO or relevant Director with responsibility for the product/service. Please provide their full name(s), job title and contact details. [redacted]
Who is your Sandbox Single Point Of Contact (SPOC)?	This is the person you want all correspondence regarding your application to be directed to. Please provide their full name(s), job title and contact details including email address. [redacted]
What is your organisation's website URL?	www.trustelevate.com
What is your ICO registration number?	'This number should start with a 'Z', 'W' or 'A' **Registration number:** ZA476685
Have you reported any incidents, or had any enforcement action taken against	Having enforcement action or reported incidents taken against your organisation is not a bar to entry to the Sandbox. However, we will need to consider the severity of the action or incidents, and the relevance of the issue to this application.

you initiated by the ICO in the last two years? **If yes, please provide brief details, and if possible include the date the matter was reported and the ICO reference number.**	**No**
Are you a micro, small, medium-sized or large enterprise/organisation?	Please use the following guide: micro = 1-9 employees; small = 10-49 employees; medium = 50-249 employees; large = 250+ employees. **Micro**
Do you employ or are you in anyway associated with former ICO staff? **If yes, please explain the role of the former ICO staff member and whether they are expected to have any**	For example, spouses, partners, children and parents, business partners, employers, managers, directors as per the terms and conditions. **No,** [redacted]

contact or dealings with the ICO during the Sandbox.	
Do you employ any staff who are related to or are in anyway associated with an ICO staff member? **If yes, please explain the role of the staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	For example spouses, partners, children and parents, business partners, employers, managers, directors as per the terms and conditions. **No**
What product or service do you wish to participate in the ICO Regulatory Sandbox?	Please include a full description of the personal data your product or service uses. As far as possible, please explain your product or service in plain English, without the use of unexplained jargon or industry-specific acronyms. Trust Elevate provides secure identity authentication and authorisation for under 16-year-olds.

	[redacted] TrustElevate enables organisations to digitally authenticate and authorise under 16's, in line with regulatory requirements. [redacted]
What do you consider to be the lawful basis for the processing in your proposed innovation?	Please reference Article 6 and Article 9 (if required) of the GDPR in your response. And refer to our guidance as necessary. We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity, which is consent. Revocation of consent will be via the privacy policy. We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable way to achieve that purpose. We have documented our decision on which lawful basis applies to help us demonstrate compliance. This information, about both the purposes of the processing and the lawful basis for the processing, is to be found in our privacy notice: https://trustelevate.com/privacy-policy/

	Currently, we do not process special category data.
What are the specific data protection issues you are dealing with that mean your product needs to enter the Sandbox?	If possible please refer to the specific provisions of GDPR/Data Protection Act 2018 that are relevant and indicate if any of the following DP challenges are relevant: ● Use of personal data in emergent or developing technology such as biometrics, internet of things, facial recognition, wearable tech, big data, cloud-based products. ● Complex data sharing at any and all levels. ● Building good user experience and public trust by ensuring transparency, clarity and explainability of data use. ● Perceived limitations, or lack of understanding of GDPR/DPA18 provisions on automated decision making, big data, machine learning or AI. ● Utilising existing data (often at scale and in linking data) for new purposes or for longer retention periods. ● Building privacy by design into product development taking account of cost issues and difficulties of doing this until testing has been undertaken. ● Ensuring the security of data and identifying data breaches in complex and innovative environments. [redacted]

Will your product or service process personal data within the UK?	**Y**
Will your product or service process special category data? If yes, please specify.	**Y**
Does your product or service involve any form of international data transfer? If yes, please specify.	**N - not during the sandbox phase**
Is your product or service likely to result in a high risk to the rights and freedoms of individuals? If yes, please specify.	**N** Please ensure you refer to ICO guidance about Data Protection Impact Assessments, when answering this question. We will expect you to be undertaking a DPIA if you are developing a product or service of this nature.
How is your product or service innovative?	We will interpret innovation broadly as any new idea, device or method, including new approaches to achieving existing objectives. Use any qualitative or quantitative measures as appropriate Pay particular attention to explaining in what way the idea, device or method is sufficiently different to previous approaches to be considered innovative.

	[redacted]

	[redacted]
How and to what extent will your product or service benefit the public?	[redacted]

	[redacted]
Does your product or service require any other form of	You remain responsible for complying with any other legal and regulatory obligations

regulatory authorisation to proceed? Or are there any other regulatory implications that we need to be aware of? **If yes, provide information on its current status and/or what these implications are.**	No
[redacted]	
What activity do you want to undertake in the ICO Sandbox?	Please describe what specific activity you want to undertake in the Sandbox, referring to both advisory assistance and adaptive mechanisms (e.g. statement of regulatory comfort upon exit). We will design and agree further Sandbox mechanisms with you, if you are successful, in your bespoke Sandbox plan. [redacted]

	[redacted]
Do you want to undertake any form of testing involving 'live' personal data as part of your sandbox participation? **If yes, provide details and how you will control any risks to data subjects.**	If you wish to include live testing in your Sandbox participation we will require you to provide assurance to us that you have mitigated risks before processing can start. Please read the ICO's guidance regarding Data Protection Impact Assessments for further information. Live testing will only be considered in relation to data subjects based in the UK. [redacted]

