PRIVACY *AND BREXIT*

OPEN RIGHTS GROUP *BRIEF*

OPEN RIGHTS GROUP

Issue

The right to privacy has become a key part of all our lives. Both online and offline, our relationship with government and business is in many ways defined by our right to privacy. Who can collect our data, for what purposes, who they can share it with and to what standards our information must be protected are questions that become more and more important as we seek the appropriate balance of power between individuals and large organisations.

Digital privacy is closely linked with the issue of data protection, which for the UK is inextricably linked to Europe. Post-Brexit, the UK must continue to engage with EU frameworks and ensure adequate standards are in place to prevent our data from being unlawfully bought, sold, shared or exploited.

Open Rights Group has fought to ensure that the right to privacy is respected by the UK, including through bringing litigation that has changed the course of fundamental rights.

EU and the Right to Privacy

The right to privacy is protected in the EU by Articles 7 (right to private and family life) and 8 (right to data protection) of the Charter for Fundamental Rights.

Strong protection of the right to privacy sets the EU apart from other digital markets, notably the US. Over the past two decades, the EU has increasingly protected the right to privacy in digital contexts through establishing rules for data protection and the privacy of electronic communications.

Data protection

Data protection across the EU is now regulated by the General Data Protection Regulation 2018 ("GDPR"). GDPR applies directly to EU Member States and is also incorporated into UK domestic law via the Data Protection Act 2018. It harmonises national data protection standards, improves individual control over personal identifying data and better regulates corporate data transfers outside the EU.

The effort to harmonise data protection standards across the EU creates a 'One Stop Shop' mechanism, whereby large organisations with offices or operations in multiple Member States can easily carry out cross-border data processing by designating a 'lead' supervisory authority (national bodies overseeing compliance with GDPR) which regulates data processing activities across all offices.

Privacy of electronic communications

Privacy and confidentiality in electronic communications across the EU is regulated by the Directive on Privacy and Electronic Communications 2002 ("cookie law"). This has been brought into force in the UK by the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"). The Directive regulates the way companies and services can market to individuals and track people online, requires individuals to opt-in before cookies or other data is stored in their browser and provides enhanced confidentiality of communications.

A new ePrivacy Regulation is expected to be passed by the EU in 2019 or 2020; this will complement the GDPR by applying improved privacy protections uniformly across the Digital Single Market.

European court of justice judgments

In a series of significant rulings since 2011, the Court of Justice of the European Union (CJEU) has interpreted and given new meaning to the right to privacy in respect of technological developments:

- It has confirmed that both static and dynamic (temporary) Internet Protocol (IP) addresses are to be treated as personal data and thus protected under the GDPR.
- It has interpreted EU law to include a "right to be forgotten", a right now explicitly enshrined in the GDPR which means that people can request removal of search engine results linking to inaccurate or outdated information about them.
- It has struck down the EU-US "Safe Harbour Agreement", ending a system whereby companies such as Facebook transferred EU citizens' data to servers located in the US without either consent or oversight.

The digital agenda in europe 2019-2024

With GDPR only a year old, and with mounting public frustration at data collection, retention and sharing

practices by Facebook, Google and other large tech companies, data protection and privacy are high on the EU policy agenda. National regulatory authorities are increasingly assessing, for example, how individuals can give genuine consent to cookie tracking and to data sharing in advertising technology processes. The EU is updating its guidance on how GDPR should be interpreted, and as GDPR issues are litigated CJEU case-law is likely to have increased significance in defining the limits and expectations for legal implementation.

The Impact of Brexit

After the United Kingdom (UK) leaves the EU:

- The UK will be outside the Digital Single Market. For personal data to continue to flow freely between the UK and the EU, the UK will have to seek an "adequacy decision" from the European Commission which determines whether the UK provides citizens with an adequate level of data protection, equivalent to that provided within the EU.

Until an adequacy decision is reached, businesses and other organisations wishing to transfer data from the UK to the EU will need to make individual arrangements to prove they are an adequate data controller, using systems such as model clauses, binding corporate rules, administrative arrangements and standard contractual clauses.

- GDPR will continue to apply in the UK by virtue of the Data Protection Act 2018. The cookie law will continue to apply in the UK by virtue of the Privacy and Electronic Communications (EC Directive) Regulations 2003. Any other EU legislation in force before Brexit, will become UK law via the European Union (Withdrawal) Act 2018.
- The Information Commissioner's Office ("ICO") (the independent UK authority overseeing data protection compliance) will not be a member of the European Data Protection Board ("EDPB") and will not be able to be a "lead supervisory authority" for the purposes of GDPR. The ICO intends to seek to retain a strong relationship with the EDPB.
- The Charter of Fundamental Rights will not apply in the UK and the CJEU will no longer have jurisdiction to decide cases referred to it by UK courts. UK courts will be able to refer to previous (and potentially future) CJEU decisions, however, as standards developed by the CJEU are to be read as if they were references to fundamental rights or principles.
- The UK will continue to be a member of the Council of Europe (separate from the EU) and therefore bound by the European Convention on Human Rights, which protects the right to privacy at Article 8.

What the Government has said

"… we will need an arrangement for data protection … the free flow of data is also critical for both sides in any modern trading relationship too ... we want to secure an agreement with the EU that provides the stability and confidence for EU and UK business and individuals to achieve our aims in maintaining and developing the UK's strong trading and economic links with the EU ... That is why we will be seeking more than just an adequacy arrangement and want to see an appropriate ongoing role for the UK's Information Commissioner's Office."

Theresa May, 2 March 2018, Speech on UK Future Economic Partnership with the EU

What ORG wants to see

The European Union subjecting the United Kingdom to the same scrutiny for adequacy of data flows as any other third-party country.

The UK Government:

- Making any necessary changes to meet the EU adequacy standard, if necessary, based on the assessment from European institutions.
- Continuing independently of the European Union to strongly protect personal data and privacy in online and digital contexts.
- Fully complying with any legal judgements determining whether it breaches EU citizens' fundamental rights to retain their personal data outside the EU.

UK courts exercising full powers to review, read down and challenge data protection and privacy legislation that infringes on fundamental rights, including assessing its adequacy against European standards of robust governance.

www.openrightsgroup.org
+44 20 7096 1079