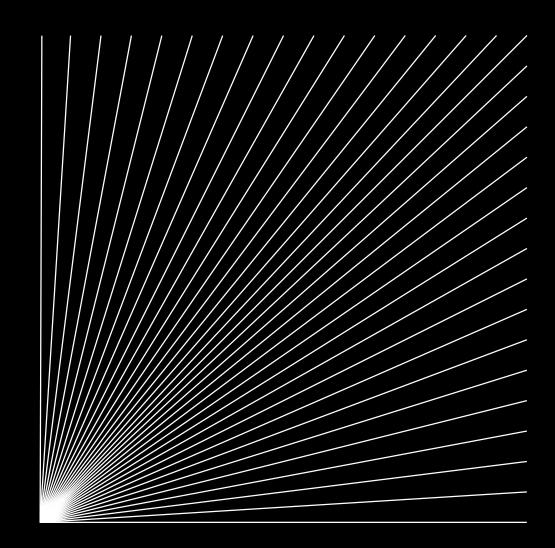


DIFC Data Protection Talks

Talk #4: Inspections and Supervision

Date: 21 June 2022

The future is here.



THEME



A N

Why does the Commissioner's Office conduct inspections, and how often?



How do I know my business is being inspected and what should I do?



What are your burning questions?

Why does the Commissioner's Office conduct inspections and how often?

Inspections are an important part of any regulatory compliance program to gauge whether:

- a) the company being inspected knows how to comply with the law (and avoids enforcement action); and
- a) The Commissioner's Office learns what issues are both understood and misunderstood, so a compliance culture can grow properly (and avoids having to take enforcement action)

Article 46(3)(b)

Inspections are a key tool for the Commissioner's Office to assure accountability of a DIFC-based entity.

100

Automated inspections at least, per year. Previously it was only 2 per month via manual inspections.

Guidance

General DP Law compliance guidance is available <u>here</u>

How do I know my business is being inspected and what should I do?

- 1. Email from DIFC Portal is sent "Inspection Questionnaire" in subject
- 2. The email indicates it's a DP inspection, with a due date with an SR number
- 3. The action is in Pending Items / search for the SR number from the email.
- 4. Complete the 3 questionnaire sections: Background information, Resource Management & Training, and Data Processing
- 5. <u>We cannot grant extensions</u>. Please provide as much information as possible anyway, even if you think the company is not compliant. We can return for more information if needed.
- 6. If you don't respond at all, we will follow up and may have to take further supervisory or enforcement action.

Details of the Applicant	Background Information - Data P	In this portion please provide as many details as you can about the current personal data			
Background Information Resource Management	Is your Notification up to date / including any new processing activities since last notification / update? • • • • • •	Could you please describe the activities conducted by the DIFC Entity*	the current personal data processing activities conducted of by this DIFC entity. You may wish to review guidance provided by the Commissioner of Data Protection as well as these		
Data Processing	Records of Processing Activities	Does your activity require you to transfer personal data autside DIFC* None	processing assessment tools: Guidance and Assessment Tools. If in the course of completing this information you find that any information in your account		
	Back	Next Save As Draft	should be updated, please do so via the appropriate Service Request, to avoid enforcement action for non-compliance with the Data Protection Law, DIFC Law No 5 of 2020, or other applicable DIFC Laws and Regulations.		

Details of the Applicant Background Information	Resource Management and Train	ing Total no of Hours spent by employees on DP related	In this portion please provide as many details as you can about the current staff and training requirements in this DIFC entity. You may wish to review guidance	Details of the Applicant Background Information	Data Processing Questionnaire	Do you process special categories of data*	In this portion please provide as many details as you can about the this DIFC entity's controls implemented in order to comply with DIFC DP Law 2020. You may wish to review guidance provided by the Commissioner
Resource Management	Partners, Professional and Support Staff*	activities*	provided by the Commissioner of Data Protection as well as these processing assessment tools: Guidance and Assessment Tools. If in the course of completing	Resource Management	Did you have any DP Personal Data Breaches over the last two years • • None •	Please describe you Cessation of Processing procedures per Article 22*	of Data Protection as well as these processing assessment tools: Guidance and Assessment Tools. If in the course of completing this information you
Data Processing	Do you instruct any Processors or Sub-Processors? () *None	Total no of Trainings organized / Updates provided to Internal Staff*	this information you find that any information in your account should be updated, please do so via the appropriate Service		Have you had any Data Subject exercise their rights as set under Articles 32 - 40 • *	Please summarise your Compliance Program () *	find that any information in your account should be updated, please do so via the appropriate Service Request, to avoid enforcement action for non-
2	Evidence of the Trainings Conducted Upload Files Or drop files		Request, to avoid enforcement action for non-compliance with the Data Protection Law, DIFC Law No 5 of 2020, or other applicable DIFC Laws and Regulations.	3	Compliance Program Upload Files Or drop files Contract Copy that includes the Data Protection Clause	Do you maintain a copy of Data Protection and / Privacy Policies and Procedures *None * Please summarise the existing and / or future technical and orgnisational measures in place to control the safety	compliance with the Data Protection Law, DIFC Law No 5 of 2020, or other applicable DIFC Laws and Regulations.

What kinds of questions should we consider regarding DP inspections?

What if I know my company is not compliant with the DP Law 2020 when being inspected?



