# The Information Commissioner's response to the House of Commons Justice Committee consultation on the implications of Brexit for the justice system

## Introduction

1. The Information Commissioner (the 'Commissioner') has responsibility in the United Kingdom for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations 2003, as amended (PECR). The Information Commissioner also has a more limited supervisory role under the Data Retention Regulations 2014 (DRR 2014) created under the Data Retention and Investigatory Powers Act 2014 (DRIPA).

2. The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals and taking appropriate action where the law is broken. Her duties include providing advice on policy and other initiatives that engage information rights concerns. The Commissioner is responsible for regulating the aforementioned legislation, and she also has supervisory responsibilities touching on the UK's participation in cooperative law enforcement arrangements across the EU including Europol and Eurojust[1]. This can be as part of data protection joint supervisory body oversight arrangements and specific duties to supervise the UK national authorities participating in these arrangements.

## Executive Summary

3. Any future arrangements for UK cooperation with criminal justice and law enforcement activities at European Union level must continue to maintain high data protection standards to an internationally recognised level.

4. There are significant changes to European Union level data protection laws and these will be implemented in the UK before it leaves the European Union. These changes will affect the law

[1] http://www.legislation.gov.uk/ukpga/1998/29/section/54A

enforcement community and this could result in them having to comply with multiple pieces of legislation. There needs to be greater clarity over the legislative measures that will be used to give these effect in the UK to help organisations prepare.

## Consultation response

5. The case for continued participation in Europol, Eurojust, the European Arrest Warrant, the European Criminal Records Information System (ECRIS) the Prüm package and other cross-border law-enforcement measures will be made by others but the Commissioner will continue to make the case for a continued high standard of data protection safeguards if the UK opts out of these regimes. Currently, the legislative basis underpinning the operation of these functions provides data protection safeguards. If current arrangements are superseded by bilateral arrangements this could mean fragmented oversight and a lessening of protections for those whose data is being processed by UK authorities.

6. The Commissioner is clear that any separate bilateral agreements entered into must not dip below current UK and internationally recognised standards. It may well be the case that to enter into a bilateral arrangement to share data with bodies such as Europol or Eurojust, the UK would have to demonstrate essential equivalence in meeting the data protection safeguards established within those bodies.

7. At a more general level, the UK's departure from the European Union comes at the very time when EU level data protection law is changing and this will take effect before the UK has left. At present, organisations processing data for law enforcement and justice purposes have to comply with the requirements of the DPA and, in respect of the processing of personal data for cross-border law enforcement purposes, to Part 4 of The Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (the '2014 Regulations'). The DPA governs all aspects of the processing of personal data for domestic law enforcement purposes, as well as the processing of personal data by law enforcement agencies which is not for law enforcement purposes (for example for their own internal record-keeping, administration, personnel records, etc). The 2014 Regulations apply in circumstances outside the reach of the DPA, for example when co-operating with an overseas law enforcement agency, but the provisions are broadly consistent with the DPA.

8. These two domestic legislative acts will be superseded, in part, by Regulation EU/2016/679 ('The General Data Protection Regulations'

or 'GDPR') and Directive EU/2016/680 ('the Law Enforcement Directive') when they come into effect in 2018. However, the UK has secured an opt-out under Article 16.1 of the Treaty on the Functioning of the European Union ('TFEU') which the Commissioner understands to mean that the Law Enforcement Directive does not have effect, in the UK, for the processing of personal data for the purposes of domestic law enforcement. As such, the Law Enforcement Directive will only apply to the processing of personal data for the purposes of the Justice and Home Affairs measures the Government opted back into in December 2014.

9. The Government has still to make clear the implementation arrangements for the Law Enforcement Directive and which legislative vehicle will cover the processing of personal data for law enforcement purposes. Uncertainty around the UK's future relationship with the European Union has compounded this uncertainty amongst those organisations likely to be affected. The potential reach of this legislation will be wide covering law enforcement agencies, public sector bodies with criminal prosecution functions, the prison service, the criminal court system and potentially other organisations which will fall within scope. The Commissioner is concerned that there will be a fragmented legislative regime. From a regulatory perspective this will be challenging and the complexities of this brings with it risks in terms of protecting the processing of the personal data of UK citizens. It is important that the arrangements for implementation are clarified as soon as possible, to enable organisations processing personal data for law enforcement purposes to start preparations and for the Commissioner to prepare guidance.

10. Potentially, bodies engaged in the sphere of law enforcement may be required to process the same piece of personal data under up to three separate pieces of legislation, depending on the purposes for which it is being processed. Clarity is needed as to what form two of these pieces of legislation will take. It is important that the maximum degree of compatibility between these pieces of legislation is achieved. From a regulatory perspective, if the same piece of personal data must be handled differently, depending on the context, then this presents profound difficulties in terms of compliance from an organisation's perspective, and also for the application of regulatory powers where it may be unclear which piece of legislation may be applicable in the circumstances. To give an example, a police force may be required to comply with different data protection laws for the same piece of personal data if it is processing its records on its own personnel, if it is processing those data for an investigation into a domestic criminal matter involving

its personnel, or if it is processing the data in relation to a cross-border criminal investigation.

11. The Commissioner recognises the complex challenge posed by the EU referendum result in respect of EU law enforcement legislation and possibly due in part to this challenge but is concerned that the timetable to implement the Law Enforcement Directive and legislation to cover processing by law enforcement bodies outside of the scope of the GDPR is falling behind where it should be at this stage. The Commissioner knows that the Government is alive to the need to increase the pace on moving matters forward .She will be continuing work with Government to help ensure this is the case.

Information Commissioner
10 November 2016