**Appendix 3**

Vivacity's sensor system was designed using data protection by design principles and is compliant with GDPR. The system does not produce any personal data when it is not necessary.

NORMAL OPERATION – NO PERSONAL DATA

Under normal operation, the system processes all video locally, produces anonymous data feeds and discards the video immediately. As such, during normal operation, the system produces no personal data and therefore presents no privacy or personal data risk.

SOFTWARE TRAINING - OPTIONAL

Our machine learning algorithms have been trained on images gathered from manual traffic surveys and from our deployed sensors. We are continuing to grow our image training set, as this will help us to continue to improve the accuracy of the system. In order to achieve this, and with the permission of our clients, we may choose to extract a few sample images from each new sensor installation to add into our training set.

We will always provide temporary signage in the vicinity of a sensor before gathering images for our training set. These signs state "New road space usage sensors Installed, Once fully operational they will only produce anonymous data. Video may be intermittently recorded at this location during this initial project phase, for the purpose of system development and testing".

Vivacity are registered with the ICO to enable us to collect and hold image data for the purpose of developing software to extract anonymous data from video feeds. We act as the data controller for the software training process. We have carried out Privacy Impact Assessments for this work, which can be provided to clients upon request. If requested, we will not extract any training data from a given sensor and following such a request, no personal data will ever be generated by that device.

MAINTENANCE – NO PERSONAL DATA

In order to calibrate and maintain our sensors, we occasionally send an image from the sensor back to our office. In order to ensure the maintenance images do not contain any personal data, we follow the following process:

• The sensor takes a photo and blurs a copy of the image prior to transmission • The blurred image is manually screened by an operator to ensure no possible personally identifying images may be present in the original image • If there is a risk that personal data may be in the unblurred image, the image is deleted and the operator will request a new blurred image • Once an image is confirmed as having no risk of containing personal data, the original unblurred image can then be transmitted to the operator. This image can then be used to confirm whether the camera lens requires cleaning.

This process is covered by our privacy impact assessments.

## JOURNEY TIME – ANONYMISED NUMBER-PLATE DATA

If the sensors are providing Journey Time, the system needs a method to identify a vehicle as being the same as one seen by a different sensor earlier up the road. Detecting number plates is the most reliable method of doing this. In order to ensure that no personal data is being gathered during this process, the number plates are anonymised on the device using a hashing algorithm. This algorithm will turn the number plated into a complex string of characters that cannot be decrypted back into the original number plate.

In order to avoid any personal data being extracted from the database by using pattern recognition of routes taken by a vehicle across multiple days, we replace the hashing seed on a daily basis. This means that the same vehicle will have a different identification on subsequent days.

To further protect data privacy - we rotate the hash key used every 24hrs. This means that the same vehicle license plate will generate a different hash after 24hrs and means we cannot identify and track the same vehicle across multiple days.

## CLOUD AND SERVER INFRASTRUCTURE

Vivacity Labs solution is hosted both on physical and virtual infrastructure. Our sensor (physical infrastructure) contains a camera and a processor which allows us to collect real time, anonymous data on how the road space is being used. The data is sent to the cloud (virtual infrastructure), and the video is discarded at source.

All communications to and from Vivacity sensors is encrypted. The sensors send data to Vivacity managed servers hosted on the Google Cloud Platform, located in Belgium. Each sensor has a unique security access key for talking to our servers and all data communications to and from a sensor is secured using HTTPs, TLS1.2. SSH connectivity to Vivacity managed servers is also used for remote software upgrades and with each sensor using a unique SSH key.

Vivacity does not provide publicly accessible dashboards and APIs. End user client access to Vivacity's data portal is managed by Vivacity and is limited to specific customer accounts. We have employed an expert security contractor to help review and architect a number of our systems and our security infrastructure has been implemented in accordance to their recommendations