Data Protection Impact Assessment – Demand Responsive Transport (DRT) Scheme

A Data Protection Impact Assessment ("DPIA") is a process that assists organizations in identifying and minimizing the privacy risks of new projects or policies.

The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Working through each section of this form will guide you through the DPIA process.

The requirement for a DPIA will be identified by answering the questions below If a requirement has been identified, you should complete all the remaining sections in order.

Conducting a DPIA should benefit the Council by producing better policies and systems, and improving the relationship with individuals.

The Data Protection Impact Assessment Statement in **Section 7** should be completed in all cases, and a copy of this document should be sent to the Data Protection Officer to record and review.

The Data Protection Officer will review the DPIA and will provide feedback. The feedback will confirm whether the proposed measures to address the privacy risks identified are adequate, and make recommendations for additional measures needed.

These measures will be reviewed once in place to ensure that they are effective.

Advice can be found at the beginning of each section, but if further information or assistance is required, please contact the Data Protection Officer on 01923 278362 or via email to bahzad.brifkani@watford.gov.uk.

More information on DPIA can be found on ICO website

This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

1. Are you collecting more than an individuals' name and contact details.

   Yes ☒ No☐operator will be running service on behalf of Council – we will be joint data controllers

2. Are you going to use the data you collect to do any evaluation or scoring relating to that individual

   Yes ☐ No☒

3. Is the system you are going to use able to make automated decisions relating to the individual

Yes ☐ No☒

4. Is the system capable of undertaking systematic monitoring of the individual

   Yes ☐ No☒

5. Is the system going to process sensitive or highly personal data

   Yes ☐ No☒ payment card details will be collected by the operator, but **not** shared with the Council

6. Is the system going to process large volumes of personal data

   Yes ☒ No☐ but the operator will be the main processor of the data on behalf of the Council

7. Is the system going to be used to record the personal data of vulnerable individuals

   Yes ☒ No☐ the operator will collect the name, email address, DOB and payment card details of users and these may include vulnerable people if they choose to register and use the scheme – however, this data will only be shared with the Council at the end of the contract/termination where data will need to be passed on to a new operator to carry on the service

8. Is the system using untried or cutting edge technology

   Yes ☐ No☒

If you have answered Yes to any of these statements a DPIA may be required

Section 1 - Identifying the Need for a DPIA

Briefly explain what the project aims to achieve, what the benefits will be to the Council, to individuals, and to other parties.

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarize why you identified the need for a DPIA.

BIKE SHARE

As part of Watford's ambitions to develop sustainable transport, one of the Mayor's commitments, embedded into the Council's Corporate Plan, is to 'is to invest in new bus services.' This will support the provision of sustainable transport as Watford grows and there is ever-increasing pressure on the transport network. It also supports the delivery of a number of our key priorities by being fully accessible, more affordable and leveraging digital technology.

The council is working on a number of sustainable transport initiatives and a Demand Responsive Transport (DRT) scheme fits within an overall Sustainable Transport programme. The programme aims to relieve the congestion on Watford's roads/parking, promote more sustainable modes of travel and improve air quality, particularly in the light of additional growth for Watford expected to be around 800 new dwellings per year. A DRT ride share service supports the programme's objectives to:-

- Encourage a change in the way we use local transport as 'a way of life'
- Improve Watford as a sustainable transport town
- Improve accessibility and mobility within the town
- Improve health and wellbeing.

Due to its compact urban nature (8 square miles), Watford lends itself to this type of transport system. It is expandable and scalable as demand increases and in the schemes researched there has been an expansion of the operating area (or it is currently under consideration) due to latent demand, which can be measured using the App technology.

A DRT scheme would continue Watford's reputation as a progressive Local Authority in Hertfordshire and drive a shift to multi-modal journeys. It will also support our Watford 2020 agenda in utilising digital technology (via an app and online) to register, book, pay for and use the service.

Watford's roads are very congested during peak travel periods, lengthening journey times, impacting air quality, putting pressure on car parking capacity and hampering sustainability efforts. Transport for London's recent decision not to proceed with the Metropolitan Line Extension (MLX) has also removed the opportunity to alleviate traffic congestion from West Watford to Watford Junction, with alternative solutions still to be explored. These issues will only increase as Watford's residential and working population continue to grow, putting further pressure on an already stretched transport network and infrastructure. There is an over-reliance on the use of private vehicles, taxis are expensive with variable customer service and the network buses have limited dedicated bus lane availability.

