EXECUTIVE SUMMARY

Advice on consent options for the purpose of making personal data public in RDS and requirements under the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**")

Consent requirements

Pursuant to the GDPR, consent must be freely given, specific, informed and unambiguous. Also, it needs to be obtained prior to the processing taking place. Controllers must be able to demonstrate that valid consent has been given and individuals have the right to withdraw consent at any time.

Under the GDPR, the obligation to obtain consent lies with the controller. The controller may instruct a third party to obtain consent from individuals on its behalf; however, doing so will not relieve the controller from its obligations under the GDPR.

Consent options

On the basis of the above requirements, the table below examines five options of obtaining consent for making personal data public in RDS and sets out the compliance considerations of each option:

No.	Option	Compliance considerations
1.	Controllers seek valid consent directly from individuals • Making personal data public in RDS is optional. • Prior to making personal data public, the controller contacts individuals directly to seek consent in line with the GDPR requirements examined above (consent wording provides adequate information in line with para 17 above, is specific to the processing operation of making the data public in RDS, explains clearly that individuals are free to say no and doing so will have no impact on them (or the registration process), and informs individuals on how they can withdraw consent if they wish to). • The communication makes available to individuals the controller's privacy notice (for example, via a hyperlink).	Seeking consent directly from individuals is the safest option as controllers will have control over the consent process, will be in a position to ensure that consent is obtained in accordance with GDPR standards and that they meet their transparency obligations. Also, it allows them to manage withdrawals of consent and promptly act upon these. Finally, in line with their accountability obligations, controllers will be able to demonstrate that valid consent has been obtained by keeping records of consent.

	• Granting consent is recorded for evidential purposes. • In the event of refusal to consent or failure to respond, the personal data will not be made public.	
2.	Registrant obtains valid consent and provides evidence to controller • Making personal data public in RDS is optional. • Prior to making personal data public, the controller requires the registrant to: (a) obtain individuals' consent using a consent method defined by the controller (for example, consent form with specific wording and format which meets GDPR requirements); and (b) provide to the controller evidence that consent has been obtained (for example by means of the registrant providing a signed copy of the consent form or the individual directly forwarding this to controller). • In the event of refusal to consent or failure to receive evidence, the personal data will not be made public.	As an alternative to the above option, controllers can require the registrant to: (a) obtain valid consent on their behalf –using an approved consent method and wording- and (b) provide proof of such consent. This way, controllers still maintain control over the consent process and are in a position to verify whether consent has been validly obtained. The method is somewhat less robust than option 1, as the controller does not receive direct confirmation from the data subject that he or she has given consent. In the (possibly rare) situation that the registrant does not obtain consent from the admin/ tech contact, then the consent would not be valid.
3.	Registrant obtains valid consent and controller confirms this with the individual • Making personal data public in RDS is optional. • Prior to making personal data public, the controller requires the registrant to: (a) obtain individuals' consent using a consent method defined by the controller (for example, consent form with specific wording and format which meets GDPR requirements); and	This option is a variant of option number 2 – in addition to receiving evidence of consent, the controller contacts individuals directly to confirm consent. This places a higher administrative burden on the controller, but would mitigate the risk that the registrant has not actually secured consent from the relevant person.

	(b) provide to the controller evidence that consent has been obtained (for example by means of the registrant providing a signed copy of the consent form or the individual directly forwarding this to controller). • Controller follows up with the individual directly: it informs them that the registrant has confirmed they have granted consent. The controller advises the individual to let them know if this confirmation has been provided erroneously and that in absence of a response from their side, the personal data will be made public within [x time]. The controller can also use this opportunity to provide all information to be made available to the individual, incl. in relation to their right to withdraw consent.	
4.	Registrant confirms they have obtained valid consent and undertakes the obligation to provide a copy if requested • Making personal data public in RDS is optional. • Prior to making personal data public, the controller requires the registrant to: (a) obtain individual's consent using a consent method defined by the controller (for example, consent form with specific wording and format which meets GDPR requirements); and (b) confirm that they have done so. • In addition, controller undertakes the obligation to keep copies of consent and provide to controller if requested.	Under this option, there is less control over the consent process compared to the above options and more reliance on the registrant to comply with their –contractual- obligations. The obligations undertaken by the registrant may provide the controller with a contractual recourse against the registrant. However, the controller will not be discharged from its obligations under the GDPR and – if the registrant has not met its obligations and/or does not provide a copy of the consent on request – then the controller will not be able to demonstrate that consent requirements are met, so this will impact on controller's compliance with GDPR.

5.	Registrant undertakes the obligation to obtain consent • Registrants are allowed to provide non-personal contact details; however, registration data is made public by default (irrespective of whether or not personal data is included). • By means of a statement, registrants undertake to ensure they have obtained individuals' consent if they choose to provide personal data.	This option is unlikely to be GDPR-compliant for a number of reasons: • The controller has taken no action to ensure that consent has been obtained, although the obligation to obtain consent continues to rests with the controller; • Also, the controller is not in a position to demonstrate compliance with Article 4(11) and Article 7 GDPR requirements or with its transparency obligation. • The controller does not hold any record of consent. • Consent will not be freely given as individuals are not in a position to effectively exercise their –unconditional-right to withdraw consent: since the publication of contact details is mandatory, withdrawing consent will be subject to the registrant providing alternative contact details.