Policing, Mass Protests & Data Protection

Doughty Street Chambers
Actions Against the Police & Media Teams
What we will cover

1. Brief overview of the GDPR/DPA 2018 framework
2. Information sharing by police forces
3. Citizen journalists
4. Challenging retention of data
Policing, Mass Protests & Data Protection

Caroline Addy
Brief overview of the GDPR/DPA 2018 framework
Brief overview of the GDPR/DPA 2018 framework

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability
Chapter 3 applies only in relation to the processing of personal data for a law enforcement purpose.
College of Policing: Sharing Police Information

Processing of personal data for “law enforcement purposes” is not covered by the GDPR but by the Law Enforcement Directive, which replaced the European Council Framework Decision 2008/977/JHA.
College of Policing: Sharing Police Information

• Sharing police information must be linked to a policing purpose.

• There must also be a pressing social need to share information.

• Sharing information under statutory obligation does not require an ISA.

• The police service must seek consent only where strictly necessary and only where it cannot establish a policing purpose for processing.

“The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and should be able to demonstrate that processing activities are in compliance with this Directive. Such measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children.”
R (M) v Chief Constable of Sussex and BCRP [2019]
EWHC 975 (Admin)

Facts:
• C was a vulnerable teenager and frequent runaway with many convictions for shoplifting and assault. Her full name, d.o.b., photograph, criminal record and bail conditions were shared by police with a Business Crime Reduction Partnership in her local area. Police also disclosed that she was judged to be at risk of child sexual exploitation.

Issues:
• Did the 2018 agreement between police and BCRP conform to the provisions of DPA 2018?
• Did the disclosures made about C under the 2017 agreement between the same parties breach the DPA 1998?
R (M) v Chief Constable of Sussex and BCRP [2019] EWHC 975 (Admin)

Decision:

• Sharing C’s bail conditions with BCRP did not breach the reporting restrictions order made re C under the CYPA or Youth Justice and Criminal Evidence Act 1999 as the BCRP were not ‘members of the public’ in this context;
• Sussex police and BCRP were joint data controllers; and
• The combination of safeguards in the information sharing scheme was sufficient to comply with the DAP 2018.
Cooper v National Crime Agency [2019] EWCA Civ 16

Facts:

• SOCA/NCA dismissed Mr Cooper on grounds that Mr Cooper’s arrest and charge for being drunk and disorderly in a public place and with assault on a police officer, had been a serious breach of the SOCA Code.

• The ET and the EAT held that in the circumstances dismissal was within the range of reasonable responses available to SOCA as employer of Mr Cooper.

• (The EAT remitted the case back to the ET for it to give proper consideration to Mr Cooper's case on data protection breaches. SOCA cross-appealed. Mr Cooper also appealed the refusal of the County Court to award him damages for unlawful processing of his sensitive personal data (the information from Sussex Police) contrary to the DPA 1998.)
Cooper v National Crime Agency [2019] EWCA Civ 16

Decision:
• SOCA became a data controller in respect of the Brighton custody material (and some of the information in that material which was provided by Sussex Police in advance of 4 May 2012) when it came into SOCA's possession;
• Processing the Sussex Police information was necessary—in this context that meant ‘reasonably necessary’ and the last restrictive means of achieving a legitimate aim;
• Applying and enforcing the provisions of its employment contract with Mr. Cooper were a part of SOCA’s statutory functions;
• SOCA had a compelling legitimate interest in processing the data as it did (internal disciplinary proceedings) and it was in the public interest;
• SOCA did not breach the second data protection principle by using Mr Cooper’s data for a purpose different from that of Sussex Police in obtaining it.
Joint data controllers

From the Article 29 Working Party’s Opinion 1/2010 on the concepts of controller and processor:

“The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Therefore, determining control may sometimes require an in-depth and lengthy investigation. However, the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. In this perspective, rules of thumb and practical presumptions are needed to guide and simplify the application of data protection law.”
Joint data controllers

From the Article 29 Working Party’s Opinion 1/2010 on the concepts of controller and processor:

“The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Therefore, determining control may sometimes require an in-depth and lengthy investigation. However, the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. In this perspective, rules of thumb and practical presumptions are needed to guide and simplify the application of data protection law.”
From the Article 29 Working Party’s Opinion 1/2010 on the concepts of controller and processor:

“The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Therefore, determining control may sometimes require an in-depth and lengthy investigation. However, the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. In this perspective, rules of thumb and practical presumptions are needed to guide and simplify the application of data protection law."
OPINION OF ADVOCATE GENERAL BOBEK
Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

The problem: who then is not a joint controller?

71. Will effective protection be enhanced if everyone is made responsible for ensuring it?

72. ... In the understandable desire to secure the effective protection of personal data, the recent case-law of the Court has been very inclusive when being asked to define, in one way or another, the notion of (joint) controller. So far, however, the Court has not been faced with the practical implications of such a sweeping definitional approach with regard to the subsequent steps of exact duties and specific liability of parties who are classified as joint controllers.
OPINION OF ADVOCATE GENERAL BOBEK
Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

The problem: who then is not a joint controller?

