DIFC DATA PROTECTION POLICY GUIDANCE
Commissioner of Data Protection

GUIDANCE RELATING TO DATA SUBJECT CONSENT

Contents

1. Introduction 3

2. Scope 3

3. Consent as a basis for Processing Personal Data 4

4. Articles 10 and 11 - requirements for consent 4

5. Article 12 – requirements for obtaining consent 6

6. Article 12 – ongoing assessment and Single Discrete Incidents 9

7. Withdrawal of consent 10

1. Introduction

The goal of the DIFC Commissioner of Data Protection (the "Commissioner") in producing this guidance is to assist organisations subject to the DIFC Data Protection Law, Law No. 5 of 2020 (the "DPL") and the Data Protection Regulations issued pursuant to the DPL (the "Regulations") to understand the requirements behind, and the consequences of, reliance on consent as a basis for the Processing of Personal Data pursuant to Articles 10(1) and 11(a) of the DPL.

Article 12 of the DPL imposes requirements in relation to obtaining valid and lawful consent.

2. Scope

The guidance is issued by the Commissioner pursuant to Article 46(3)(h)(iii) of the DPL. In accordance with Schedule 1, Section 2(g) of the DPL, guidance issued under the DPL is indicative and non-binding.

This guidance is based on the DPL and the Regulations (collectively, "Legislation") as at 1 July, 2020 and remains current unless and until updated, withdrawn or replaced. Please visit www.difc.ae to read the full text of the Legislation.

This guidance comprises the Commissioner's interpretation of the Legislation and is issued in furtherance of the Commissioner's obligation to pursue the objectives of promoting observance of the Legislation and promoting greater awareness and public understanding of data protection and the requirements of the Legislation in the DIFC, pursuant to Article 46(2) of the DPL.

If a capitalised term is used in this guidance then it has the meaning given to it in the Legislation unless another meaning is specified.

This guidance may be updated from time to time. Readers are advised to check the DIFC website or contact the Commissioner's office for updates.

Please note that this guidance does not have the force of law and it is not intended to constitute legal advice; you should not rely on it as such. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations.

3. Consent as a basis for Processing Personal Data

3.1 Processing of Personal Data

Article 9(1)(a) of the DPL imposes various general requirements on the Processing of Personal Data, including that the Processing must be in accordance with Article 10 of the DPL.

Article 10 of the DPL provides six principal bases for Processing Personal Data which can be summarised as:

- consent
- necessary for performance of a contract
- necessary for compliance with law
- necessary to protect the vital interests of a person
- necessary in the public interest / official powers
- necessary for legitimate interests

Consent is only one of the available bases and is often one of the most contentious and difficult to manage. If a Controller can satisfy one of the other bases it is not necessary, and in certain cases, not advisable, to obtain consent.

Consent is not a prerequisite of lawful Processing under the DPL; it is one available basis on which the requirements of Article 9(1)(a) can be satisfied.

3.2 Processing of Special Categories of Personal Data

Where Special Categories of Personal Data are Processed, it is also necessary to comply with Article 11 of the DPL. Article 11 prohibits Processing of Special Categories of Personal Data unless one of the grounds in Article 11 applies (in addition to the requirements of Articles 9 and 10, which continue to apply).

Article 11(1)(a) provides that "explicit consent" is one of the grounds on which Special Categories of Personal Data can be Processed.

4. Articles 10 and 11 - requirements for consent

4.1 The wording of the DPL

Article (10)(1)(a) of the DPL (emphasis added):

> "a Data Subject has given consent, *which complies with Article 12*, to the Processing of *that* Personal Data *for the specific purposes*"

Article 11(a) of the DPL (emphasis added):

> "a Data Subject has given *explicit* consent, *that complies with Article 12*, to the Processing of *those* Special Categories of Personal Data *for one (1) or more specified purposes*"

Both Articles contain several separate requirements that must be complied with.

4.2 Compliance with Article 12

This is discussed in more detail in section 5 below.

4.3 "That / those" Personal Data

The consent which is obtained can relate only to an identified scope of Personal Data. It is up to the Controller to make the scope of the Personal Data clear to the Data Subject when the consent is obtained. For example, where the consent is obtained by the Data Subject ticking a box on a form (electronically or in paper copy) the associated wording should make it clear for what purpose or use the collection of the Personal Data is meant for and therefore what the consent relates to. **A general consent, including but not limited to consent included**

generally in contractual terms and conditions (discussed further below), to the Processing of any unspecified use or purpose for Personal Data that may be collected will not be valid.

