British Institute of International and Comparative Law

BREXIT

FAQ: Data Protection Law in the UK

Contents

If you are a citizen of an EU Member State, then you are an EU citizen and have a number of rights, including the right to protection of personal data.

This FAQ discusses:

- The right to data protection in EU law
- The scope of EU data protection law
- Specific rights and obligations under EU law
- The EU's data protection reform package
- The future of UK data protection post-Brexit

It is intended to present an outline of the main issues relating to EU data protection law in the UK, and is therefore not comprehensive.

Citizens of European Economic Area (EEA) Member States (Iceland, Liechtenstein and Norway), and Switzerland, have rights equivalent to EU nationals and should be presumed as included in the term 'EU citizen' when used in this FAQ

Author: Rosie Slowe, Intern,
binghamcentre@biicl.org

Key EU Instruments Ensuring the Protection of Personal Data	
Primary EU Law	
Treaty on the Functioning of the European Union OJ C 326/47 (2012)	Article 16
EU Charter of Fundamental Rights OJ C 326/02 (2012)	Article 8 – Protection of Personal Data
Secondary EU Law	
Data Protection Directive (1995/46/EC)	Harmonises national laws so as to require high-quality data management practices on the part of the "data controllers" and guarantee a series of rights for individuals by setting strict limits on the collection and use of personal data and demanding that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data.
E-Privacy Directive (2002/58/EC)	Regulates the processing of personal data and the protection of privacy in the electronic communications sector.
Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2008/977/JHA)	Aims to protect personal data when processed for the purposes of preventing, investigating, detecting or prosecuting a criminal offence, or of executing a criminal penalty.
Pending Legislation	
Proposed Data Protection Framework Regulation (COM/2012/11)	Designed to supersede the Data Protection Directive as of 25 May 2018. As a regulation, it will become binding Member State law, meaning no implementing legislation would be needed as it is with directives.

1. Introduction

Q: Is there a right to protection of personal data under EU law?

A: Yes. Data protection is enshrined in various sources of primary EU law. First, despite being a manifestation of the right to privacy, the right to protection of personal data was elevated to a free standing fundamental right by Article 8 of the EU Charter of Fundamental Rights. The Charter binds the EU institutions as well as the Member States when they are interpreting and applying EU law.

Second, the right to protection of personal data is enshrined in Article 16 of the Treaty on the Functioning of the European Union (TFEU).

Further, the right to protection of personal data is concurrently ensured through various pieces of EU secondary legislation.

Q: Why does the EU ensure the protection of personal data?

A: Free movement of goods, capital, services and people within the internal market require the free flow of data. The European Commission realised that diverging data protection legislation amongst Member States impeded the free flow of data within the EU. Encompassing two of the core ambitions of European integration, protection of fundamental rights and the effective functioning of the internal market, the Data Protection Directive was adopted in 1995 to harmonise Member States' data protection laws.

2. Scope of Data Protection under EU Law

Q: What are 'personal data'?

A: Any personal information which can be used to identify you, directly or indirectly, such as your name, telephone number, email address, place and date of birth, etc. Any kind of information can be personal data provided that it relates to a person.

Q: In what contexts do the protection of personal data apply?

A: Due to limitations in EU competence at the time, the material scope of the 1995 Data Protection Directive was restricted only to matters of the single market. The scope of application of EU data protection law has since been extended to cover judicial cooperation and law enforcement.

Q: What about when data is transferred outside the EU?

A: The EU's data protection legislation applies to Member States of the European Economic Area (EEA), which includes three non-EU states: Iceland, Liechtenstein and Norway. Personal data can only be transferred to third states outside the EU and the EEA when an adequate standard of data protection is guaranteed.

3. Rights and Obligations under EU Law

Q: What are your rights regarding your personal data?

A: When your personal data is collected and processed, you have enforceable rights. These include:

- The right to be informed that your personal data is being collected and/or processed.The right to know what the data is going to be used for and to whom your data may be transferred.
- The right to have access to your own data.
- The right to rectify any wrong or incomplete information.
- The right, in some cases, to object to the processing of your data on legitimate grounds.
- The right to receive compensation from the data controller for any damage you suffer.

Q: What are data controllers' obligations?

A: Data controllers are the people or bodies that collect and process personal data, for example a medical practitioner is usually the controller of his patient's data. Both public and private data controllers are bound by EU law when handing the data. They must:

- Ensure that your rights are observed, for example by giving you access to your data.
- Only collect and process personal data that is relevant and not excessive for specified, explicit and legitimate purposes.
- Ensure that collected data is accurate, updated where appropriate and kept no longer than is necessary.
- Protect personal data against accidental or unlawful destruction, loss, alteration and disclosure.
- Respond to any complaints regarding breaches of data protection rules.
- Collaborate and cooperate with national data protection supervisory authorities.

