25 January 2017

The GDPR and NIS Directive
A new age of accountability, security and trust?

Laurence Kalman
Legal director, Olswang LLP

OLSWANG

Agenda

1. Overview of GDPR and NISD
2. Impact of Brexit
3. GDPR – key principles
4. GDPR – main changes from current law
5. How does this affect data processors?
6. What do I need to know about breach notifications?
7. What should I be doing now?
8. How does this relate to cyber security?
9. NISD – key principles
10. Reform of e-privacy law

Overview of GDPR and NISD

- **GDPR (Regulation (EU) 2016/679)**:
  - Adopted on 27 April 2016
  - Will be directly binding on EU member states
  - No requirement for implementation into national law
  - Entered into force on 24 May 2016 and will apply from 25 May 2018
  - Introduces a new sanctions regime and an increased regulatory burden on controllers and processors
- **NISD (Directive (EU) 2016/1148)**:
  - Adopted on 6 July 2016
  - Entered into force on 8 August 2016
  - Not directly effective – EU member states have 21 months to implement into national laws
  - A further six months to "*identify the operators of essential services with an establishment on their territory*" that will be subject to the new rules

GDPR – a quick overview

- **Anti-trust style fines** of up to 4% of global turnover – for a wide range of breaches
- Sizeable organisations will need to **appoint a DPO** (or engage an outsourced service)
- **Processors will be subject** to the rules (and enforcement action)
- Overall, a **more prescriptive regime** with more "papering" requirements
- Privacy will need to be **actively factored** into systems and process design, up front
- Existing principles and rights strengthened
- Plus a number of new obligations and new rights
- A directly effective Regulation (not a Directive) – to achieve greater harmonisation
- Numerous national derogations will remain

GDPR and Brexit: Will GDPR apply in the UK?

OLSWANG

GDPR formally adopted

May 2016

DPA applies till 2018

GDPR takes effect

May 2018

Brexit takes effect?

Great Repeal Act?

March 2019

What will the UK's DP law be post Brexit?

GDPR – key principles

- Article 5 of the GDPR sets out the major principles that all organisations are required to comply with when they process personal data:
  - ***Fair and lawful***: PD must be processed lawfully, fairly and transparently
  - ***Purpose limitation***: PD must be collected for specific explicit and legitimate purposes
  - ***Data minimisation***: PD must be adequate, relevant and limited to what is necessary
  - ***Accuracy***: PD must be accurate and kept up to date
  - ***Storage limitation***: PD must be kept in a form that permits identification of data subjects for no longer than necessary
  - ***Integrity and confidentiality***: PD must be processed in a way that ensures appropriate security
  - ***Accountability***: Controller to be responsible for compliance with principles

GDPR – key concepts

- Article 4(1) – personal data:
  - *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*
  - A very broad definition
  - Anonymised data isn't subject to the rules
  - Neither is "pseudonymised data"
- Article 4(5) – pseudonymisation:
  - *the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*

GDPR – key concepts

- Article 9(1) – **sensitive** personal data:
  - *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*
- Article 4(2) – processing:
  - *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*

GDPR – key concepts

- Article 4(7) – **controller**:
  - *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*
- Article 4(8) – **processor**:
  - *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*

- Under GDPR, processors will be subject to various direct obligations and risk of sanctions

GDPR – key changes

- **Scope**
  - Expanded definition of **personal data**
  - Greater **territorial scope** – non-EU controllers and processors will be caught where processing relates to: (i) offering goods or services to EU data subjects; or (ii) monitoring behaviour of EU data subjects
  - A **one-stop shop** – with lead authority, concerned authorities and a cooperation procedure
- **Compliance and accountability**
  - Greater **transparency** around data processing
  - Stricter rules re **documented policies/procedures** to ensure and evidence compliance
  - Data protection by **design and default**
  - Some companies will need to appoint a **Data Protection Officer**
  - Role of **data protection impact assessments**

GDPR – key changes

- **Individuals' rights**
  - New **"right to be forgotten"**, building on existing right to erasure. Individuals can request that a controller deletes personal data and also erase links etc.
  - Right to **data portability** – entitles individuals to obtain a copy of their data in a structured, commonly used and machine-readable format
- **Security**
  - Enhanced **information security obligations**, which also apply to data processors
  - Long list of required **flow-down provisions** for data processing contracts
  - Tighter rules on **international transfers** of personal data

