The right of access and "Third Party Information"

information commissioner
Barrantagh Fysseree

Responding to a subject access request ("request") may occasionally involve the provision of *"third party information"* ("TPI") to the data subject.

There is an exemption to protect the rights of others, set out in paragraph 8 of Schedule 9 to the GDPR and LED Implementing Regulations 2018, which can be applied by controllers, when 'necessary and proportionate'. A controller must be able to demonstrate that it was 'necessary and proportionate' to apply the exemption.

The exemption states that the provisions of Article 15 (the right of access):

> *"do not oblige a controller … to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information."*

However, the presence of TPI, for example, in a document that also contains the data subject's personal data ("PD"), does not negate the data subject's right of access.

On the contrary, the exemption states that the existence of third party information:

> *"is not to be construed as excusing a controller … from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise"*

A controller only needs to consider applying the exemption if it is not possible to separate or extract the PD from the TPI, or omit, redact or otherwise remove the TPI. *A flowchart is provided at the end of this document.*

Considerations given to the necessity and proportionality of relying on the exemption

If the PD and TPI cannot be separated, a controller must comply with a request and provide the data subject's PD and the TPI if:

1. it is reasonable in all the circumstances to disclose the TPI to the data subject without the third party's consent; or

2. the third party has consented to the disclosure of the TPI to the data subject.

A controller therefore needs to consider the following:

1. **Is it reasonable in all the circumstances to disclose the TPI without consent?**

A controller must consider whether it is 'reasonable in all the circumstances' to disclose the TPI:

a. where the controller has not sought consent, or
b. if the third party refuses to give consent.

Paragraph 3(3) of the exemption contains a non-exhaustive list of factors to be taken into account by the controller when deciding whether disclosure of the TPI would be 'reasonable'.

These include:

- the type of information that would be disclosed;
- any duty of confidentiality owed to the third party by the controller;
- any steps the controller has taken to try to get the consent of the third party;
- whether the third party is capable of giving consent; and
- any express refusal of consent by the third party.

'Type of Information'

The type of TPI may be as simple as the name, or initials, of the third party, a pseudonym, avatar, or could include their private contact details, or other more significant information.

A controller should assess the appropriateness of disclosing TPI and the scope of that TPI.

For example, the disclosure of a name may not affect the rights and freedoms of the third party, particularly if the data subject knows them, whereas it may not be appropriate or necessary to disclose an address or other contact details, if doing so may put the third party at risk.

Confidentiality

One factor in assessing how reasonable a disclosure of TPI would be is whether the controller owes a duty of confidentiality to the third party. This will only arise where genuinely 'confidential' information has been disclosed to the controller, i.e. the information has the 'necessary quality of confidence' and is not generally available to the public. A 'confidential' marking on a document does not necessarily equate to a 'duty of confidence'.

However, in most cases where a clear duty of confidence does exist between the third party and the controller, it will usually be reasonable to withhold the TPI unless you have the consent of the third party to disclose it, or it is otherwise in the public interest to disclose.

Other points to consider in assessing reasonableness:

- Circumstances relating to the data subject will be relevant, in particular, how critical the access to the TPI is to upholding other general rights of the data subject.

  In *Gaskin v United Kingdom [1990] 1 FLR* (European Court of Human Rights), the individual, who had been in local authority care for most of his childhood, wanted to see the local authority records relating to him as they were the only coherent record of his early childhood and formative years. The court held that the local authority had to weigh the public interest in preserving confidentiality against the individual's right to access information about his life, even where consent to release the information had been withheld. The Court held that, in all the circumstances of the case, the personal data and third party data were to be disclosed.

- Where the third party is the source of the information, there may be a strong case for their identification if the data subject needs to correct some damaging inaccuracy. This is often a consideration where a complaint has been lodged about the data subject.

- If the data subject and third party are known to each other (for example, a familial connection, employment context ,or professional relationship (such as health professional and patient)), or where the TPI is in communications between the data subject and the third party, it may be reasonable to disclose the TPI. This will depend, however, on the state of the relationship between the data subject and third party and any duty of confidentiality owed to the third party.

2. Seeking the consent of the third party

Consent means *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

Consent cannot be *"specific, informed and unambiguous"* if either the controller or the third party does not know what TPI is to be processed (disclosed).

