Morgan Lewis

COMPLYING WITH SUBJECT ACCESS REQUESTS UNDER THE GDPR

Under the EU General Data Protection Regulation (GDPR), a data subject has the right to access any of his or her personal data that a controller holds and to exercise that right at "regular intervals," in the form of a subject access request (SAR), in order to verify the lawfulness of processing. The right to access includes the right to receive confirmation that the individual's data is being processed, the right to receive a copy of the data, and the right to receive additional information about the data, including the following:

- The purposes of the processing

- The categories of personal data concerned

- The recipients to whom or categories wherein the personal data has been or will be disclosed

- The period for which the personal data will be stored and the criteria used to determine that period

- The right to request rectification or erasure of personal data

- The right to restriction of processing of personal data

- The right to object to such processing

- The right to lodge a complaint with a supervisory authority

- Where the personal data is not collected from the data subject, any available information as to its source

- The existence of automated decisionmaking and meaningful information about the logic involved, and when based on profiling, the consequences of such processing for the data subject

- If the data controller or data processor transfers the personal data to a third country or an international organization, information on the appropriate safeguards in relation to the transfer

Morgan Lewis

COMPLYING WITH SUBJECT ACCESS REQUESTS
UNDER THE GDPR

CONTROLLERS SHOULD DO THE FOLLOWING WHEN RESPONDING TO SARS

- Must respond to a data request within one month of receiving the request
    - Can be extended up to two months for complexity and volume of the request
- Respond in writing unless specifically requested otherwise
- Respond in "concise, transparent, intelligible and easily accessible form, using clear and plain language" (GDPR Art. 12)
- Provide access to data through
    - Remote, direct access to the data
    - Copy of the data
- Provide the data free of charge or ask a reasonable fee if the request is excessive
- Ask for clarification of the request if the request is vague
- Make certain of the identity of the requestor
- Seek to limit the specific data requested by the subject
- Ensure that the data of other subjects is not disclosed while providing access

RECOMMENDATIONS FOR CONTROLLERS RESPONDING TO SARS

- Train all employees on how to recognize SARs and forward any such requests to the proper personnel
- Identify employees who will respond to SARs and provide the proper training regarding responses
- Design a SAR form that individuals can complete and submit electronically (optional use)
- Develop a standard log of received SARs in order to keep track of all timeline requirements
- Confirm the requestor's identity before responding to the SAR
- Evaluate the data request and immediately reach out to the requestor for more information if it is needed or warranted to expedite the response
- Immediately (within one month of receipt of the request) notify the individual of the delay and the reasons for the needed time extension
- Immediately (within one month of receipt of the request) notify the individual of the refusal or the fee charged, including the reasons the company believes the request is unfounded or excessive, and that the individual has the right to file a complaint with the company's data protection officer or the relevant data protection authority
- Respond to the data request in whatever format the individual has requested
- As recommended in the GDPR, provide an individual with remote access to his or her personal data where feasible
- Design template responses or language regarding the information to be included in SAR responses

www.morganlewis.com