GDPR – key changes

- **Breach notifications**
  - Controllers must notify supervisory authority of a security incident **within 72 hours of becoming aware** if feasible
  - Individuals must be notified where an incident could cause **serious harm**
  - Processor to notify controller **"without undue delay"**
- **Fines**
  - 2 tiers: (i) **lower tier** is €10m or 2% of worldwide annual turnover; and (ii) **higher tier** is €20m or 4% of worldwide annual turnover
  - Higher tier applies to breaches of principles, data subject rights, international transfers; lower tier applies to breaches of security, breach notification. Member states must impose "*effective, proportionate and dissuasive*" penalties
  - Right to compensation for material or immaterial damage. Controller or processor can be liable

GDPR – some more on data processors

- Distinguishing a mere “processor” from a joint controller – a tricky question
- Factors have previously been considered to include:
  - level of prior instructions by data controller and receiving entity’s “margin of manoeuvre”;
  - extent of data controller’s monitoring; and
  - “visibility” of receiving entity to the data subject (e.g. in a call centre context)
- Under GDPR, controllers and processors will need to document data processing and responsibilities more clearly (Articles 26 and 30)
- More rigorous due diligence exercise when selecting a processor
- Much longer list of obligations to include in the processing contract
- Negotiations may become much longer and potentially more contentious
- Likely to affect data processing risk profile

GDPR – some more on breach notification

- Current law – Data Protection Act 1998 – no absolute requirement to notify data breaches under the DPA. But ICO recommends that **serious breaches** should be notified
- **GDPR Article 32** – security of processing – *appropriate technical and organisational measures*
- **GDPR Article 33** – notification of personal data breach ("*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*"):
  - Data controller must notify supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of a personal data breach
  - Notification not required if breach is unlikely to result in a risk to the rights and freedoms of individuals
  - GDPR sets out minimum information to be provided
  - Data controller must document personal data breaches in a way that enables the supervisory authority to verify compliance

GDPR – some more on breach notification

- **GDPR Article 34** – data controller must communicate data breach to data subject without undue delay if it "*is likely to result in a high risk to the rights and freedoms of natural persons*"
- Not required if:
  - data was unintelligible (e.g. because it was encrypted);
  - controller has taken subsequent action to mitigate the risk; or
  - it would involve disproportionate effort – but in this case, there must be a general public communication
- Obligations on data processors
  - Notify data controller without undue delay after becoming aware of a breach
  - Assist data controller in complying with its data breach-related obligations
- Consequences of non-compliance – enforcement actions, compensation and fines

