HILL DICKINSON

Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)

Ian MacLean MBA LLM
Partner / Master Mariner

Hill Dickinson LLP

HILL DICKINSON

GDPR – The key issues

- Why should I be concerned about GDPR?
- What is personal data?
- The data audit
- Data subject rights
- The three month road map
- Cybersecurity.

HILL DICKINSON

Why should I be concerned about GDPR?

Who does it apply to?

- Article 3 GDPR
- The processing of personal data in the context of the activities of an establishment of a controller or processor in the Union
- Data subjects outside EU?
- Definition of an establishment
- Also - Applies to EU and non-EU entities providing goods and services or monitoring behaviour of EU subjects in the EU
- Does not matter where processing takes place.

HILL DICKINSON

Why should I be concerned about GDPR?

- EU Regulation - 99 Articles with a 173 paragraph preamble
- Enters into force on 25 May 2018
- Fines of up to €20m or 4% of annual global turnover whichever is higher for some offences or 2% and up to €10m for others
- New obligations – e.g. self reporting – requires culture shift
- Contractual obligations.

HILL DICKINSON

What is personal data?

- Any information relating to an identified or identifiable person – data subject
- Name, address, passport details, biometric data, disabilities, medical conditions, bank account details, next of kin, union membership, ethnic group, religion etc.
- Applies where a data subject can be identified directly or indirectly by an identifier such as:
  - A name, ID number, location data, online identifier, or,
  - One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

HILL DICKINSON

The data audit

- What data do you have and why – six legitimate reasons?
- Who needs access to it and why?
- How long do you need it for?
- Do you have consent to hold it and how do you demonstrate this?
- Who the data is provided to and why?
- What conditions are imposed on those that the data is provided to?
- How you record the movement of data?
- How you correct data found to be incorrect?
- How do you ensure data subject's rights are protected?

HILL DICKINSON

Data subject rights

- Consent freely given by statement or clear affirmative action with procedure for withdrawal of consent
- Reason for processing / contact details of data controller
- Who will receive the data and why
- How long data will be held or criteria for erasure
- Right of access to data / rectification
- Right to complain to supervisory body
- Right to be informed of breach
- Right to portability.

HILL DICKINSON

The three month road map

- Documented management system / record keeping procedures
- Data audit, risk assessment & training
- Draft compliance policy, privacy notices and consent procedure
- Define access, responsibilities, authorities and reporting lines
- IT Security
- Comply with the rights of data subjects
- Self reporting procedures for breaches (72 hours)
- Data impact audit / appointment of DPO
- Liaise with “Supervisory Authority”
- Allocate resources and involve data handlers in process mapping.

HILL DICKINSON

Cyber Security

- Cyber Security and GDPR are distinct disciplines with some commonality
- IMO - Guidelines on Maritime Cyber Risk Management
- Distinguish between information technology and operational technology
- Additional Guidelines – BIMCO et al, ISO/IEC 27001, USA – NIST
- ISM Code – Resolution MSC.428 (98) – Does not change the Code
- Risks addressed no later than first annual verification of DOC after 1 January 2021
- Detention - Danger to ship, personnel or unreasonable threat to environment
- Use the Safety Management System architecture – the DPA is your friend.

HILL DICKINSON

Questions