Spring-2024 Google Cloud Services Statement of Applicability	
Rationale Definitions	
Risk	Control is selected specifically to address an identified risk.
Contractual	Control is selected to fulfill a specific or general contractual obligation.
Regulatory	Control is selected to fulfill a specific or general regulatory obligation.
Culture	Control is selected to fulfill company policy, guidelines, or common practice based on Google's mission and values.

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] 10.1.1 Policy on the use of cryptographic controls	Public cloud PII protection implementation guidance: The public cloud PII processor should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The public cloud PII processor should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.	Terms of Service - External Communication	The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Availability, Confidentiality, Integrity, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] 10.1.1 Policy on the use of cryptographic controls	Public cloud PII protection implementation guidance: The public cloud PII processor should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The public cloud PII processor should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.	Shared responsibility within a cloud computing environment	The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] 10.1.1 Policy on the use of cryptographic controls	Public cloud PII protection implementation guidance: The public cloud PII processor should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The public cloud PII processor should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.	Customer communication of cryptographic protections	The organization provides customers with information regarding default encryption methods used to protect user data. Additional applications of cryptographic protections are documented and shared through public sites.	Confidentiality, Integrity	Risk, Culture, Contractual
ISO/IEC 27018:2019	[ISO 27018] 5.1.1 Policies for information security	Public cloud PII protection implementation guidance: The information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). Contractual agreements should clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question (e.g. a service of an IaaS, PaaS or SaaS category of the cloud computing reference architecture). For example, the allocation of responsibility for application layer controls can differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service on which the cloud service customer can build or layer its own applications. Other information for public cloud PII protection: In some jurisdictions, the public cloud PII processor is directly subject to PII protection legislation. In others, PII protection legislation can apply to the PII controller only. A mechanism to ensure the public cloud PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the public cloud PII processor. The contract can call for independently audited compliance, acceptable to the cloud service customer, e.g. via the implementation of the relevant controls in this document and in ISO/IEC 27002.	Policies for information security	The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 5.1.1 Policies for information security	Public cloud PII protection implementation guidance: The information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). Contractual agreements should clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question (e.g. a service of an IaaS, PaaS or SaaS category of the cloud computing reference architecture). For example, the allocation of responsibility for application layer controls can differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service on which the cloud service customer can build or layer its own applications. Other information for public cloud PII protection: In some jurisdictions, the public cloud PII processor is directly subject to PII protection legislation. In others, PII protection legislation can apply to the PII controller only. A mechanism to ensure the public cloud PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the public cloud PII processor. The contract can call for independently audited compliance, acceptable to the cloud service customer, e.g. via the implementation of the relevant controls in this document and in ISO/IEC 27002.	Equipment siting and protection	The organization has policies and guidelines that govern how to keep the organization’s physical workplaces, facilities, and property safe.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 6.1.1 Information security roles and responsibilities	Public cloud PII protection implementation guidance: The public cloud PII processor should designate a point of contact for use by the cloud service customer regarding the processing of PII under the contract.	Information security roles and responsibilities	The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 7.2.2 Information security awareness, education and training	Public cloud PII protection implementation guidance: Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor (e.g. legal consequences, loss of business and brand or reputational damage), on the staff member (e.g. disciplinary consequences) and on the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII. Other information for public cloud PII protection: In some jurisdictions, the public cloud PII processor can be subject to legal sanctions, including substantial fines directly from the local PII protection authority. In other jurisdictions, the use of International Standards such as this document in setting up the contract between the public cloud PII processor and the cloud service customer should help establish a basis for contractual sanctions for a breach of security rules and procedures.	Information security and privacy awareness, education and training	The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 7.2.2 Information security awareness, education and training	Public cloud PII protection implementation guidance: Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor (e.g. legal consequences, loss of business and brand or reputational damage), on the staff member (e.g. disciplinary consequences) and on the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII. Other information for public cloud PII protection: In some jurisdictions, the public cloud PII processor can be subject to legal sanctions, including substantial fines directly from the local PII protection authority. In other jurisdictions, the use of International Standards such as this document in setting up the contract between the public cloud PII processor and the cloud service customer should help establish a basis for contractual sanctions for a breach of security rules and procedures.	Disciplinary process	The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] 9.2.1 User registration and de-registration	Public cloud PII protection implementation guidance: In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access. The objective specified in ISO/IEC 27002:2013, 9.2 applies. The following sector-specific guidance also applies to the implementation of all of the controls in this subclause. Public cloud PII protection implementation guidance: In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.	