Template DPIA for Google Cloud

About this Template DPIA for Google Cloud

This Template has been prepared by Google as a resource to assist customers in complying with their data protection regulatory obligations when using Google Cloud. It should be read in conjunction with the guidance and materials available in our Cloud DPIA Resource Center.

You can use this Template as a guide when you are documenting your data protection impact assessment (DPIA), including how and why you will be processing personal data, the risks you have identified and your mitigation measures. Once recorded, your DPIA assessment should be reviewed on an ongoing basis. In particular, if there are significant changes in how you process data, you should review the risks you documented and assess whether the measures you have put in place are still sufficient to meet your regulatory obligations.

Please note that this Template is just an example of how a DPIA can be structured. There is no set format for a DPIA and you can use any approach you choose, provided it complies with the relevant regulatory obligations. Some data protection authorities have published their own template DPIAs, so you may want to have a look at their suggested formats as well.

> **Important note:** *This Template is only intended to provide Cloud customers with assistance in carrying out DPIA exercises concerning their use of the Cloud Services, as well as a starting point to document their DPIAs as required under the GDPR. This information does not constitute legal advice, and is not a replacement for reviewing guidance issued by the data protection authorities on the subject or seeking independent legal advice where necessary.*

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DPIA information	
Name of the data controller	
Name of the project	
Name of the person(s) responsible for preparing and/or updating this DPIA	
Estimated date the data processing will start	

STEP 1 - Determining if a DPIA is required	
Overview of the project	**Drafting note:** *Briefly describe what your project involves and how personal data will be processed. If helpful, you may refer to a project plan or to your detailed description of the processing in the following section.*
Are any of the mandatory DPIA triggers met?	**Drafting note:** *Indicate whether your personal data processing triggers one of the mandatory DPIA criteria in Article 35(3) GDPR:* ● *Automated processing of personal data involving a systematic and extensive evaluation of personal aspects of individuals (including any profiling), where that processing informs decisions producing legal (or similarly significant) effects on those individuals. For example, if you are using Google Cloud to analyze personal data relating to your employees (e.g., their work performance) and this could impact their individual employment conditions or salary, you will likely need a DPIA.* ● *Large-scale processing of special categories of data, or data regarding criminal convictions or offenses. For example, if you are using Google Cloud to store large datasets of individuals' health data, such as medical records or clinical test results, you will likely need a DPIA.* ● *Systematic monitoring of publicly accessible areas on a large scale. In this context, a publicly accessible area would be any area open to any member of the public. For example, if you intend to integrate your CCTV system with the Cloud Services, e.g. by storing CCTV footage of your office premises in the cloud, you will likely need a DPIA.*

Are any of the indicative DPIA criteria met?	**Drafting note:** *Indicate whether your personal data processing meets any of the nine factors identified by the European Data Protection Board (EDPB) as likely to result in a high risk to the rights and freedoms of individuals:* ● *Your processing involves profiling, evaluation or scoring of individuals (e.g. credit reference scoring).* ● *You make automated decisions using personal data which have legal or similarly significant effects on individuals (e.g. e-recruiting or refusing an online credit application).* ● *You systematically monitor individuals (e.g. CCTV or location tracking).* ● *You process special category data or personal data of a highly personal nature (e.g. medical records).* ● *You process personal data on a large scale (as 'large scale' is not defined in the guidance, this will be a matter for your judgment).* ● *You match or combine different datasets (e.g. if you have obtained a separate dataset from a third party to enrich an existing dataset).* ● *You process data about vulnerable individuals (e.g. children or patients).* ● *You apply new technological or organizational solutions, or you make innovative use of technologies (e.g. Artificial Intelligence).* ● *Your processing prevents individuals from exercising a right, or from using a service or contract (e.g. refusing an individual a loan).* *Also indicate whether you have identified any other factors not listed above relevant to your decision as to whether the processing is likely to result in a high risk, and therefore requiring a DPIA. For example, the EDPB is of the view that many public sector processing operations relying on cloud services are likely to result in a high risk, so you should record whether your organization is a public body or engages in processing of personal data within the public sector.*
Decision whether to conduct a DPIA	**Drafting note:** *Based on the DPIA triggers and other risk factors you have identified above, record your conclusion as to whether you are required by law to prepare a DPIA (or that you have decided to prepare a DPIA even if it is not required by law).* *The GDPR requires that you prepare a DPIA if your processing meets even one of the mandatory triggers in Article 35(3) GDPR. The EDPB is of the view that you will likely need to prepare a DPIA if your processing meets at least two of its indicative DPIA risk criteria, or if you engage in public sector processing operations relying on cloud services.*

