LTIMindtree

Point of View

GDPR
Risk for Procurement

Author
Vikram Patil
DPO, LTIMindtree

GDPR – Risk for Procurement

The General Data Protection Regulation (GDPR), which came into effect on 25th May 2018, is designed to ensure enhanced protection of personal data, thus empowering EU &EEA living individuals who share their personal data with the firms and the organizations. The law imposes strict guidelines on businesses that process data. It is, therefore, mandatory for all organizations and their partners to comply with the regulation.

Under GDPR, the description of 'personal data' is broad, encompassing multiple categories.

For instance, the educational sector can potentially include any information relating to an identifiable living person such as:

1. An individual's name, address, phone number, date of birth, place of work, and dietary preferences.
2. Opinions about them, groups they are associated with, like trade unions.
3. Their political beliefs, ethnicity, religion, email address and professional designation, etc.

Approach to Sustainable GDPR Compliance

Purchase orders and contracts with suppliers and vendors have Personally Identifiable Information (PII) of the point of contact shared, for the purpose of getting goods and services delivered. Everyone needs to comply with the EU and EEA GDPR regulation, when an individual's personal information is shared with suppliers and vendors to meet business requirements.

LTIMindtree

Contracts That Are Likely to Be Affected

Many of the typical goods and services contracts enacted by establishments are likely to be affected by GDPR. Individual organizations should check their own contract registers to identify all contracts that could be potentially impacted. Typical categories may include:

- Management information systems
- Payroll
- Finance
- Cashless payments
- Outsourced IT management
- Awarding body organizations
- Subcontracted training provision
- Employee benefit schemes
- Recruitment advertising
- Agency staff
- Employee screening contracts
- Mobile phones
- Insurance
- Audit
- Software products
- Legal services
- Transport contracts

What Can Be Done, and How?

1) Existing Contracts

Contract Register: review current Contract Register to identify contracts, where personal data is shared with suppliers.

- **Data Mapping:** within these contracts, identify how personal data flows through the supply chain, determine the key recipients of the data, and how the data is processed.
- **Review Terms:** evaluate the current contracts, and the data protection clauses that are mentioned therein; verify if these clauses meet new GDPR requirements.
- **Give Notice:** contact suppliers and notify them of the changes you intend to make to ensure e-contract compliance with GDPR.
- **Issue Variations:** update relevant contract terms by issuing contract variations, under the mechanisms provided in your original contract; ensure you include the right to audit within the contract, alongside other mandated data processing provisions.
- **Get Guarantees:** conduct due diligence on your suppliers, and obtain guarantees they - and any other processors within their supply chain - will comply with GDPR requirements.

2) Future Contracts

- **Document Revisions:** update your standard documents, such as terms and conditions, ITT, specifications, and service delivery schedules to clearly define the roles and responsibilities of the data controller.

- **Supplier Selection:** Establish a robust due diligence process to assess new suppliers.

3) Other Considerations

- Ensure you include standard terms and conditions in your Purchase Order as per GDPR requirements.

- Verify if internal systems are set up, to ensure you satisfy the 72-hour breach notification requirement.

- See to it that your existing insurance policies cover data protection and security breaches, including breaches by suppliers.

- Consider how procurement systems store data, and the procedures planned for gaining staff consent and parental consent for children below 16 years of age when handling their personal information.

4) Be Aware of Price Increases

EU council guidance advises against accepting contract price increases on a routine basis from suppliers, as a result of work associated with GDPR compliance. Moreover, the council advises against accepting liability clauses where Data Processors are indemnified against fines or claims under GDPR. In fact, GDPR represents a potential opportunity for suppliers who are well-prepared, as they will perhaps have a competitive advantage over their less-organized competitors.

Data Subjects - the living natural individuals of EU and EEA countries need to obtain explicit consent for sharing personal sensitive information with the data controllers. They have also been given certain rights to be executed, like right to access, right to notification, right to object, right to restrict processing, right to rectification, right to erasure, right to data portability, and right to appropriate decision making and profiling.

5) Follow GDPR principles of data privacy & protection

The key principles of GDPR that data controllers and data processors must follow while processing the personal data of the EU and EEA residents are:

- Accountability & privacy

- Lawfulness, Fairness, and Transparency

- Integrity and Confidentiality

- Storage and Purpose Limitations

- Data Minimization & Maintain Accuracy of the Data at All Time

Conclusion

The GDPR compliance requirements need to be documented in the purchase order copy, informing the vendors and suppliers for the delivery of the required material.

And ensure that personal information of the EU residents is protected at all the time while processing & executing an order. In case of any privacy breach, the vendors and suppliers involved in it need to pay the entire penalty amount to the affected data subject.

About the Author

Vikram Patil

DPO, LTIMindtree

Vikram Patil has over 18 years of experience and has delivered large scale data security & privacy compliance implementation for projects across sectors such as Manufacturing, BFS, Insurance, and Healthcare for Fortune 500 clients of EU, EEA & US.

His areas of expertise include Data Protection & Privacy, ISMS, Compliance, Risk Management, Project Management, People & Process Management, Policy Making & Implementation, and Global Stakeholder Management.

In his current role as a Data Protection Officer (DPO), Vikram is responsible for ensuring GDPR compliance for LTIMindtree as a data controller, data processor and change management expert for the clients and customers in EU & EEA.