All Organizations who control and/or process EU citizen data will need to reach compliance with the General Data Protection Regulation to avoid astronomical fines in the event of an information incident or breach. When reviewing the GDPR, one requirement is laid out quite clearly, Organizations who monitor large scale data subjects are required to appoint a Data Protection Officer (DPO).

With an estimate of 9000 Data Protection Officers need in the United States alone to satisfy GDPR requirements, organizations are asking questions.1

1) **Who** is the Data Protection Officer?
2) **What** are their required credentials?
3) **What** is their role as required by the GDPR?
4) **Where** will I find a person to fill this role?

A significant number of U.S. based organizations have or will appoint a DPO from either the legal or information security teams in order to be compliant. While there is no right or wrong answer regarding which team should own this role, it’s important to note that the DPO has requirements around the monitoring of compliance with the regulation and with interpreting the results of data protection impact assessments (DPIAs). For this reason, it’s important to not underestimate the technical acumen required to successfully perform this function.

GDPR Articles 37, 38, & 39 Summary: Data Protection Officer

<table>
<thead>
<tr>
<th>Qualifications:</th>
<th>Core Requirements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Data Protection officer must report to the highest levels of management and maintain independence.</td>
<td>DPO’s are bound to secrecy or confidentiality concerning required tasks of the position. They may hold other responsibilities as long as they don’t interfere with requirements. Data subjects must be able to contact to DPO in regards to the processing of their data.</td>
</tr>
</tbody>
</table>

DPO’s are the point of contact with the supervisory authority on issues related to processing and any other GDPR matter. DPO’s are required to cooperate with the supervisory authority.

Responsibilities:

| The Data Protection Officer must monitor compliance of regulation along with other relevant regulations in the relation to personal data to include assigning responsibilities, awareness and the training of staff. | With due regard to the risk associated with processing operations, the DPO shall, in the performance of his or her tasks, take into account the nature, scope, context and purposes of processing. |

---

1International Association of Privacy Professionals