The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city

Shakila-Bu-Pasha

It is assumed that privacy of personal and location data will be at risk in the 5G and other network-based platforms in the smart city services because of inter-connected smart sensors and devices and the use of other latest technologies. According to Article 35(1) of the GDPR, data controllers are required to carry out a data protection impact assessment (DPIA), if data processing activities, especially those using new technologies, are "likely to result in a high risk to the rights and freedoms of natural persons".

Article 29 Data Protection Working Party (A29 WP) has drafted a useful set of guidelines, that is WP 248 Guidelines to determine when DPIA is necessary and other relevant factors related to DPIA. The article took into account the WP 248 guidelines and found that 'high risk' is likely exist in smart city services requiring DPIAs.

Controllers have to carry out a DPIA prior to the processing. Since DPIA is a part of the principle of data protection by design, controllers should start designing it as early as possible, even if they still do not know all of the processing operations. This approach is beneficial for a number of reasons. For example, they can identify the possible risks in an early stage which is easier and economical to handle. The organisations can become aware beforehand regarding privacy and data protection and will be less likely to breach the provisions of the GDPR. Thus, individuals as data subjects or users of the services of the smart cities will receive positive effects. If a set of similar processing operations presents similar high risks, then a single DPIA may be enough, in circumstances where it is reasonable and economical.