Q: What can you do if your rights are violated?

A: When you believe that your rights have been breached or that your data has been compromised you can send a complaint to the data controller. If the data controller's handing of a complaint is not satisfactory, you can file a complaint with the national data protection authority. EU law requires that every Member State provides one or more of these independent supervisory authorities. The data controller should cooperate with the supervisory body and complainant by investigating complaints and redressing any legitimate grievances. You can also seek a judicial remedy for any breach of rights and obligations guaranteed by national law.

4. The EU Data Protection Reform Package

Q: What is the new data protection reform package?

A: In 2012, the European Commission proposed its EU Data Protection Reform, described as a key building block of the digital single market and essential to protect the fundamental rights to privacy and protection of personal data in the digital age. It takes the form of a general Data Protection Regulation and a Data Protection Directive for police and criminal justice authorities. These two legislative acts were adopted in 2016 after four years of deliberations. They will replace existing EU data protection legislation and come into operation in May 2018. While the Directive will require transposition in order to become part of Member State's national law, the Regulation will be directly applicable in all Member States without the need for implementing national legislation.

Q: What will change under the general Data Protection Regulation?

A: Individuals are provided with a bolstered set of entitlements under the Regulation, including the right to object to personal data being processed for direct marketing purposes and the right to receive back personal data in a structured and commonly used form so that it can be easily transferred to another data controller. Additional changes under the Regulation include:

- *Consent*: It must be as easy to withdraw as to give consent for the processing of one's personal data, and consent must be explicitly given for sensitive data.
- *Accountability*: Onerous accountability obligations are placed on data controllers to demonstrate compliance.
- *Data Protection Officers*: In certain circumstances data controllers must designate a Data Protection Officer as part of their accountability programme.

- *Data breach notification:* Data controllers must notify most data breaches to the national data protection authority without undue delay and, where feasible, within 72 hours of awareness.
- *Fines:* A tiered approach to penalties for breach is established, enabling national data protection authorities to impose fines for some infringements.
- *Expanded territorial reach:* The Regulation applies to data controllers outside the EU whose processing activities relate to certain activities within the EU.

5. Right to Protection of Personal Data Post-Brexit

Q: How has EU data protection law been transposed into the domestic legal order?

A: Data protection rules in the UK are currently primarily governed by the Data Protection Act 1998, which implemented the 1995 Data Protection Directive.

Q: Will the general Data Protection Regulation apply in the UK?

A: It seems unlikely, on present estimates, that the UK will have left the EU by May 2018. The Regulation will therefore have direct effect in the UK from that date until Brexit occurs.

Q: What will happen to UK data protection law after the UK leaves the EU?

A: The Great Repeal Bill, announced to Parliament on 10 October 2015, will preserve and convert into domestic law the whole body of EU law applying to the UK at the time it leaves the EU. It follows that all EU data protection law, including the Data Protection Regulation if Brexit occurs after May 2018, will initially remain as part of the domestic legal order. It will subsequently be Parliament's prerogative to decide which elements of the law to keep, amend or repeal. It is possible that the UK may use Brexit as an opportunity to review law-making in this area and move to a lighter touch regime. Indeed, the Minister for Digital and Culture has said that there may be "changes to data protection regulatory landscape after the UK exits the European Union". However, any changes to the protection of personal data under UK law are unlikely to be substantial.

As set out in the Government's White Paper, presented to Parliament in February 2017, the UK seeks to secure 'the freest and most frictionless trade possible in goods and services between the UK and the EU' [p.35]. If the UK wants to trade with the single market it will have to prove that its data protection standards are adequate or essentially equivalent to the Data Protection Regulation in order to be considered a safe third country for the receipt of personal data. Many businesses and services operate across borders, and international data flows are essential to UK business operations across multiple sectors. In fact, half of all global trade in services already depends on access to cross-border data flows. It is therefore vital that the UK maintains data protection rules in line with EU rules after Brexit if it wants to remain a major player on the digital world stage. Further, given that the Data Protection Regulation applies to non-EU organisations that offer goods or services to, or monitors the behaviour of, EU citizens, post-Brexit UK organisations with EU customers and operation will still need to comply with the Regulation.

British Institute of International and Comparative Law
Charles Clore House,17 Russell Square, London WC1B 5JP
+44 (0)20 7862 5151 info@biicl.org www.biicl.org