Introduction to the General Data Protection Regulation

The GDPR

Regulation (EE) 2016/679:

- Entered into force in May 2016
- Shall apply in May 2018
- Repeals Directive 95/46/EC
- Allows Member States some flexibility
- Draft Bill for implementing certain provisions of the GDPR
- The Bill shall replace Law 138(I)/2001

Why do need new rules?

- Remedy existing shortcomings
- Uniform instead of fragmented rules
- Globalization
- Technological advancements
- Increased cross- border data flows
- New risks and challenges

3

Outlining the GDPR:

- Protection of individuals
- Free movement of data in the EU
- Balance data protection against other fundamental rights
- Balance against public and legitimate interests
- Regulatory tool

4

Why the GDPR concerns the shipping Industry:

- Processing office employees' personal data
- Processing crew's personal data
- Processing cruise passengers' data
- Shipping cargos of natural persons
- Ship supply services (needs of individual sailors, for ex. prescribed medicines)
- Crew recruiting services (In CY or abroad)

5

Economic impact of the GDPR:

- Less bureaucracy (electronic v printed forms)
- Reduction of administrative costs (one - stop shop: 1 instead of 28 DPAs to deal with)
- Competitive EU economy in global markets
- Specific provisions for SMEs
- Cross border flow of data
- Investing in citizens' trust
- Promoting e-commerce

6

Aims of the GDPR:

- Uniform instead of defragmented rules
- One stop shop
- Strengthen existing rights & introduce new
- Tackle technological challenges
- Transparency, accountability self-regulation
- Risk based: obligations proportional to risks
- Strengthen DPAs' cooperation
- Stringent sanctions

7

The GDPR applies to:

- The territory of Cyprus (offices)
- Where Cypriot law applies by virtue of international law (embassies, CY flag ships)
- Cross border cases concerning persons in several MSs (affiliated companies)
- Processing outside the EU for people in EU
- Processing in the EU for people outside EU
- Main establishment: must be designated if a company has establishments in several MS

8

Some definitions:

- Personal data: any information relating to an identified or identifiable data subject
- Data subject: a natural living person
- Controller: the owner of the data
- Processor: acts on behalf of the controller
- Special categories: health, race, religion etc
- Processing: collection, storage, disclosure, transfer, profiling etc
- Profiling: analysis/ prediction of behaviour

9

Questions shipping companies should ask:

- What personal data do I process?
- Do I act as controller or processor?
- What are my core and secondary activities?
- Do I operate in several MS?
- Where is my main establishment?
- Do I belong in Group of Undertakings?
- Do I transfer data to third countries?
- Do I need to appoint a Data Protection Officer (DPO)?

10

Appointment of Data Protection Officer (DPO) Article 37:

Mandatory for controller & processor when:

- Public authority or body
- Core activities consist of operations that require regular and systematic monitoring of data subjects on a large scale
- Core activities require processing of special categories of personal data or criminal convictions and offences, on a large scale

11

Guidelines for appointment of DPO:

- regular: ongoing, at intervals or recurring
- systematic: pre-arranged, scheduled, methodical, according to a system
- large scale: number of people, volume of data, duration, geographic extend
- special categories: information that may lead to discriminations
- convictions & offences: require justification why needed, only if absolutely necessary

12

Position of the DPO Article 38:

- Involved in all issues relating to the GDPR
- Necessary resources to perform his tasks
- Independent, cannot be dismissed for exercising his tasks
- Liaises with management & data subjects
- Bound by secrecy and confidentiality
- May have other duties if no conflict of interests

13

Guidelines for position of DPO:

Conflict of interests:

- DPO vs Director
- DPO vs Personnel Manager
- DPO vs AML Compliance Officer
- DPO vs IT Security Officer
- DPO vs any position that requires taking instructions on data protection issues

14

Tasks of the DPO Article 39:

- Advises management & employees
- Monitors compliance with the GDPR
- If requested, advises management for Data Protection Impact Assessment (DPIA) or monitors the DPIA's performance
- Cooperates with Data Protection Authority
- Contact point for the DPA on all data protection issues, including prior consultations

15

Guidelines for tasks of DPO:

- Identify core & secondary process activities
- Check that all activities comply with GDPR
- Inform & advise controller & processor
- Educate colleagues
- DPIAs: Is the DPIA mandatory? What method should it follow? In-house or outsourced? Measures to mitigate risks? Must we consult with the Commissioner?

