DECISION NOTICE 1 of 2022

Declaration of Contravention of Data Protection Law, DIFC Law No. 5 of 2020 (DIFC DPL)

Issued: **26 September 2022**

[REDACTED]

Executive Summary:

A. Complainant received an email from FTI Consulting for a data protection information event. It was sent to his personal email address. He had never before contacted or shared this address with FTI through their website or other means. It was collected by FTI through an upload from a new joiner, FTI 1, who was hired [redacted – in January 2021]. Complainant is also a data protection professional, and felt that the collection and use of his personal (or potentially any email address of his) in this manner and for this purpose contravened the DIFC DP Law.

B. As such, Complainant contacted FTI Consulting on March 30, 2021, as follows:

MARCH 30 Email / SAR 1

---------- Forwarded message ---------
From: ***Complainant***
Date: Tue, 30 Mar 2021, 15:18
Subject: Re: Webinar Invitation: Navigating Data Privacy in the ADGM and DIFC
To: <info@fticonsulting.com>

Hi,

I never consented to using my email for marketing purposes.

I am exercising my right to have access to my data, who my information was shared with and how evidence of obtaining my consent.

C. In short, Complainant submitted a subject access request at this time. This SAR was never responded to, as apparently the FTI info@ email address is not monitored. Complainant states that he never got a bounce back to let him know, but it appears that now a bounce back email is provided stating that the address is not monitored.

D. When the March 30, 2021, SAR was not responded to, he followed up and eventually submitted both a complaint to the Commissioner and a SAR to FTI, copying the FTI contact he had connected with via Linked In but prior to the contact joining FTI. The exchange is as follows:

DECEMBER 5 Email thread:

From: *Complainant*
Sent: *05 December 2021 09:07*
To: *Info <info@fticonsulting.com>; commissioner@dp.difc.ae; FTI 1*
Subject: *[EXTERNAL] FW: Webinar Invitation: Navigating Data Privacy in the ADGM and DIFC*

Dear Commissioner,

I never consented to my information to be used for marketing purposes and despite me challenging FTI, I have received no response. 3 times I emailed asking how they got my details, my right to exercise deletion of my details and evidence that I provided explicit consent. To date I have received at least 10 emails from the organization.

I now wish to raise an official complaint against FTI Consulting, the irony is that this organization provide data protection advisory services to clients!!!!!

For your kind action and confirmation of next steps.

From: *FTI 1*
Sent: *Sunday, December 5, 2021 9:02 AM*
To: *Complainant; Info <info@fticonsulting.com>; commissioner@dp.difc.ae*
Subject: *RE: Webinar Invitation: Navigating Data Privacy in the ADGM and DIFC*

Dear Complainant,

I apologise for your details having erroneously been entered into our systems. I will ensure that you are removed from all of our marketing lists and, as requested, remove your data from our systems.

Regards,

FTI 1

From: *Complainant*
Sent: *Sunday, 5 December 2021 10:23 AM*
To: *FTI 1; Info <info@fticonsulting.com>; DIFC DP Commissioner <commissioner@dp.difc.ae>*
Subject: *RE: Webinar Invitation: Navigating Data Privacy in the ADGM and DIFC*

Dear FTI 1,

I would like to know how my details were obtained in the first place, it is worrying you have a system where details are being entered erroneously.

From: *DIFC DP Commissioner*
Sent: *Monday, 6 December 2021 9:09 AM*
To: *Complainant; FTI 1; Info <info@fticonsulting.com>*
Subject: *RE: Webinar Invitation: Navigating Data Privacy in the ADGM and DIFC*

Dear Complainant, thank you for your email.

I note the complaint you've raised and that FTI have stated they will remove your data. I ask that they do so immediately, and to please provide you with an explanation as to how it was obtained as soon as possible, no longer than within the time frame requirements of the DP Law 2020.

[end of email]

E. At this point, FTI 1 confirmed that the data had been removed from the FTI contacts database, but did not consider the December 5 email from Complainant or the instructions from the Commissioner's Office to be a SAR, so no subject access information was provided until February 22, 2022, which is beyond the 30 days response requirement as set out in Article 33 of the DPL. The investigation commenced formally at this point upon the request of Complainant, the data subject.

Issues Investigated and Brief Summary

Issue 1 - Direct Marketing / Legitimate Interests:

1. **Who connected with whom, when and for what purposes / in what context (if known / recalled)?** Complainant connected with FTI 1

2. **Had Complainant and FTI any previous connection such that any appropriate processing notice or other "opt in / out" option might apply?** It appears that Complainant's information only entered the FTI CRM systems when FTI 1 joined in or around January 2021.

3. **What factors or particulars, when considered as part of relevant legal assessments such as purpose, necessity and balancing tests, about the Linked In relationship or any other relationship indicators led FTI 1 / FTI to the conclusion that Complainant should be considered a prospective client or contact?**

   This was determined considering Complainant and FTI 1's relationship via Linked In and an interpretation of laws and policies governing this type of processing. However, the filtering exercise should have also considered the applicable portions of the DIFC DPL and other applicable laws and regulations, as well as the relevant tests required to ascertain the value of FTI 1's assessment as it applied to FTI's use of Complainant's personal data. FTI's policies should reflect these factors as well, going forward.