What is your proposed timeline and the key milestones of your proposed participation in the Sandbox?	Although the Sandbox beta phase ends in September 2020, there is no requirement for your participation to last up until this date. We are equally interested in short engagements. [redacted]
What are the key risks to data subjects of your involvement in the sandbox?	[redacted]
What control mechanisms will you use to prevent harm to data subjects?	[redacted]

What actions will you take in the event of a control mechanism failure and in particular in case of any breach?	[redacted]
What is your proposed exit plan if it is unsuccessful (i.e. there is a technological failure)?	[redacted]

ico.
Information Commissioner's Office

Application to the Sandbox beta phase

Getting Started

Please submit all completed applications to applysandbox@ico.org.uk, no later than midday **24 May 2019.**

Please include all the information we need to assess your application within this Word document and mark up any sections that are confidential or commercially sensitive.

Please do not use web-links or signpost to further information.

By submitting this form you are certifying that the information you have provided is true and accurate and that you have the relevant authority to make this application.

Your organisation's details

What is the name of your organisation?	Tonic Analytics Limited. Company Number 09634032
What is your registered address?	Chancery House, 30 St John's Road, Woking, Surrey, GU21 7SA
Where is the team developing your product	[redacted]

or service based (if different from above)?	
Who is your authorising senior manager?	[redacted]
Who is your Sandbox Single Point Of Contact (SPOC)?	[redacted]
What is your organisation's website URL?	https://tonicanalytics.com
What is your ICO registration number?	ZA197592
Have you reported any incidents, or had any enforcement action taken against you initiated by the ICO in the last two years? **If yes, please provide brief details, and if possible include the date the matter was reported and the ICO reference number.**	[redacted]

Are you a micro, small or medium-sized enterprise/organisation ?	Small = 10-49 employees.
Do you employ or are you in anyway associated with former ICO staff? **If yes, please explain the role of the former ICO staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	[redacted]
Do you employ any staff who are related to or are in anyway associated with an ICO staff member? **If yes, please explain the role of the staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	[redacted]

Your product or service	
What product or service do you wish to participate in the ICO Regulatory Sandbox?	The Galileo Programme was launched in 2017 and is jointly sponsored by Highways England and the National Police Chiefs' Council, [redacted] Galileo's primary focus is on using innovative data analytics technology to provide data driven intelligence that enables partners to pursue better decisions and actions [redacted]

[redacted]

[redacted]

What do you consider to be the lawful basis for the processing in your proposed innovation?	[redacted]
What are the specific data protection issues you are dealing with that mean your product needs to enter the Sandbox?	[redacted]

[redacted]

	[redacted]
Will your product or service process personal data within the UK?	[redacted]
Will your product or service process special category data? If yes, please specify.	[redacted]
Does your product or service involve any form of international data transfer? If yes, please specify.	
Is your product or service likely to result in a high risk to the	

rights and freedoms of individuals? If yes, please specify.	[redacted]
How is your product or service innovative?	[redacted]

[redacted]

[redacted]

	[redacted]
How and to what extent will your product or service benefit the public?	

	[redacted]
Does your product or service require any other form of regulatory authorisation to proceed? Or are there any other regulatory implications that we need to be aware of?	

If yes, provide information on its current status and/or what these implications are.	[redacted]
[redacted]	
What activity do you want to undertake in the ICO Sandbox?	
Do you want to undertake any form of testing involving 'live' personal data as part of	

your sandbox participation? **If yes, provide details and how you will control any risks to data subjects.**	[redacted]
What is your proposed timeline and the key milestones of your proposed participation in the Sandbox?	[redacted]

	[redacted]
What are the key risks to data subjects of your involvement in the sandbox?	
What control mechanisms will you use to prevent harm to data subjects?	

	[redacted]
What actions will you take in the event of a control mechanism failure and in particular in case of any breach?	
What is your proposed exit plan if it is unsuccessful (i.e. there is a technological failure)?	

ico.
Information Commissioner's Office

Application to the Sandbox beta phase

Getting Started

Please submit all completed applications to applysandbox@ico.org.uk, no later than midday **24 May 2019.**

Please include all the information we need to assess your application within this Word document and mark up any sections that are confidential or commercially sensitive.

Please do not use web-links or signpost to further information.

By submitting this form you are certifying that the information you have provided is true and accurate and that you have the relevant authority to make this application.

