03/2018

MOORE STEPHENS

GDPR in shipping:
Roadmap to compliance in 10 essential steps

Shipping

PRECISE. PROVEN. PERFORMANCE.

The European General Data Protection Regulation (GDPR) comes into full effect on 25 May 2018. Designed to increase protection of individuals' rights and freedoms, GDPR has strengthened privacy rules, thus increasing the companies' privacy obligations. Stakes are high as administrative fines can reach Euro 20 million or 4% of an organisation's global turnover (whichever is greater), but the true cost in the case of a severe data breach is obviously the loss of reputation and potential claims.

Why is GDPR particularly relevant to shipping?

Although GDPR will probably affect every organisation that processes personal data, the shipping industry will be particularly affected due to the following reasons:

- Even small shipping companies process personal data of their crew on a daily basis. Most shipping companies keep records of their crew members between embarkations and for some time after the last debarkation.
- Personal data processed by shipping companies includes personal identification documents, bank details, travel documents, training records but also data considered to be 'sensitive' such as medical records.
- Shipping companies receive personal data from many sources such as the individuals themselves, manning agents, port agents and other third parties, in the normal course of business.
- They send personal data to many recipients such as port agents, travel agents and P&I clubs.
- They regularly make data transfers to a large number of jurisdictions, with particular interest in those made to countries outside the EU, and in specific, those where certain conditions must be met in order for the transfer to be allowable.

What should shipping companies do?

1. AWARENESS

It is crucial that shipping companies kick-start their GDPR project with raising awareness among top management on what GDPR requires and what the key risks for their particular organisation are. Engaging the right people at top management level is necessary to ensure that the organisation commits the necessary time and resources and develops a culture that respects privacy.

2. TEAM

With the full support of management, organisations need to assemble a multi-discipline team to run the project ensuring risk, legal and IT are included. The appointment of a Data Protection Officer may be required, under certain circumstances, in which case the organisations need to consider who that person might be. Trusted external advisors can bring technical expertise, perspective and help save time.

3. IDENTIFICATION OF DATA PROCESSING ACTIVITIES

It is then time to identify and record the data processing activities, ensuring that for each activity, the entire data lifecycle is captured (from collection all the way to destruction). Data processors and joint-controllers should also be identified at this stage.

4. GAP ANALYSIS AND COMPLIANCE PLAN

Whilst capturing the flows, organisations should look for the weaknesses in the data flows, evaluate the resulting risk and respond to that risk with a specific practical plan of action, so that the risk can be mitigated to an acceptable low level. To identify weaknesses they will also need to consider their policies and procedures, their current compliance framework (for example ISM, MLC etc) as well as tools and enablers, including legal documents (forms, terms and conditions, etc) and of course the IT environment.

5. IMPLEMENTATION OF CHANGES IN POLICIES, PROCEDURES, NOTICES, LEGAL, IT

Once the specific action plan is complete, organisations can then proceed to the implementation phase. This would normally include making changes in privacy policies, contracts with manning agents, P&I clubs, information notices to port agents, staff and crew as well as drafting appropriate consent forms. Implementation could also include changes in manual procedures, IT security (firewalls, encryption etc) and business continuity & disaster recovery plan. External advisors can again help carry out various aspects of the implementation but also assist in managing the effort.

6. DATA BREACH READINESS

It is crucial that organisations design an Incident Report Plan to include detailed actions that will need to take place so that, if required, notifications can be made timely to the Supervisory Authority (within 72 hours from detection of the data breach) and to the data subject. The Plan should include a clear pre-determined set of consecutive actions and a clear allocation of responsibility for those actions as well as notification templates, investigation requirements, reporting, media and communications management etc. Shipping companies should also maintain an incidents log, containing details of privacy incidents identified and how they were followed up, irrespective of whether they were reportable to the Authority and/or the data subjects or not.

7. PRIVACY IMPACT ASSESSMENT

GDPR requires that companies consider the impact to data privacy, when making important business decisions so that the notions of privacy 'by design' and 'by default' are embedded in new projects at the design phase. Decisions such as the selection of a new manning agent based outside the EU, would require a detailed assessment of the data privacy conditions relevant to data transfers from and to the agent, in order for the relevant considerations and potential risks to be surfaced and mitigated appropriately at inception of the agreement. A well thought-through privacy impact assessment can help determine those terms and conditions that will eventually allow the parties to transfer data securely and reliably, having resolved accountability issues right from the start of their contract. A well thought-through privacy impact assessment can also expose a potentially high risk business partner.

8. TRAINING

Once the GDPR compliance plan has been fully implemented, it is highly advisable to roll out GDPR training to all staff and crew, highlighting any changes that were implemented because of GDPR and the reasons thereto. Personal data such as original travel documents as well as other records are being held aboard the vessels so it is important that training, to the appropriate extent is also provided to the officers on board.

9. ONGOING MONITORING

Like all companies subject to GDPR, shipping companies need to demonstrate that they monitor their compliance on a continuous basis, by updating their policies and procedures when needed, training their staff and crew as well as updating their formal documents and agreements, when these are relevant to personal data. In addition, shipping companies should design (and incorporate in their ongoing compliance monitoring framework) tests of operational effectiveness for controls mitigating significant risks associated with GDPR and data privacy in general and follow up on the weaknesses identified.

10. FOSTERING A GOVERNANCE-DRIVEN CULTURE

No matter how many safeguards are put in place in an organisation's internal control environment, effective risk mitigation will always eventually come down to how well people understand, appreciate and implement those safeguards. Establishing and maintaining a governance-driven culture that will empower people to actively protect their organization creates a much more effective shield against privacy threats, compared to a compliance-driven approach that can prove bureaucratic.

How can shipping companies better manage GDPR compliance cost?

Compliance costs in shipping have increased exponentially in the past few years. GDPR does not need to be another heavy compliance burden: By embedding the principles of privacy to the current structures, policies and procedures that were created to respond to various other requirements coming from regulations, authorities or other counterparties, shipping companies can implement GDPR – as well as other privacy projects - in a truly risk-focused, effective and efficient way.

Costas Constantinou
costas.constantinou@moorestephens.gr

Pinelopi Kassani
pinelopi.kassani@moorestephens.gr

Moore Stephens AE
93 Akti Miaouli 185 38 Piraeus, Greece PO Box 80 132
T +30 213 0186 100
www.moorestephens.gr