4. **Would uploading Complainant's contact details in this manner (after the conclusion of the filtering exercise) provide Complainant with appropriate notice or the opportunity to consent, opt in, etc., regarding FTI's collection and processing purposes or interests?** No

5. **Was it reasonable, as an outcome of the filtering exercise, to upload Complainant's information from Linked In, or specifically, to upload his personal email address instead of the business address (also available on Linked In) to the FTI CRM systems on the legitimate interests basis generally, or as it relates to marketing and electronic communications (e-comms)?** No, with respect to notice and accountability requirements of DIFC DP Law, or in accordance with FTI social media policy (based on applicable data protection laws) and parties' relationship.

6. **Was the legitimate interests basis, as set out in Article 10(f) of the DIFC DPL, in this case for the purpose of sending marketing to any email address, and specifically, Complainant's personal data, the most appropriate basis?** No

7. **Is there a contravention of the DIFC DP Law regarding the obligations of a Controller to provide information about a data subjects rights, use of personal data for direct marketing, and on what lawful basis it was being processed per Articles 30 and 34?** Yes

8. **Is there sufficient evidence to support a finding of contravention of Article 10(f) of the DIFC DP Law based on the filtering exercise conducted against the legitimate interests basis for processing Complainant's personal data?** Yes

Issue 2 - The SARs:

9. **Was a valid subject access request (SAR) made either on March 30, 2021, or December 5, 2021?** Yes, on both dates

10. **Is the use of the info@ email address for the March 30 request reasonable?** Possibly not, as if the email is not monitored and a privacy policy exists that contains an email address to which they should be sent, Complainant (as a privacy professional in Qatar working for an EU organisation) could have simply checked that. However, it is not necessarily unreasonable to send an email to an info@ address. Giving Complainant the benefit of the doubt, he said that he did not get a bounce back like the one received on June 21, 2022, by the Commissioner's Office, so had no reason to believe it was not a valid email address to contact.

11. **In accordance with Article 40, were 2 methods provided anywhere and easily accessible?** No, but data subject may not have read the privacy policy / had proper notice anyway.

12. **What did FTI understand the Commissioner's instructions to be? Why no response to SAR provided?** FTI 2 (note: manager of investigation) stipulated that FTI 1 did not acknowledge or understand the access portion of the request, only the deletion portion of the request, despite follow up.

13. **Is there a contravention of Article 33 of the DIFC DP Law regarding the response (or lack thereof) to the December 5, 2021, SAR?** Yes.

Ancillary Issues

14. **When and in what manner was FTI 1 trained on FTI policies?** June 2021, after joining in Jan 2021 and completing the filtering exercise for uploading contacts to the FTI CRM. As such, may not have been aware of the FTI policies relevant to this issue, but as a privacy consultant, presumably should have made a more informed, nuanced decision.

15. **Is there any documentation to support the assessment that marketing based on legitimate interests is a sufficient, valid basis for such processing? Was a DPIA done?** No DPIA, primarily trust in employee's judgement based on reading of the relevant policies and assessment criteria.

16. **Is it excusable that the initial SAR of March 30, 2021, sent to a dormant email address was missed?** Debatable, given the data subject's position as a privacy professional and the origination address of the event email.

TIMELINE
Complainant and FTI 1 were Linked In contacts; Complainant's personal email address was his Linked In contact information
March 30, 2021: Complainant received marketing email regarding upcoming webinar – SAR 1 is sent to info@fticonsulting.com but apparently not received as that mailbox "is not monitored".
Complainant makes first request to remove data / unsubscribe and to access personal information that FTI processes by sending request to info@fticonsulting.com No response, no acknowledgement
December 5, 2021: Commissioner's Office receives complaint, 2nd SAR and request to remove data. Commissioner's Office responds instructing removal of data and to respond to SAR within time frame. Commissioner's Office checks in with FTI to confirm message has been received and appropriate action taken. Only response to request to remove is provided but no acknowledgement of SAR and no response provided.
Investigation begins, discussions with FTI and Complainant, and then final response to SAR provided

Issues and Findings

Issue 1 - Direct Marketing / Legitimate Interests:

---

1 Who connected with whom, when and for what purposes / in what context (if known / recalled)?

1.1 This was not fully answered. It is known however that FTI 1 and Complainant were connected prior to FTI 1 joining FTI.

2 Had Complainant and FTI any previous connection such that any appropriate processing notice or other "opt in / out" option might apply?

2.1 It appears that Complainant's information only entered the FTI systems when FTI 1 joined in or around January 2021.

3 What factors or particulars, when considered as part of relevant legal assessments such as purpose, necessity and balancing tests, about the Linked In relationship or any other relationship indicators led FTI 1 / FTI to the conclusion that Complainant should be considered a prospective client or contact?

3.1 The existing Linked In relationship appears to be the basis for the assertion that legitimate interests was a lawful basis on which to add Complainant's information to the FTI CRM.