The scheme will enable regular and one-off users to book a ride, be picked up within a short walk of their location and be dropped off at their destination…

…the DRT ride share scheme will be inexpensive and will enable regular users to obtain discounts on pricing. As this is a ride share scheme passenger rides will be aggregated to ensure a more sustainable mode of transport.

Registration via the app/online will require the user to input certain information and payment card details.

Section 2 - Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Data is collected, stored, controlled and deleted by the DRT operator on behalf of the Council. The Council will not directly collect, store or delete an individual's personal data. The Council will be joint data controller with the operator. Data is stored in the App provider's cloud located within the EU. The system has a 'role' based authentication system (RBAC flexible per product), so no person has independent access to the system. The Council will only receive the customer data on completion/termination of the contract so that it can be passed to a new operator to carry on the service. The Council will only ever share this data with a third party in these circumstances.

The operator collects some personal data from its users, and none of this data falls into any special category. It stores a user's personal data for as long as their account is in active use and as much as 2 years after a user last used the service (which could include logging into the app, booking a ride etc). The exception to this is if a user requests that we delete their personal data, in which case their account will be closed and personal data deleted upon request.

In order to register for the service users are required to provide a first and last name, mobile number and an optional email address. This email address is stored in their backend systems and sent to third-party analytics and support services, but is not accessible to anyone outside the company. On registration, the user reviews and signs up to the operator's app data privacy policy.

The operator may use a user's mobile number (and e-mail address if provided) to contact them as part of the normal operations of our service (e.g. payment receipts, journey summaries). It will only send the user marketing or promotional texts/emails if they explicitly consent to receive such communications during the registration process.

Payment card details are required at registration and entered via the App using a STRIPE interface – Card number, expiry date and CVC are entered and held in the STRIPE interface, not in the App. STRIPE services in Europe are provided by a STRIPE affiliate - STRIPE Payments Europe Limited ("STRIPE Payments Europe") - an entity located in Ireland.

For journey history, the operator will track and keep a record of each individual's bookings and journey history – this will be used for analytics and to continuously improve the service.

The scheme is a digital service via a dedicated app and website. The app and website are designed, owned and run by the operator on behalf of the Council.

There is risk of data breach whereby personal data collected, stored and controlled by the operator could be lost or compromised via the app/servers.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The operator collects some personal data from its users, and none of this data falls into any special categories. It stores a user's personal data for as long as their account is in active use and as much as 2 years after a user last used the service (which could include logging into the app, hiring a bike etc). The exception to this is if a user requests that they delete their personal data, in which case their account will be closed and personal data deleted upon request.

- First name – on registration
- Surname – on registration/updated on change of name
- Mobile number – on registration/updated on change of name
- Optional e-mail address - on registration/updated on change of e-mail address
- Payment card details – on registration/updated on expiry
- History of previous hires/journeys – whenever a journey is booked/taken

Any person, regardless of where they are located, will be able to download the app or access the website. However, the area of bus operation will only cover the Watford Borough Council boundary to begin with.

Forecasting is done on number of bus rides, rather than number of individuals registered. Hence, rides forecast are 130,614 in year 1 and 269,347 in year 4 - the majority of individuals will take multiple rides throughout the year.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Although a joint data controller, the Council will not have any direct relationship with the individuals, as all registration and ongoing processing of data will be undertaken by the operator on behalf of the Council. The Council would only see and receive the scheme's personal data on completion/termination of the contract so that a different operator can take forward the service and the people of Watford do not lose access to their DRT ride share service.

It is possible that vulnerable customers will use the scheme.

The Council is assured by the GDPR compliance, technology and data integrity arrangements of the operator.

Personal data is only collected from users who register to use the operator's service. Under the GDPR, users are able to request a copy of all personal data held, as well as request deletion of their personal data in the form of deleting their account (meaning they are no longer able to use the service).

