Question Report

Topic	# Question
MENA Data Privacy Series: Data Subject Access Requests	21

Question Details

#	Question	Answer
1	How can we access the recording previous events?	You will find the recordings for past DP programs on the MENA webpage here - https://www.acc.com/chapters-networks/chapters/middle-east-and-north-africa/sector-interest-groups/data-privacy-1
2	We get a lot of data deletion requests sent by Mine. I often email the individual to understand their relationship to our company, but I almost never get a response. We don't have our data mapping for the company finished, and it takes a long time. In the meantime, have I adequately complied if I get no response back from the data subject?	You do not need to comply with the request until you have received the additional information required to verify identity. However, you should only be asking for I.D. where its reasonable in the circumstances. If you have the information to verify the individual held on your systems, such as a matching email address to the requestor's email account, then it would not be reasonable to ask for I.D. Regulators expect information management systems to be set up in a way that facilitates data subject rights. One of the factors regulators consider in assessing compliance is the size and resources of the organisation.
3	When can I ask for ID verification, and when should I avoid asking for ID - especially if I don't know the individual's relationship to the company?	As above, you need to be satisfied that you know the identity of the requester (or the person the request is made on behalf of) and the data you hold relates to the individual in question. Where the request is made via a third party such as a solicitor or agent, you should request evidence of their authority to act, such as a signed letter of authority. The key point is that you must be reasonable and proportionate about what you ask for. If you don't know the individual's relationship to the company and have no record of them on your systems, then it is reasonable to ask for I.D. However, if it was an employee for example, whose information is readily available within your organisation, then you should not ask for I.D

4	What is the process of handling and storing details collected for verification of requester during DSAR request process.	As with any personal data you should only retain and store data for as long as it is needed (storage limitation principle). Therefore, once you have verified the identity, it would be good practice to delete the information within a reasonable period of time after the request has been responded to. Whilst you do not need to keep copies of ID documents, you should keep a note of: •what ID documents the individual provided; •the date you verified them; and •details of who in your organisation verified them The above could be retained in a data rights log.
5	When a data access right is exercised, does an organisation require to disclose that the individual's data might be on security tools(eg -DLP)?	We would need to understand what the data categories being collected on your security tools. If these are security logs which reveal information such as website traffic or visits or business application usage, then this could all be in scope, unless an exemption applied.
6	So, processor needs to tell you about the SAR and give you the data to give to the individual. Is it okay to let the processor respond directly to the SAR to minimize duplication of data across both entities?	The controller is responsible for dealing with the SAR with help from the processor. Therefore, if a Processor is processing personal data on behalf of the Controller on the Processor's own systems, which the Controller doesn't have access to, it should retrieve this information and provide it to the Controller. Whilst it is the Controller's responsibility to respond, it could technically instruct it's Processor to respond on its behalf. However, this would need to be made clear to the individual that the Processor is responding on behalf of the Controller, who is responsible for complying with the request. There should not be any duplication of data across entities though, as you would only need a Processor to retrieve information which the Controller is not storing on its own systems.

7	Is the form of the DSAR equally as broad if received from an employee?	In short - yes. The test as to whether employee data is disclosable or not has to be considered on a case by case basis, as there will be a lot of business as usual data which the individual may be identified in, which does not necessarily contain personal data. The information must both identity and relate to the individual. The Art 29WP Opinion on the “concept of personal data” is helpful for this assessment.
8	How can a retail business protect itself from clients who later accuse you of violating their rights after giving you information with their consent? SECURITY OF DATA?	Please can we clarify the question further and what you mean by being accused of a violation of rights? Subject to your clarification, evidencing compliance with the “lawfulness, fairness and transparency” principle will be key for accountability purposes. Where consent is relied upon for certain processing of personal data, then a record of consent given should be stored. Further, a privacy notice should be in place and presented to individuals before collecting their data, to ensure they are aware of the purposes for processing and who information may be shared with. Please note that consent also needs to be kept evergreen. The consent you obtained in the past may need to be refreshed, perhaps because prior to new DP Laws, consent may have not have been express (need to opt in), or you may not have defined the purposes, legal basis, or thiird parties who'd receive the data.
9	How do we save data deletion email requests to record that we have complied, or do we delete those?	It may be helpful to save these requests for audit purposes and defending legal claims. In line with the storage limitation principle, you should only keep information for as long as it’s necessary for its purpose much– therefore once the request is dealt with, it should be removed after a reasonable period of time. The exact time period should be objectively justifiable. In any event, its good practice to retain a log of data subject requests which includes information as to when or how you responded.

10	is there a third party tool available in the market to help with DSR?	There are many third party tools available which can help simplify DSRs. The IAPP Tech Vendor Report (available at https://iapp.org/resources/article/privacy-tech-vendor-report/) lists solutions available on the market to help organizations facilitate DSRs. Popular vendors providing automated DSR solutions include OneTrust, BigID and Securiti.
11	Do we need to keep a register of all DSRs? in case of data deletion request, do we keep records of the request?	The laws do not require you to keep a register of all DSRs but it is good practice to keep one. Article 24 GDPR does state the Controller should have appropriate data protection policies where proportionate to its processing activities. **Please see response to 9 above.**
12	Legislations did not distinguish what personal information is. HOW CAN WE LEGALLY PROTECT OUR BUSINESS?	All our regional laws, including GDPR, do define what personal data is. Personal data is defined within EU and UK GDPR and various regulatory guidance is available in the EU / UK. For example, the ICO guidance can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
13	ex: my office does not have any cctv in the office, however we do have cctv in the bldg. How would we handle this if we receive a SAR?	If the CCTV is processed by the building owner as an independent controller, then your organisation would not be responsible for complying. The request should be redirected to the CCTV operator. However, we would need to understand the roles of the parties further and if your organisation ever has access to the CCTV records and the contract terms in place governing your organisations occupation of the building.
14	What strategies have been effective in overcoming the culture of hoarding data?	Regular training and making staff aware of data protection law compliance and risks is key. As discussed on a call, having a clear retention procedure and policy in place is important – this can allocate record retention owners across the business, responsible for overseeing their own teams / divisions are complying with the policy. Having a documented chain of responsible stakeholders is key.