**Data Protection Impact Assessment**

Newcastle City Centre: Pedestrian counting and still image sharing

|  |
| --- |
| 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. Summarise why you identified the need for a DPIA. |
| The most reliable and cost effective method for us to count people in urban areas is by using existing and new CCTV cameras, positioned in a manner that allows machine learning and image processing techniques to automatically identify shapes of objects, including people, and thereby provide totals. This data collection is required as part of the Urban Observatory’s ambitions to empower people to make informed decisions about the risk of visiting the city centre. Only cameras covering the busiest shopping streets are to be included.  A DPIA is required when systematically monitoring a publicly accessible place. |
| **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? |
| **Collection**  A secure connection to cameras on the CCTV network will be used. The network is isolated from the rest of the organisation and connected via dedicated equipment only used for this processing.  **Use**  Counting is performed in real-time on a stream from the camera, or with caching for short periods to balance necessary computational capacity and allow system maintenance. These counts are numbers of people crossing a line in each direction or remaining within a region, within a five-minute window, hence are considered anonymous except when counts are extremely low. Still images taken every five minutes are transferred to a web server to provide a ‘web cam’ of the street.  **Storage**  Only the still images and count data is kept.  **Deletion**  Still images are kept for no more than an hour ordinarily before being deleted automatically.  **Sharing**  The still images and counts will be publicly accessible on a website.  **High-risk processing**  Systematic monitoring of a public area using CCTV and applied AI is considered high risk per the recommendations of the ICO, and requires mitigation. |

|  |
| --- |
| **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? |
| Cameras are positioned on lamp posts and other high structures, and directed towards thoroughfares. The video streams allows movements of these people to be seen, but is typically too low in resolution to distinguish the features of a face. Only the machine learning algorithm consumes the video stream data except during maintenance and setup. The video makes it possible to determine the direction of travel, position, and in some cases activities undertaken by people within these public spaces. It may be possible with the still images to identify clothing, and with enough data, establish patterns of movements that could indicate an individual. Establishing these patterns is not possible from the people count data published. Processing is on a continuous basis for the purposes of counting and is expected to continue until there is no longer a need to inform people of the busyness of the area, which may become a permanent need. The geographic area is constrained to Blackett Street and Northumberland Street in the centre of Newcastle upon Tyne. |

|  |
| --- |
| **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)? |
| Those captured by the video footage are members of the public potentially including children or vulnerable groups, often with no pre-existing relationship, and potentially unaware of the processing even with prominent signage. However, they are likely to be aware or expect the existence of CCTV and its processing by local authorities for public safety and traffic operations. Notices also refer to the council’s “partners,” which may include contractors assisting with the setup of this system. Counting of people for statistical purposes is not uncommon, is already in operation elsewhere in the city by other operators (e.g. for Business Improvement Districts and shopping centres) and is employed extensively in other cities (e.g. Vivacity technology used in Milton Keynes and London). Counting from video streams is not new technology. |

|  |
| --- |
| **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? |
| The SARS-CoV-19 pandemic has led to multiple lockdowns and restrictions on movement to prevent the spread of the virus. Many people remain concerned about large and dense crowds and the risk of transmission it might bring. This service is intended to communicate how busy the main shopping district in Newcastle is so people can make their own decisions based on their own perception of the risk to them, such as avoiding the busiest times. The count data and images combined were found during user research to be effective at communicating how busy the area was. |
| **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 organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
| Consultations were held before processing began, with:  **Detail names:** and conservations here |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 minimisation? 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? | | | | | | | |
| **Lawful basis for processing**  People counting is conducted on the basis of legitimate interests/public task (only one, see ICO guidance), to communicate how busy the area is for the benefit of the local economy and reduced virus transmission. It is thought unlikely that people will object to this processing, given the anonymous nature of the resulting count data and the low frequency of the still images which are insufficient to identify people in most cases.  **Function creep**  Any extension of the processing undertaken will result in a review of this DPIA. Its use beyond the SARS-CoV-19 pandemic will be given further consideration before the end of 2021.  **Alternative methods**  Manual counts are prohibitively expensive for long durations. Radar-based counting was considered; however, the cameras already exist for public safety activities and radar methods are not as accurate in dense crowds where the beam is obscured. Large crowds are expected in these areas.  **Data quality and minimisation**  The quality of images will be degraded such that images capture faces with less than 25 pixels of height, preventing recognition in almost all cases.  **Providing information and supporting individual rights**  Notices are displayed on lamp posts around the city indicating the processing by Newcastle City Council and its partners for public safety and operational purposes. The website will be publicised including on social media and details for complaints will be made available on that website. If made aware of reasons why our activities could cause harm or an individual’s interests or override ours, then we will make alternative arrangements to disable processing at specific times, move our equipment, or cease dissemination activities as appropriate. | | | | | | | |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | | | **Likelihood of harm** | | **Severity of harm** | | **Overall risk** |
| **Hacking**: Unauthorised access to the CCTV network, allowing higher quality video footage to be accessed. | | | Possible | | Severe | | High |
| **Identification:** Persons with distinctive appearance could be identified from still images (such as from clothing). Only information this would provide is a direction of travel from a particular location. The same data could easily be obtained by a person on the street. | | | Possible | | Minimal | | Low |
| **Identification by combination**: Potential for people to be identified from still images, when data is combined, or with additional prior knowledge. | | | Possible | | Minimal | | Medium |
| **Accidental disclosure**: Long duration video footage transmitted by email or on web servers by accident, or lost on mobile devices and memory sticks. | | | Possible | | Significant | | Medium |
| **Identification by statistical obscurity**: Persons performing repetitive actions at times when other people are not active could potentially be identified, such as counting those on an incredibly quiet street every night at 3am. The streets in question are relatively busy at all hours. | | | Remote | | Minimal | | Low |
| **Intentional leak**: Large volumes of recorded video footage or images intentionally released. | | | Remote | | Severe | | Medium |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | | **Residual risk** | | **Measure approved** | |
| Intentional leak | Access logs kept for the systems involved and imagery and video data kept only for very short durations. | Reduced | | Low | | Yes | |
| Hacking | Two-factor authentication enabled on servers. IP limitations to constrain access to small number of machines. Software updates performed on servers on weekly basis. | Reduced | | Low | | Yes | |
| Identification | Small counts (<5) removed from the statistics or aggregation period adjusted to avoid these small counts. Some randomisation in the timing of the snapshots. Reduced resolution for the images. Cameras not used in locations where people might linger for longer durations, such as where street cafes and restaurants are operating. | Reduced | | Low | | Yes | |
| Accidental disclosure | Data only retailed for very short durations and video footage not retained. Additional network security constraints applied to egress from the CCTV network. | Reduced | | Low | | Yes | |

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/date** | **Notes** |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: |  | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| 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 DPO should also review ongoing compliance with DPIA |