Personal data is fully secured within the app system using a secure payment gateway through the Stripe Payment Service Provider. The operator uses SMS verification, allowing no more than two accounts on a single phone. In addition, it can regulate the amount of credit a person can accumulate for the service. It's customer operations centre regularly audits the systems to regulate and identify anomalous behaviour and identify these for further analysis.

The collection of route data against journeys taken by users is not a particularly new concept (this is similar to ride-sharing apps and some other DRT services), and while this does raise some privacy concerns (detailed later), they are not specific to the chosen operator. The App collects this data through a user's registration and booking history, their mobile device is not tracked itself.

During the registration process, the operator makes full disclosures on the data it is collecting and what is done with the data. Consent is also obtained to use their personal data for marketing (not from third parties, only from the chosen operator).

The complete IT infrastructure is hosted by INNOVO Cloud in Eschborn (Germany). INNOVO CLOUD is certified: ISO 27001, ISO 9001, ISO 14001, ISAE Type I & II and SAP Certified Provider in Cloud Operations Platform.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

There are three core drivers for the collection and processing of data:

1. To enable the delivery of the service to users. A mobile phone number is required for users in order for them to create an account and use the service. This is used to engage with them around billing and support (as well as marketing, if they consent). Location data is used when booking to provide journey information to users and to calculate journey costs.
2. To enable the operator to improve the service to users. The operator uses data on how users interact with the mobile app and journeys taken to help them understand how it can improve the digital experience (through the change or addition of features), as well as to help improve the operations that support the service.
3. To engage third parties in the improvement of mobility services & infrastructure. The operator uses aggregated journey and route data to work with third party organisations, such as local authorities and transport bodies, to understand how improvements to mobility services and infrastructure can be made. This data is never linked back to individual users and is not sold or shared with the intention of being able to market additional services to our users.

Section 3 – Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organization? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

All operators bidding under the tender process completed the relevant GDPR checklist and schedule, including the winning bidder.

T&Cs were published to operators on the portal and included terms relating to Data Protection & Disclosure and Council Data.

Legal has been involved in the procurement process and the Data Protection officer is now being engaged through this DPIA process.

The chosen operator has undertaken user testing to understand any privacy concerns and to ensure it communicates disclosures in a clear way during the registration process. The collection and processing of data described has been determined through an internal design process to understand what data is required, why and measures taken to ensure the protection of that data.

Section 4 Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The Council will not have any direct relationship with the individuals, as all registration and ongoing processing of data will be undertaken by the operator on behalf of the Council.

The collection and processing of data described is a core requirement in order to provide Ride share services to users, and supports efforts to engage third parties in understanding and improving mobility services and infrastructure in urban areas. The level of personal data collected and processed is the minimum required to achieve these outcomes and the operator has taken every effort to address and minimise any privacy concerns.

The chosen operator has chosen to demonstrate compliance with the GDPR in order to best protect the data and privacy of its users.

The chosen operator has chosen to locate all our data within the EU and ensures that any third party processors are fully GDPR compliant, with data processing agreements in place.

Users will be able to update their personal information via the app or online and ensure data quality.

Section 5- Identifying & Reducing the Privacy Risks

Source of risk and nature of potential impact on individuals	Measures to reduce the risks	Arriva commentary
1. Unauthorised access to operator databases giving access to email addresses, journey data and payment identifiers	Conduct regular security reviews and penetration tests to spot potential areas for attack	Security reviews are in place within Arriva's policies and procedures. For this contract specifically, it will be reflected in Arriva/ioki's ways of working underpinned with contractual clauses for compliance.
	Use cloud infrastructure and products rather than self hosting to draw on the security and expertise of other teams	The complete IT infrastructure is hosted by INNOVO Cloud in Eschborn (Germany). INNOVO CLOUD is certified: ISO 27001, ISO 9001, ISO 14001, ISAE Typ I & II and SAP Certified Provider in Cloud Operations Platform. The system has a Role based authentication system (RBAC flexible per product), so no person has independent access to the system – administrators need to create a user.
	Regular training and controlled permissions for the internal team to prevent accidental leak of credentials/data	This takes place within Arriva in line with our Group InfoSec policy and procedures. Ioki has a similar practice based upon policies in place that have been audited by their parent, DB.
2. Unauthorised access to third party analytics services giving access to email addresses and app usage data	Conduct a level of due diligence and research when choosing the third parties to work with, ensuring they meet certain standards for data protection	All third parties are assessed using Arriva's procurement framework which feature DP extensively. This is also reflected through any contractual agreements put in place with third parties with an extensive number of DP clauses that outline clear responsibilities of data processor and data controller. ioki has a similar approach to its third party selection and these are all listed and named within the Arriva/ioki contract, with obligations on ioki to ensure that they have completed due diligence
3. Unauthorised access to support services giving access to support services giving access to email addresses and the ability to impersonate operator staff	Use of single sign-on, staff training and regular review of access/accounts	Single sign on in place within both Arriva and ioki with passwords being updated on a 90 day cycle. Accounts are updated regularly with a leaver policy in place to delete accounts and a regular review of number of users. Where users are dormant for a period of time, their accounts are removed.

