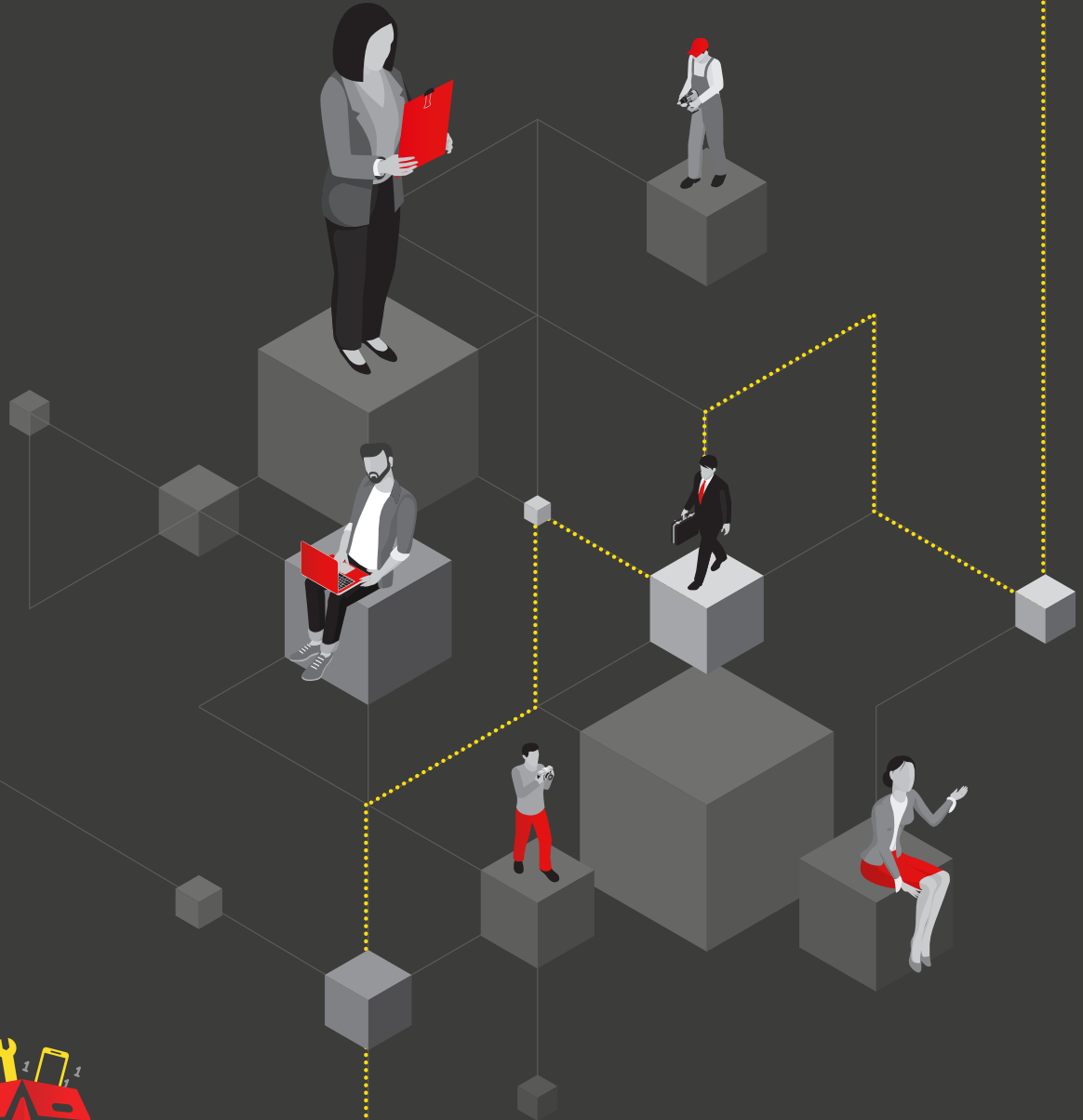




APPOINTING A DATA PROTECTION OFFICER (DPO) CHECKLIST



Guidance for Organisations

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.



WWW.JERSEYOIC.ORG



Appointing a Data Protection Officer (DPO) - Checklist

The Data Protection (Jersey) Law 2018 places obligations on those processing personal information.

This checklist helps to identify whether or not you need a Data Protection Officer.

Appointing a DPO

- We are a public authority or body and have appointed a DPO (except if we are a court acting in our judicial capacity);
- We are not a public authority or body, but our core activities require regular and systematic monitoring of individuals on a large scale and have appointed a DPO;
- We are not a public authority or body, but our core activities consist of processing special category data on a large scale and have appointed a DPO;
- We need to appoint a DPO because of a relevant law, for example, the law of Jersey, another jurisdiction in the British Islands, a Member State or the European Union;
- We are a group of undertakings or a group of public authorities or bodies and we've decided to appoint a single DPO for all of us;
- We aren't required to appoint a DPO under the Data Protection (Jersey) Law 2018 but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO. We support our DPO to the same standards;
- We have appointed a DPO based on their professional qualities and expert knowledge of data protection law and practices and we carried out appropriate due diligence before appointing them formally. We are satisfied that the DPO is able to fulfil their duties as set out in the DPJL.

Position of the DPO

- Our DPO reports directly to our highest level of management and is given the required independence to perform their tasks;
- We involve our DPO, in a proper and timely manner, in all issues relating to the protection of personal data;
- Our DPO has access to all relevant personal data and processing operations necessary to carry out their duties;
- Our DPO is sufficiently well resourced to be able to perform their tasks in order to carry out their duties and maintain their expert knowledge;



- We do not penalise the DPO for performing their duties;
- We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

- Our DPO is tasked with monitoring compliance with the Data Protection (Jersey) Law 2018 and other data protection laws where relevant, our data protection policies, awareness-raising, training, and audits. They draw the controller's attention to any failure to comply with the applicable data protection rules. The appointment, position and duties of a DPO can be found in **Schedule 5 of the DPJL**;
- We will take account of our DPO's advice and the information they provide on our data protection obligations. If we do not follow the advice of our DPO we carefully document the reasons for this;
- When carrying out a **Data Protection Impact Assessment (DPIA)**, we seek the advice of our DPO who also monitors the process. If we do not follow the advice of our DPO we carefully document the reasons for this;
- When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO

- Our DPO is easily accessible as a point of contact for our employees, members of the public and the Jersey Office of the Information Commissioner;
- We have published the contact details of the DPO and communicated them to the Jersey Office of the Information Commissioner.