Controllers should note the information requirement provisions of Part 5 of the DPL, which are also relevant in the context of the information to be provided to the Data Subject and the obtaining of consent during the process of Personal Data collection.

4.4 "for the specific purposes / for one (1) or more specified purposes"

The consent must relate to the purposes for which the Personal Data is to be Processed. If a Controller obtains consent to Processing a Data Subject's Personal Data for the purposes of running a competition, for example, and no further purposes are specified then the Controller may not use the consent as the basis for using the same Personal Data to carry out other activities such as direct marketing activities. Controllers must clearly specify the purposes to which the consent relates, and must be able to document and manage the secure and specific use of such Personal Data.

4.5 "explicit" consent for Processing Special Categories of Personal Data

The requirement for consent to be "explicit" is a specific condition for Processing of Special Categories of Personal Data. "Explicit" refers to the way consent is expressed by the Data Subject. "Explicit" consent must be affirmed in a clear statement of words (whether oral or written; it will generally be easier for a Controller to be able to establish consent if a written record is presented; an initial oral consent could be further supported by a follow-up email, for example). The words can be provided by the Controller and agreed to by the Data Subject (they do not need to be authored by the Data Subject or the Data Subject's own original words) but the Data Subject needs to undertake an affirmative act to clearly agree with the words (by signing or by ticking a box, for example, or saying, "I agree"). The words should refer to the Special Categories of Personal Data to be Processed and the specific purposes in question.

By contrast, consent under Article 10(1)(a) could potentially be inferred from a clear affirmative action or conduct, without an explicit statement of consent. **Consent which is inferred cannot be explicit consent**.

EXAMPLE:

A fitness club asks its members to complete a feedback form, stating that the data provided will be kept within the Controller's organisation and used solely for management purposes to make decisions relating to investment in and improvement of the club for the members.

The form contains various fields for the Data Subject to fill-in, some of which ask for Personal Data relating to the member's preferences and activities.

The form does not contain an express statement of consent or any tick-box or other mechanism for the members to give explicit consent.

By entering Personal Data in the form and submitting it to the club, the members can arguably be said to be consenting to the club's Processing of the Personal Data. Clearly there must be an expectation on the part of the Data Subject that the Personal Data provided will be Processed (otherwise there is no point gathering the submissions via the forms) and completion of the form was entirely optional and voluntary; the form was completed by a free affirmative act of the Data Subject. It may be reasonable to infer consent, and this may be sufficient for the purposes of Article 9(1)(a) and Article 10(1)(a).

By contrast, if the club asks a member to provide Personal Data relating to the member's physical condition, including medical conditions, then the club may be collecting Special Categories of Personal Data. In this case, consent cannot be inferred and the form must include an explicit statement of consent given by the Data Subject, such as: "I consent to any data relating to my health being Processed by [health club] for the purposes of making decisions relating to investment in and improvement of the club for the members", accompanied by a tick-box and signature box.

In both cases, the fitness club should also comply with the general information provision requirements of the DPL.

5. Article 12 – requirements for obtaining consent

As seen, both of Articles 10 and 11 require that any provision of consent complies with Article 12.

The material parts of Article 12 are as follows.

5.1 Consent must be "freely given" (Article 12(1))

The Data Subject must have the option not to provide consent if consent is to be valid. **If the Data Subject does not have a genuine choice or is put in a position where he is compelled to consent or to endure negative consequences otherwise then the consent will not be valid**.

> EXAMPLE:
>
> A bank provides a credit card to its customer. The bank writes to the customer telling them that it intends to increase the interest rate payable on outstanding balances to three times the current rate unless the data subject agrees to provide a comprehensive amount of Personal Data to the bank and consents to the bank selling the data to other businesses.
>
> In the Commissioner's view, consent in this context would not be freely given.

If consent is bundled-up in a set of non-negotiable terms and conditions then it is unlikely to be freely given, particularly where there is an imbalance of power and resource between the Data Subject and the Controller.