Source of risk and nature of potential impact on individuals	Measures to reduce the risks	Arriva commentary
4. Unauthorised access to the operator dashboard giving access to email addresses and journey data	Use of email authentication (taking advantage of security on email accounts) and staff training	There are strict policies and procedures in place to ensure no unauthorised access to Arriva's operator dashboard. This will be fully outlined once a specific review and privacy impact assessment is undertaken on the Watford solution.
	Regular review of permissions and security built into the product, understanding what this means for the level of data access for different users	This will be fully outlined once a specific review and privacy impact assessment is undertaken on the Watford solution
5. Unauthorised access to the operator's Stripe account giving access to payment history, bank transfers and the ability to charge users	Enforce 2FA, regular review of roles and reduce the number of people with accounts with access to Stripe	STRIPE is PCI DSS and SOC 1 and SOC 2 certified (industry standards) and complies with the PSD2 payment guidelines. The passenger can pay digitally via the ioki App. The payment data is not stored with ioki, furthermore the PSP is integrated into the passenger app via SDK (Software Development Kit), i.e. no credit card data (only the last 4 digits are visible) is received by ioki when entering the payment data. This allows data security whilst still allowing the operator (Arriva) to trace which payments have been made in the respective trip details via the operator tool "Stellwerk". ioki also provides Arriva with a complete overview of the transactions in Tableau, but Arriva does not have access to extract the platform options, so that, for example, necessary refunds must always run via ioki (platform).
6. Being able to identify individual users from aggregated journey data shared with third parties	Conduct reviews of how we aggregate data and produce reports to try and spot whether patterns can be drawn that compromise user privacy	All reports drawn through Tableau are aggregated and anonymised. Where data sets are small and could be used to compromise user privacy, these are reviewed and removed from reporting until the numbers grow. We regularly review how complaints/enquiries are dealt with to ensure necessary data pertaining to the investigation of that complaint

Section 6 - Identifying measures to reduce the Risks

See table in section 5 (above).

Section 7 – Sign Off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Bahzad Brifkani Data Protection Officer 09/09/2019	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Data Protection Officer Bahzad Brifkani	The measures proposed to implement will reduce the potential risk
DPO advice provided:	Whilst there is always potential risks in processing personal data, however this DPIA demonstrate the consideration of the appropriate measures to minimize such risks.	Step 5 and 6 of this DPIA have addressed any potential risks, but it will be useful to have a regular review of this risk preferably every 3 to 6 months from the implementation of the App
Summary of DPO advice: The operator will store all of the personal data within EU according to this DPIA, it is important to be mindful that if a no deal Brexit scenario happens this could cause disruption to this service particularly when it comes to this operator transferring data to UK. ICO has issued new guidance on UK organizations which receive any transfers of personal data of EU citizens, or any personal data from EU member states, need to prepare for the possibility of no deal. Initially, at the least, the UK will not be deemed an adequate country and there will be a burden for compliance with GDPR on organizations sending personal data to the UK. This contract might need to be reviewed again closer to the Brexit time (when we are certain of a no deal scenario) to amend all the relevant clauses in relation to data transfer within EU/EEA. The DPO also advises that this DPIA is reviewed towards end of October 2019 (if we are certain of a no deal scenario) in order to update the DPIA accordingly.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		

Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	The Project Manager until launch of service Mar 2020 and the Contract Manager from Mar 2020 onwards	The DPO should also review ongoing compliance with DPIA