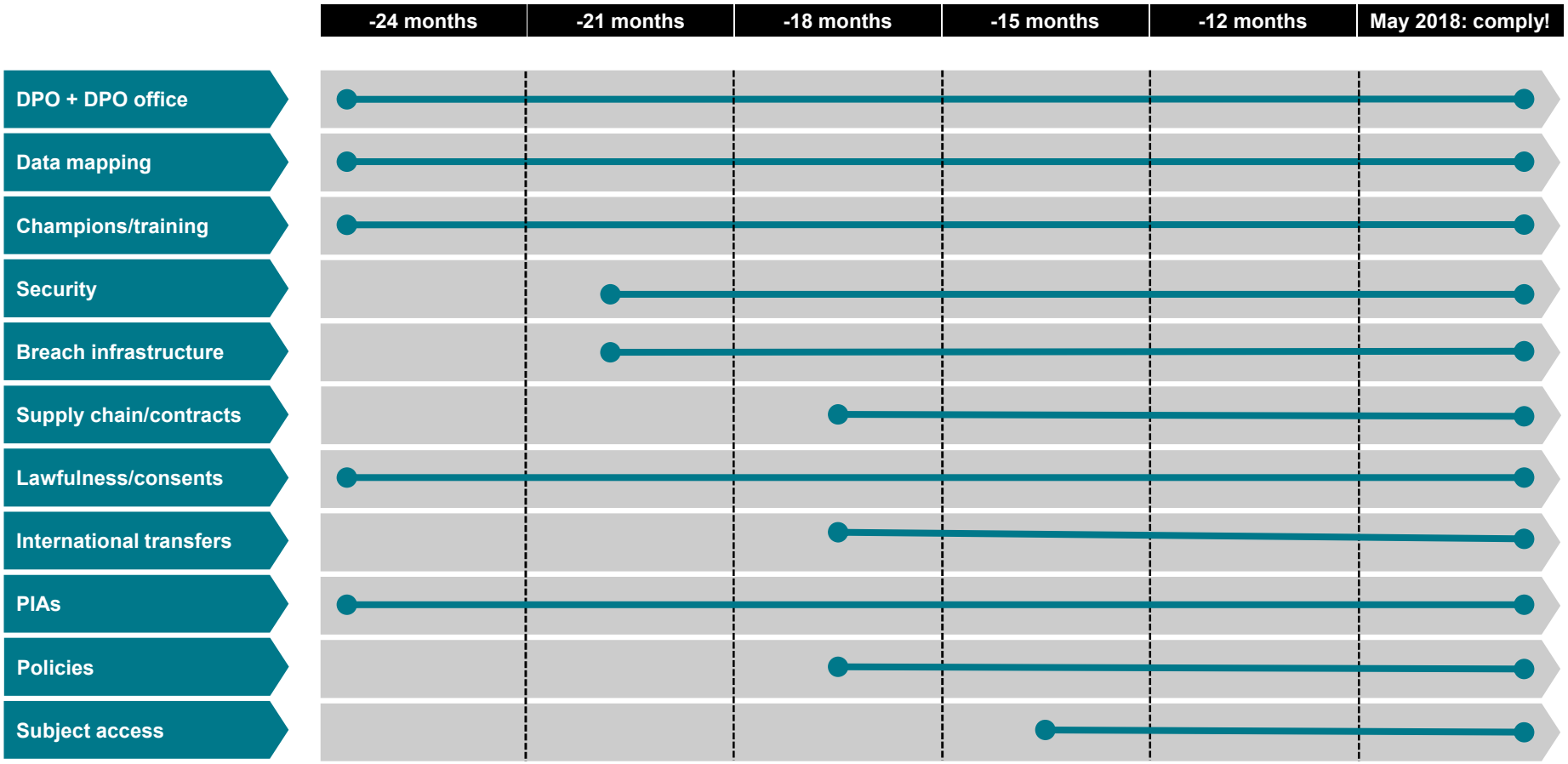
What should I be doing now?

- Assemble cross-functional GDPR working group, with management buy-in
- Review the personal data that your organisation holds; where is it held? how is it used? who can access it? to where is it being transferred? do you need to keep it?
- Review and update privacy notices for customers
- Assess whether IT systems and business processes can satisfy requirements for data portability and "right to be forgotten"
- Check procedures for subject access requests; can you meet the one-month response deadline?
- Review data protection provisions in supplier agreements and allocation of risk
- Develop template data protection impact assessment for higher-risk projects
- Develop training materials to raise staff awareness of the new rules

What should I be doing now – breach notification?

- Establish robust breach notification infrastructure, including:
  - internal / external incident management team and response plan
  - effective reporting tools and procedures
  - incident severity categorisation
  - clear notification protocols
- Monitor, train and test – DPIAs; focus on readiness; rehearse comms; use war gaming
- Manage supply chain risk:
  - due diligence to choose the right supplier
  - get the support you need from your suppliers
  - establish processes for when things go wrong
  - ensure your contract allows you to hold suppliers to account

GDPR project plan: what do you need to do now?




Know your data
Identify your team and regulator
GAP analysis
Workshops
PIAs
Review consents and contracts
Test your data breach plan

How does all of this relate to cyber security?