Supporting evidence

FTI 2 stated the following in an initial response to questions from the Commissioner's Office:

> *Prior to uploading the data, FTI 1 confirmed that he had carried out a filtering exercise of his LinkedIn contacts and then provided to the local Dubai CRM team to action, a spreadsheet setting out the relevant data of contacts who were limited to (1) individuals known to be in the GCC region; and (2) individuals out with the GCC region but who were reasonably determined by FTI 1 to likely to want to benefit from the services being carried out by FTI 1 within FTI.*

3.2 Complainant confirmed that he and FTI 1 were connected via Linked In, but no client relationship existed, and there was no further contact of any substance. Complainant is a privacy professional that was working in Qatar.

4 Would uploading Complainant's contact details in this manner (after the conclusion of the filtering exercise) provide Complainant with appropriate notice or the opportunity to consent, opt in, etc., regarding FTI's collection and processing purposes or interests?

Finding 1: In this case, because his information came from a) another platform entirely (i.e., not from visiting the FTI website or providing his information to FTI directly), and b) through contact made *before FTI 1 even joined FTI*, Complainant did not receive an appropriate privacy notice containing information about his rights or any other options to determine electronic or other communication preferences from FTI. He did not know until he received the webinar email nor should he have known that his contact details were being processed by FTI based on FTI 1's judgment that he was a "prospective client". He did not have the opportunity to consent, opt-in or out, or to utilize the FTI Preference Center, which is something FTI website users would (or should) have had, had FTI collected his information directly.

Reasoning

4.1 The DIFC DPL does not specifically address the same level of detail that applicable EU and UK e-privacy in electronic communications laws set out. This is granted. However, it does refer to notice requirements if personal data, when not collected from a data subject, is to be processed, in Articles 30 and 34.

4.2 Article 30(1) lists a slew of information that must be provided to a data subject if they have indirectly collected his or her personal data, specifically the purpose of the processing and associated lawful basis, as well as to share specific circumstances for which it will be processed, to ensure fair and transparent processing, including:

> *(ii) if the Controller's lawful basis for the Processing is legitimate interests or compliance with any Applicable Law to which the Controller is subject, the Controller shall state clearly what those legitimate interests or compliance obligations are;*
>
> *(iii) notice of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;*

4.3 Article 30(2)(b) states that this information must be provided if the personal data is to be used for communicating with the data subject, no later than the first communication. Noting the exception in Article 30(3)(b) to the applicability of Article 30(1), it is reasonable to conclude that providing such email or other introductory notice when new contacts shared by a new employee are uploaded to the FTI CRM would not be s impossible or would involve a disproportionate effort.

4.4 Articles 34(1)(b) and (c) of the DIFC DPL state that

> *A Data Subject has the right to… be informed before Personal Data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses, subject to any provision of this Law that does not permit disclosure and… where Personal Data is Processed for direct marketing purposes, object at any time to such Processing, including Profiling to the extent that it is related to such direct marketing…*

4.5 Generally, as FTI are a global organization, it is fair to note as well that EU and UK privacy laws and e-privacy and electronic communications (PEC) regulations also apply, such as the relevant versions of the GDPR and e-Privacy Directive / PECR.

4.6 Given all of the above, relevant guidance around the appropriate basis for processing personal data for electronic communications purposes, including direct marketing, makes it clear that legitimate interests may be used as a lawful basis for such processing but in limited circumstances, having passed specific purpose, necessity and balancing tests.

4.7 The DIFC Commissioner's Office provides direct marketing and e-comms guidance[1], addressing consent / opt-in options, soft opt-in and indirect consent. In each case, it is clear in the Commissioner's guidance that use of personal data via any of those means should not be relied on. Soft opt-in guidance specifically states, "Do not use Soft Opt-in as a basis for sending electronic marketing if it is to be used by any third party other than the original collecting organization." Arguably, use of Complainant's data in this manner and even prior to this, uploading it on the basis of the Linked In relationship, being in the GCC and maybe wanting to hear about privacy related topics is not fair or lawful. It may be fair for FTI 1 to get in touch directly, but not for FTI to send a general e-comm on the tangential basis that FTI 1 now happens to work for them and therefore his contacts are now their contacts.

4.8 Further, as supporting guidance, the UK Information Commissioner's Office (ICO) sets out a clear three part test for making such determinations, assessing the purpose of the marketing or e-comms, necessity and balancing considerations to respect the data subject's rights vs those of the controller.[2]

4.9 The ICO guidance states the following:

> *In terms of the purpose test, **some forms of marketing may not be legitimate if they do not comply with other legal or ethical standards** or with industry codes of practice. However, as long as the marketing is carried out in compliance with e-privacy laws and other legal and industry standards, in most cases it is likely that direct marketing is a legitimate interest.*

[1] DIFC Commissioner's Guidance on Direct Marketing and Electronic Communications
[2] ICO Guidance on Legitimate Interests as a Lawful Basis for Direct Marketing

However this does not automatically mean that all processing for marketing purposes is lawful on this basis. You still need to show that your processing passes the necessity and balancing tests.