Administrator's operational security	Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] 9.2.1 User registration and de-registration	Public cloud PII protection implementation guidance: In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access. The objective specified in ISO/IEC 27002:2013, 9.2 applies. The following sector-specific guidance also applies to the implementation of all of the controls in this subclause. Public cloud PII protection implementation guidance: In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.	User registration and de-registration	The organization maintains formal user registration and de-registration procedures for granting and revoking access.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 9.4.2 Secure log-on procedures	Public cloud PII protection implementation guidance: Where required, the public cloud PII processor should provide secure log-on procedures for any accounts requested by the cloud service customer for cloud service users under its control. The objective specified in ISO/IEC 27002:2013, 9.2 applies. The following sector-specific guidance also applies to the implementation of all of the controls in this subclause. Public cloud PII protection implementation guidance: In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.	Secure log-on procedures	Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 11.2.7 Secure disposal or re-use of equipment	Public cloud PII protection implementation guidance: For the purposes of secure disposal or re-use, equipment containing storage media that can possibly contain PII should be treated as though it does.	Secure disposal or reuse of equipment	The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 12.1.4 Separation of development, testing and operational environments	Public cloud PII protection implementation guidance: Where the use of PII for testing purposes cannot be avoided a risk assessment should be undertaken. Technical and organizational measures should be implemented to minimize the risks identified.	Separation of development, testing and operational environments	Development, testing and build environments are separated from the production environment through the use of logical security controls.	Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 12.3.1 Information backup	Public cloud PII protection implementation guidance: Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Multiple copies of data in physically and/or logically diverse locations (which can be within the information processing system itself) should be created or maintained for the purposes of backup and/or recovery. PII-specific responsibilities in this respect can lie with the cloud service customer. Where the public cloud PII processor explicitly provides backup and restore services to the cloud service customer, the public cloud PII processor should provide clear information to the cloud service customer about the capabilities of the cloud service with respect to backup and restoration of the cloud service customer data. Procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event. The use of sub-contractors to store replicated or backup copies of data being processed is covered by the controls in this document applying to sub-contracted PII processing. Where physical media transfers take place this is also covered by controls in this document. The public cloud PII processor should have a policy which addresses the requirements for backup of information and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup purposes.	Service Redundancy	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Integrity, Availability	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] 12.3.1 Information backup	Public cloud PII protection implementation guidance: Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Multiple copies of data in physically and/or logically diverse locations (which can be within the information processing system itself) should be created or maintained for the purposes of backup and/or recovery. PII-specific responsibilities in this respect can lie with the cloud service customer. Where the public cloud PII processor explicitly provides backup and restore services to the cloud service customer, the public cloud PII processor should provide clear information to the cloud service customer about the capabilities of the cloud service with respect to backup and restoration of the cloud service customer data. Procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event. The use of sub-contractors to store replicated or backup copies of data being processed is covered by the controls in this document applying to sub-contracted PII processing. Where physical media transfers take place this is also covered by controls in this document. The public cloud PII processor should have a policy which addresses the requirements for backup of information and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup purposes.	Shared responsibility within a cloud computing environment	The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] 12.4.1 Event logging	Public cloud PII protection implementation guidance: A process should be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, event logs should record whether or not PII has been changed (added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance. The public cloud PII processor should define criteria regarding if, when and how log information can be made available to or usable by the cloud service customer. These procedures should be made available to the cloud service customer. Where a cloud service customer is permitted to access log records controlled by the public cloud PII processor, the public cloud PII processor should ensure that the cloud service customer can only access records that relate to that cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.	Event logging	Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 12.4.1 Event logging	Public cloud PII protection implementation guidance: A process should be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, event logs should record whether or not PII has been changed (added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance. The public cloud PII processor should define criteria regarding if, when and how log information can be made available to or usable by the cloud service customer. These procedures should be made available to the cloud service customer. Where a cloud service customer is permitted to access log records controlled by the public cloud PII processor, the public cloud PII processor should ensure that the cloud service customer can only access records that relate to that cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.	Administrator's operational security	Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] 12.4.2 Protection of log information	Public cloud PII protection specific implementation guidance: Log information recorded for purposes such as security monitoring and operational diagnostics can contain PII. Measures, such as controlling access (see 9.2.3), should be put in place to ensure that logged information is only used for its intended purposes. A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.	Security logs are protected and access restricted	Security event logs are protected and access is restricted to authorized personnel.