Data Subject Access Requests (DSARs)
Standard Operating Procedure
(last updated October 21, 2019)

1. We receive an inquiry about how to submit a Data Subject Access Request (referred to as a "DSAR").	To respond to inquiry about how to submit a request, provide the following information: (1) requests may be made via [email] or toll-free number at [number], [written request to mailing address], [submission of web form], (2) must include information sufficient to confirm the requestor's identity and (3) must include sufficient information to allow us to determine what information is requested.	Go to step 2.	

2. We receive a DSAR either (a) directly from a client's customer or another individual whose data we process <u>or</u> (b) from a client acting on behalf of the client's customer.	All requests should be directed to [Designated Person or Department]. Go to step 3.		

3. Verify: Do we process the data requested?	If yes, go to step 4.	If no, then we are unable to provide the requested data and should notify the requesting individual or the client accordingly. (End.)	

4. Verify: Is the request directly from a client's customer or another individual whose data we process?	If yes, go to step 5.	If no, go to step 6.	

5. Verify: Are we the "controller"[1] of the relevant data?	If yes, go to step 7.	If no: (1) inform requestor that we are not the data controller and refer them to controller (if known, usually our client) and (2) notify controller (if known) of receipt of the DSAR and request instructions from the controller how to assist. Unless we receive further instructions from the controller on how to assist, END of DSAR process.	

6. Verify: Is the request from a client acting on behalf of the client's customer?	If yes, go to step 7.	If no, and if the request is also not directly from a client's customer or another individual whose data we process, END of DSAR process.	

INSTRUCTION

The following steps apply if (a) we are the "controller" of the data processing or (b) we are not the "controller" but our client (the "controller") instructs us to respond to the DSAR on the client's behalf. If either (a) or (b) applies, go to step 7. If neither (a) nor (b) applies, END of DSAR process.

7. Verify: Did the requestor or client provide sufficient information to allow us to verify the requestor's identity?	If yes, go to step 8. NOTE: For requests received from a client on behalf of the client's customer, verification of requestor's identity is responsibility of the client. However, process with client should confirm that client has properly verified identity of the customer in compliance with applicable data protection law.	If no, contact the requestor or client and obtain additional verifying information and fee (if applicable).	If requestor or client provide sufficient information to allow us to verify the requestor's identity or to determine what data is requested to be accessed, deleted or corrected and/or fee (if applicable), we may refuse to provide the requested data and should notify the requesting individual or client accordingly. (End.)

8. Verify: Did the requestor or client provide sufficient information to allow us to determine what information is requested to be accessed, deleted or corrected?	Important because of broad scope of data covered by access rights. Requestor will likely seek only certain personal data rather than every kind of data that falls within GDPR's scope.	If yes, go to step 9.	If no, request additional information. If requestor or client is still unable to provide sufficient information to allow us to determine what information is requested, information should not be provided. We may refuse to provide the requested data and should notify the requesting individual or client accordingly. (End.)

[1] NOTE: For purposes of this document, (1) "controller" refers to both "controllers" under GDPR and "businesses" under CCPA and (2) "personal data" and "data" refer to both "personal data" under the GDPR and "personal information" under the CCPA.

9. Verify: Is the request for personal data about the requestor?	If yes, go to step 10.	If no, then this request is not a DSAR. We may refuse to provide the requested data and should notify the requesting individual or client accordingly. (End.)	

10. Verify: Is the requestor a citizen of California or of the EU?	If yes, go to step 11.	If no, we may refuse to act on the request, and should notify the requesting individual accordingly. (End.) Or...	… we may still comply with the request depending on company policy or if we are instructed to do so by our client (the "controller"), in which case, go to step 11.[2]

11. Determine: Is the request unfounded, excessive, repetitive or vexatious?	If no, go to step 12.	If yes, we may charge a reasonable fee to handle the response. Or… we may refuse to act on the request, and should notify the requesting individual or client accordingly. (End.)	Alternatively, we may still comply with the request depending on company policy or if we are instructed to do so by our client (the "controller"), in which case, go to step 12. But we are under no legal obligation to do so.

12. Determine: What type of data request is being made? (e.g. request to review? Rectify? Delete? Etc.)	Go to step 13.		

13. Determine: If the request is for review of data, does the request fall under any exemptions?	(Requests under GDPR) For EU residents there are exemptions when the requested information is subject to legal privilege, is publicly available or would disclose confidential information of the controller or a third party to which the controller is under confidentiality obligation. (Requests under CCPA) For California residents, there are exemptions when we have already disclosed the requested	If yes, we may refuse to act on the request, and should notify the requesting individual and client accordingly. (End.)	If no, go to step 14. Also, we may still comply with the request depending on company policy or if we are instructed to do so by our client (the "controller"), in

[2] NOTE: There is no requirement that we verify EU or California citizenship, because we could simply choose to fulfill these requests from individuals regardless of location.

	information to the same consumer in the last 12-month period, or the requested information is about a single, one-time transaction for which information was not retained in a way that could personally identify the consumer.		which case, go to step 14.