STEP 2 - Description of the processing	
Nature of the personal data processed	**Drafting note:** *Describe the types of personal data you will be processing as a controller using Google Cloud, and the scale of the processing, i.e. how much data you will be processing.* *In relation to Google Cloud, you should cover any personal data that your organization processes as a controller, and that falls within the definition of "Customer Personal Data" in the Cloud Data Processing Addendum (CDPA). This could for example include:* • *Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description.* • *Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, performance appraisals, training records, and security records.* • *Financial details, including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information.* • *Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records.* • *Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving license details.* • *Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organizations.* • *Any other personal data controlled by your organization.*
Sensitive personal data processed	**Drafting note:** *Indicate whether the personal data you process includes:* • *special category data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation); or* • *Data relating to criminal convictions and offenses.*

Data subjects whose personal data is processed	**Drafting note:** *Indicate the categories of individuals that the personal data relates to, e.g. employees, other staff such as contractors and temporary workers, customers and clients (including their staff), other end users, suppliers (including their staff), relatives and associates of the above, advisers, consultants and other professional experts, shareholders, members or supporters, and students and pupils.*
Nature of the processing	**Drafting note:** *Describe your processing activities involving personal data, such as how the personal data is obtained, stored and used by your organization. You could also include a flow chart or other visual aids as part of your description.* *Google Cloud comprises over 150 cloud computing, data analytics and machine learning products. When describing how you use them to process the personal data, you may want to refer to how the different available services are described in the Google Cloud Services Summary. If you need more detailed information about the features of each service, see here.* *You can also find information about the infrastructure (e.g. hardware and networks) used for storing and processing Customer Personal Data in our Security Infrastructure Design Overview and Google security overview whitepapers.*
Purposes of the processing	**Drafting note:** *Describe the purposes of the processing, i.e. the reasons why you plan to process personal data and the intended benefits of that processing. If you will be relying on your legitimate interests as a lawful basis to process the data, indicate what those legitimate interests are.* *In addition to describing your own organization's purposes, also mention the purposes for which you instruct your processors to process the data. Note that when you use Google Cloud you engage Google Cloud to process Customer Personal Data on your behalf in furtherance of one or more of your organization's purposes. As a controller of that data, you instruct Google, as your processor, to process the it in accordance with your Cloud Services agreement (including the CDPA) and applicable law, only for the following purposes:* ● *to provide, secure, and monitor the Cloud Services and technical support services supplied under your Cloud Services agreement;* ● *as further specified via your use of Google Cloud and technical support services, or via any other written instructions given by you under the CDPA and acknowledged by Google as such.* *Google will comply with your instructions under the CDPA (unless prohibited by European law) with respect to such processing.*

Retention periods	**Drafting note:** *Indicate for how long you will keep the personal data.* *Note that, unless you decide to delete it earlier, when you use Google Cloud to process personal data, Google will process the Customer Data (including Customer Personal Data) on your behalf:* ● *for the duration of the Term of the CDPA (which will end when the provision of the Cloud Services ends); and* ● *for a short period after the end of the Term until the data is deleted. After a recovery period of up to 30 days, Google will delete the data as soon as reasonably practicable and within a maximum of 180 days, unless the law requires storage. If you wish to retain the data after the end of the Term, you can instruct Google to return it to you before the Term ends using built-in functionality, such as data export tools.* *You can also delete the Customer Data (including Customer Personal Data) at any point during the Term using the built-in functionality of the Cloud Services you use. When you use Cloud Services functionality to delete Customer Data (including Customer Personal Data), Google will delete the data as soon as reasonably practicable and within a maximum of 180 days, unless the law requires storage.* *For more information about retention and deletion, see our Data deletion on Google Cloud page.*
Involvement of third parties	**Drafting note:** *Indicate the identity of any third parties you are sharing personal data with, and describe their involvement in the processing.* *When you use Google Cloud, you will be sharing Customer Personal Data with the Google contracting entity indicated in the CDPA, who will be a processor of that data. You can check the correct entity here.* *Google also uses subprocessors to perform limited activities in connection with Google Cloud, such as technical support services, data center operations, or service maintenance. When you enter into a contract with Google to use Google Cloud, you authorize the appointment of these third parties.* *You can find a list of the subprocessors, as well as information about what activities they support here.*