87. ... the GDPR appears to be introducing a new regime of joint liability in its Article 26.

88. ... what seems to be a regime of joint liability for joint controllers introduced in Article 26(3) of the GDPR could turn into quite a challenge. On the one hand, Article 26(1) of the GDPR makes it possible for joint controllers to ‘determine their respective responsibilities for compliance with the obligations’. On the other hand, however, Article 26(3) of the GDPR makes it clear that the ‘data subject may exercise his or her rights’ ‘in respect of and against each of the controllers’ irrespective of any such arrangement. Any of the joint controllers can thus be held liable for the data processing in question.
Policing, Mass Protests & Data Protection
Clare Duffy
Citizen journalists: 

*Sergejs Buivids* [2019] EUECJ C-345/17
Mr Buivids “wished, by the publication of the video in question, to bring to the attention of society something which he considered to constitute unlawful conduct on the part of the police” (§18)
Citizen journalists: Sergejs Buivids [2019] EUECJ C-345/17

Art.9 of Directive 95/46

“Member States shall provide for exemptions or derogations ... for the processing of personal data carried out solely for journalistic purposes ... only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.”
Citizen journalists: Sergejs Buivids [2019] EUECJ C-345/17

(1) Did the recording and subsequent publication of the recording fall within the scope of Directive 95/46?

(2) Could Mr Buivids rely on the derogation for journalists purposes under Art.9 of Directive 95/46?
Citizen journalists: Sergejs Buivids [2019] EUECJ C-345/17

(1) Did the recording and subsequent publication of the recording fall within the scope of Directive 95/46? **YES (§47)**

(1) Could Mr Buivids rely on the derogation for journalists purposes under Art.9 of Directive 95/46?
(1) Did the recording and subsequent publication of the recording fall within the scope of Directive 95/46? **YES (§47)**

(1) Could Mr Buivids rely on the derogation for journalists purposes under Art.9 of Directive 95/46? **YES (in principle; §69)**
Citizen journalists: *Sergejs Buivids* [2019] EUECJ C-345/17

The Court’s reasoning:
1. Applicability of Art.9
2. Definition of “journalistic activities”
3. Relevant factors
4. Balancing privacy & speech
Citizen journalists: *Sergejs Buivids* [2019] EUECJ C-345/17

“... the video recording of police officers in a police station, while a statement is being made, and the publication of that recorded video on a video website, on which users can send, watch and share videos, may constitute a processing of personal data solely for journalistic purposes ... in so far as it is apparent from that video that the sole object of that recording and publication thereof is the disclosure of information, opinions or ideas to the public...”
Citizen journalists: Sergejs Buivids [2019] EUECJ C-345/17

Art.9 of Directive 95/46

“Member States shall provide for exemptions or derogations ... for the processing of personal data carried out solely for journalistic purposes ... only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.”
Art. 9 of Directive 95/46
“Member States shall provide for exemptions or derogations ... for the processing of personal data carried out solely for journalistic purposes ... only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.”

Article 85 of the GDPR
“For processing carried out for journalistic purposes ... Member States shall provide for exemptions or derogations ... if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information”
Citizen journalists: Sergejs Buivids [2019] EUECJ C-345/17
Challenging data retention
Policing tactics

Black Lives Matter protests: London demonstrators ‘were kettled, photographed and had names taken by police’

Protesters said they were left without food, water or access to toilets during a six-hour kettle on Sunday night
R (Segalov) v Chief Constables of Sussex & Greater Manchester Police [2019] ACD 17

“… is known XLW [Extreme Left Wing] activist. He has been involved in a number of protests in London including anti-austerity demonstrations and in a number of protests against BNP on 1/6/2014 at which several dozen anti-fascist protestors were arrested, and he was involved in a protest against the Commissioner of the Metropolitan Police at Sussex University on 25/2/2015”
“Personal data processed for any of the following purposes—
(a) the prevention or detection of crime, are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3...
Law enforcement processing

- Data Protection Act 2018, Part 3
- Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (aka The Law Enforcement Directive)
Rights under Part 3 of the DPA 2018 (ss.29-81)

1. Right of access
2. Right to rectification
3. Right to erasure
4. Right to restrict processing
5. Right not to be subject to automated decision-making
Rights under Part 3 of the DPA 2018 (ss.29-81)

1. Right of access
2. Right to rectification
3. Right to erasure
4. Right to restrict processing
5. Right not to be subject to automated decision-making
Right of access

Article 14

Right of access by the data subject

Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

(f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;

(g) communication of the personal data undergoing processing and of any available information as to their origin.
Right of access

• DPA 2018, s.45 and LED Art.14
• Restricted by:
  – Identity – s.52(4) DPA 2018
  – Manifestly unfounded or excessive requests – s.53 DPA 2018
  – Fundamental rights & legitimate interests – s.44(4) and s.45(4) DPA 2018
Right of erasure

Article 16

Right to rectification or erasure of personal data and restriction of processing

1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
Right of erasure

• DPA 2018, ss.47-48 and LED Art.16
• Restricted by:
  – Data processing principles
  – Obligations applicable to the processing of sensitive personal data