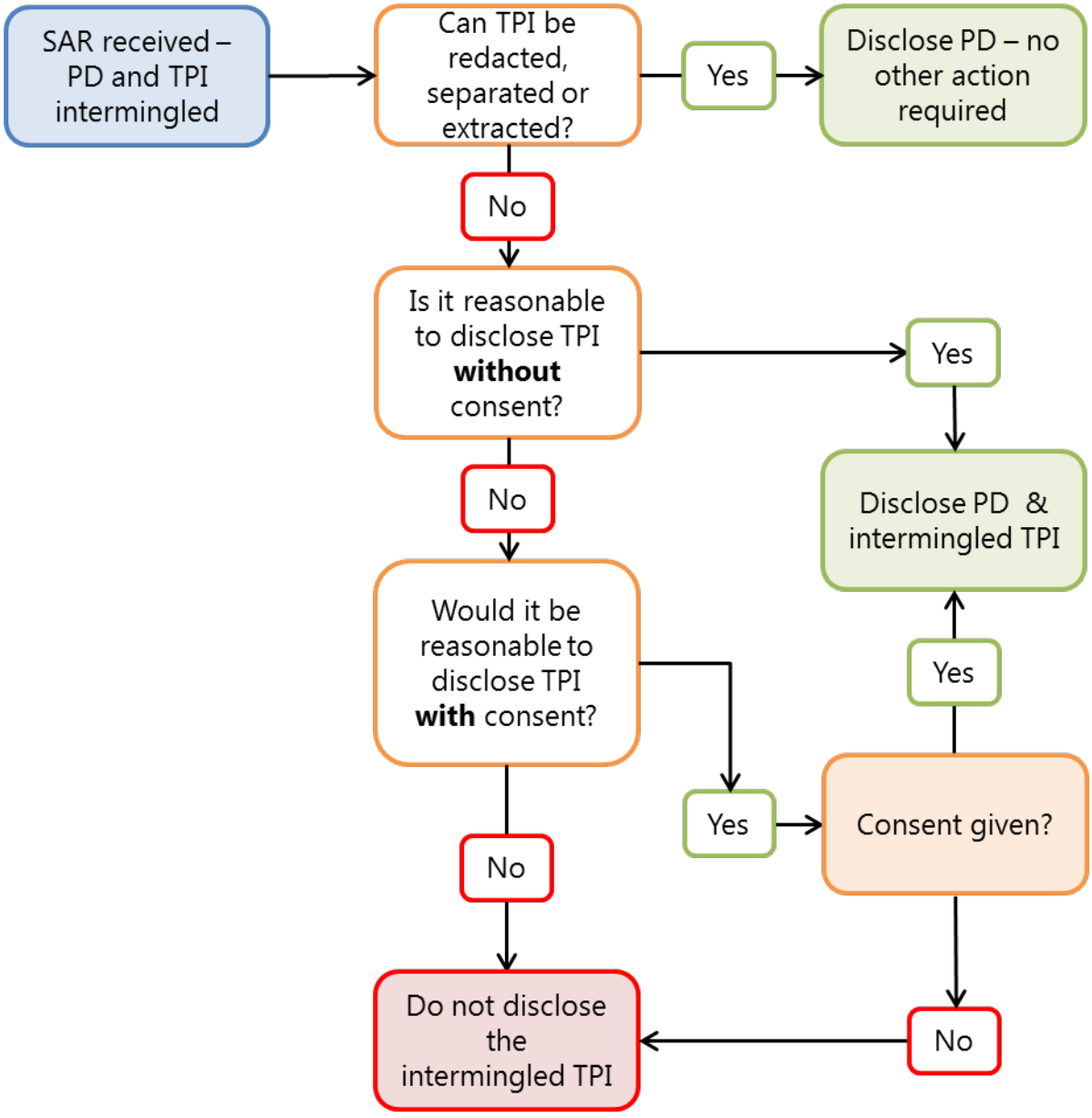
In order for consent to be valid, the controller must be able to explain to the third party precisely what TPI is under consideration for disclosure. Controllers cannot just ask the third party a general question about whether they consent or agree to disclosure of unspecified TPI.

Further points about seeking consent:

- *In practice, it may be difficult to get consent, for example, the controller may not know the third party, or existing contact details may not be up to date.*

- *In Durant v Financial Services Authority ([2003] EWCA Civ 1746), the Court of Appeal decided it would be legitimate for the Financial Services Authority (the controller) to withhold the name of one of its employees who did not consent to disclosing the requested information because Mr Durant (who made the request) had abused them on the telephone.*

June 2020


SAR received – PD and TPI intermingled
Can TPI be redacted, separated or extracted?
Yes
Disclose PD – no other action required
No
Is it reasonable to disclose TPI **without** consent?
Yes
Disclose PD & intermingled TPI
No
Would it be reasonable to disclose TPI **with** consent?
Yes
Consent given?
Yes
No
Do not disclose the intermingled TPI
No