

DATA PROTECTION (JERSEY) LAW 2005

***SUBJECT ACCESS AND
THIRD PARTY
INFORMATION***



DATA PROTECTION (JERSEY) LAW 2005:

Subject Access and Third Party Information

Contents

Introduction	1
Non-compliance with a subject access request	2
To disclose...or not to disclose?	3
Consent	4
Assessing reasonableness	6
Confidentiality	6
Disclosure flowchart	9

Introduction

The Data Protection (Jersey) Law 2005 (the “Law”) provides a right of access to individuals in respect of personal data of which they are the subject. Upon making a written request and paying the requisite fee, amongst other things an individual is entitled to have communicated to him in intelligible form:

- the information which forms any such personal data, and
- any information available to the data controller as to the source of those data.

In some circumstances, responding to a request may involve providing information relating to another individual who can be identified from that information (“third party information”). This can give rise to conflict between the data subject’s right of access and the third party’s right to respect for his or her private life.

When dealing with such requests therefore the data controller should be sensitive to and give proper consideration to this potential conflict before deciding whether to disclose third party information.

This guidance document has been designed to assist data controllers when dealing with subject access requests, which may involve the disclosure of third party information.

Non-compliance with a subject access request

If the data controller decides not to comply with the request (in whole or in part) there may be a contravention of the sixth data protection principle.

The sixth principle requires that personal data shall be processed in accordance with the rights of data subjects (which include subject access rights). The data subject, or someone on his or her behalf, may request the Data Protection Commissioner (the "Commissioner") to make an assessment as to whether or not failure to comply with the subject access request is in compliance with the Law.

Such an assessment may involve the Commissioner in reviewing the data controller's decision not to provide the information. Where the Commissioner considers the data controller was not justified in withholding information and has contravened the sixth data protection principle, she may take enforcement action requiring the data controller to provide it.

Further, the individual making the request may seek an order for disclosure from the courts. In addition, where the individual suffers damage or distress as a result of the failure to respond, he may seek compensation from the data controller.

On the other hand the disclosure of third party information in compliance with a subject access request may also expose the data controller to complaint or action by the third party, for example, a complaint to the Commissioner that the data controller has breached the principles or an action in the courts for breach of confidence.

To disclose...or not to disclose?

Relevant factors to which the data controller should give consideration in deciding whether, or to what extent, the Law requires them to disclose third party information are set out in this guidance.

Firstly, the data controller should consider to what extent it is possible to communicate the information sought without disclosing any third party information (here the term "disclosure" means revealing information which is not already known to the data subject).

In considering this the data controller should take into account not only the information being disclosed but also any other information which the data controller reasonably believes is likely to be in or to come into the data subject's possession.

The data controller should give as much information as possible to the data subject without revealing the identity of the third party. This might be achieved by editing the information to remove names or other identifying details.

However, in such cases, there may be residual third party information and so in all such cases the data controller will need to consider further factors before they are in a position to establish whether they are obliged to comply with the request in respect of the excised residual third party information.

Consent

Where the third party has consented to the disclosure to the person making the request, the data controller is obliged to comply with the request and disclose the third party information. Failure to do so could amount to a breach of the Sixth Principle.

What if consent has not been given? Consent may not have been given for one or more reasons examples of which are:

- consent has not been sought;
- it is not possible to obtain consent because the third party's whereabouts are unknown;
- the third party does not have legal capacity to consent;
- the third party declines to consent.

Where consent has not been given (for whatever reason), the data controller is nevertheless required by the subject access provisions to comply with the request and disclose third party information if it is reasonable in all the circumstances to disclose without consent.

However to avoid falling foul not only of the Law, but other provisions of law e.g. confidentiality, disclosure without consent should not be made until proper consideration has been given to all the relevant factors.

When is it reasonable in all the circumstances to make the disclosure even though consent has not been given? The Law highlights some of the factors to be taken into account in deciding this but the list is not exhaustive. They are:

- any duty of confidentiality owed to the third party;
- any steps taken by the data controller to seek the consent of the third party;
- whether the individual is capable of giving consent;
- any express refusal of consent by the other individual.

The data controller may at the very least need to take steps to seek consent in order to demonstrate that it was reasonable in the circumstances to make the disclosure without consent.