- December 2016 – DCMS published its *Cyber Security Regulation and Incentives Review*. Considered whether there is a need for additional regulation or incentives to boost cyber risk management in UK economy
- Government seeking to improve cyber risk management in the wider economy through the GDPR. To be supplemented by measures to link data protection with cyber security
- For now, Government will not seek to pursue further general cyber security regulation for the wider economy over and above the GDPR
- Part of broader national cyber security strategy – launched in November 2016 with £1.9bn funding. Designed to underpin the government's three key objectives:
  - ***Defend*** – ensure UK can defend itself against rapidly evolving cyber threats, respond to incidents etc.
  - ***Deter*** – make UK tough target for cyber criminals and ensure UK can take offensive action if required
  - ***Develop*** – invest in research and development and ensure the UK has a strong pipeline of talent
- For **critical national infrastructure** operators, the NIS Directive is on its way…

NIS Directive – key principles

- NIS Directive sets out measures to ensure critical IT systems in central sectors of the economy are secure – e.g. banking, energy, financial market infrastructure, health, transport, water, digital infrastructure
- Will apply to operators of "***essential services***" and to "***digital service providers***"
- Each EU member state will determine:
  - which organisations are operators of essential services and subject to the rules; and
  - "*effective, proportionate and dissuasive*" penalties for infringement
- Digital service providers are subject to slightly different rules – online marketplaces, online search engines and cloud computing service providers

NIS Directive – key principles

- Operators of **essential services** will be required to:
  - "*take appropriate and proportionate technical and organisational measures to **manage the risks** posed to the security of network and information systems*"; and
  - "*take appropriate measures to **prevent and minimise the impact of incidents** affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services*"
- New incident notification regime will require operators to report "*incidents having a significant impact on the continuity of the essential services they provide*" **without undue delay**
- Notification to "competent authorities" or Computer Security Incident Response Teams set up by each EU member state

NIS Directive – key principles

- **Digital service providers** will also have obligations to ensure the security of their network and information systems and minimise the impact of incidents affecting that security
- These obligations will be lighter-touch and more reactive
- Member states can't increase these requirements (except for reasons of national security or law and order) but they can place more stringent obligations on essential service operators
- Digital service providers will be required to notify incidents that have a “substantial” impact on the provision of a service they offer in the EU without undue delay

Reform of e-privacy regulation

- With GDPR on the horizon, EU is now overhauling and expanding reach of privacy rules relating to **direct marketing**, **cookies** and other forms of **online monitoring**
- Current law is based on Privacy and E-communications Directive (PECD) from 2002. Being overhauled as part of Digital Single Market package
- Proposed new rules are designed to align with GDPR. Proposed as a directly-effective Regulation to harmonise laws across EU member states
- Draft Regulation published earlier in January. Commission aims for it to apply from 25 May 2018 – same date as GDPR comes into force
- Will replace PECD and (possibly) Privacy and Electronic Communications (EC Directive) Regulations 2003

Reform of e-privacy regulation

- Key aspects of proposed Regulation:
  - **fines** are in line with GDPR;
  - also proposed to have **extra-territorial effect** – applies to electronic communications services in the EU (regardless of where processing takes place);
  - extends from traditional voice, text and email services to: (i) "over the top" service providers; (ii) M2M communications (i.e. IoT technology); and (iii) probably all services with an electronic communications element; and
  - rules on direct marketing and use of cookies and other tracking technologies would apply to all marketers and websites
- **Cookie rules** are proposed to be amended. Consent will be required (same meaning as GDPR) and may be expressed by browser settings. Some limited exceptions introduced

Reform of e-privacy regulation

- **Direct marketing**: Rules for opt-in and opt-out marketing consents are similar to the current position under the PECD (and 'soft opt-in' appears to have been retained)
- Some important points to note:
  - restrictions on unsolicited marketing communications appear intended to cover instant messaging applications, MMS and Bluetooth;
  - organisations still required to obtain end-users' prior consent, before sending commercial electronic communications for direct marketing purpose;
  - once given, the end-user's consent can then be withdrawn at any time; and
  - "soft opt-in" remains for the use of e-mail contact details within the context of an existing customer relationship for the offering of the marketer's own similar products or services.

For more information

please contact:

OLSWANG

Brussels
+32 2 647 4772

London
+44 20 7067 3000

Madrid
+34 91 187 1920

Munich
+49 89 206 028 400

Paris
+33 17 091 8720

Singapore
+65 6720 8278

Thames Valley
+44 20 7067 3000

Olswang:
Changing Business.
www.olswang.com