You may also need to be more specific about your purposes for some elements of your processing in order to show that processing is necessary and to weigh the benefits in the balancing test. For example, if you use profiling to target your marketing.

***It is sometimes suggested that marketing is in the interests of individuals**, for example if they receive money-off products or offers that are directly relevant to their needs. This is unlikely however to add much weight to your balancing test, and we recommend you focus primarily on your own interests and avoid undue focus on presumed benefits to customers unless you have very clear evidence of their preferences.*

In some cases marketing has the potential to have a significant negative effect on the individual, depending on their personal circumstances. For example, someone known or likely to be in financial difficulties who is regularly targeted with marketing for high interest loans may sign up for these offers and potentially incur further debt.

When looking at the balancing test, you should also consider factors such as:

- ***whether people would expect you to use their details in this way;***
- ***the potential nuisance factor of unwanted marketing messages;** and*
- *the effect your chosen method and frequency of communication might have on more vulnerable individuals.*

Given that individuals have the absolute right to object to direct marketing** [under Article 21(2) of the UK GPDR], **it is more difficult to pass the balancing test if you do not give individuals a clear option to opt out of direct marketing when you initially collect their details (or in your first communication, if the data was not collected directly from the individual). The lack of any proactive opportunity to opt out in advance would arguably contribute to a loss of control over their data and act as an unnecessary barrier to exercising their data protection rights.

[emphasis added above]

4.10 In this instance, FTI had an obligation to give fair notice to Complainant that they were processing his data for the purposes of communicating with him. They did not do so, and confirmed that they did not send a "consent" email or the opportunity to utilize the FTI Preference Center[3] to set his communications preferences. In fairness, FTI's privacy notice sets out certain elements of these obligations to a data subject who may be a potential client, but Complainant had no reason to believe or know that his data was even in the possession of FTI and logically would not have reviewed the FTI online privacy policy.

[3] FTI Consulting Preference Center- this website does not, as of June 30, 2022, contain a link to the FTI privacy policy. Please see screen shot in Annex 1 below.

4.11 In addition, FTI's own Direct Marketing Policy states:

> *Your connections on LinkedIn and followers on other social media platforms can be added to Salesforce **with a relationship map** to represent how well you know them. Simply being connected via social media is not sufficient to justify sending direct marketing email communications, **you will still need evidence of your relationship or consent from the contact**. **Links to the Preference Centre can be posted on social media to invite your connections/followers to sign-up.***

4.12 Complainant has confirmed, and FTI 2 has corroborated, that he did not have any such notice or opportunity to set preferences, provide consent, etc.

4.13 Particularly, as with any privacy notices that contribute to the concept of legitimate interests and in accordance with the guidance documents cited above, the organization doing the marketing should consider what the data subject recipient should expect.

4.14 The UK Direct Marketing Association guidance states:

> *Under legitimate interests, it's necessary for organisations to communicate to the data subject the type of processing that is taking place. For example, a charity informs new donors during its website registration process that their personal details will be used to send them postal direct marketing with fundraising messages. The charity offers a clear opt-out at this stage and comprehensively explains how people's personal data may be used.*

4.15 Complainant was not afforded any of the above notice or opt out options as, again, he had no reason to seek them out.

Supporting Evidence

<u>Then-existing FTI online privacy policy of Jan 2021 [excerpt]</u>

When do we collect personal information?

We collect information about you if:

- *you use this (or any other FTI Consulting) website;*
- *you enquire about, or engage FTI Consulting to provide, its Services (either in a personal capacity, or as a representative for your employer or client);*
- *the use of your personal information is reasonably necessary to provide our Services (in these circumstances, your personal information may be disclosed to us by our client who may, for example, be your employer or service provider, or we may obtain your personal information from a range of public or subscription sources, directly from you, or from your associates or persons known to you);*
- *you apply for a position with FTI Consulting;*
- *you attend an FTI Consulting hosted or sponsored event or webinar;*

- *you invest in FTI Consulting stock (please see our investor site [link] for more information); or*
- *you contact us with any other enquiry, complaint or notice.*

What is our legal basis for collecting personal information?

(bullet point 3): the processing is in our legitimate interests, subject to due consideration for your interests and fundamental rights (this is the basis we rely upon for the majority of the processing of personal information in connection with the provision of our Services, and also for the purposes of most client on-boarding, administration and relationship management activities).

In limited circumstances, we will use your consent as the basis for processing your personal information, for example, where we are required by applicable law to obtain your prior consent in order to send you marketing communications.

5 Was it reasonable, as an outcome of the filtering exercise, to upload Complainant's information from Linked In, or specifically, to upload his personal email address instead of the business address (also available on Linked In) to the FTI systems on the legitimate interests basis generally, or as it relates to marketing and electronic communications (e-comms)

Finding 2: FTI 1 and Complainant were connected on Linked In prior to FTI 1 joining FTI, but to assert that on this basis alone, with no evident further interaction, that Complainant was a "potential client" for FTI is flawed. To then include his personal email address as the uploaded contact rather than the business email address further aggravates the argument that business contacts were evaluated and uploaded, particularly on the basis of legitimate interests, whether generally applied or applied in the context of obligations to notify Complainant of the purposes for which processing will occur.