> EXAMPLE:
>
> A bank asks customers for consent to use their payment details for marketing purposes. This Processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer’s refusal to consent to this Processing purpose would lead to the denial of banking services, closure of the bank account, or an increase of the fee, in the Commissioner's view, consent cannot be freely given or revoked.

In the Commissioner's view, compliance documentation relating to the DPL’s consent requirements should be easily distinguishable and distinct from contractual terms and conditions. Note that this should not curtail the ability of a Controller to carry out normal business relationships and contracts, given that Article 10(1)(b)[1] is a potential basis for Processing the Personal Data (but not Special Categories of Personal Data), instead of consent.

> EXAMPLE:
>
> An online service provider provides the information it is required to provide to Data Subjects on its online platform but in order to access the information, the Data Subject must click through several pages of terms and conditions, including selecting relevant hyperlinks, in order to find the information. The terms and conditions operate across the entire, substantial, span of the providers services and are long and complicated, containing multiple hyperlinks to various other documents of varying relevance depending on the specific services being used.
>
> It may be hard for the Controller, in the Commissioner's view, to establish that any consent based on such information is properly informed and therefore freely given or unambiguous (see below).

In the context of an employer asking for consent from employees to perform Processing, it may be hard for the employer to establish that consent was freely given. There is typically an imbalance of power between an

[1] Article 10(1)b): "the Processing is necessary for the performance of a contract to which the a Data Subject is a party, or in order to take steps at the request of the a Data Subject prior to entering into such a contract".

employer and an employee, and an employee may feel unable to withhold consent for fear of harming their career prospects or receiving adverse treatment as a result, or fear of inferences being drawn about them. For example, if an employer wants to conduct additional monitoring of employees and requests consent to do so, then the employees in question are likely to feel pressure to give such consent, for fear of arousing suspicion or being treated less favourably if they do withhold consent.

Even where consent is being requested for less intrusive purposes, employees may feel unable to freely exercise their judgment. In addition, employers should also note the potential difficulties that could arise if consent has been relied on as a basis for processing employee data and employees subsequently decide to withdraw consent (see section 7).

In the Commissioner's opinion, consent is therefore unlikely to be a good basis for employers to rely on and may be subject to challenge.

Employers may instead consider whether "legitimate interests" under Article 10(1)(f) is a valid basis for the Processing in question, although it should be noted that this basis is not available if the data in question falls within a Special Category of Personal Data (although in such cases Article 11(1)(b), which is specifically concerned with Special Categories of Personal Data in an employment context, might apply).

EXAMPLE:

An employer has a team of people within its business which carry out travel bookings on behalf of members of staff as and when needed. There is no systematic Processing of the Personal Data of the entire employee cohort for this purpose and the system is very ad hoc, collecting data as and when needed.

The employer decides to outsource its travel booking arrangements to a third party supplier to improve efficiency and obtain cost savings. The third party supplier requires that an upload of various Personal Data relating to all employees within the scope of the booking service is provided and refreshed as necessary to take account of joiners / leavers.

The employer decides to ask all relevant staff for consent to provide the data in question to the third party supplier. Some of the staff are concerned about the outsourcing and refuse consent. Some of the staff did consent, but felt that they did not really have any choice because if they did not consent it could affect their ability to travel for their business and their prospects of being considered for important assignments.

The employer, having relied on consent, cannot provide the data of the staff who withheld consent and must therefore maintain parallel systems or give up on the outsourcing. If the employer does go ahead with the partial outsourcing, it is unlikely that the consents which were obtained are valid for the purposes of the DPL, in any case.

A better route would have been for the employer to conduct an assessment as to whether the Processing falls within the "legitimate interests" basis (no Special Categories of Personal Data are to be shared). The employer concludes that the supplier has contractually committed to provide appropriate safeguards for the Personal Data, there is no undue risk of harm to the Data Subjects, the outsourcing is in furtherance of legitimate business purposes and the results achieved by the outsourcing (efficiency and cost savings) are ultimately in the interests of the employees in question as well as the interests of the controller. Accordingly, the employer decides it does not need to request consent and can rely on legitimate interests.

[***Note***: this scenario does not address other questions that may be relevant in relation to such an outsourcing, such as whether there is a transfer of data outside the DIFC, whether the contract in question complies with the DPL etc.]

