



# Data Protection Bill

## Factsheet – Law enforcement processing

(Clauses 29–81)

### What are we going to do?

- Update our data protection laws governing the processing of personal data for law enforcement purposes by the police, prosecutors and others.
- Strengthen the rights of data subjects, whilst ensuring that criminal justice agencies and others can continue to use and share personal data to prevent and investigate crime, bring offenders to justice and keep communities safe.
- Ensure that, following the UK's exit from the European Union, our criminal justice agencies can continue to share data with partner agencies in other EU Member States and remain at the forefront of the international effort to tackle serious organised crime and other threats to our security.

### City of London Police Commissioner Ian Dyson QPM, National Police Chiefs' Council lead on information management, said:

"The new Data Protection Bill will replace its 20th century predecessor with modern legislation and a package of reforms that protect both individuals and organisations, strengthens the regulator and introduces a bespoke framework for law enforcement.

"It is vital that policing is enabled to perform our duties by maintaining public approval of our actions. In a digital age the way we handle personal data; how we collect, store, use and dispose of it is coming under growing scrutiny. In return for willing cooperation, the public expect a proportionate balance across law enforcement of how we manage their information."



## How are we going to do it?

Provide a bespoke framework for law enforcement processing, tailored to the needs of the police, prosecutors and others (referred to in the Bill as “competent authorities”). This framework will protect the rights of victims, witnesses and suspects while ensuring we can continue to effectively tackle crime and other threats to community safety, both at home and abroad.

## Background

Processing of personal data for law enforcement purposes is currently governed by the Data Protection Act 1998 (“DPA”) and the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014. The DPA and 2014 Regulations together established a robust regime for the protection of personal data by law enforcement agencies, both domestically and when transferred internationally.

Since the advent of the DPA, advancements in technology have led to increasing rates of personal data processing and transferral, both internally and cross-border. An increase in the collection and sharing of personal data comes with the need for a stronger and more coherent framework for the protection of personal data.

In April 2016, the EU agreed the Law Enforcement Directive (“LED”) to govern “the processing of personal data by the police and other criminal justice agencies for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data”. The LED applies in relation to the cross-border processing of personal data for law enforcement purposes. To ensure a coherent regime, the provisions in Part 3 of the Bill also apply to the domestic processing of personal data for such purposes. This will ensure that there is a single domestic and trans-national regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector.

## Key law enforcement data processing provisions

Part 3 of the Bill strengthens the rights of data subjects whilst enabling a controller to restrict these rights where this is necessary to, amongst other things, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences, for example by revealing to a person that they are under investigation. This Part:



- Sets out six data protection principles which apply to law enforcement processing by a competent authority. The requirements are that:
  - processing be lawful and fair;
  - the purposes of processing be specified, explicit and legitimate;
  - personal data be adequate, relevant and not excessive;
  - personal data be accurate and kept up to date;
  - personal data be kept no longer than is necessary; and
  - personal data be processed in a secure manner.
  
- Sets out the rights of individuals over their data. These include:
  - rights of access by the data subject to information about the data processing (including the legal basis for processing, the type of data held, to whom the data has been disclosed, the period for which it will be held and the right to make a complaint);
  - the right to rectification of inaccurate data and of erasure of data (or the restriction of its processing) where the processing of the data would infringe the data protection principles; and
  - rights in relation to automated decision-making (that is, decision making that has not involved human intervention).
  
- Places restrictions on those rights, but only where necessary and proportionate in order to:
  - avoid obstructing an investigation or enquiry;
  - avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
  - protect public security;
  - protect national security; and
  - protect the rights and freedoms of others.