NEW EU DATA PROTECTION LAW: COMPLIANCE CHECK

The General Data Protection Regulation (GDPR) of the EU will come into force on 25 May 2018 and it will affect organizations worldwide working with or within the EU. The GDPR promotes accountability and governance. Organizations are required to put into place comprehensive governance measures to ensure compliance. The accountability principle expressly requires the organizations to be able to demonstrate that they comply. Non-compliance can lead to heavy fines up to €20 million or 4% of the global annual turnover, whichever is higher. You must prepare in advance to assess and ensure compliance by May 2018 by going through the following steps.

1. Getting informed
You have to gather information on the new requirements and set up internal assessment.

2. Identify the data processing activities
You need to identify the areas where data processing activities take place: typically HR (incl. job applications), CRM and marketing (newsletters, fidelity cards, CCTV etc.).

3. Evaluate the lawfulness of processing
Each processing activity needs to be evaluated separately, as to whether it is in line with the data protection principles (purpose limitation, data limitation, ensuring confidentiality etc.). In addition, organizations need to identify the legal basis for each processing activity (consent or statutory grounds). Where the processing is based on consent, organizations need to review how consent is obtained, whether mandatory information was provided to the data subject and how this is evidenced.

4. Evaluate the internal processes
Both the internal human intervention processes and the IT systems must be reviewed. Organisational and technical measures to ensure data protection shall be defined and responsibilities allocated. Data protection authorities expect data protection reporting lines to run to the top management level. It is also required to consult with an IT expert how data protection and security requirements can be achieved from a technical point of view.

5. Review of policies and statements
Once the internal processes are reviewed, the necessary organisational and technical measures should be incorporated in internal policies. Organizations shall have an HR policy for employee data, another for customer data and further policies for specific processings, such as CCTV, lotteries etc. Such policies shall also cover the process around data breaches and data transfers. Also a privacy statement shall be drafted or updated informing the persons interacting with your organization how you use their personal data.

6. Documentation
Certain activities fall under mandatory documentation obligation. However, we recommend maintaining similar documentation of any processing activities in order to comply with the general principle of accountability.

7. Evaluate the necessity of a DPO
Certain category of organisations is obliged to appoint a data protection officer. You have to consider whether your organization is affected.

8. Raise awareness, educate your colleagues
Staff which has access to personal data must be educated on the new requirements and a senior member of the management shall monitor the implementation.

Please note, that monitoring and security are ongoing processes that you need to focus on continuously during the whole data processing cycle.

Present summary intends to offer a general guidance on data protection audit which on the basis of the particularities of your organization and your jurisdiction may well require further analysis. Should you need a customized assessment, please contact one of our offices for further assistance.