European Privacy Update

Robert Carolina, BA, JD, LL.M
Executive Director, Institute for Cyber Security Innovation
Robert.Carolina@rhul.ac.uk; +44 7712 007 095

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Robert Carolina

INSTITUTE FOR CYBER SECURITY INNOVATION

- Royal Holloway, University of London
  - Executive Director,
    Institute for Cyber Security Innovation
  - Law & Regulation module leader,
    Information Security Group
- Lawyer (US & England)
  - Solicitor, Origin Ltd (London)
  - Law & regulation of ICT;
    Law & ethics in cyber security
  - BA (University of Dayton); JD (Georgetown);
    LL.M (London School of Economics)

About this talk

- Introduction
  - Why care about EU data protection
  - What is it really about, anyway
- The General Data Protection Regulation
  - Biggest overhaul of EU data protection rules in two decades
  - Adopted April 2016
  - Becomes effective in May 2018
  - Everybody is working to understand what it will mean in practice

Once upon a time

… it was the 1990's

Case study: Cross-border M&A due diligence on a UK target company. Purchase price >$20,000,000. Target presents a data protection disaster – core to business – poorly managed.

Question (by New York general counsel): "What's the largest fine ever recorded in UK history for violating this (old 1984) law?"

Answer (by UK practitioner): "£80,000 ($120,000)"

[End of story]

And then what happened?

Spanish data protection regulator got a lot of attention in the 2000's by imposing headline-grabbing fines of €500,000+. They fined Google €900,000 in one case. **A One Million Dollar Fine!**

But, a One Million Dollar data protection fine isn't cool anymore.

Do you know what's cool?

A One BILLION Dollar data protection fine
(maximum administrative fines now set at greater of €20M or 4% of global turnover; more than 140 European companies alone with $25B+ turnover)

-with apologies to Sean Parker & "The Social Network"

Data protection generally

- What is it?
  - Restrictions on collection / disclosure / use of “personal” data
  - “Personal” data? Any data about a living individual. (Much broader than “personally identifying information”.)
- More than “privacy”
  - Data protection law attempts to vest some measure of control in the hands of living “data subject” about the manner in which “their” personal data is used.
  - Opinion: data protection law is a reaction to the birth and growth of the modern administrative nation-state and modern enterprise

The “players”

Player	Definition
Data Subject	The living person to whom that personal data relates
Data Controller	A person (natural or legal) who controls the dissemination of the personal data
Data Processor	A person (natural or legal) who merely processes personal data at the instruction of a Data Controller

Legislation

- Legislation
  - **Current Core**: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
    - Commission Decisions, especially as regards trans-border data flow
    - National implementing legislation and guidance
  - **New Core**: Directive 95/46/EC is in the process of being replaced by the new General Data Protection Regulation.

General Data Protection Regulation

- Title:
  - Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Effective date
  - GDPR "applies" from 25 May 2018 (Art 99)
  - Repeals Directive 95/45/EC on that same date (Art 94)

General Data Protection Regulation

- What's wrong with the old Directive?
  - EU Directives normally do not have direct effect on member state law. They are directions to member states to amend domestic law in accordance with stated principles.
  - Criticism that Directive 95/46 has been implemented in widely divergent fashion among member states. EU-wide compliance is challenging.
- Why a "Regulation"?
  - Regulation is a single statement of positive law that applies immediately in all member states

Territorial Scope – Directive 95/46

Party has establishment in EU	Party using equipment in EU[1]	Party offers goods or services to, or monitors, persons resident in EU	Directive 95/46 applies? (Article 4(1))
Y	Y	n/a	YES
Y	N	n/a	YES
N	Y	n/a	YES
N	N	n/a	Possibly NO[2]

Notes:

1. Addressing cookie on remote PC probably constitutes "using" the PC.
2. Difficult, and potentially risky, to fashion a compliance theory under the Directive based on territoriality of operations.