Reasoning

5.1 FTI's own Direct Marketing Policy states:

> *Your connections on LinkedIn and followers on other social media platforms can be added to Salesforce **with a relationship map** to represent how well you know them. **Simply being connected via social media is not sufficient to justify sending direct marketing email communications**, you will still need evidence of your relationship or consent from the contact. Links to the Preference Centre can be posted on social media to invite your connections/followers to sign-up.*

5.2 The feedback (below) from FTI 2 regarding the FTI filtering process has relevance here, as the final assessment was not checked when FTI 1 completed it and provided the contact information to the FTI CRM. FTI 1 was free to use his sole judgement in the end, based on the above process guidelines.[4] When the filtering exercise was complete, Complainant's personal email address, rather than even his business email address, was uploaded to the CRM. While both types of email

[4] Checks and balances on the proper functioning of these polices may be necessary, which appear to be underway by enlisting the services of legal experts to create a more robust process, as confirmed by FTI DF.

addresses are personal data under the DIFC and most data protection laws, for direct marketing purposes, a more appropriate contact detail to upload would have been a business email address. Even if relevant legal and ethical standards had been complied with, and assuming it was fair and lawful for FTI to process Complainant's personal data, he could not have reasonably expected that his personal email address would be shared with FTI via FTI 1's Linked In connection with him.

5.3 Further, as noted above, FTI 2 confirmed that no "consent" email was sent, nor was any direction or notice given regarding the preference center or other rights after it was determined that Complainant was a "potential client".

5.4 Incidentally, it was confirmed by the Commissioner's Office that FTI 1 was trained on the data protection related policies mentioned, but only in June 2021, after the contacts filtering took place and the damage done. It is unclear whether the Social Media Policy and filtering process was part of that training. It is safe to assume so but the Commissioner's Office is open to further clarification or confirmation of this.

Supporting evidence

Email 26 May 2022, from FTI 2

FTI 1 provided an excel list to CRM/marketing and the list was uploaded from there. We acknowledge that there was no specific review of FTI 1's filtering or score decision making process however we believe that the policies in place provide the relevant guidance for individuals to be able to filter appropriately and view has been that it is then reasonable to rely on appropriate judgement subsequently being exercised by our employees to make such determinations of individuals that could be potential clients.

We acknowledge that no additional 'consent' email was sent to Complainant following this filtering exercise and in this regard, we note that we have engaged third party law firm [content removed] to assist us with a review of our process/enforcement of process in EMEA and steps we should be taking in respective jurisdictions before an individual receives any communications/invites.

[from initial FTI response, referred to in this email] Prior to uploading the data, FTI 1 confirmed that he had carried out a filtering exercise of his LinkedIn contacts and then provided to the local Dubai CRM team to action, a spreadsheet setting out the relevant data of contacts who were limited to (1) individuals known to be in the GCC region; and (2) individuals out with the GCC region but who were reasonably determined by FTI 1 to likely to want to benefit from the services being carried out by FTI 1 within FTI.

The "filtering exercise" was effectively a broad assessment in which FTI 1 determined that the filters were the two criteria identified [above][5]. Then from this subset, in addition he did not upload any personal or other business contacts in professions not linked with services FTI 1 provides (i.e., any recruitment individuals or former colleagues who had simply added FTI 1 as a contact for purpose of expanding contacts, or otherwise who were not really interested in data privacy matters).

FTI 1 was confirmed as the relationship holder for all contacts provided by FTI 1 and which were uploaded. A relationship score of '4' (which is 'Strong Relationship and/or social relationship') was

[5] Wording revised slightly as highlighting originally mentioned is not included in this decision. Original email is available upon request.

allocated by FTI 1 to all individuals included in the file provided to the CRM team for uploading (and the additional piece of information noted in the upload file to support the relationship score was 'Existing Contact').

Email 27 February 2022, from Complainant

a. *My query is do you have a legitimate interest assessment complete for marketing in this manner since you are using legitimate interest as the lawful basis for processing this information, how else would you balance the rights of a data subject and proportionality etc.*

b. *My point here is being missed. My LinkedIn contacts have visibility to see my business email address. FTI used my personal login email address, this is why I raised the DSAR in the first place. I totally appreciate companies have to market and try expand their outreach, but the frustration is my business email address is already available. It is not reasonable to expect login details are business emails, this is because most individuals change jobs/ profession and therefore would have to update their personal login each time they change jobs. We all know this is not the case, individuals majority of the times sign up and use their personal logins so to assume it is strictly B2B is incorrect.*

c. *Based on (b) a proper filtering exercise was not conducted by FTI 1 otherwise he would have used my business details*

6 Was the legitimate interests basis, as set out in Article 10(f) of the DIFC DPL, in this case for the purpose of sending marketing to any email address, and specifically, Complainant's personal data, the most appropriate basis?