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 12.4.2 Protection of log information	Public cloud PII protection specific implementation guidance: Log information recorded for purposes such as security monitoring and operational diagnostics can contain PII. Measures, such as controlling access (see 9.2.3), should be put in place to ensure that logged information is only used for its intended purposes. A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.	Monitoring for security threats	The organization monitors its networks and systems for threats to information security.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 12.4.2 Protection of log information	Public cloud PII protection specific implementation guidance: Log information recorded for purposes such as security monitoring and operational diagnostics can contain PII. Measures, such as controlling access (see 9.2.3), should be put in place to ensure that logged information is only used for its intended purposes. A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.	User Data log Deletion and Retention plans	The organization deletes logs containing User Data in accordance with the documented deletion and retention plans. This control is only applicable to Google Workspace	Confidentiality, Integrity, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] 13.2.1 Information transfer policies and procedures	Public cloud PII protection implementation guidance: Whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where possible, cloud service customers should be asked to put additional measures in place (such as encryption) to ensure that the data can only be accessed at the point of destination and not en route.	Information transfer policies and procedures	The organization has policies and guidelines in place for the exchange of information.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] 13.2.1 Information transfer policies and procedures	Public cloud PII protection implementation guidance: Whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where possible, cloud service customers should be asked to put additional measures in place (such as encryption) to ensure that the data can only be accessed at the point of destination and not en route.	Control of Asset Deliveries	The organization authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items. * Deliveries of Assets GPN's IN and Out of DC's	Confidentiality, Integrity, Availability	Risk, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 16.1.1 Responsibilities and procedures	Public cloud PII protection implementation guidance: An information security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place (see A.9.1). An information security event should not necessarily trigger such a review. An information security event is one that does not result in actual, or the significant probability of, unauthorized access to PII or to any of the public cloud PII processor's equipment or facilities storing PII, and can include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log- on attempts, denial of service attacks and packet sniffing. Public cloud PII protection implementation guidance In the context of the whole cloud computing reference architecture, there can be shared roles in the management of information security incidents and making improvements. There can be a need for the public cloud PII processor to cooperate with the cloud service customer in implementing the controls in this subclause.	Incident Management Team	The organization has a dedicated team responsible for managing security & privacy incidents.	Availability, Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 16.1.1 Responsibilities and procedures	Public cloud PII protection implementation guidance: An information security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place (see A.9.1). An information security event should not necessarily trigger such a review. An information security event is one that does not result in actual, or the significant probability of, unauthorized access to PII or to any of the public cloud PII processor's equipment or facilities storing PII, and can include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log- on attempts, denial of service attacks and packet sniffing. Public cloud PII protection implementation guidance In the context of the whole cloud computing reference architecture, there can be shared roles in the management of information security incidents and making improvements. There can be a need for the public cloud PII processor to cooperate with the cloud service customer in implementing the controls in this subclause.	Incident Response Policy - Management's Responsibility	The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 18.2.1 Independent review of information security	Public cloud PII protection implementation guidance: In cases where individual cloud service customer audits are impractical or can increase risks to security (see 0.1), the public cloud PII processor should make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the public cloud PII processor's policies and procedures. A relevant independent audit as selected by the public cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the public cloud PII processor's processing operations, provided sufficient transparency is provided.	Independent review of information security	The organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] 18.2.1 Independent review of information security	Public cloud PII protection implementation guidance: In cases where individual cloud service customer audits are impractical or can increase risks to security (see 0.1), the public cloud PII processor should make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the public cloud PII processor's policies and procedures. A relevant independent audit as selected by the public cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the public cloud PII processor's processing operations, provided sufficient transparency is provided.	Public cloud PII processor's purpose	The organization only processes user data in accordance with the applicable data processing terms and does not process user data for any other purpose.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.2.1 Obligation to co-operate regarding PII principals' rights	ISO Control: The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. Public cloud PII protection implementation guidance: The PII controller's obligations in this respect can be defined by law, by regulations or by contract. These obligations can include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this can include the correction or deletion of PII in a timely fashion. Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.	Obligation to cooperate regarding PII principals' rights	Customers of the organization's services are provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.2.1 Obligation to co-operate regarding PII principals' rights	ISO Control: The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. Public cloud PII protection implementation guidance: The PII controller's obligations in this respect can be defined by law, by regulations or by contract. These obligations can include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this can include the correction or deletion of PII in a timely fashion. Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.	Customer Control over Customer Data	A service administrator is provided a mechanism to facilitate a service user's right to access, correct, and erase Customer Data pertaining to the user, consistent with the functionality of the services.	Privacy	Regulatory, Contractual, Risk