14. (For GDPR requests only) Determine: Does the requested data also involve personal data on other individuals? (i.e. would providing the requested data also necessarily include other data on other individuals?)	If yes, redact, filter or (if practical) anonymize other data before the requested data set is provided to requestor. If successful, or this is a CCPA request, go to step 15.	If disclosure of other data cannot be protected, contact other parties and obtain affirmative, written consent to disclosure as part of the DSAR. If successful, go to step 15.	If consent from the other parties cannot be obtained or is impractical, we must refuse to act on the request, and should notify the requesting individual and the client accordingly. (End.)

15. Acknowledge receipt of the DSAR and inform the requestor or the client of any fees charged (if applicable) for the processing of the request.	Respond to the DSAR within 30 days (for EU residents) or within 45 days (for Cal and all other requestors), providing all requested information or providing an explanation of why we cannot fulfill the request. 30-day (GDPR) and 45-day (CCPA) periods start after receiving the DSAR and after receiving all information necessary to verify identify of the requestor. Go to step 16.	If the request is refused due to invalid request, explain to the individual how to make a valid request. (See above steps.) (END – unless request is re-submitted.)	If the request is refused due to other reasons above, notify requestor or the client of grounds for refusal. (END – unless request is re-submitted.)

16. Determine: Is this a request to review data?	If yes, search and locate the requested data by a reasonable and proportionate search, even if there is a possibility that additional relevant personal data might still be found if a more extensive search were conducted. For CCPA only, we may limit the data provided to the 12-month period preceding our receipt of the verifiable request. (GDPR's requirement is to provide "data undergoing processing" without time limitation.) Requestor is entitled to a legible and understandable copy of records. Data should be provided in a commonly used electronic form if the requestor has submitted the DSAR electronically. Just because an individual's name is mentioned in a document does not mean that the entire document must be provided. If a document contains personal data, then those data (and not	If no, go to step 17.

	necessarily the whole document) must be provided in response to the DSAR. Go to step 28.		

17. Determine: Is this a request to delete or erase data?	If yes, go to step 18.	If no, go to step 20.	

18. Determine: If this is a request under GDPR, are we required to comply with the request to delete or erase data?	Deletion is required for the below for GDPR requests: 1. The data are no longer necessary for the purposes for which they were collected or otherwise processed. However if we still need to maintain the data requested to be deleted, we may keep the data and inform the individual of the reason for denying the deletion request. 2. Where the data were collected or otherwise processed on the basis of consent, the individual withdraws consent on which the processing is based and there is no other legal ground for the processing. So if the data was being processed based solely on consent, the data must be deleted. 3. The individual objects to the use of his or her data where legal basis of the use is legitimate interest, and there are no overriding legitimate grounds for use of the data. So if there is no overriding legitimate reason for use of the data, it must be deleted. 4. The data have been unlawfully processed. Must be deleted. 5. The data have to be deleted for compliance with other legal obligations to which we are subject. Must be deleted.	If yes, or if this is a request under CCPA, go to step 19.	If this is a request under GDPR and the answer is no, we may refuse to act on the request, and should notify the requesting individual or client accordingly. (End.)

19. Determine: Does the request to delete or erase data fall under any exemptions?	For GDPR requests, processing is necessary for any of the below: 1. To comply with other legal obligations to which we are subject 2. For the establishment, exercise or defense of legal claims For CCPA requests, processing is necessary: 1. To complete the transaction for which the data was collected, provide a good or service requested by the individual (or reasonably anticipated within the context of a business's ongoing business relationship with the individual), or otherwise perform a contract between the business and the individual. So we may maintain the information if required to fulfill our contractual obligations to the data subject. 2. To detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity; or prosecute those responsible for that activity. 3. To debug to identify and repair errors that impair existing intended functionality. This permits keeping certain information such as server logs to identify and remove errors from existing software, but only to maintain intended functions, not to create new functions. 4. To comply with the California Electronic Communications Privacy Act obligations to respond to warrants and access requests by law enforcement. 5. To comply with other legal obligations to which a business is subject. 6. Otherwise to use the individual's data, internally, in a lawful manner that is compatible with the context in which the individual provided the data.	If yes (i.e. the request to delete or erase falls under an exemption), we may refuse to act on the request, and should notify the requesting individual or client accordingly. (End.)	If no, delete the requested data and go to step 28.

20. Determine: Is this a request under GDPR to restrict processing of data? (NOTE: No analogous right under CCPA.)	If yes, go to step 21.	If no, go to step 22.	