Territorial Scope - GDPR

Party has establishment in EU (GDPR Art 3(1))	Party using equipment in EU	Party offers goods or services to, or monitors, persons resident in EU	GDPR applies? (GDPR Art 3)
Y	n/a	Y	YES
Y	n/a	N	YES
N	n/a	Y	YES[1]
N	n/a	N	NO[2]

Notes:

1. US-based cloud services with EU subscribers, or who monitor EU persons, will now undoubtedly fall within scope of regulation. ***Party has OBLIGATION to name a representative in the EU*** who can answer enquiries, etc – GDPR Art 27.
2. As territoriality shifts focus to residence of data subjects, territorial scope of the law has become more predictable in application – and (in my opinion) makes for more sensible public policy.

"Establishment" in EU and corporate form

- GDPR retains broad approach to analysing corporate form
  - "Establishment implies the effective and real exercise of activity through stable arrangements. *The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect*."
    – Recital 22 (emphasis added); see also Directive 95/46 at Recital 19.
  - Not a "corporate veil" issue, per se. This makes an important point about the artificiality of "off-shore" status of service provider.

- Google Spain SL & Google Inc v AEPD & González (2014)
  - Court confirmed that Google Inc (resident in USA, the supplier of search services) is processing personal data in the context of an "establishment" in Spain. The fact that their Spanish subsidiary offers in-country marketing services helps confirm the DP "establishment" of the parent company.
  - ***Observation and Warning***: Whether someone is processing personal data in the context of an "establishment" in EU for DP law is MUCH different that concept of "permanent establishment" used in international tax law

Consent from children (Art 8)

- When lawfulness of processing relies upon "consent" of a child data subject:
  - Child >= 16 years old can give consent for processing
  - Member States may adopt rules that reduce this age to as low as 13, but no lower
  - Consent for any child below the cut-off age must come from a person holding "parental responsibility"
- Does not alter applicable contract law on questions of capacity
  - Possible for a child who lacks capacity to enter into a contract, nonetheless to provide "consent" for purpose of processing personal data
- Controller required to "make reasonable efforts" to verify parental consent
  - Observation: Not clear how controller will be treated if they "make reasonable efforts", but consent has in fact failed (e.g., 9 year old spoofs parent identity). Such processing appears to be unlawful.

“Special categories of personal data”

- GDPR retains traditional categories of special data – Art 9(1)
  - “… data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership … data concerning health or data concerning a natural person's sex life or sexual orientation…”.
  - **now we add,** “… processing of genetic data, biometric data for the purpose of uniquely identifying a natural person…”
- Higher level of responsibility
  - Compliance strategies often depend upon data subject consent
  - Observation: if client controls data in these categories, then their spending on data protection advice goes up by a factor of many.

Data subject rights include…

- Access (show me my data) – Art 15
- Rectification (correct my data) – Art 16
- Automated decision making – Art 22
  - Data subject has right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects…"
  - Famous British comedy sketch: "Computer says 'no'"
- Data portability – Art 20
  - Stop messing around with old-fashioned "discovery" games – printing my records rather than offering them in electronic form, etc.
  - Give me my data, or give it to another party I name (like my replacement service provider) in an electronic form that can be used

Right of erasure ('right to be forgotten') – Art 17

- Right applies if:
  - Data no longer needed for original purpose
  - Data subject withdraws consent and there is no other lawful basis for processing
  - Data subject shows that "public interest" or "legitimate interest of party" should not apply as basis for lawful processing
  - Data subject objects to use of data for direct marketing – Arts 17(1)(c) & 21(2)-(3)
  - Personal data unlawfully processed
  - Required by provision of member state law
  - Data processed is based only upon consent of child or child's parent

- What if data is in the public?
  - "Personal data" that is made public is still "personal data"
  - If erasure is appropriate, then publisher "shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data" – Art 17(2)

Right of erasure ('right to be forgotten') – Art 17

- Exceptions, to the extent that its necessary:
  - "for exercising the right of freedom of expression and information" (*looking forward to disputes over this one*)
  - to comply with various legal obligations, for protection of public health, for overriding public interest reasons,
  - for certain archiving, scientific and statistical research purposes, etc
  - "for the establishment, exercise or defence of legal claims"

- Right of restriction – Art 18
  - A half-way remedy – limits processing

What about “Security”? – Directive 95/46 Art 17(1)

Member States shall provide that the controller must implement **appropriate technical and organizational measures** to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure **a level of security appropriate to the risks represented** by the processing and the nature of the data to be protected.

