FACT SHEET ON YOUR DATA RIGHTS IN RELATION TO POLICE SURVEILLANCE AT PROTESTS

This is based on UK data protection legislation. The UK's General Data Protection Regulation (UK GDPR) does not apply to processing of personal data for law enforcement purposes by relevant authorities.

What can happen to my personal data at a peaceful protest?

- The most common personal data processed at a protest are notes and photographs taken by police officers, along with voice and video recordings taken from body-worn cameras or drones.
- Data processing can also happen with sophisticated surveillance tools and techniques that you might not be aware of, including facial recognition technology, mobile phone extraction, IMSI catchers and hacking.
- There is no requirement that the protest be violent or at risk of becoming violent before data processing can begin. Moreover, the police are not limited to processing data in relation to preventing offences at the protest. For example, they may process data for the purpose of identifying individuals who are subject to an arrest warrant unrelated to the protest.
- The police do not have to obtain your consent before processing your data.

Are there limits on what the police can do when it comes to my data?

- The police can process personal data at protests, but there are limits. They have to be exercising law enforcement functions and it has to be necessary for the administration of justice (or any other function of a public nature).[1]
- When it comes to sensitive data, like facial images which could be used to identify an individual, the data can only be processed where it is strictly necessary for the administration of justice.[2]
- There are also some forms of data processing that can amount to an interference with the human rights of individuals attending the protest, specifically the right to private life.[3] In order for the police to justify the interference it must be proportionate to the objectives of maintaining public order and preventing or detecting crime.[4] The use of facial recognition technology is one example of data processing which might violate human rights if the proportionality criteria have not been met.[5]
- The police must conduct a Data Protection Impact Assessment before processing data in a way which presents a high risk of violating individual rights.[6] Although there is no legal obligation to publish the assessment, many police forces do so on their websites.
- Police may only hold data for as long as it is necessary to do so.

1. Data Protection Act 1998, Schedule 2(5)
2. Data Protection Act 2018, Section 35
3. Human Rights Act 1998, Schedule 1, Article 8 ECHR
4. R (Catt) v Commissioner of Police of the Metropolis [2015] 1 AC 1065; [2015] UKSC 9 at [17]
5. R (Bridges) v Chief Constable of South Wales Police [2020] 1 WLR 672; [2019] EWHC 2341 (Admin)
6. Data Protection Act 2018, Section 64

Do the police have to inform me that they are processing my personal data?

- Police must make information about their data processing activities generally available to the public.[7] This includes general information necessary for accessing your data and making a complaint about how the police have processed your data. But they don't need to tell you more than that.
- The police are not required to provide notification to you each time they process your data.

Can I see the personal data that was collected on me by the police?

- Individuals can request access to the data about them held by the police. The police must respond by providing access to the data without undue delay and at the latest within one month of receiving the request.[8]
- In addition to receiving the actual data, individuals are entitled to information about the data, including the purposes for which it is held and who it has been disclosed to.
- Individuals have the right to access data about them held by the police, including the right to information about whether the police have processed data about the individual.[9]

What happens if the police refuse to tell me what data they have collected about me?

- The police may refuse to disclose data they have retained about you where it is necessary to protect investigations or prosecutions, protect national or public security and to protect the rights and freedoms of other people.[10]
- Ordinarily the police must provide reasons for refusing to disclose the information, unless providing reasons would undermine the purpose of refusing to provide the information.
- The police may also refuse to disclose data which has been deleted in accordance with the law.[11]

What happens if the personal data held by the police is inaccurate

- Individuals have a right to have their personal data rectified if it is inaccurate or incomplete.[12] If the individuals make a request to have data about them corrected, then the police must fix the inaccuracy without undue delay although there is no fixed deadline.

I'm worried that the police unlawfully processed my data/ unfairly restricted my rights. What can I do?

- You can make a complaint to the police force which processed your data or to the Information Commissioner's Office.[13] In every decision made about your data and communicated to you by the police, you should be provided the contact details of the ICO.

7. Data Protection Act 2018, Section 44
8. Data Protection Act 2018, Section 45(3), Section 54
9. Data Protection Act 2018, Section 45
10. Data Protection Act 2018, Section 45(5)
11. Data Protection Act 2018, Section 39(1)
12. Data Protection Act 2018, Section 46
13. Data Protection Act 2018, Section 165