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] A.2.1 Obligation to co-operate regarding PII principals' rights	ISO Control: The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. Public cloud PII protection implementation guidance: The PII controller's obligations in this respect can be defined by law, by regulations or by contract. These obligations can include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this can include the correction or deletion of PII in a timely fashion. Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.	User Data log Deletion and Retention plans	The organization deletes logs containing User Data in accordance with the documented deletion and retention plans. This control is only applicable to Google Workspace	Confidentiality, Integrity, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.3.1 Public cloud PII processor's purpose	ISO Control: PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer. Public cloud PII protection implementation guidance: Instructions can be contained in the contract between the public cloud PII processor and the cloud service customer including, e.g. the objective and time frame to be achieved by the service. In order to achieve the cloud service customer's purpose, there can be technical reasons why it is appropriate for a public cloud PII processor to determine the method for processing PII, consistent with the general instructions of the cloud service customer but without the cloud service customer's express instruction. For example, in order to efficiently utilize network or processing capacity it can be necessary to allocate specific processing resources depending on certain characteristics of the PII principal. In circumstances where the public cloud PII processor's determination of the processing method involves the collection and use of PII, the public cloud PII processor should adhere to the relevant privacy principles set forth in ISO/IEC 29100. The public cloud PII processor should provide the cloud service customer with all relevant information, in a timely fashion, to allow the cloud service customer to ensure the public cloud PII processor's compliance with purpose specification and limitation principles and ensure that no PII is processed by the public cloud PII processor or any of its sub-contractors for further purposes independent of the instructions of the cloud service customer.	Public cloud PII processor's purpose	The organization only processes user data in accordance with the applicable data processing terms and does not process user data for any other purpose.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.3.2 Public cloud PII processor's commercial use	ISO Control: PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.	Public cloud PII processor's commercial use	The organization will not use customer provided content for advertising purposes as specified in the data processing amendments to Google Cloud Services.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.5.1 Secure erasure of temporary files	ISO Control: Temporary files and documents should be erased or destroyed within a specified, documented period. Public cloud PII protection implementation guidance: Implementation guidance on PII erasure is provided in A.10.3. Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they may not be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used. PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.	Secure erasure of temporary files	The organization has mechanisms in place to erase temporary files from distributed storage systems.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.6.1 PII disclosure notification	ISO Control: The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited. Public cloud PII protection implementation guidance: The public cloud PII processor should provide contractual guarantees that it will: — reject any requests for PII disclosure that are not legally binding; — consult the corresponding cloud service customer where legally permissible before making any PII disclosure; and — accept any contractually agreed requests for PII disclosures that are authorized by the corresponding cloud service customer.	User Data disclosure notification	Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.6.2 Recording of PII disclosures	ISO Control: Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. Public cloud PII protection implementation guidance: PII can be disclosed during the course of normal operations. These disclosures should be recorded (see 12.4.1). Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.	Records of disclosure requests	The organization records requests to disclose user data. The organization's records of requests for user data include information regarding when the request was submitted, the identity of the requester, user data that was requested, any data that had been disclosed, and when disclosure had occurred.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.6.2 Recording of PII disclosures	ISO Control: Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. Public cloud PII protection implementation guidance: PII can be disclosed during the course of normal operations. These disclosures should be recorded (see 12.4.1). Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.	User Data disclosure notification	Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.6.2 Recording of PII disclosures	ISO Control: Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. Public cloud PII protection implementation guidance: PII can be disclosed during the course of normal operations. These disclosures should be recorded (see 12.4.1). Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.	Obligation to cooperate regarding PII principals' rights	Customers of the organization's services are provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	Privacy	Regulatory, Contractual, Risk

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] A.8.1 Disclosure of sub-contracted PII processing	ISO Control: The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use. Public cloud PII protection implementation guidance: Provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud PII processor and the cloud service customer. The contract should specify that sub- contractors can only be commissioned on the basis of a consent that can generally be given by the cloud service customer at the beginning of the service. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract. Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub-contractors, but not any business-specific details. The information disclosed should also include the countries in which sub-contractors can process data (see A.12.1) and the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud PII processor (see A.11.12). Where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available. Where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available.	Public cloud PII processor's purpose	The organization only processes user data in accordance with the applicable data processing terms and does not process user data for any other purpose.