5.2 Consent must be given by a "clear affirmative act that shows an unambiguous indication of consent" (Article 12(1))

The Data Subject must undertake an act which affirmatively and unambiguously indicates consent (ticking a box, applying a signature, validating a link sent by email, confirming by a clear email, confirming orally that consent is given etc.).

Failing to un-tick a pre-ticked consent box does not, in the Commissioner's view, constitute a clear affirmative act and accordingly pre-ticked boxes should not be used to obtain consent under the DPL.

> EXAMPLE:
>
> A provider of an online service asks the Data Subject to set various preferences the first time the Data Subject logs-in to his account. The preferences include consent to the use of Personal Data for marketing purposes and the sharing of Personal Data with third parties. The default account setting is for permission to be granted, unless the Data Subject actively switches the setting.
>
> In the Commissioner's view such permissions will not constitute valid consent. The platform should incorporate privacy by default and the Data Subject should be required to switch the setting from no-consent to consent, in order for the consent to be valid (or tick a box or take a similar affirmative act).

Controllers are able to implement different and varied processes to collect consents that the Controller feels best suit the Controller's organisation. For example, a clear affirmative act could include "swiping left" on a touch-screen application or moving a device in a figure-eight motion if the application user interface is best-suited to such actions, provided that the Data Subject is clearly made aware that the act will constitute consent (and provided all other relevant aspects of the DPL are complied with). In the Commissioner's view, as a general principle, the more unorthodox or unconventional the requested action, the clearer the information relating to the consequences of the action will need to be.

Controllers should note the contents of section 5.3 below when considering the method by which consent is obtained.

5.3 Where Processing is based on consent, a Controller must be able to demonstrate that consent has been freely given (Article 12(2))

Note that this sub-Article effectively places the burden of proof of establishing valid consent on the Controller. **The Controller must be able to demonstrate that consent has been freely given**. By way of example, if the Controller has relied on an oral statement of consent (in a face-to-face scenario or over the telephone, for example) then the Controller will need to take further measures in order to be able to demonstrate that consent was freely given; for example, the Controller may keep a recording of the conversation or may subsequently send an email or SMS to the Data Subject with a link for the Data Subject to click to reconfirm consent. Similarly, if a Controller obtains consent in written form then for as long as the Controller is undertaking the Processing that the consent relates to, the Controller should ensure that the written consent is kept on file.

5.4 If the Processing is intended to cover multiple purposes, consent must be obtained for each purpose in a manner that is clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language (Article 12(3))

This sub-Article is effectively a further elaboration on the elements of Articles 10(1)(a) and 11(1)(a) which require that the consent relates to specific purposes.

The principle is that the broader the purposes the consent is sought for, the more granular the consent needs to be and the Data Subject should be able to consent to some purposes, but not other purposes, if the purposes are not necessarily inter-linked. For example, a consent to use data for marketing purposes should not be bundled with a consent to use data for research purposes or to improve the service offering of the Controller; each should be a separate consent and the Data Subject should be provided with clear and sufficient information to assess each consent request.

5.5 If a Controller seeks to obtain consent for one (1) or more other matters not expressly concerned with the Processing of Personal Data, the request for consent for the Processing of Personal Data must be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language (Article 12(4))

Again, this sub-Article is reinforcing the need to keep consent for Processing of Personal Data for specified purposes clear and distinct from any wider consent that is being requested.

6. Article 12 – ongoing assessment and Single Discrete Incidents

Consent should not be presumed to last indefinitely. A Controller needs to evaluate what period the Data Subject would objectively have reasonably expected to be covered by the consent given and implement appropriate and proportionate measures to assess the ongoing validity of the consent (Article 12(6)).

In the Commissioner's view it is not helpful to try to set out specific "shelf-lives" for consents or specific measures that must be taken as these will be context-specific, with reference to the volume and nature of Personal Data concerned, the nature of the Processing in question and the resources available to the Controller.

By way of example, if a Controller is using consent as a basis to send marketing emails with clickable links to promotional offers and has analytics tools deployed which record whether or not the recipient clicks on the links, then it may be reasonable to rely on consent given by a Data Subject which regularly clicks on the links for a longer period than the consent given by a Data Subject which very rarely or never clicks on a link.