Finding 3: The legitimate interests basis was not an appropriate basis for FTI's actions.

Reasoning

6.1 Based on the information obtained through the complaint and subsequent information, as set out above, legitimate interests, a lawful processing basis set out in Article 10(f) of the DIFC DPL, was not the most appropriate basis for FTI to process Complainant's information in this manner, or at all. No notice was given that Complainant's information was collected or processed in this manner, and no valid determination of whether FTI's interests were overridden Complainant's.

7 Is there a contravention of the DIFC DP Law regarding the obligations of a Controller to provide information about a data subjects rights, use of personal data for direct marketing, and on what lawful basis it was being processed per Articles 30 and 34?

Yes.

Reasoning

7.1 Apart from the possibility that he could have received a Linked In notification that FTI 1 joined FTI, Complainant would have had no reason to know FTI 1 joined FTI or that FTI 1 conducted a filtering process that would lead to FTI collecting his (personal) email address for marketing and electronic communications purposes based on legitimate interests. Only FTI 1 would have reasonably known. Again, in accordance with the FTI Social Media policy, a connection via social media without more of a relationship is not sufficient to pass a contact through the filtering process.

Supporting evidence

Email 26 May 2022, from FTI 2

In summary FTI 1's view was that as LinkedIn is primarily a business platform and that given the individual's job/role, it was considered reasonable to believe that the individual had connected with FTI 1 to understand FTI 1's insights into data privacy matters and therefore as FTI 1 had carried out a filtering exercise to narrow his contacts to such group of individuals who were connected with FTI 1 in LinkedIn for this reason, it was considered a reasonable basis to determine that he was a prospective client and therefore a legitimate interest basis for processing.

8 Is there sufficient evidence to support a finding of contravention of Article 10(f) of the DIFC DP Law based on the filtering exercise conducted against the legitimate interests basis for processing Complainant's personal data?

8.1 **Yes**. The use of the legitimate interests basis was misapplied in the course of the relationship assessment and to the conclusion that it was a lawful basis to upload a Linked In contact's (personal email) information. Clearly in this instance FTI's interests are overridden by the interests or rights of Complainant, which much be assessed as per Article 10(f) in order to validly support legitimate interests as a fair and lawful basis for processing. Also, this determination was not made properly as required by Articles 30 and 34, because Complainant was not effectively afforded access to such information or rights at the point that FTI obtained and subsequently used his personal data via the upload to the CRM.

Issue 2 - The SARs:

9 Was a valid subject access request (SAR) made either on March 30, 2021, or December 5, 2021?

Finding 4: Yes, the December 5, 2021 email from Complainant to FTI and follow up communications were valid access requests under Article 33(1) and (2), and, arguably so is the March 30, 2021, email to FTI.

Reasoning

9.1 The Commissioner's current and then-existing guidance on individual rights has relevance, as a subject access request may be made in any manner an at any time, for arguably almost any reason.[6]

10 Is the use of the info@ email address for the March 30 request reasonable?

Finding 5: Whether Complainant should or shouldn't have used the info@fticonsulting.com email address is not the main issue, as he in fact made a subject access request in December 2021 that also was not responded to properly, despite instructions from and follow up by the DIFC Commissioner's Office as well. The relevant information requested on December 5, 2021, was not actually provided until February 24 / confirmed March 31, 2022

Reasoning

10.1 Google search results conducted when this complaint was lodged and general knowledge suggests that it would be fair to write to an info@ email address for this type of business.[7] FTI confirmed from the outset that this address is not monitored.[8]

10.2 It is reasonable to expect a data subject (especially one working as a data protection advisor such as Complainant) at that point, having already received the e-comms, to check the website and / or privacy policy of the marketing entity for an appropriate contact address to submit an SAR. However, a variety of options for making an SAR are reasonable, including verbal communication or even a written letter to a valid company address.[9]

[6] DIFC Commissioner's Guidance on Individuals' Rights to Access and Control Personal Data

[7] As of 21 June 2022, an automatic reply comes back stating that the info@fticonsulting.com email address is not monitored. It is not confirmed when this automated reply was implemented, or if it was in use at the time of the March 30 email from Complainant.

[8] Commissioner could further confirm if FTI knew they had it and if it was ever monitored elsewhere in the firm, as well as what the monitoring procedures for info@email addresses are generally.

