Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) high level summary of recommendations

Compliance of GDPR is required by 25 May 2018. It applies to personal data of identifiable living individuals (irrespective of where in the world they are located or domiciled) processed by a business that has an established presence in the EU regardless of whether the processing takes place in the EU. It also applies to non EU businesses that are providing goods and services or monitoring the behaviour of EU subjects in the EU.

GDPR introduces accountability for the secure processing and compliance of GDPR for personal data transferred to other entities. Fines of up to €20 million or 4% of annual global turnover whichever is higher for some offences or €10 million and up to 2% for others

Shipowners, ship managers, crew managers and crew agencies will not all have the same challenges and each company will implement procedures which best suit its business model. This document sets out suggestions for the various steps to be adopted in preparing for the GDPR. The tasks are largely sequential but some areas such as training and security of processing can be performed concurrently. The phases listed below are not an exhaustive list but a high level summary.

Caution should be exercised in respect of the following:

1. It should not be assumed that compliance with Directive 95/46/EC will be sufficient for compliance with GDPR.
2. Treating GDPR as an IT department issue. GDPR is a board issue.
3. Buying off the shelf solutions and subcontracting the implementation to consultants.
4. Signing onerous or unreasonable requests to implement the GDPR procedures and or providing unlimited or wide ranging indemnities from suppliers and business partners without legal advice.
5. Liabilities under existing contractual obligations based on 'Directive 95/46/EC as amended' need to be reviewed and automatic exposures under GDPR considered.

Phase 1: awareness, information audit/risk assessment

- GDPR awareness and training from the board downwards and identify line management responsibility.
- Review/audit personal data collected and processed at present, what you have, why, where it comes from, who sees it, who needs to see it, how long it needs to be kept, its accuracy, lawfulness, whether consent required and if so how obtained, whether shared, sent to third countries or cross border etc. See attached document and adapt for your information audit.
- Assess the risk of breach by looking at what controls are in place now in respect of personal data held and what further controls are needed.
- Conduct a data impact protection assessment where personal data processing gives rise to a high risk to individuals.

Phase 2: make decisions

- Assess the results of the information audit and risk assessment, consult and make policy decisions i.e. whether to have a DPO, whether consent required, lawfulness of processing etc.
- Identify and consider guidelines given by the supervisory authority and Article 29 Working Party and consult where necessary with the relevant supervisory authority.

Phase 3: develop policies procedures and documents

- Update data protection and privacy policy, to comply with GDPR following phases 1 and 2.
- Consider employees' and others' provision of information, access, verification, rectification, erasure rights under GDPR and develop procedures and forms which justify policies made.
- Draft policies and procedures, to include reporting, audits, transfer of data intercompany, outside the EU and third countries, informing third parties of changes.
- Seek to cover the issues in the employment contracts, contracts with suppliers, consumers, business partners etc.

- Map out joiner, mover, access recertification, and leaver processes from the data asset perspective.
- Check and approve any contracts or agreements with third parties that may handle personal data.
- Review/draft procedures to keep the board updated about GDPR responsibilities, risks and issues.
- Implement a programme to review all data protection procedures and related policies, in line with an agreed schedule.
- Implement procedures to detect, report and investigate breaches.
- Review/draft a crisis management/continuity plan in the event of breaches.

Phase 4: review security

- Review security of processing as required by Article 32 of GDPR.
- Review IT and cyber security and processes.
- Map out network shares and how access is shared to them.

Phase 5: training and governance

- Training of data controller, data processor and DPO if appointed on their GDPR responsibilities and procedures.
- Training of employees.
- Handling data protection questions from staff and anyone else covered by the policy.
- Education/notification of suppliers, business partners etc.
- Review/audit compliance.
- Reports to the board.
- Crisis management drill.
- Consider cyber insurance.