16

Data protection principles Article 5:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability: The controller is obliged to demonstrate compliance with all of the above principles

17

Lawfulness of processing Article 6:

- With Consent
- Without consent when:
  - Contractual obligation
  - Legal obligation
  - Vital interest
  - Public interest
  - Overriding legitimate interest

18

Processing of special categories Article 9

Conditions applicable to shipping sector:

- Consent
- Legal obligations in employment field
- Vital interest
- Processing by Trade unions
- Defense of legal claims

19

Conditions for consent and conditions applicable to children Articles 7 & 8:

- Obligation to demonstrate consent
- Separate consent for different processing
- Clear, plain language, specially for children
- Right to withdraw consent
- Consequences of refusal to consent
- Guardian's consent for information society services offered directly to children

20

Rights of data subjects Articles 12-22

- Transparent information provided when data collected from the person, or from a third party
- Right to access my own data (free of charge)
- Rectification of inaccurate/ incomplete data
- Erasure (right to be forgotten): when data are no longer necessary or consent is withdrawn or person objects for legitimate grounds or data have been unlawfully processed or there is legal obligation for erasure or data collected in relation to information society services

21

Rights of data subjects Articles 12-22

- Restriction of processing: contested accuracy or unlawful processing or legal claims or decision is pending on exercised right to objection
- Data portability: receive data that I have given, in human or machine readable form & ask to transmit these data to other controller, when processing is based on consent or contract
- Objection (including profiling): when processing is based on public interest or legitimate interest
- Object to decisions based solely on automated processing, including profiling

22

Responsibilities of the controller
Articles 24 - 27

- Demonstrate compliance with GDPR
- Implement appropriate technical and organizational measures for protection
- Data protection by design & by default
- If there are joint controllers, determine their respective responsibilities
- If the controller is based outside the EU, to appoint a representative in the EU

23

Responsibilities of the processor
Article 28

- Acts only under directions of controller
- Implements appropriate technical and organizational measures for protection
- Engages other processor(s) only with the authorization of the controller
- The processing is governed by written, binding contract with the controller or by other legal act

24

Responsibilities of controller & processor Record of processing activities Art. 30

The controller & the processor keep written record of all processing activities:

- Contact details
- Categories of processing
- Transfers to third countries
- Security measures

The record is given to the DPA, on request

The record is also kept in electronic form

25

Responsibilities of controller & processor Cooperation with DPA & security Art.31,32

- The controller & the processor & where appropriate their representatives shall cooperate with the DPA, on request
- They must implement appropriate security measures, taking into account state of the art technology, costs and possible risks

26

Responsibilities of controller & processor Data breach notification Article 33

- The controller notifies the DPA about data breach within 72hrs unless there is no risk
- Justification required, after 72 hrs
- The processor informs the controller about data breach immediately
- The notification includes: nature of breach, number of persons affected, risks involved, measures taken or considered to be taken to mitigate risks

27

Communication of data breach Art. 34

- If the breach is likely to result in high risks the controller informs the affected persons without delay
- In plain language, nature of breach, risks involved, measures taken, or to be taken
- No obligation to inform if there is no risk or if measures were taken to mitigate risk
- Public announcement if individual is difficult
- The DPA may instruct the controller to inform the affected persons

28

Impact assessment & prior consultation Articles 35,36:

- If a new measure is likely to result in high risks, the controller must carry out a data protection impact assessment (DPIA)
- If an organization has a DPO, the controller must seek his advise for the DPIA
- A DPIA is mandatory, in particular when: profiling, processing of special categories or convictions/ offenses on a large scale and when monitoring public areas on a large scale

29

Impact assessment & prior consultation Articles 35,36:

DPIA + prior consultation = 4 + 1 steps:

1. Description/ purpose of foreseen measure
2. Legal basis, necessity, data minimization
3. Identify possible risks
4. Identify measures to mitigate these risks
5. If you can't find any measures to mitigate the risks or if you' re not 100% sure that the foreseen measures mitigate the risks, you MUST consult with the DPA

30

Guidelines for DPIA & prior consultation Articles 35,36:

- Risk based approach: obligations proportional to risks
- Risky operations include:
- Profiling & decisions based solely on scoring
- Processing of special categories of data that may lead to discriminations
- Drones or CCTV in public places
- Transfers to third countries in the absence of appropriate safeguards

31

Codes of conduct & their monitoring Articles 40,41:

- Adherence to a code of conduct is voluntary
- Useful tool to demonstrate compliance with the GDPR. Accountability is mandatory
- Useful tool for transfers to third countries & international organizations, in the absence of other tools
- Useful tool for associations, bodies representing categories of controllers and regulated professions

32

Codes of conduct & their monitoring Articles 40,41:

- EU codes of conduct are approved by the European Data Protection Board (EDPB)
- National codes are approved by DPAs
- All codes of conduct must be monitored by an expert body: DPA or accredited by DPA Regulator (Bar Association, ETEK etc)
- A code of conduct can be used as a tool for transfers, if it creates binding & enforceable commitments to controllers & processors

33

Certification & Certification Bodies Articles 42,43:

- EU certifications are approved by the EDPB
- National certifications can be approved by the DPA or by a certification body, which has been accredited, either by the DPA or the national accreditation authority or both
- A certification can be used as a tool for transfers, if it creates binding & enforceable commitments to controllers & processors

34

Transfers to third countries and international organizations Art. 44-50:

Tools for transfers of data outside the EU:

- Adequacy Decision (No authorization):

- The European Commission determines that a country or an organization ensures an adequate level of protection
- Privacy Shield: Free transfer to companies in the US, which register in the PS under the 3 regulators for trade (FTC), transport (DoT) & commerce (DoC). A self regulatory tool

35

Transfers to third countries and international organizations Art. 44-50:

Tools for transfers of data outside the EU:

- Appropriate safeguards (no authorization):

- legally binding instrument (public authorities)
- binding corporate rules (group of companies)
- Standard clauses adopted by the Commission
- Standard clauses adopted by DPA & approved by the Commission
- Codes of conduct
- Certification mechanisms

36

Transfers to third countries and international organizations Art. 44-50:

Tools for transfers of data outside the EU:

- Appropriate safeguards (with authorization):
- Contractual clauses (controllers & processors)
- Provisions in administrative agreements (public authorities)

These are adopted by the competent DPA alone or in cooperation with other concerned DPAs, in the frame of a consistency mechanism

37

Transfers to third countries and international organizations Art. 44-50:

Tools for transfers of data outside the EU:

- Derogations (prior consultation required)
- Consent
- Contract between data subject and controller
- between controller & third party, in the interest of the data subject
- Public interest
- Legal claims
- Vital interests
- Transfers made from public registries

38

Supervisory authority (DPA) Art. 51-59:

- Independent
- Monitors the implementation of the GDPR
- Raises awareness
- Cooperates with other DPAs
- Joint inspections & mutual assistance
- Acts as lead, competent or concerned DPA
- Examines complaints & imposes sanctions
- Extensive investigative, corrective, advisory and authorization powers

39

Corrective powers Article 58:

- Warnings & reprimands
- Temporary or permanent ban of processing
- Order compliance with GDPR
- Order communication of data breach
- Order rectification, erasure, restriction
- Withdraw certifications
- Suspend transfers
- Impose fines

40

Liability and fines Articles 82,83:

- Liability to controllers, processors & their representatives
- Shared liability to joint controllers
- For violations of obligations of controllers & processors and certifications:

  €10 million or 2% of last year global turnover
- For violations of principles, rights, transfers & for non compliance with other sanctions:

  €20 million or 4% of last year global turnover

41

Thank you for your attention

Office of the Commissioner
For Personal Data Protection
1, Iasonos Street, 1082 Nicosia
Tel: 22-818456, Fax: 22-304565
Email: commissioner@dataprotection.gov.cy
www.dataprotection.gov.cy

42