Data transfers to third countries	**Drafting note:** *Indicate whether the personal data is being transferred to, or accessed from, a country outside of the UK or the European Economic Area (EEA). This could for example happen because you have locations, employees, or third party processors or subprocessors in those countries.* *Given the global nature of Google's public cloud services, we maintain facilities in all regions (globally) to store and process Customer Data (including Customer Personal Data). You can check the locations where Google and its subprocessors maintain facilities.* *Information about the infrastructure, such as hardware and networks, used for processing Customer Data is available in our Security Infrastructure Design Overview and the Google security overview.*

STEP 3 - Engagement with stakeholders	
Internal stakeholders involved in this DPIA	**Drafting note:** *Indicate all key stakeholders within your organization you have decided to involve in the DPIA process, such as your Data Protection Officer (who must always be involved if your organization has one), or other relevant business functions like Legal, Compliance, IT, etc.*
Consultation with data subjects	**Drafting note:** *Indicate whether you have consulted with the individuals whose personal data you will be processing (or their representatives). If you have concluded that this is not necessary, e.g. because you consider that it would be disproportionate or would compromise confidentiality, explain your reasoning.*
Engagement with processors and other third parties	**Drafting note:** *Depending on the circumstances of your processing, you may decide that you need third parties to assist you in completing your DPIA. Indicate whether you have asked your processors to assist, or if you have engaged any other third parties in the process, e.g. information security consultants. While you have engaged Google to provide Google Cloud, there may be other third parties involved in your project.*

STEP 4 - Assessing the necessity and proportionality of the processing	
Lawful basis for the processing	**Drafting note:** *Indicate the GDPR lawful basis you will rely on to process the personal data involved in your project, e.g. consent, performance of a contract, legitimate interests, etc. You may rely on different lawful bases for different aspects of the processing.* *If you will be relying on consent, indicate how you will gather that consent and how it can be withdrawn. You may decide to include a copy of the consent language.* *If you will be relying on your legitimate interests, indicate what those interests are.*
Necessity and purpose limitation	**Drafting note:** *Indicate whether you are satisfied that the personal data will only be processed for the purposes for which it was collected, or for compatible purposes. Also indicate how the processing is necessary to achieve those purposes, and whether you are satisfied that you cannot achieve them without processing the personal data.*
Data quality and minimization	**Drafting note:** *Indicate whether you are satisfied that you have adequate controls in place to ensure the quality of the personal data you process, and that you will not be processing more data than you need to in order to achieve your purposes.* *You may wish to consider whether you could anonymize the data (i.e. process it in a way that the data subjects are no longer identifiable) or pseudonymize the data (i.e. process it in a way that they could only be identified with the use of additional information). Google Cloud offers certain features and functionality that can help you implement these measures, see for example our documentation on De-identifying sensitive data and Pseudonymization.*

Transparency	**Drafting note:** *Indicate how you will be providing individuals with the required information about your processing of their personal data, e.g. via a privacy notice or some other form of communication.* *Note that, among other things, you should inform individuals:* ● *that you will be using the services of third party processors to process the data, including Google and its subprocessors; and* ● *that some of the processing may take place in a country outside the EEA, UK or other countries with adequacy decisions, and that you are satisfied that there are appropriate safeguards in place to protect the data. See the "Supporting your DPIA" section in our DPIA Resource Center on Google's safeguards and security measures for more information.*
Data subject rights	**Drafting note:** *Explain how you will be supporting individuals' rights in relation to their personal data, such as their rights of access, erasure and portability, and how you intend to respond to any requests you receive from individuals exercising those rights.* *Google will enable your organization, in a manner consistent with the functionality of the Google Cloud services (including the Admin Console), to delete, access, rectify or restrict processing of Customer Data (including Customer Personal Data), as well as to export the data.* *If Google's Cloud Data Protection Team receives a request from an individual that relates to Customer Personal Data and identifies your organization, Google will advise that individual to submit their request to you. Google will notify you promptly that it has received the request and will not otherwise respond to it without your authorization.*