Your organisation's details

What is the name of your organisation?	Ministry of Housing, Communities and Local Government (Department of Work and Pensions, and Blackpool Council are also involved in the project, though MHCLG are leading on data collection, which is the reason for the Sandbox application).
What is your registered address?	Fry Building, 2 Marsham St, London, SW1P 4DF
Where is the team developing your product	N/A

or service based (if different from above)?	
Who is your authorising senior manager?	[redacted]
Who is your Sandbox Single Point Of Contact (SPOC)?	[redacted]
What is your organisation's website URL?	https://www.gov.uk/government/organisations/ministry-of-housing-communities-and-local-government
What is your ICO registration number?	Z7123035 (MHCLG)
Have you reported any incidents, or had any enforcement action taken against you initiated by the ICO in the last two years? **If yes, please provide brief details, and if possible include the date the matter was reported and the ICO reference number.**	[redacted]

	[redacted]
Are you a micro, small, medium-sized or large enterprise/organisation?	Large
Do you employ or are you in anyway associated with former ICO staff?	[redacted]

If yes, please explain the role of the former ICO staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.	[redacted]
Do you employ any staff who are related to or are in anyway associated with an ICO staff member? **If yes, please explain the role of the staff member and whether they are expected to have any contact or dealings with the ICO during the Sandbox.**	[redacted]
Your product or service	
What product or service do you wish to participate in the ICO Regulatory Sandbox?	The Ministry of Housing, Communities and Local Government (MHCLG) private rented sector policy team, along with the Department of Work and Pensions (DWP) and Blackpool Council are running a pilot programme to try and improve the quality of housing in Blackpool [redacted]

What do you consider to be the lawful basis for the processing in your proposed innovation?	*Please reference Article 6 and Article 9 (if required) of the GDPR in your response. And refer to our guidance as necessary.* [redacted]
What are the specific data protection issues you are dealing with that mean your product needs to enter the Sandbox?	*If possible please refer to the specific provisions of GDPR/Data Protection Act 2018 that are relevant and indicate if any of the following DP challenges are relevant:* • *Use of personal data in emergent or developing technology such as biometrics, internet of things, facial recognition, wearable tech, big data, cloud-based products.* • *Complex data sharing at any and all levels.* • *Building good user experience and public trust by ensuring transparency, clarity and explainability of data use.* • *Perceived limitations, or lack of understanding of GDPR/DPA18 provisions on automated decision making, big data, machine learning or AI.* • *Utilising existing data (often at scale and in linking data) for new purposes or for longer retention periods.* • *Building privacy by design into product development taking account of cost issues and difficulties of doing this until testing has been undertaken.* • *Ensuring the security of data and identifying data breaches in complex and innovative environments.* [redacted]

	[redacted]
Will your product or service process personal data within the UK?	[redacted]
Will your product or service process special category data? If yes, please specify.	
Does your product or service involve any form of international data transfer? If yes, please specify.	
Is your product or service likely to result in a high risk to the rights and freedoms of individuals? If yes, please specify.	
How is your product or service innovative?	*We will interpret innovation broadly as any new idea, device or method, including new approaches to achieving existing objectives.* *Use any qualitative or quantitative measures as appropriate*

	Pay particular attention to explaining in what way the idea, device or method is sufficiently different to previous approaches to be considered innovative. [redacted]
How and to what extent will your product or service benefit the public?	*We will interpret public benefit broadly to encompass any demonstrable positive benefit to the public with no form of benefit being more valued than any other (e.g. health and wellbeing or financial). We also consider public benefit to cover business benefit in terms of 'back-office' solutions; however care needs to be taken to ensure that the ultimate benefit to the public is articulated (e.g. in efficiency savings).* *In assessing public benefit we will consider the potential depth (the amount of benefit experienced) and breadth (the volume of people benefiting) of your product or service using the criteria indicators provided alongside the other criteria and factors listed.* *Please use any qualitative or quantitative measures as appropriate.* *Particular attention should be given to explaining the extent of benefit realised 1) as a direct result of sandbox participation or 2) should the product/service be successful post-sandbox.* *Products/services need not be both broad and deep in their benefit to be considered.* [redacted]

Does your product or service require any other form of regulatory authorisation to proceed? Or are there any other regulatory implications that we need to be aware of? **If yes, provide information on its current status and/or what these implications are.**	[redacted]
Your proposed Sandbox plan	
What activity do you want to undertake in the ICO Sandbox?	*Please describe what specific activity you want to undertake in the Sandbox, referring to both advisory assistance and adaptive mechanisms (e.g. statement of regulatory comfort upon exit).* *We will design and agree further Sandbox mechanisms with you, if you are successful, in your bespoke Sandbox plan.* [redacted]
Do you want to undertake any form of	*If you wish to include live testing in your Sandbox participation we will require you to provide assurance to us that you have mitigated risks before processing can start.*

testing involving 'live' personal data as part of your sandbox participation? **If yes, provide details and how you will control any risks to data subjects.**	*Please read the ICO's guidance regarding Data Protection Impact Assessments for further information. Live testing will only be considered in relation to data subjects based in the UK.* [redacted]
What is your proposed timeline and the key milestones of your proposed participation in the Sandbox?	*Although the Sandbox beta phase ends in September 2020, there is no requirement for your participation to last up until this date. We are equally interested in short engagements.* [redacted]

What are the key risks to data subjects of your involvement in the sandbox?	[redacted]
What control mechanisms will you use to prevent harm to data subjects?	
What actions will you take in the event of a control mechanism failure and in particular in case of any breach?	
What is your proposed exit plan if it is unsuccessful (i.e. there is a technological failure)?	