ORGANISATIONS

APPOINTING A **DATA PROCESSOR**

digital **TOOLKIT**

Guidance for Organisations

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Appointing a Data Processor Checklist

You should use this Checklist if you intend to use a third party/supplier to process data on your behalf; for example, an external payroll provider. Article 19 of the Data Protection (Jersey) Law 2018 (the DPJL) says that processing carried out by a processor must be governed by a contract or other legal act and it must set out the:

- Subject-matter and duration of the processing;
- The nature and purpose of the processing;
- The type of personal data and categories of data subjects; and
- The obligations and rights of the controller.

The contract or other legal act must also stipulate that the supplier/third party (see Article 19 of the Data Protection (Jersey) Law 2018):

- Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation;
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Takes all measures required by Article 21 of the DPJL in terms of having appropriate technical and organisational measures in please to ensure security of the data;
- Respects the conditions set out in the DPJL relating to the use of any sub-processor;
- Taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;
- Assists the controller in ensuring compliance with the obligations under Articles 16, 20 and 21 of the DPJL (review re high risk processing, dealing with a personal data breach and ensuring security of the information), taking into account the nature of processing and the information available to the processor;
- At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the relevant law requires storage of the personal data;
- Makes available to the controller all information necessary to demonstrate compliance and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

For further guidance on the meaning of 'controller' and 'processor', see our other guidance note entitled '**Controller or Processor**'

These are the types of things you should consider when drawing up any agreement with your third party/supplier. It is not intended to cover every single thing that can be covered in a formal agreement and it is not a substitute for formal legal advice and should not be relied on as such.

Checklist

A: Key data processing specific commercial and legal considerations

Parties:
- Set out who the parties to the agreement are.

Commencement and duration

Commencement:
- Confirm start date of the agreement.

How long the agreement is to last?
- Is the agreement fixed term or rolling contract?
- How much notice does a party need to give if they want to terminate the relationship?

Any preconditions:
- Does the processor need to confirm/do anything before the proposed agreement can take effect, for example approval of the supplier's data processing facility or achieve certain qualifications such as ISO 27001.

Data processing services

Data:
- Set out what data (e.g. relating to employees, customers or marketing prospects) will be processed under the proposed agreement;
- Confirm the extent to which such data is personal data;
- Set out where the relevant data will originate from (including geographic location);
- Set out how and when the supplier will obtain the data to provide the services;

Services:
- Set out exactly what data processing services will be provided (e.g. payroll processing) (when and how will they services be provided).

Security:
- Ensure the agreement places appropriate security obligations on the supplier (taking into account matters such as market practice, legal requirements and the customer's policies and expectations).

Remedies:
- Identify remedies for breach of agreed service standards and data protection compliance and other obligations.

Ownership:
- Identify who owns;
  (a) the original data processed under this agreement;
  (b) any additions or modifications to it.

Sub-contracting:
- Set out whether the performance of obligations can be sub-contracted by the supplier to its sub-contractors, including sub-processors of the data. If sub-contracting is permitted, what remedies will the customer have in respect of those sub-contractors, particularly if they are based outside Jersey/the EEA? Where the data includes personal data, make sure you include any appropriate restrictions and/or provisions regarding sub-processing as required to comply with the DPJL and any other applicable laws.

Pricing, fees and expenses

Fees:	• Set out whether the fees for the services will be a fixed fee or hourly/daily rate, and whether expenses are recoverable (make sure this part is as clear as possible). Set out the relevant currency and any other payment terms/ requirements you have regarding invoices being received from the supplier. Identify the timeframe for payment of invoices.

B: Other general legal terms and conditions

Liability:	• Carefully identify any exclusions and limitations on liability and any types of loss for which a party has unlimited liability. Who is going to be responsible if something happens to the data and to what extent? In particular: • Ensure any limits on the supplier's liability in respect of liability for lost data and breaches of confidentiality, intellectual property and data protection obligations are carefully considered and document within the agreement whether liability for indemnities is capped, limited or excluded.
Termination:	• Ensure termination can take place for material breach or breach of key data protection and other provisions. Ensure that you have the ability to terminate for convenience. Consider if termination can take place for insolvency and/or change of control. What notice needs to be given?
Obligations on termination:	• Confirm what each party must do on termination, in particular with return or destruction of data as required by the DPJL or help with transitioning any data to a replacement service supplier.
Confidentiality:	• Identify specific obligations regarding confidentiality and publicity and their duration. Make sure these are consistent with any provisions relating to use of the customer's data and with those provisions relating to personal data.
Dispute resolution:	• Consider if the contract should identify a specific resolution process: e.g. expert, mediation, arbitration and/or courts. Where and how should notice of these matters be given?
Governing law and jurisdiction:	• Confirm that the agreement is governed by laws of Jersey and whether Jersey will have exclusive jurisdiction.
Other clauses:	• Are there any other you want to include e.g. non-solicitation; notice; variation; reporting; audits and investigations etc?
Completion:	• Confirm how the agreement will be signed/executed. Consider counterparts, execution clauses, electronic completion and further assurance clause.