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.8.1 Disclosure of sub-contracted PII processing	ISO Control: The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use. Public cloud PII protection implementation guidance: Provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud PII processor and the cloud service customer. The contract should specify that sub- contractors can only be commissioned on the basis of a consent that can generally be given by the cloud service customer at the beginning of the service. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract. Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub-contractors, but not any business-specific details. The information disclosed should also include the countries in which sub-contractors can process data (see A.12.1) and the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud PII processor (see A.11.12). Where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available. Where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available.	Disclosure of Subprocessors of Customer Data and Service Data.	Where the organization is a data processor, the organization maintains and makes available a list of subprocessors and updates that list, as contractually required.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.10.1 Notification of a data breach involving PII	ISO Control: The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII. Public cloud PII protection implementation guidance: Provisions covering the notification of a data breach involving PII should form part of the contract between the public cloud PII processor and the cloud service customer. The contract should specify how the public cloud PII processor will provide the information necessary for the cloud service customer to fulfill his obligation to notify relevant authorities. This notification obligation does not extend to a data breach caused by the cloud service customer or PII principal or within system components for which they are responsible. The contract should also define the maximum delay in notification of a data breach involving PII. In the event that a data breach involving PII has occurred, a record should be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident (including the person in charge and the data recovered) and the fact that the incident resulted in loss, disclosure or alteration of PII. In the event that a data breach involving PII has occurred, the record should also include a description of the data compromised, if known; and if notifications were performed, the steps taken to notify the cloud service customer and/or regulatory agencies. In some jurisdictions, relevant legislation or regulations can require the public cloud PII processor to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a data breach involving PII.	Notification of a data breach	The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.10.2 Retention period for administrative security policies and guidelines control	ISO Control: Copies of security policies and operating procedures should be retained for a specified, documented period on replacement (including updating). Public cloud PII protection implementation guidance: Review of current and historical policies and procedures can be required, e.g. in the cases of customer dispute resolution and investigation by a PII protection authority. A minimum retention period of five years is recommended in the absence of a specific legal or contractual requirement.	Security & Privacy Policies/Guidelines - Retention Period	The organization archives historical security policies and guidelines for a minimum of 6 years.	Privacy	Regulatory, Contractual, Risk

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] A.10.3 PII return, transfer and disposal	ISO Control: The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. Public cloud PII protection implementation guidance: At some point in time, PII can need to be disposed of in some manner. This can involve returning the PII to the cloud service customer, transferring it to another public cloud PII processor or to a PII controller (e.g. as a result of a merger), securely deleting or otherwise destroying it, anonymizing it or archiving it. The public cloud PII processor should provide the information necessary to allow the cloud service customer to ensure that PII processed under a contract is erased (by the public cloud PII processor and any of its sub-contractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the cloud service customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards should be provided for contractually. The public cloud PII processor should develop and implement a policy in respect of the disposition of PII and should make this policy available to cloud service customer. The policy should cover the retention period for PII before its destruction after termination of a contract, to protect the cloud service customer from losing PII through an accidental lapse of the contract.	Data retention and deletion policy	The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	Confidentiality, Privacy	Risk, Culture, Contractual
ISO/IEC 27018:2019	[ISO 27018] A.10.3 PII return, transfer and disposal	ISO Control: The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. Public cloud PII protection implementation guidance: At some point in time, PII can need to be disposed of in some manner. This can involve returning the PII to the cloud service customer, transferring it to another public cloud PII processor or to a PII controller (e.g. as a result of a merger), securely deleting or otherwise destroying it, anonymizing it or archiving it. The public cloud PII processor should provide the information necessary to allow the cloud service customer to ensure that PII processed under a contract is erased (by the public cloud PII processor and any of its sub-contractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the cloud service customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards should be provided for contractually. The public cloud PII processor should develop and implement a policy in respect of the disposition of PII and should make this policy available to cloud service customer. The policy should cover the retention period for PII before its destruction after termination of a contract, to protect the cloud service customer from losing PII through an accidental lapse of the contract.	Removal of cloud service customer assets	The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Confidentiality, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.1 Confidentiality or non-disclosure agreements	ISO Control: Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation. Public cloud PII protection implementation guidance: A confidentiality agreement, in whatever form, between the public cloud PII processor, its employees and its agents should ensure that employees and agents do not disclose PII for purposes independent of the instructions of the cloud service customer (see A.3.1). The obligations of the confidentiality agreement should survive termination of any relevant contract.	Code of Conduct acknowledgement	Personnel of the organization are required to acknowledge the code of conduct.