What about “Security”? – GDPR Art 32(1)

“Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller ***and the processor*** shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Breach Notification to Supervisory Authority

- Personal data breach
  - "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, ***or access to***, personal data transmitted, stored or otherwise processed" – Art 4(12)
  - Processor ***must notify Controller*** "without undue delay" – Art 33(2)
  - Controller ***must notify supervisory authority*** of breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it" – Art 33(1)
  - Prescribed list of information to supply – Art 33(4)
- Exception to obligation to notify supervisory authority
  - If "data breach is ***unlikely to result in a risk to*** the rights and freedoms of natural persons" – Art 33(1)
  - Controller must be able to demonstrate that it has made this calculation "in accordance with the accountability principle" – Recital 85

Breach Notification to Data Subjects

- Personal data breach
  - "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, ***or access to***, personal data transmitted, stored or otherwise processed" – Art 4(12)
  - Controller ***must advise Data Subjects*** "without undue delay" if the breach "is likely to result in a high risk to the rights and freedoms of natural persons" – Art 34(1)
- Supervisory authority can order breach notification to data subjects

- Exception to obligation to notify data subjects if:
  - data lost is technically rendered harmless (e.g., lost data was encrypted);
  - Controller takes after-the-fact steps which "ensure" that risk "no longer likely to materialise";

  OR

  - individual notifications involve "disproportionate effort" – make a public communication to inform data subjects

Joint controllers – Art 26

- Affirmative obligation to "determine their respective responsibilities for compliance"
- Keen focus on handling data subject demands
- Requirement to advise data subjects of arrangements, contact points, etc

- Joint responsibility
  - "Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers." Art 26(3)

Data protection by design and default – Art 25

- The controller shall
  - "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation…"
  - at both design stage and operational stage
  - subject to same cost-benefit analysis imposed by the security obligation

- The controller shall
  - "implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed"

- Clear policy move to push data protection into system design phase rather than trying to implement as an "add on" later

Data Protection Impact Assessment – Art 35

- Controller must
  - Carry out a data protection impact assessment
  - PRIOR to carrying out a new type of processing
  - WHEN a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons"
- Supervisory authority
  - Must publish a list of types of processing for which DPIA is mandatory
  - May publish a list of types of processing for which DPIA is unecessary
- Prior consultation
  - Controller must undertake prior consultation with supervisory authority when DPIA "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk " – Art 36(1)
  - Prescribed list of information to be provided – Art 36(3)
  - "back and forth" window of discussion with supervisory authority

International Transfers – Art 44, et seq

- Basic principle unchanged – no transfer outside EEA unless [pick one]
  - includes transfer to international organisations
- Adequacy decisions – Art 45
  - Extensive list of factors to consider include examining legislation and rules of hist state concerning "public security, defence, national security and criminal law" – para (2)(a)
  - Periodic review now baked in – max 4 years.
  - Old "adequacy" decisions remain in force – Art 45(9)
- Appropriate safeguards (Art 46) such as
  - Export contracts
  - Standard export clauses
  - Binding corporate rules (BCR)
- Binding Corporate Rules – Art 47
  - Must be approved by supervisory authority "in accordance with the consistency mechanism set out in Article 63"
  - Codifies much of current practice on BCR
- Others (e.g., consent)

Data protection officer (DPO

- Controllers and processors must designate a DPO if:
  - processing is carried out by a public authority;
  - operations "require regular and systematic monitoring of data subjects on a large scale"; or
  - operations deal with large amount of data from "special" categories
- Mandate to involve the DPO in decision-making
- DPO serves as point of contact for supervisory authority
- DPO must be appropriately skilled

Questions & Discussion

European Privacy Update

Robert Carolina, BA, JD, LL.M
Executive Director, Institute for Cyber Security Innovation
Robert.Carolina@rhul.ac.uk; +44 7712 007 095

ROYAL HOLLOWAY UNIVERSITY OF LONDON