[9] DIFC Commissioner's Guidance on Individuals' Rights to Access and Control Personal Data

Supporting evidence

From Complainant email of 27 Feb 2022:

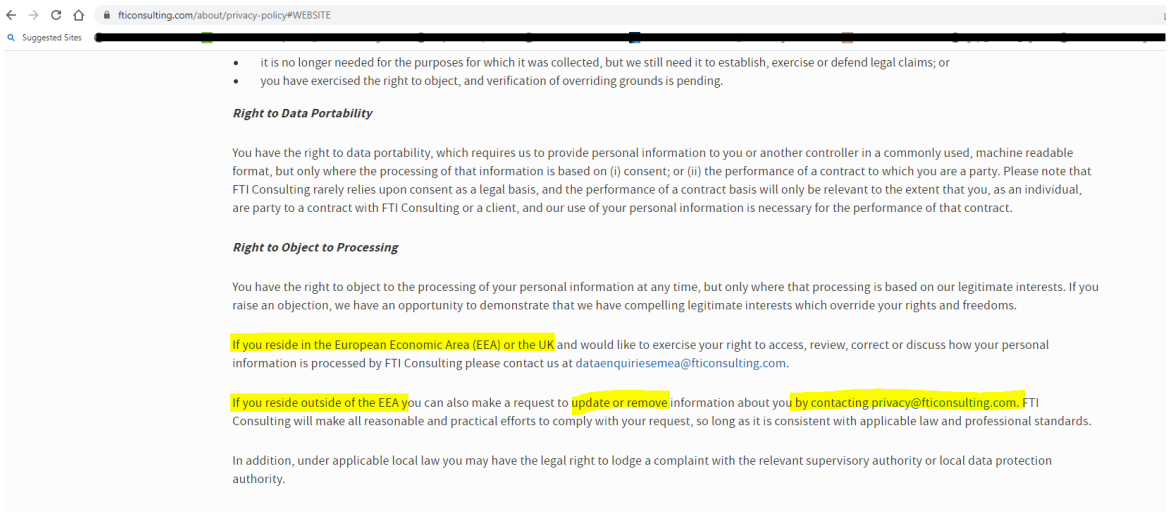
> *…If I called FTI consulting office today and requested DSAR are you suggesting this is invalid because I did not check FTI privacy statement and send an email accordingly? If not, then the same applies in my scenario. info@fticonsulting.com is a working email, with no bounce back and therefore my request is valid. Furthermore, I am sure you are a DSAR can be requested via multiple reasonable methods, not just through the privacy statement where an email can be found. If you are denying this then in my humble opinion you are violating the law.*
>
> *…Based on my interpretation of the Law in my opinion your assumption is incorrect; info@fticonsulting.com is the address used to send marketing it is reasonable for any person who did not explicitly consent to marketing to reply back to that particular address. If the account is dormant you would expect a bounce back email and 'do not reply to this email' within the body of emails sent. Neither occurred therefore it is a valid working email address.*

11 In accordance with Article 40, were 2 methods provided anywhere and easily accessible?

Finding 6: The FTI privacy policy in existence at the time that Complainant received the e-comms contained and currently only contains one form of contact for DIFC data subjects.

Reasoning

11.1 On review of the FTI privacy policy, there is only one option for making contact for this purpose, apart from the two contact methods provided for Californica residents. Further, the mention of the non-EEA contact information may be confusing, as it only alludes to the rights to update or remove information about the data subject requestor:



11.2 In any case, Complainant may not have read the privacy policy / had proper notice anyway, as set out in Part 1 above. This is, however, something that FTI should rectify or clarify to the Commissioner.

12 What did FTI understand the Commissioner's instructions to be? Why no response to SAR provided?

Finding 7: FTI 2 stipulated that FTI 1 did not acknowledge or understand the access portion of the request, only the deletion portion of the request, despite follow up by both Complainant and the Commissioner's Office.

Supporting evidence

From FTI 2 email of 22 Feb 2022:

The matter became known to FTI 1 on 5 December 2021 (and we also briefly wish to note that your issue was not intentionally or knowingly disregarded by FTI prior to 5 December 2021) and whilst we have been able to see that an initial response was provided to you on 5 December 2021, it is evident that the response did not provide you with the second part of the information you requested in relation to how and why we had his information and we unreservedly apologise for the fact that this was not provided (or subsequently provided until now).

From FTI 2 email of 24 Feb 2022:

We note that neither FTI (nor any individual within FTI) became aware of your data access request until 5 December when it was escalated to the Commissioner (and following FTI 1 then receiving an email from the Commissioner). The reason that we had not been aware prior to 5 December is that the email that was sent by you on 30 March 2021 was sent to info@fticonsulting.com and this email address was a dormant/not monitored email address. Despite looking into the matter we have not been able to ascertain why that particular email address would have been used at that time as the email was dormant as at 30 March 2021, was not the email notification address included in our data privacy policy (available on our website) and as far as we have reasonably been able to determine was not publicly listed on any FTI website at that time. So, whilst we are aware and understand following the various exchanges that your initial attempted communication to an FTI email was on 30 March and therefore appreciate that from your perspective it appears that we flagrantly disregarded your request, we confirm that this is certainly not the case.

13 Is there a contravention of Article 33 of the DIFC DP Law regarding the response (or lack thereof) to the December 5, 2021, SAR?

13.1 **Yes**. In accordance with Article 33(2), FTI was obligated to respond to the SAR made on December 5, 2021, both by Complainant and as directed by the Commissioner's Office, within one month of such request. This did not happen until further follow up and intervention of the Commissioner's Office occurred, a few weeks after the one month deadline passed. FTI 1 offered

an apology and confirmed that Complainant's personal data had been removed as required by Article 33(2), but did not act on the Article 33(1) SAR.