21. If this is a request under GDPR to restrict processing, does the request meet any of these circumstances? (NOTE: No analogous right under CCPA.)	GDPR requires that requests to restrict processing of data be honored where one of the following is met and for the relevant time period: 1. If the accuracy of the data is contested by the individual, we must stop processing while the accuracy is verified, for a period enabling the controller to verify the accuracy of the data.	If yes, stop or pause processing the relevant data for the relevant time period and go to step 28.	If no, we may refuse to act on the request, and should notify the requesting individual or client

	2. The processing is unlawful, and the individual opposes the erasure of the data and requests the restriction of their use instead. 3. The controller no longer needs the data for the purposes of the processing, but the individual requires retention of the data for the establishment, exercise or defense of legal claims. 4. The individual has objected to processing, and it is pending whether the legitimate grounds of the controller for processing override those of the data subject.		accordingly. (End.)

22. Determine: Is this a request made by a California consumer under CCPA to opt out of the sale of personal data? (NOTE: No analogous right under GDPR.)	CCPA gives California consumers a right to opt out of the sale of their personal information.	If yes, refer the individual to our "Do Not Sell My Information" webpage where they can opt-out of the sale of their information. (End)	If the request to opt-out is not made under CCPA, we may refuse to act on the request, and should notify the requesting individual or client accordingly. (End.) If the request is for something other than opt-out by a California consumer under CCPA, go to step 23.

23. Determine: Is this a request under GDPR to object to processing of data? (NOTE: No analogous right under CCPA.)	If yes, go to step 24.	If no, go to step 25.	

24. Does the request to object to processing meet any of these circumstances?	For GDPR, requests to object to processing of data must be honored where one of the following is met: 1. The individual objects to processing of his or her data that was based on a controller or third party's legitimate interest, and there are no overriding legitimate grounds for use of the data or for the establishment, exercise or defense of legal claims. This includes objection to processing for automatic decision making (GDPR Article 22) including profiling. 2. Where an individual's data is processed for purposes of direct	If yes, permanently stop processing the subject data and go to step 28.	If no, we may refuse to act on the request, and should notify the requesting individual or client accordingly. (End.)

	marketing (GDPR Article 21), and the individual objects to processing for direct marketing, including profiling related to such direct marketing. 3. The individual objects to being subject to automated decision-making, and the decisions have legal effect on the individual or otherwise significantly affect the individual, unless one of the following are met: The processing is necessary for entering into or performing a contract between the individual and the controller; or the processing is based on the data individual's explicit consent (GDPR Article 22)		

25. Determine: Is this a request to port data?	If yes, provide the requested data to the requesting individual or to the new third party to whom the requesting individual has requested data be transferred in a commonly used and machine-readable format, and go to step 28.	Data should be provided in a commonly used and machine-readable format.	If no, go to step 26.

26. Determine: Is this a request to rectify or correct data?	If yes, go to step 27.	If no, go to step 28.	

27. Review whether the data requested to be rectified or corrected is factually inaccurate.	If yes, correct the inaccurate data and inform the data subject of the rectification. Go to step 28.	If no, notify the requesting individual or the client that the data is accurate. (End.)	

28. For any response to a DSAR: Ensure that the data will not be changed as a result of the DSAR. (Except for routine changes as part of the associated processing activities.)	Provide the following additional info as part of any response (can be done via directing the requestor to our Privacy Policy): (a) The purposes of the processing; (b) categories of personal data concerned; (c) recipients or categories of recipients to whom personal data has been or will be disclosed; (d) the	The CCPA prohibits discrimination against consumers who have exercised any of their CCPA rights, and prohibits businesses from taking retaliatory actions such as denying consumers goods or services, charging different prices or rates or providing a different quality of goods or services to consumers who have exercised the rights, or suggesting that a consumer might be	Go to step 29.

	anticipated period for which personal data will be stored (if known); (e) the existence of the DSAR rights; (f) the right to lodge a complaint with a supervisory authority; (g) if we did not collect the data directly from the data subject, the source of the personal data; and (h) the existence of any automated decision-making, including profiling.	retaliated against in such a way. However, the CCPA does permit charging a different price, or providing a different quality of goods or services, or providing some other financial incentive for allowing the business to maintain or use the consumer's data, if the difference is reasonably related to the value of the consumer's data, if the business provides notice to the consumer and the consumer opts in.	

29. If the data request is <u>not</u> one provided for in GDPR or CCPA …	We may refuse to act on the request, and should notify the requesting individual accordingly. (End.)	Alternatively, we may still comply with the request depending on company policy or if we are instructed to do so by our client (the "controller"), in which case, go back to step 12. But we are under no legal obligation to do so. (End.)

(End.)