Controllers should note that under Article 12(9) the Controller must be able to demonstrate that appropriate methods and procedures are in place to manage the recording, withdrawal and periodic evaluation of consent.

If the assessment determines that the Data Subject would no longer reasonably expect the Processing to continue then the Controller must, if it wishes to continue Processing the Personal Data in question, contact the Data Subject and obtain renewed consent (unless another basis for Processing the Personal Data applies), in accordance with Article 12(7). Such request for renewed consent must comply with all the requirements for valid consent. If the Data Subject does not reaffirm consent within a reasonable period then consent shall be deemed to be withdrawn, in accordance with Article 12(8).

An exception to the requirement to assess the ongoing validity of consent is where the consent relates to a Single Discrete Incident, which is defined as:

> *"a Processing operation or a collection of Processing operations that relates to a:*
>
> *(a) a single, non-recurring transaction; or*
>
> *(b) a non-recurring and clearly defined purpose that the a Data Subject is seeking to achieve,*
>
> *in each case, with a definable end point."*
>
> \- *Article 12(11), DPL*

Where consent relates to a Single Discrete Incident (and provided that sufficient information has been provided such that the Data Subject is aware of the Single Discrete Incident and its likely duration), then the consent is presumed valid for the duration of the Single Discrete Incident unless the Data Subject exercises his right to withdraw consent.

EXAMPLE:

A Data Subject agrees to install a tracking device in their motor vehicle which sends information in relation to their motoring habits and practices to their vehicle insurer. In return, the insurer offers a cheaper premium to the Data Subject. If the insurer Processes this Personal Data on the basis of consent then it is reasonable for the insurer to view the consent as being valid for the term of the policy and to treat it as a Single Discrete Incident. [2]

[2] If the data is being Processed solely for the administration of the insurance contract then the insurer might prefer to rely on Article 10(1)(b). If it is a term of the contract that the tracking device is installed and the data is provided to the insurer then clearly the Processing of the Personal Data is necessary for the performance of the contract. If, however, the insurer is also using the Personal Data for broader purposes (further analysis, marketing etc.) then such use is unlikely to be necessary for the performance of the contract, and consent or another alternative lawful basis may be needed.

7. Withdrawal of consent

7.1 Process and requirements

Controllers should be aware that Data Subjects have a right to withdraw consent. This right is set out in Article 32 of the DPL.

Article 12(5) of the DPL requires Controllers to inform the Data Subject of the right and how to exercise it at the time the consent is obtained. This principle is further enforced by Articles 29(h)(iii) and 30(g)(iv) which require the information to be included within the scope of the general information provision requirements (where consent is the basis for Processing).

Article 12(5) also provides that withdrawing consent should not require undue effort on the part of the Data Subject and should be at least as easy as the process of giving consent.

Article 40 contains requirements in relation to the methods by which Data Subjects may exercise their rights (not just limited to the right to withdraw consent). A Controller must make available a minimum of two (2) methods, which shall not be onerous, by which a Data Subjects can contact the Controller to request to exercise his rights. If the Controller maintains a website, at least one (1) method of contact shall be available without charge via the website, without the need to submit data to create an account of any sort. At least one of the methods should correspond to the contact details provided under the information requirements of Article 29 or Article 30, as applicable.

7.2 Implications

Data Subjects are free to withdraw consent at any time. This means that there is no guarantee that any ongoing Processing based on consent will remain lawful for any specific time period (because the Data Subject may withdraw consent).

Controllers will want to carefully consider if any of the other bases for Processing Personal Data apply. **Controllers should avoid an approach where consent is used but another basis for Processing is relied on as a "back-up", or vice versa, as this makes the information provided to Data Subjects unclear and makes the exercise of Data Subject rights more complicated**. Being mindful of the above, this is why it is important for Controllers to identify the different types of Processing operations that Personal Data undergoes and why Controllers should seek to avoid an overly broad-brush approach to providing information to the Data Subject. It is quite likely that in many business interactions with Data Subjects a large amount of the business-as-usual Processing of Personal Data may fall within the bases related to the performance of a contract. It would be counterproductive for the Controller to tell the Data Subject that such Personal Data is Processed on the basis of consent. Where Personal Data is to be used for purposes not necessary for the performance of the contract the Controller may wish to consider if it can rely on the legitimate interests basis in Article 10(1)(f)[3]. If neither the "contract basis" nor the "legitimate interests basis" applies, or there is a specific legal requirement for consent, the Controller may then wish to consider consent as a basis (or, indeed, one of the other bases, if relevant).