Ancillary Issues

---

14 When and in what manner was FTI 1 trained on FTI policies?

14.1 June 2021, after joining in Jan 2021 and completing the filtering exercise for uploading contacts to the FTI CRM. As such, may not have been aware of the FTI policies relevant to this issue, but as a privacy consultant, presumably should have made a more informed, nuanced decision.

15 Is there any documentation to support the assessment that marketing based on legitimate interests is a sufficient, valid basis for such processing? Was a DPIA done?

15.1 No DPIA was done. The main filtering process results reflect that only trusting FTI 1's judgement based on reading of the relevant policies and applying certain criteria were the basis of this assessment.

16 Is it excusable that the initial SAR of March 30, 2021, sent to a dormant email address was missed?

16.1 Debatable, given the data subject's position as a privacy professional and the origination address of the event email.

Declaration of Contraventions and Directions:

17 In consideration of all issues and findings set out above, I issue a declaration of the following contraventions of the DIFC DP Law by FTI Consulting:

17.1 **Contravention 1 - Not providing valid notice to data subjects that contacts of new or existing employees would be collected and used for marketing purposes.**

17.1.1 Any possible soft opt in or legitimate interest basis for collecting and processing the personal email address was not determined appropriately in this regard, as the connection existed before FTI 1 joined FTI, and Complainant's personal data was not collected for or on behalf of FTI business in the first place, at which point Complainant could have received proper notice of collection and processing purposes (i.e., general notice and in particular direct marketing as set out in Article 29).

17.1.2 As FTI did not collect the personal data directly from Complainant, Articles 30 and 34 of the DIFC DP Law take priority, such that appropriate notice should have been given to Complainant when his data was uploaded to the FTI CRM. It is clear that in line with FTI's own filtering and social media contacts policy that simply being connected is not enough to upload contact information from a previous / any connection.

17.1.3 Lastly, the FTI privacy policy does not provide for 2 methods of contact for rest of world data subjects, only for those subject to California DP Law. DIFC DP Law requires two methods of contact for data subjects' rights requests, in accordance with Article 40.

17.1.4 **These contraventions carry a range of maximum fine amounts, the highest maximum amount being $75,000. For these contraventions based on the circumstances and mitigating factors, it is recommended that a collective fine of $5000 should be issued.**

17.2 **Contravention 2 - Not responding to the valid December 5, 2021, subject access request within the period prescribed by the DIFC DP Law.**

17.2.1 While the March 30 SAR was not responded to, FTI was not aware of it and, giving the benefit of the doubt, did not deliberately ignore it. However, better email monitoring processes and responses should be provided, and perhaps disable the info@email entirely. The December 5 SAR, however, was not properly responded to. Although the data was erased, the remainder of the response regarding access to know who else had Complainant's information, etc., was not responded for some time. The Commissioner's Office even followed up to ensure it was being managed as per the direction given.

17.2.2 **The maximum fine for this contravention is $100,000 but based on the circumstances and mitigating factors, it is recommended to issue a single fine of $10,000.**

18 Ancillary issues such as whether training of FTI 1 as a new employee or adherence to compliance policies was appropriately conducted or reviewed shall not be addressed.

19 In light of the contraventions and reasons declared above and in conclusion, I direct that notice of the fines delineated herein are issued to FTI Consulting as soon as practicable.

20 I further direct that FTI Consulting undergo a privacy compliance program review based on an initial, through inspection of the entity, and including recommended updates to all technical and organizational measures that, if implemented properly, may have prevented these contraventions from occurring. Further, a follow up inspection should be conducted to ensure that all recommendations were properly implemented.

Review and appeal

21 FTI Consulting may ask the Commissioner to review a direction ordered under Article 59 of the DIFC DPL. Article 59(7) provides that:

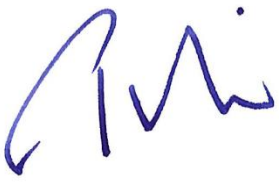
> *"Any affected party may ask the Commissioner to review the direction within fourteen (14) days of receiving a direction under this part of the Law. The Commissioner may receive further submissions and amend or discontinue the direction"*

22 FTI Consulting may also seek an appeal of the decisions or directions of the Commissioner FTI Consulting may seek to appeal this Direction within thirty (30) days, in accordance with Article 63 of the DIFC DPL, or, in accordance with Article 59, FTI Consulting may seek judicial review by the DIFC Courts of:

(i) the decision of the Commissioner to issue the direction; or

(ii) the terms of the direction

23 The Court may make any orders that it may think just and appropriate in the circumstances, including remedies for damages or compensation, penalties and imposition of administrative fines and findings of fact or alternative findings of fact in relation to whether or not the Law has been contravened

Signed: 

Jacques Visser
Commissioner of Data Protection
Level 14, The Gate
DIFC
Dubai, UAE

DIFC

Annex 1: Additional Evidence and Feedback from the Parties Considered in this Declaration

A. From FTI 2 initial narrative response to Commissioner's questions, provided April 15, 2022

[REDACTED]

B. Screen shot from June 30, 2022