How many Processors are we sharing data with and what DP laws are in place where they operate?

What if I don't respond to an inspection request?



What activities does my business perform?

Where does my company collect Personal Data?



Can I request an extension to respond to an inspection request?



Does any data leave the DIFC?



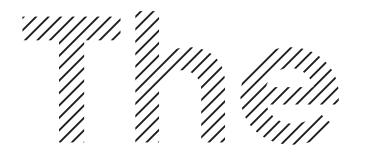
Have I evaluated the risk that processing creates regarding the personal data we store?

What are YOUR burning questions?

How do you navigate differences between the mainland and free zone data protection regulations? What about localization requirements in DIFC vs UAE?	The mainland DP Law and the DIFC DP Law are rather similar. We will have to wait to see what the implementing regulations look like – they are pending. But generally, if you comply with the DIFC DP Law, you could be close to overall compliance with the UAE DP Law. Currently, the DP Law in DIFC does not contain localization requirements, but we are unsure what will happen with the UAE DP Law.
Are there are any data protection related filings to be made in the DIFC?	The primary requirement is if your company processes personal data, to notify the Commissioner's Office, as set out in Article 14(7). This is one of the major areas of non-compliance. If you appoint a DPO, there is an annual DPO assessment that must be filed as well.
What is the key difference between UK GDPR and DIFC Data Protection Law?	Very little. In fact, DIFC DP Law is being evaluated for equivalence with the UK GDPR. Please see the press release from August 2021, providing information about the UK and DIFC collaboration.
What is the biggest challenge you are finding organizations are reaching out to the DIFC with when it comes to data protection?	The most common issue we get asked about most is about international transfers of personal data and what to do to ensure compliance with the many different laws on this. The EU is on one end of the spectrum for specific, technical requirements, and other regulators have their own degrees of requirements. DIFC's requirements are set out in our Data Export & Sharing Handbook. Please have a look at the <u>Data Export & Sharing link</u> of the DIFC website for more support.
Why are board members thinking that privacy function is only a 'good to have' function? How can we break that mental barrier?	Lack of regulator supervision and enforcement (due largely to lack of resources) is one part of the reason why Boards of companies may see DP compliance as less than urgent. If you can get away with speeding down the highway, won't you keep doing it? Same with non-compliance with DP Laws. Also, the impact and education about ethical data management is not well understood by many organizations. Communicate, Communicate, Communicate!!!
Is it mandatory for all companies, including foundations, prescribed corporations, and partnerships, to have a data protection policy? Does one still need to file for compliance (aka a notification) even if currently there are no employees in the organisation?	Yes – if the company processes personal data in any way, it should have at least an appropriate level of compliance structure in place, including a privacy policy. To be fair, most PCs don't process personal data, nor do certain types of holding companies. But this decision can only be made by those in the company itself.
Are data controller permits required any more?	No. Please see <u>FAQs</u> for further information.

What are YOUR burning questions? (/2)

Due to budget limitations, please advise methods of implementing a privacy program using open-source tools and free solutions.	 Please look at the DIFC Guidance website. There are loads of templates for policies, a compliance checklist available, contract document templates, etc., available, and lots of assessment tools to help you understand your obligations. There is even a free compliance maturity tool provided by a third party that may help. Always check the <u>DIFC DP website</u> and sub-menus such as the Guidance site above for updates. Linked In, Twitter and general email communications to portal users are all sources of updates as well.
Does the Office of the Commissioner of Data Protection have plans to become a data-lead regulator?	Excellent question. The Commissioner's Office has arguably already done so, by creating a DP Law that makes sense for the types of businesses in DIFC, that looks at thematic trends, and keeps accountability at the heart of supervision.
What are the requirements for adding Standard Contractual Clauses to (intra-company) agreements?	The requirements for implementing the SCCs are set out in the DIFC DP Law Article 27, and the DIFC Regulations, Regulation 5. In short, if your company transfers personal data (exporter) to an importer in another jurisdiction not on the "adequate countries" list (even within the same group), then the SCCs are one of the possible safeguards that may be used.
Is it necessary to replace our currently still valid data export clauses with the new version released on DIFC website?	The updated DIFC SCCs should replace the old ones <i>ideally</i> by 31 December 2022 (so you have some time). Please have a look <u>here</u> for the SCCs template and <u>here</u> for the guidance of how to use them (Section 3(C) in particular!)
Article 41(1) definition of breach is very wide. Despite online guidance please define severity threshold to notify the Commissioner.	If you check the <u>"Should I Notify a Breach?</u> " Assessment, there are 3 fundamental questions as the end: <i>Please tell us if any of the following high risk factors apply:</i> •Someone's physical safety is in immediate danger •Someone's psychological safety is at immediate risk •There is immediate risk of serious financial harm
How can consent be managed in the absence of specific rules in the region?	At least for DIFC, consent guidance is available <u>here</u> .
How do we deal with marketing outside of DIFC?	Guidance is available about marketing and electronic communications <u>here</u> . This guidance provides insight about compliance with other e-privacy laws, i.e., PECR and the EU-driven requirements.





///

Contact

For further information please contact:

DIFC DP Commissioner's Office <u>commissioner@dp.difc.ae</u>

+971 4 362 2222

Gate Building Level 14 DIFC, Dubai, UAE PO Box 74777