Upon receipt of a valid request to withdraw consent the Controller should take steps as soon as reasonably practicable to cease the Processing of that Personal Data in question, including ensuring that any Processors which are engaged are also bound to take such steps. The Commissioner recognises that it may not be possible for practical reasons to instantly cease all Processing of Personal Data. For example, if a Data Subject withdraws consent to receive marketing communications then there will need to be a business process carried out to remove the relevant data from the marketing system in question which may, itself, involve the Processing of such Personal Data. Further, withdrawal of consent does not imply that the Controller must erase all Personal Data relating to the Data Subject where there is a legitimate and lawful reason to retain it. For example, consent for Personal Data to be used in future research projects may be withdrawn but the Controller is

[3] Note that this basis is not available in connection with the Processing of Special Categories of Personal Data.

not compelled to revisit research datasets for previous projects and purge the Data Subject's data if it is not feasible or proportionate to do so.

Article 12(5) of the DPL makes it clear that withdrawal of consent does not affect the lawfulness of Processing carried out before the time date of withdrawal.

7.3 Article 29(1)(g)(ix) – derogations from the exercise of Data Subject rights

Article 29(1)(g)(ix) of the DPL has been introduced to provide some flexibility for Controllers which wish to benefit from technical innovations which, at first glance, are less compatible with the exercise of Data Subject rights than some traditional methods of Processing. As an example, blockchains are often said to be immutable. Where Personal Data is stored on a blockchain it is therefore hard to reconcile the tension between the immutable characteristic of a blockchain and the right of a Data Subject to have Personal Data erased when the original purpose of the Processing has been exhausted.

The DIFC is a cutting-edge financial centre and wants to ensure that Data Subject rights are balanced against the legitimate business needs of its community, which needs include the prudent adoption of new technical methods. If the Controller complies with enhanced information provision requirements under Article 29(1)(g)(ix) and satisfies itself that the Data Subject understands the restrictions involved, then the controller can refuse certain Data Subject requests to exercise rights in accordance with Article 33(4) of the DPL.

Controllers must note that the right to withdraw consent is not one of the Data Subject rights which can be compromised in accordance with Article 33(4). Accordingly, it is not appropriate to rely on consent as a basis to Process Personal Data if such Processing will be conducted in a way which is incompatible with the possible withdrawal of such consent.

Conclusion and Key Take-aways:

- Consent is not required for all Processing, and is often the most complex approach to Personal Data collection and Processing management.
- Consent is not a prerequisite of lawful Processing under the DPL, it is one available basis on which the requirements of Article 9(1)(a) can be satisfied.
- A general consent, including but not limited to consent included generally in contractual terms and conditions, to the Processing of any unspecified use or purpose for Personal Data that may be collected will not be valid.
- Consent which is inferred cannot be explicit consent.
- If the Data Subject does not have a genuine choice or is put in a position where he is compelled to consent or to endure negative consequences otherwise then the consent will not be valid.
- Consent is unlikely to be a good basis for employers to rely on and may be subject to challenge.
- Failing to un-tick a pre-ticked consent box does not, in the Commissioner's view, constitute a clear affirmative act and accordingly pre-ticked boxes should not be used to obtain consent under the DPL.
- The Controller must be able to demonstrate that consent has been freely given.
- Consent should not be presumed to last indefinitely.
- Where consent relates to a Single Discrete Incident (and provided that sufficient information has been provided such that the Data Subject is aware of the Single Discrete Incident and its likely duration), then the consent is presumed valid for the duration of the Single Discrete Incident unless the Data Subject exercises his right to withdraw consent.
- Controllers should avoid an approach where consent is used but another basis for Processing is relied on as a "back-up", or vice versa, as this makes the information provided to Data Subjects unclear and makes the exercise of Data Subject rights more complicated.
- Upon receipt of a valid request to withdraw consent the Controller should take steps as soon as reasonably practicable to cease the Processing of that Personal Data in question, including ensuring that any Processors which are engaged are also bound to take such steps.