New Rules on Privacy and Protection of Personal Data in the EU

The ‘General Data Protection Regulation’ (GDPR)

CIAB, November 14, 2017

Steptoe

STEPTOE & JOHNSON LLP

GDPR SUMMARY

- http://www.eugdpr.org/
- New EU regulation on protection of personal data
- Substantive rules
  - Principles for processing; lawful processing; data subject's rights
- Compliance
  - Points to note and documentation
- Enforcement
  - Supervisory authorities, remedies and sanctions
- GDPR and insurance agents and brokers ('intermediaries')
  - Specific concerns/opportunities for the intermediary sector

BY WAY OF INTRODUCTION……

Checklist for insurance intermediaries:

- What is the GDPR?
- When does the GDPR apply?
- What are the key definitions intermediaries need to be aware of?
- On what basis can an intermediary lawfully process personal data?
- How should an intermediary safeguard individuals' rights?
- What should the intermediary know about privacy programme management?
- What should the intermediary do in the event of a breach of the GDPR?

LEGAL FRAMEWORK (1/2)

Fundamental provisions:

- 1950 Convention for the Protection of Human Rights and Fundamental Freedoms
- Council of Europe 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- Charter of Fundamental Rights of the European Union: Articles 7 (Respect for private and family life) and 8 (Protection of personal data)
- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Data Protection Directive')
- The GDPR repeals Directive 95/46 and introduces 'a strong and more coherent data protection framework' in the EU

LEGAL FRAMEWORK (2/2)

Regulation 2016/679 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 ('GDPR'):

- 'Natural persons' – referred to as 'data subjects'
- 'Controllers' and 'processors' process personal data of data subjects
- Applicable on 25 May 2018 – six months left to prepare!
- Applies in 28 EU countries (including the UK despite Brexit) + Iceland, Norway and Liechtenstein
- 'Long-arm' jurisdiction: the GDPR applies to a controller or processor of personal data not established in the EU, where the processing activities are related to:
  - '(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the EU.'

PRINCIPLES FOR PROCESSING (Article 5, GDPR)

If you are processing personal data of individuals ('data subjects') in the EU, you must follow seven golden principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

LAWFULNESS OF PROCESSING (Article 6,GDPR)

Processing is only lawful in specified circumstances:

- The data subject **consents**
- Processing is necessary to **perform a contract**
- The controller of the data is under a **legal obligation** to process
- Processing is necessary for the **vital interests** of data subject or another natural person
- Processing is in the **public interest or official authority** of controller
- Processing is in the **legitimate interests** of controller or other
  - Unless overriding interest of fundamental rights and freedoms of data subject (especially child)

RIGHTS OF DATA SUBJECT (Chapter III, GDPR)

The data subject enjoys rights in the EU which insurance intermediaries must respect:

- Information
- Access to data
- Rectification and erasure (aka ‘right to be forgotten’)
- Restriction of processing
- Data portability
- Objection
- Restrict ‘automated individual decision making’, including profiling

(all subject to restrictions in order to safeguard national security, etc.)

- Be told of a data breach

PRIVACY PROGRAM MANAGEMENT (Chs. IV-V, GDPR)

The GDPR develops existing rules/practices and introduces new requirements for controllers and processors (intermediaries):

- Data protection ‘by design’ and ‘by default’
- Maintenance of records
- An ‘appropriate level of security’ through ‘appropriate technical and organisational measures’ *e.g.* encryption
- Notification of data breach to supervisory authority and data subjects
- Data protection impact assessment and possible prior consultation of supervisory authority
- Appointment of a Data Protection Officer in specified circumstances; role and duties
- Codes of conduct and certification
- Transfers of personal data outside the EU/‘**protection travels with the data**’

SUPERVISORY AUTHORITIES (Chapters VI - VIII, GDPR)

Supervisory authorities are an ‘essential component’ under the GDPR:

- Independent public authority per Member State
- With extensive tasks
- And extensive powers
- ‘one-stop-shop mechanism’ for case handling

NB: establishment of the European Data Protection Board (Chapter VII, GDPR)

REMEDIES (Chapter VIII, GDPR)

The GDPR provides for various remedies:

- Right to lodge a complaint with a supervisory authority
- Right to a judicial remedy against a supervisory authority
- Right to an effective judicial remedy against a controller or processor
- Representation of data subjects

COMPENSATION AND LIABILITY (Chapter VIII, GDPR)

Subject to general EU law rules on jurisdiction, the GDPR provides for compensation and liability:

- Right to compensation
- Compensation:
  - Controller always liable unless proven not responsible
  - Processor liable only where:

  (i) Not compliant with specific obligations of the GDPR,

  (ii) Acted outside or contrary to lawful instructions of controller

- Joint liability for entire damage

ADMINISTRATIVE FINES AND PENALTIES

'In order to strengthen and harmonise administrative penalties for infringements':

- **Administrative fines**
  - Imposed by supervisory authority
  - Effective, proportionate, dissuasive
  - Various scales (depending on infringement)
    - For less serious infringements, *e.g.* failure in by design and by default: up to €10 Mio or 2% of total worldwide annual turnover of the preceding financial year, whichever is higher
    - For serious infringements, *e.g.* breach of basic processing principles or data subject's rights: up to €20 Mio or 4%
- **Other penalties**
  - National (criminal) law under Member State competence
  - Effective, proportionate and dissuasive
- **National authorities already 'flexing muscles'**

GDPR AND INSURANCE INTERMEDIARIES (1/3)

The GDPR is not specific to insurance. It is cross-sector/'horizontal'. This raises questions for intermediaries, such as:

- Reputational risk
- Interplay with insurance-specific rules (public policy, no discrimination, segmentation of risks, adverse selection, etc.)
- Relations with insurers and avoiding (joint) liability
- The EU's Insurance Distribution Directive, *e.g.* 'product oversight and governance' and requirements for organisational structure and controls
- General data security and protection of personal data
- Insurance supervisors/regulators and the risk of 'double indemnity'
- Dialogue between data protection authorities and other supervisors

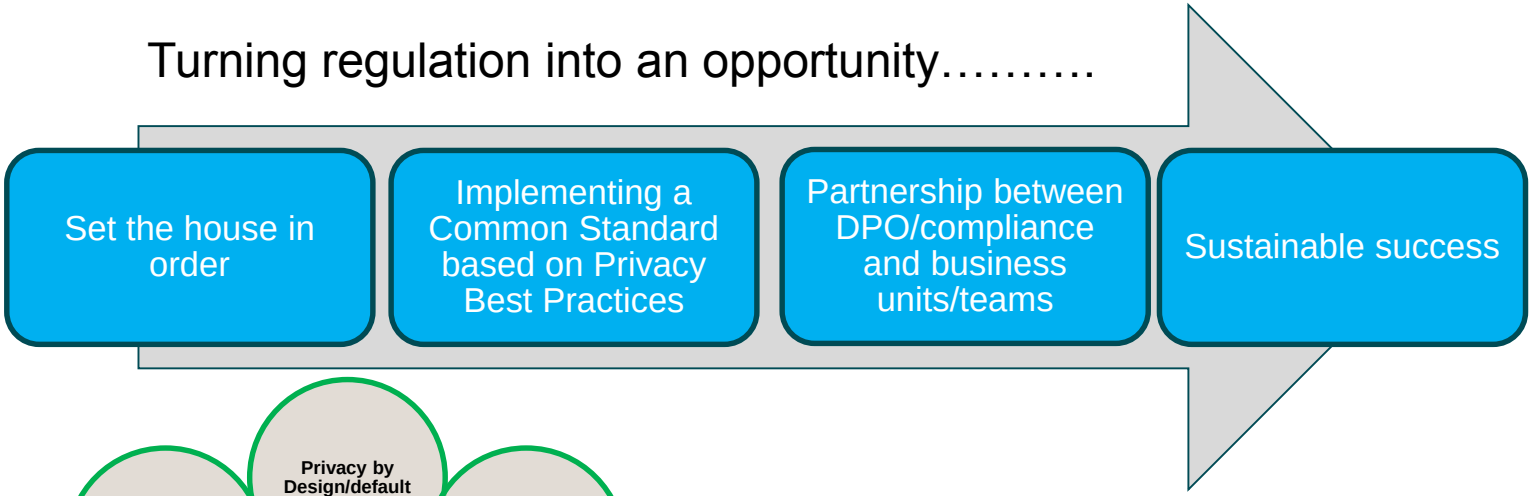
GDPR AND INSURANCE INTERMEDIARIES (2/3)

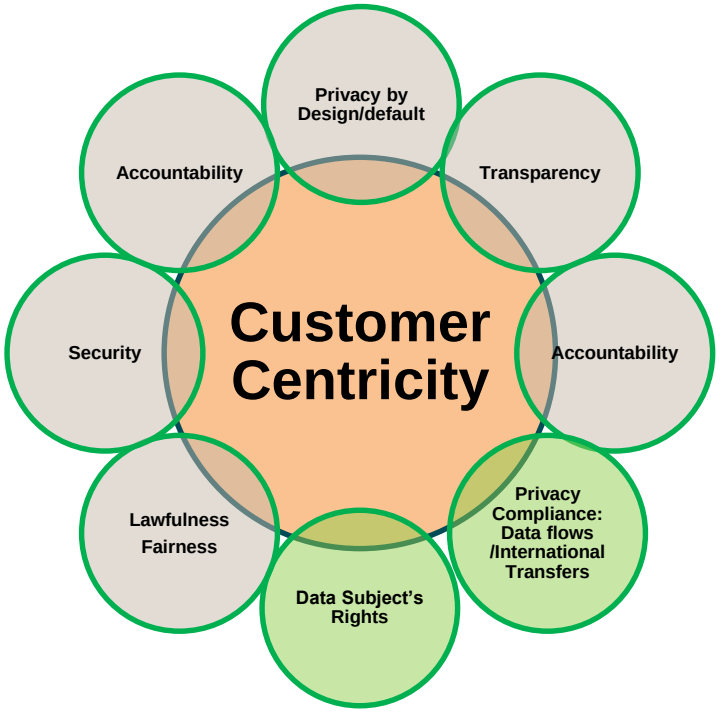
DP authorities have issued general guidance on how to comply with the GDPR, which insurance intermediaries can adapt to their sector:

- **Appointing** senior executive
- **Mapping** data, *e.g.* data subjects (clients, personnel, suppliers, etc.), any special/sensitive data, and processing activities
- **Prioritising** compliance action, *e.g.* bases for international transfers
- **Managing** risks, *e.g.* whether EU representative needed
- **Organising** review of data protection procedures, insurance contracts, terms of business, service agreements, privacy notices, consents, etc.
- **Documenting** compliance measures

GDPR AND INSURANCE INTERMEDIARIES (3/3)

Turning regulation into an opportunity…….





"**GDPR** is all about **TRUST** and providing **CUSTOMER-CENTRIC** products and services…"

Steptoe
STEPTOE & JOHNSON LLP