



MERGER AND ACQUISITIONS CHECKLIST



digital 
TOOLKIT

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.



JOIC

JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG



Data Protection considerations for when you're Buying or Selling a Business

The Data Protection (Jersey) Law 2018 (DPJL) includes a core set of principles, with which organisations must comply.

Data protection does not prevent you from selling or merging your business or acquiring someone else's and you will likely be required to share information as part of the merger/acquisition process.

If you're planning on buying or selling a business, data protection issues must be considered by all parties at each stage of the process and all parties must ensure that they adhere to the data protection principles as set out in Article 8 of the DPJL:

- The lawfulness, fairness and transparency principle;
- The purpose limitation principle;
- The data minimisation principle;
- The accuracy principle;
- The storage limitation principle;
- The integrity and confidentiality principle.

This means that both parties must:

- Consider data sharing as part of any due diligence carried out as part of the transaction;
- Establish a legal basis for sharing personal data that forms part of the transaction;
- Be able to explain to data subjects what is being done with their personal data;
- Ensure that any data shared is done so subject to appropriate standards of confidentiality and security (including restricting access to personal data to specific individuals on a need to know basis);
- Document the sharing;
- Consider what will happen with any personal data that has been shared in circumstances where the transaction does not ultimately proceed.

Depending on whether you are the buyer or the seller, you may have different data protection considerations from each other. For example,

If you are a seller, you need to be able to identify:

- The personal data that will need to be provided to the buyer for its due diligence (this includes being able to explain what categories of personal data is being processed by you);
- The data processing conditions (if any) pursuant to which you are able to provide personal data to the buyer;
- Where you may need to redact, anonymise or pseudonymise personal data;
- The prospective buyer's level of data protection compliance (are you confident that any information provided to them will be dealt with in accordance with the law; will it be secure for example).



If you are a buyer, you need to be able to:

- Identify what information you need from the seller to progress with the acquisition or merger (including identifying what information actually needs to be transferred for the buyer's intended purposes i.e. do they need all the information to be transferred);
- Understand exactly what personal data is being provided by the seller and on what basis was it collected.
- Investigate and satisfy yourself of the seller's compliance with data protection legislation (including satisfying yourself that the buyer can demonstrate their compliance with the data protection principles) so that you can identify any potential areas of risk. What policies and procedures are in place regarding data protection and what are the retention periods applicable to any personal data that is transferring across?
- Consider any confidentiality issues;
- Understand what data subjects know about the proposed transaction (including understanding what notifications have been given/consents obtained);
- Know which processors/third parties may also be involved in processing the relevant personal data;
- Have in place appropriate systems and procedures to deal with migration and integration of the personal data into your own systems;
- Know whether there are any existing claims relating to any of the personal data that is being transferred/ any requests that have been made by data subjects (such as subject access requests) that are in train and what insurance cover is in place, if any. Are there any potential breach of the DPJL 2018 that you need to be aware of?

What do you need to tell data subjects?

Where a seller is considering disclosure of a data subject's personal data to a buyer, you should consider the right to be informed, what information you will provide to data subjects affected and how and when such will be provided.

It may not be possible to tell the data subjects about the proposed transfer whilst negotiations are on-going but both parties must bear in mind Article 8(1)(a) of the DPJL 2018 which states that personal data must be processed in a transparent manner.

Article 12 also sets out that where a controller obtains personal data about a data subject, and not from the data subject directly, that the data subject must be provided/have made available to them, the information set out in Article 12(4) of the DPJL:

- (a) The identity and contact details of the controller, and (where applicable), the controller's representative;
- (b) The contact details of the data protection officer (if any);
- (c) The purposes for which the data are intended to be processed and the legal basis for the processing;
- (d) An explanation of the legitimate interests pursued by the controller or by a third party, if the processing is based on those interests;
- (e) The recipients or categories of recipients of the personal data (if any);
- (f) Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and whether or not there is an adequate level of protection for the rights and freedoms of data subjects within the meaning of Article 66;



- (g) The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - (h) Information concerning the rights of data subjects under Part 6, to the extent that these apply;
 - (i) Where the processing is based on consent, the existence of the right to withdraw consent under Article 11(3)(e);
 - (j) The existence of any automated decision-making, as referred to in Article 38, and any meaningful information about the logic involved in such decision-making as well as the significance and the envisaged consequences of such processing for the data subject;
 - (k) A statement of the right to complain to the **Jersey Office of the Information Commissioner**;
 - (l) Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failing to provide such data;
 - (m) Where the personal data are not obtained directly from the data subject, information identifying the source of the data;
 - (n) Any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.
- (6) Paragraph (2) does not apply if the controller believes that –
- (a) Providing the specified information is impossible, would involve a disproportionate effort on the part of the controller, or is likely to prejudice the objectives of the processing and the controller records the reasons for its belief and retains this record while it retains the data; or
 - (b) The recording of the information to be contained in the data, or the disclosure of the data by the controller, is necessary for compliance with any legal obligation to which the controller is subject, other than an obligation imposed by contract; or
 - (c) The data are held subject to an obligation of professional secrecy regulated by law (whether in Jersey or elsewhere).
- (7) Where the controller does not provide the information the controller must take appropriate measures to protect the data subject's rights and interests, which may include making the specified information publicly available.

You should put yourselves in the shoes of the data subject: if you were the customer and it was your personal data that was being transferred, what information would you wish to receive?

Jersey Office of the Information Commissioner, 2nd Floor, 5 Castle Street, St Helier, Jersey JE2 3BT

Telephone number: +44 (0) 1534 716530 | **Email:** enquiries@jerseyoic.org