It may not always be appropriate to seek consent, for example if to do so would inevitably involve a disclosure of personal data about the data subject to the third party. In general, however, although the Law does not expressly state that the data controller is obliged to seek consent, the data controller should consider whether

- a) consent has already been given or
- b) he ought to obtain consent.

The fact that the same information has previously been provided to the data subject or is already known to him/her will also be relevant in assessing reasonableness. As will the fact that particular information is generally publicly available.

Example: The data controller's records detailing the data subject's claim for benefit include the name of the officer dealing with the claim. The officer had provided his/her name on an earlier occasion when he/she met the claimant in interview to complete the claim forms. The data controller would not be justified in withholding the officer's name in these circumstances.

It follows that a data controller is less likely to be able to justify withholding the information where the third party is a member of staff acting in the course of his/her duties rather than an individual acting in a private capacity.

Consequently, unlike the position under the Data Protection (Jersey) Law 1987, where the data controller could withhold information already known to the data subject, under the Law the data controller is likely to be obliged to provide it.

Sometimes subject access requests are made by someone else on the data subject's behalf. There may be circumstances where the third party is prepared to consent to the disclosure being made to the data subject, but may object to it being provided to the person making the request on the data subject's behalf.

The data controller is entitled to take these circumstances into account in deciding whether it is reasonable to disclose without consent. Although in such a case the option of disclosing directly to the data subject may be considered.

Assessing Reasonableness

What circumstances relating to the data subject are relevant in assessing reasonableness?

The Law does not provide any guidance on this. There is limited general law from which to draw guidance on this specific issue. The mechanism provided by the Law to address the balance between the two conflicting rights is rooted in a European Court of Human Rights case.

An individual had been in local authority care for most of his childhood. The local authority records relating to his time in care were considered to provide the only coherent record of his early childhood and formative years. The Court considered that people in his situation had a “vital interest, protected by the Convention, in receiving the information necessary to know and understand their childhood and early development”.

Confidentiality

Broadly speaking, a duty of confidence arises when information which is generally inaccessible to the public, is disclosed to another in circumstances where there is an expectation that it will remain confidential.

A duty of confidence is characteristic of several types of relationships for example, medical (doctor/patient), employment (trade secrets), legal (solicitor/client), financial (bank/customer) and caring (teacher/pupil, counsellor/client etc). On the other hand, the data controller should guard against assumptions of confidentiality.

For example a duty of confidence does not necessarily arise just because a letter is marked "confidential", although such a marking may be indicative of an expectation of confidentiality.

Where a clear duty of confidence arises, disclosure of identifying information without third party consent is unlikely to be reasonable.

Where there is no duty of confidence, it will in many cases be reasonable to disclose third party information without consent. However there will be circumstances where disclosure should not be made without consent even where the information to be disclosed is not confidential in nature e.g. where it is sensitive, or where it is likely to cause harm.

