



Snowflake Data Protection Impact Assessment (DPIA) Fact Sheet¹

This DPIA Fact Sheet is intended as guidance and for exemplary purposes only. Each organization should conduct its DPIA in accordance with its own unique processes, use cases, data, and interpretation of the requirements of Art. 37 of the GDPR.

DPIA Requirements & Sub-requirements	Snowflake Customer DPIA Response
A systematic description of the processing is provided (Art. 35(7)(a)):	Provide a systematic description of your use of Snowflake:
<input type="checkbox"/> Nature, scope, context and purposes of the processing are taken into account (Recital 90);	<input type="checkbox"/> Snowflake MSA / Terms of Service / DPA Annex 2, Determined by customer;
<input type="checkbox"/> Personal data, recipients and period for which the personal data will be stored are recorded;	<input type="checkbox"/> Determined by customer;
<input type="checkbox"/> A functional description of the processing operation is provided;	<input type="checkbox"/> Determined by customer (commonly, data analytics, data science);
<input type="checkbox"/> The assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;	<input type="checkbox"/> Determined by customer (commonly, data sources, transfer tools, the Snowflake service, customer-selected cloud hosting & infrastructure provider, BI tools);
<input type="checkbox"/> Compliance with GDPR-approved codes of conduct is taken into account (Art. 35(8)).	<input type="checkbox"/> No codes of conduct or certifications specifically applicable to Snowflake have been approved under the GDPR at this time, but if a code of conduct applicable to your organization has been approved, you can describe your compliance with it here and the effects of your compliance on data protection.
Necessity and proportionality are assessed (Art. 35(7)(b)):	Assess the necessity and proportionality of the processing your organization performs in Snowflake:
<input type="checkbox"/> Measures contributing to the proportionality and the necessity of the processing on the basis of:	<input type="checkbox"/> Necessity and proportionality:
<input type="checkbox"/> Specified, explicit and legitimate purpose(s) (Art. 5(1)(b));	<input type="checkbox"/> Determined by customer (e.g., product improvement, customer service);
<input type="checkbox"/> Lawfulness of processing (Art. 6);	<input type="checkbox"/> Determined by customer (e.g., consent, legitimate interest);
<input type="checkbox"/> Adequate, relevant and limited to what is necessary data (Art. 5(1)(c));	<input type="checkbox"/> Determined by customer (e.g., data processed is directly related to the purposes identified);
<input type="checkbox"/> Limited storage duration (Art. 5(1)(e)).	<input type="checkbox"/> Determined by customer (e.g., data deleted after data is no longer relevant and/or in compliance with customer's data retention policy).
<input type="checkbox"/> Measures contributing to the rights of the data subjects:	<input type="checkbox"/> Rights of data subjects:
<input type="checkbox"/> Information provided to the data subject (Art. 12-14);	<input type="checkbox"/> Determined by customer (e.g., Privacy Notice, Cookie Notice);
<input type="checkbox"/> Right of access and to data portability (Art. 15, 20);	<input type="checkbox"/> The right of access and to data portability, as well as all other data subject rights, can be fulfilled by the customer in the Snowflake service;
<input type="checkbox"/> Right to rectification and to erasure (Art. 16, 17, 19);	<input type="checkbox"/> The right of access and to data portability, as well as all other data subject rights, can be fulfilled by the customer in the Snowflake service;

¹ This DPIA Fact Sheet is based on Annex 2 of the Article 29 Working Party (Now European Data Protection Board) "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679".

<ul style="list-style-type: none"> ○ Right to object and to restriction of processing (Art. 18, 19, 21); 	<ul style="list-style-type: none"> ○ The right to object and to restriction of processing, as well as all other data subject rights, can be fulfilled by the customer in the Snowflake service;
<ul style="list-style-type: none"> ○ Relationships with processors (Art. 28); 	<ul style="list-style-type: none"> ○ Information about Snowflake sub-processors can be found here;
<ul style="list-style-type: none"> ○ Safeguards surrounding international transfer(s) (Chap. V); 	<ul style="list-style-type: none"> ○ Please see Snowflake’s DPA containing Standard Contractual Clauses (which is incorporated by reference into customer contracts) here, Privacy Shield certification here, and Privacy Shield Statement here. While Privacy Shield has been invalidated as a transfer mechanism by the ECJ as of July 16, 2020, the U.S. Department of Commerce will continue to administer the framework and Snowflake will continue to abide by the Privacy Shield Principles, which act as safeguards facilitating international transfers.
<ul style="list-style-type: none"> ○ Prior consultation (Art. 36). 	<ul style="list-style-type: none"> ○ Prior consultation is determined by customer based on the risks identified during its DPIA of its particular use of Snowflake.
<p>Risks to the rights and freedoms of data subjects are managed (Art. 35(7)(c)):</p>	<p>Describe how your organization manages risks to the rights and freedoms of data subjects:</p>
<ul style="list-style-type: none"> □ Origin, nature, particularity and severity of the risks are appreciated (Rec. 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects: 	<ul style="list-style-type: none"> □ Origin, nature, particularity and severity of the risks of illegitimate access, undesired modification, and disappearance of data:
<ul style="list-style-type: none"> ○ Risk sources are taken into account (Rec. 90); 	<ul style="list-style-type: none"> ○ Determined by customer’s configuration, integrations, and security practices (e.g., insider threat, insufficient monitoring);
<ul style="list-style-type: none"> ○ Potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data; 	<ul style="list-style-type: none"> ○ Determined by customer data processed (e.g., fraud, identity theft, reputational damage);
<ul style="list-style-type: none"> ○ Threats that could lead to illegitimate access, undesired modification and disappearance of data are identified; 	<ul style="list-style-type: none"> ○ Customer to identify most probable threats in customer’s environment (e.g., inadequate controls, stolen laptop);
<ul style="list-style-type: none"> ○ Likelihood and severity are estimated (Rec. 90); 	<ul style="list-style-type: none"> ○ Generated using above information and any other relevant factors in customer’s environment;
<ul style="list-style-type: none"> ○ Measures envisaged to treat those risks are determined (Art. 35(7)(d) and Rec. 90). 	<ul style="list-style-type: none"> ○ This will depend on the customer’s configuration and security controls. Some controls available to Snowflake customers include encryption in transit and at rest, role-based access controls, auditability, multi-factor authentication, logging and monitoring, and IP whitelisting.
<p>Interested parties are involved:</p>	<p>Involve interested parties:</p>
<ul style="list-style-type: none"> □ The advice of the DPO is sought (Art. 35(2)); 	<ul style="list-style-type: none"> □ Review the DPIA results with your DPO (if applicable); if you do not have a DPO, review them with the resource responsible for privacy compliance in your organization, such as a Chief Privacy Officer;
<ul style="list-style-type: none"> □ The views of data subjects or their representatives are sought, where appropriate (Art. 35(9)). 	<ul style="list-style-type: none"> □ If appropriate, consult your customers / users / data subjects about the processing performed (e.g., Snowflake leverages its customer users’ responses to voluntary customer surveys to facilitate meeting its own consultation requirement).