Safeguards for data transfers	**Drafting note:** *Where personal data will be transferred to any third countries outside the EEA, the UK or other countries with adequacy decisions, indicate what safeguards are in place to protect the data.* *Both you as the controller and Google as a processor are responsible for ensuring that any such transfers comply with the GDPR's requirements on data transfers. Unless Google has adopted an Alternative Transfer Solution (for example, the EU-U.S. Data Privacy Framework, or "DPF"), then, where data is transferred to a third country, we rely on the EU Commission's approved Standard Contractual Clauses (SCCs), as described in our Google Cloud's Approach to European Standard Contractual Clauses whitepaper. In particular, you may wish to review the section of the whitepaper headed "Google Cloud's Updated Approach to SCCs" to understand which SCC module(s) are applicable with respect to relevant transfers of Customer Personal Data. Our contractual commitments in respect of transfers of Customer Personal Data to third countries are set out in the "Data Processing Locations" section of the CDPA.* *Google will inform our customers, as required by the CDPA, when we adopt the DPF as an Alternative Transfer Solution. Once Google has adopted the DPF as an Alternative Transfer Solution, we will ensure that the relevant international data transfers are made in accordance with it.* *You can find more information about the technical, legal, and organizational safeguards Google has put in place to protect international data transfers in our Safeguards for International Data Transfers with Google Cloud whitepaper. This document includes information about United States law and its applicability to Google Cloud, to help customers with any risk assessments they may need to complete in light of the Court of Justice of the European Union's ruling known as "Schrems II".*
Compliance with approved codes of conduct	**Drafting note:** *Indicate whether the processing will comply with any code of conduct approved by a data protection authority. This is not mandatory but should be taken into account if that is the case.* *Google adheres to the EU GDPR Cloud Code of Conduct with respect to Google Cloud. The Code is a mechanism for cloud providers to demonstrate how they offer sufficient guarantees to implement appropriate technical and organizational measures as processors under the GDPR. See here to find out which Google Cloud Services are in scope.* *The Cloud Code of Conduct was approved by the Belgian Data Protection Authority on 20 May 2021, based on a positive opinion by the European Data Protection Board.*

STEP 5 - Identifying the risks of the processing

Drafting note: *Identify the risks to the rights and freedoms of individuals which could result from your personal data processing. The impact and risks are likely to vary depending on your organization's activities, the nature of the personal data, and the individuals concerned. Examples of possible risks may include:*

- *Surprising or unexpected use of personal data for the individuals.*
- *Loss of control by individuals over their personal data.*
- *Discrimination or bias.*
- *Increased risk of identity theft or fraud.*
- *Invasion of people's personal lives.*
- *Loss of confidentiality.*
- *Re-identification of pseudonymized data.*
- *Revealing sensitive information or information about vulnerable individuals.*
- *Collecting inaccurate information, or making inaccurate assumptions about the individual.*

You may want to include in your assessment your own risks as an organization, such as any risk of reputational damage, regulatory action, or loss of public trust.

Note that there are many ways to assess the data protection impact and risks of a project. The GDPR does not require any particular approach, and you do not have to follow the approach proposed in this template. Some data protection authorities have published materials and tools to help organizations carry out this assessment, which you may find helpful in deciding what approach to take to assessing the risks involved in your project.

Description of the risk	**Likelihood of harm** *(e.g. remote, possible, more likely than not)*	**Severity of harm** *(e.g. minimal, moderate, severe)*	**Overall risk** *(e.g. low, medium, high)*

STEP 6 - Safeguards and security measures to mitigate the risks

Drafting note: *Once you have assessed the level of risk, indicate any steps you plan to take to mitigate those risks, including any technical and organizational measures and other safeguards you plan to implement into your processing. Also indicate if you have gathered any necessary internal approvals to implement those measures prior to starting the processing. At a general level, examples of mitigating steps may include:*

- *Deciding not to collect some of the personal data.*
- *Anonymising or pseudonymizing the data.*
- *Excluding vulnerable individuals or children from the dataset.*
- *Implementing measures to ensure a level of security that is appropriate to the risk.*
- *Implementing internal data handling policies for staff.*
- *Training staff on how to use personal data.*
- *Taking additional steps to inform individuals about how the organization will be handling their personal data.*
- *Giving individuals a choice as to how their personal data will be used.*

Record whether any residual risk will continue to exist even after the measures are implemented. Note that you do not need to entirely eliminate all risks, but you should be able to reduce the overall risks to an acceptable level, in line with your obligations under GDPR. When assessing the residual risks, you can take into account the benefits of your project, including benefits for those individuals.