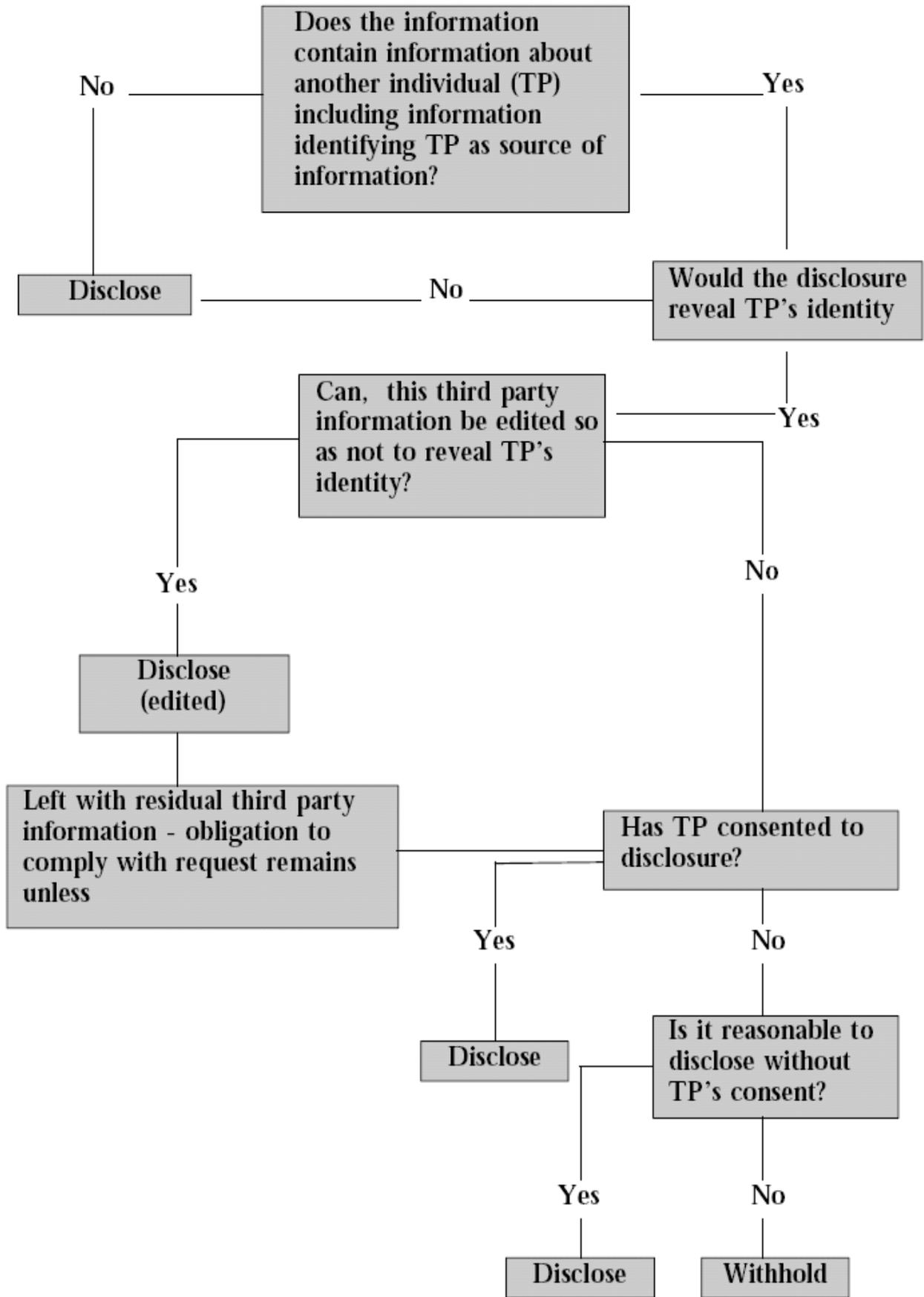
Where consent has not been given and the data controller is not satisfied that it would be reasonable in all the circumstances to disclose third party information without it, the safer course for the data controller is to withhold the information. Although this could expose the data controller to the scrutiny of the Commissioner and possibly ultimately enforcement action, this would serve as an independent review by the Commissioner on the question of whether or not it is reasonable to disclose without consent.

Should the Commissioner conclude that it would not be reasonable to disclose without consent and the data controller maintains its decision to withhold the information, the Commissioner's view could be persuasive argument should court action for disclosure as described be brought by an individual.

Should the Commissioner conclude that it would be reasonable to disclose without consent and serves an enforcement notice on the data controller requiring him to disclose, a disclosure made in compliance with such a notice should be protected by the defence of compulsion of law should a claim be brought by an individual for breach of confidentiality.

Key questions for data controllers when dealing with subject access requests involving third party information: -

- Does the information being accessed contain information about a third party?
- If so, would its disclosure reveal the identity of the third party?
- In deciding this has other information which the data subject has/may get been taken into account?
- To what extent can the information be edited so it can be given promptly without revealing the third party's identity? N.B. This does not overcome the data controller's obligation to comply with the request by disclosing third party information where the third party consents to such disclosure or it is otherwise reasonable to comply with the request without the consent of the third party.
- Has the third party previously given the information to the person making the request?
- If, or to the extent that, the information will identify the third party, has the third party consented to the disclosure?
- If not, should consent be sought?
- Is it reasonable to disclose the third party information without consent?
- Is the third party information confidential or sensitive or harmful?
- Is the third party information of particular importance to the data subject?



CONTACT THE COMMISSIONER:

Enquiries and Publication Requests:

T: 01534 441064

F: 01534 441065

E-Mail: dataprotection@gov.je

W: www.dataprotection@gov.je

Office of the Data Protection Commissioner

Morier House

Halkett Place

St. Helier

Jersey

JE11DD

