NEC Europe Ltd.

GDPR Consultation Paper

NEC response to government consultation on General Data Protection Regulation (GDPR) 2018 lawful processing, consent and processing of personal data relating to criminal convictions and offence guidance.

As context, this document covers information about NEC relevant to the consultation and asks that the views contained in this report be taken into account in the government review of the legislation before the implementation of the GDPR legislation in 2018.

About NEC: NEC offers a full range of facial recognition solutions built upon its award winning, industry-leading NeoFace, facial recognition algorithms. In the realm of public safety, using images and video evidence of varying quality, NeoFace enables law enforcement to investigate, solve crimes and bring more offenders to justice by accurately searching photo databases. For real-time surveillance applications, NeoFace allows for rapid and accurate searching of live camera feeds against a known watch list, providing an alert when a face in a watch list is detected. Border and immigration control, perimeter and office security as well as retail loss prevention are among the extensive use cases of NeoFace applications.

The strength of NEC's NeoFace technology is with its tolerance for poor quality images. Highly compressed surveillance videos and images, previously considered of little or no value, can now be a source of useable evidence and lead to higher rates of positive identification. There is a significant difference in NEC facial recognition technology and other facial recognition systems in the market; as evidenced by the independent tests carried out by the US National Institute of Standards and Technology. NEC's facial recognition technology is used worldwide for fighting crime, preventing fraud and improving public safety.

Our Response: NEC facial recognition products provide solutions for highly reliable and accurate identification. Faced with ever-increasing threats, as well as the need for improved customer engagements and loss prevention, public safety agencies (such as law enforcement, national security, border control, and immigration) along with private sector enterprises around the world are increasingly turning to facial recognition. We believe the data protection reform scheduled for May 2018 and the ICO guidance is useful and appropriate. However, we have concerns for certain groups who are currently using facial recognition technology, that would under GDPR end up with no legal basis for processing special categories of personal data. Technological advances such as facial recognition now play an important role in the detection and prevention of crime and GDPR would potentially compromise this activity. This response underlines those concerns.

- **Lawful processing/Consent**

GDPR broadens the definition of personal data (by expressly including identification numbers and location data) and sensitive data (by including biometric data)

Facial recognition data would under GDPR therefore be deemed as sensitive personal data. Consent to store it would require some form of clear affirmative action to gain explicit consent. However, with the prime purpose of facial technology being used for crime prevention and detection, then it would be highly unlikely that an offender would provide their explicit consent. As there would then be no legal grounds for the lawful processing of biometric data for the purposes of crime and disorder or anti-social behaviour, then this would significantly compromise the ability of law enforcement agencies to prevent or detect crimes

In addition to law enforcement and national security, the private sector also needs to process special categories of data to manage crime and disorder in their environments and premises, and the same challenges would exist here that those who should be placed on a facial recognition watch list (such as those who have committed acts of violence at sporting stadia, or those who have committed theft from retail establishments) would be highly unlikely to provide their explicit consent.

We would be very grateful if the government would considers the impact of Article 6, provide additional grounds for the processing of special category data, and explicit consent guidance which would not compromise the purpose of processing.

- **Processing of personal data relating to criminal convictions and offences**

Currently, organisations including law enforcement agencies, airport authorities, border control agencies, retailers, hoteliers, stadiums, and casino's are processing data using facial recognition technology for the purposes of managing crime and disorder, minimising the risk to the public; and meeting compliance with regulatory requirements. This makes the United Kingdom a safer and smarter country to live in. Currently under Directive 95/46/EC "*Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law…*". The UK implemented the Directive in the form of the Data Protection Act 1998 and included criminal conviction data within the definition of "sensitive personal data" which therefore provides "suitable specific safeguards". Organisations are therefore currently able to process criminal conviction data in reliance on one of the processing conditions set out in Schedule 3. This interpretation of the law allows organisations in both the private and public sector to process this data with the appropriate safeguards.

However, GDPR Article 10 states that "*processing of personal data relating to criminal convictions and offences or related security measures based on Article 6 (1) shall be carried out……when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*". The private sector will therefore be unable to process criminal conviction data unless: (a) it is explicitly authorised by UK law – maintaining the current arrangements will not be adequate as consent alone is not an adequate basis for processing or holding this data under GDPR; and (b) such authorising law provides for appropriate safeguards for data subjects. The private sector organisations will therefore require the government adapt the existing GDPR legislation to authorise them to process criminal conviction data for the purposes of identifying risk and preventing fraud and ensure that any such authorising legislation provides for appropriate safeguards. The technological advances of facial recognition are providing our society with benefits of less crime and a safer place to live.

We would ask that the government consider widening the definition to include private sectors and apply the appropriate safeguards required for special categories of data to be put in place.

It would also be useful to encourage the consideration of data sharing with the appropriate parameters in place. Under the GDPR it would not be possible to share data between the private and public sector. This is required for the purposes of data matching, verifying details and ensuring data is accurate. Currently the private sector supports the government agenda and strategies for Counter Terrorism, Serious Organised Crime, Business Crime and Anti-Social Behaviour. This would be much more difficult in the future should the GDPR legislation remain as it stands.

➢ The legitimate interests and freedoms of individuals

With GDPR giving data subjects more rights and putting in more safeguards it is clear that any processing should be carefully considered and the appropriate safeguards should be put in place.

At NEC we are keen and very supportive of following guidelines which include the Protection of Freedoms Act, CCTV surveillance laws and any other relevant laws in this area including the data protection reform. We consider the below points are paramount to the processing of special category data and we work in line with these initiatives:-

- Privacy by design and default to be an initiative of the beginning of any product or service to ensure it is not a mere afterthought. This allows NEC products and services to provide leading technology that is compliant with the applicable laws and embed design privacy in design features.
- Have appointed a Data Protection Officer to be accountable and take responsibility for data protection and is also a member of the management board.
- Privacy impact assessments to be carried out for the processing of sensitive data and also assist third parties.
- Privacy impact statements are not meant to be in place to override consent and allow data subjects to opt-out, but is used to show openness and transparency wherever possible in public areas in the legitimate interests, freedoms and privacy of individuals.
- To document, follow and review storage, retrieval, retention and deletion of data and the access to such data.
- Apply the appropriate technical and organisational security measures are in place with the aim to minimise risks and apprehend crime.

NEC facial recognition technology can be used less intrusively as a result of the above safeguards being in place and is less intrusive than CCTV as the system can be configured to store the watch list and matches only, rather than retaining images of everyone passing through the CCTV cameras. This ensures that personal privacy is maintained and ensures that NEC complies with the legislation and the spirit of the legislation.

This document explains the view of NEC that the government does need to amend the GDPR legislation to keep people safe and allow the private sector to support the government strategies for Counter Terrorism, Serious Organised Crime, Business Crime and Anti-Social Behaviour.