When you use Google Cloud, your personal data processing benefits from industry-leading security measures implemented and maintained by Google; additional security resources, features, functionality and/or controls available to Google Cloud users, which you may use at your option; and contractual commitments from Google as to technical, organizational and physical security measures.

When you enter into the CDPA, you agree that these measures provide an appropriate level of security in light of the risks involved in your processing, and it may be useful to refer to some of these to describe how you intend to mitigate the risks of your processing.

Security measures implemented by Google

Our Google's Security Infrastructure Design Overview provides more information on how our globally scaled technical infrastructure is designed to provide secure deployment of the Cloud Services, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators. Our Google Security Overview and Google Cloud Security whitepapers provide more specific information about the measures in place for Google Cloud. If you need more information, we offer additional resources about Google's technical and organizational security measures for the Cloud Services at our Security Best Practices Center and Privacy Resource Center.

Optional security controls available in Google Cloud

Google also offers optional additional security controls to help Google Cloud customers meet their security and compliance needs. These are security resources, features, functionality and controls that customers may use at their option, including the Admin Console, encryption solutions, logging and monitoring tools, and identity and access management. Our Google Cloud Architecture Framework describes best practices and implementation recommendations. The framework helps you individually design your Google Cloud deployment so that it matches your business needs.

Contractual commitments provided by Google

The Cloud Data Processing Addendum (CDPA) sets out Google's contractual commitments in respect of Customer Data, including Customer Personal Data. Google commits to implement and maintain technical and organizational measures to protect Customer Data (including Customer Personal Data) against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. These measures are described in more detail in Appendix 2 of the CDPA, and include commitments as to data center and network security, access and site controls, data storage and erasure, personnel security, and subprocessor security.

Google's policy regarding law enforcement requests

Google has developed a transparent and thorough process that meets international best practices when it comes to data access requests from law enforcement agencies and governments. Google provides a response on a case-by-case basis, taking into account different circumstances and informed by legal requirements, customer agreements, and privacy policies. The process Google will follow with respect to any such requests is described in the Government Requests for Cloud Customer Data whitepaper.

Google's security compliance and other certifications

The Cloud Services undergo regular independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance. You can access various certifications (including ISO 27001, 27017, 27018 and 27701), audit reports (including SOC 1, 2 and 3) and other relevant resources via our Compliance Reports Manager. As mentioned above, Google also adheres to the EU GDPR Cloud Code of Conduct, a mechanism for cloud providers to demonstrate how they offer sufficient guarantees to implement appropriate technical and organizational measures as processors under the GDPR.

Risk	**Relevant safeguards and security measures** *(Indicate if the measure is already in place or requires approval)*	**Effect on risk** *(e.g. eliminated, reduced, accepted)*	**Measure approved** *(Yes / No)*	**Residual risk** *(e.g. none, low, medium, high)*

STEP 7 - Record the outcome of the DPIA	
Project approval	**Drafting note:** *In light of the risks identified and your assessment of the necessity and proportionality of the processing, determine whether the project can go ahead.*
Measures approval	**Drafting note:** *Indicate whether you will implement additional measures prior to starting the processing to reduce or eliminate any residual risks you have identified.*
Residual risks accepted	**Drafting note:** *Indicate whether you have decided to accept any residual risks and explain the reasons. If you have concluded that any of the residual risks remain high, you must consult with your supervisory data protection authority before starting the processing.*
Consultation with supervisory authority	**Drafting note:** *If you have consulted with your supervisory authority, record the details of that consultation and its outcome (including, for example, any further measures you have agreed to implement).*
DPIA sign-off and date	**Drafting note:** *Indicate the name and job title of the person signing off the outcome of this DPIA. If this DPIA has been reviewed by your DPO, indicate their name and title, and the date of their review.*

DPIA version control			
Drafting note: *Keep track of any changes to your DPIA as different stakeholders contribute to it, and as you keep it up to date over time.* *Your DPIA should be reviewed on an ongoing basis. If there are any significant changes to how the personal data is processed (e.g., if you decide to use Cloud Services for new workloads or to process different datasets), you should re-assess the risks and determine whether any additional measures may be needed to address them.*			
Version No.	**Description**	**Created / edited by**	**Date**