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.2 Restriction of the creation of hardcopy material	ISO Control: The creation of hardcopy material displaying PII should be restricted. Public cloud PII protection implementation guidance: Hardcopy material includes material created by printing.	Event logging	Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.2 Restriction of the creation of hardcopy material	ISO Control: The creation of hardcopy material displaying PII should be restricted. Public cloud PII protection implementation guidance: Hardcopy material includes material created by printing.	Restriction of the creation of hardcopy material	The organization has guidelines in place to restrict the creation of hard copy PII.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.3 Control and logging of data restoration	ISO Control: There should be a procedure for, and a log of, data restoration efforts. Public cloud PII protection implementation guidance: Note, The above control makes generic the following requirement which applies in certain legal jurisdictions. The log of data restoration efforts should contain: the person responsible, a description of the restored data, and the data that were restored manually.	Control and logging of data restoration	Where the organization is a data processor, the organization provides data controllers the mechanism to restore customer data and logs all restoration activity.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.3 Control and logging of data restoration	ISO Control: There should be a procedure for, and a log of, data restoration efforts. Public cloud PII protection implementation guidance: Note, The above control makes generic the following requirement which applies in certain legal jurisdictions. The log of data restoration efforts should contain: the person responsible, a description of the restored data, and the data that were restored manually.	Service Redundancy	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.4 Protecting data on storage media leaving the premises	ISO Control: PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	Management of removable media	The organization has guidelines in place for the management and use of removable media.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.4 Protecting data on storage media leaving the premises	ISO Control: PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	Use of unencrypted portable storage media and devices	The organization prohibits the use of removable media for the storage of PII and SPII unless the data has been encrypted.	Confidentiality, Integrity, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.5 Use of unencrypted portable storage media and devices	ISO Control: Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	Use of unencrypted portable storage media and devices	The organization prohibits the use of removable media for the storage of PII and SPII unless the data has been encrypted.	Confidentiality, Integrity, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.6 Encryption of PII transmitted over public data-transmission networks	ISO Control: PII that is transmitted over public data-transmission networks should be encrypted prior to transmission. Public cloud PII protection implementation guidance: In some cases, e.g. the exchange of e-mail, the inherent characteristics of public data-transmission network systems can require that some header or traffic data be exposed for effective transmission. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance.	Encryption of data-in-transit between users and the organization's production facilities	The organization uses encryption protocols to secure user data in transit between users and the organization's production facilities	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.7 Secure disposal of hardcopy materials	ISO Control: Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Secure disposal or reuse of equipment	The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] A.11.7 Secure disposal of hardcopy materials	ISO Control: Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Restriction of the creation of hardcopy material	The organization has guidelines in place to restrict the creation of hard copy PII.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.8 Unique use of user IDs	ISO Control: If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	Access to information processing resources	Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.	Confidentiality, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.9 Records of authorized users	ISO Control: An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained. Public cloud PII protection implementation guidance: A user profile should be maintained for all users whose access is authorized by the public cloud PII processor. The profile of a user comprises the set of data about that user, including user ID, necessary to implement the technical controls providing authorized access to the information system.	User Access on Demand	Where "on demand request" mechanisms are implemented to restrict human access to production resources, access requests are reviewed and approved by a second individual prior to being granted and the event is logged.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.9 Records of authorized users	ISO Control: An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained. Public cloud PII protection implementation guidance: A user profile should be maintained for all users whose access is authorized by the public cloud PII processor. The profile of a user comprises the set of data about that user, including user ID, necessary to implement the technical controls providing authorized access to the information system.	Periodic Access Review	Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.10 User ID management	ISO Control: De-activated or expired user IDs should not be granted to other individuals. Public cloud PII protection implementation guidance: In the context of the whole cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of user ID management for cloud service users under its control.	User ID management	The organization has mechanisms in place to prevent deactivated or deleted user accounts from being reassigned to new users.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.11 Contract measures	ISO Control: Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor. Public cloud PII protection implementation guidance: Information security and PII protection obligations relevant to the public cloud PII processor can arise directly from applicable law. Where this is not the case, PII protection obligations relevant to the public cloud PII processor should be covered in the contract. The controls in this document, together with the controls in ISO/IEC 27002, are intended as a reference catalogue of measures to assist in entering into an information processing contract in respect of PII. The public cloud PII processor should inform a prospective cloud service customer, before entering into a contract, about the aspects of its services material to the protection of PII. The public cloud PII processor should be transparent about its capabilities during the process of entering into a contract. However, it is ultimately the cloud service customer’s responsibility to ensure that the measures implemented by the public cloud PII processor meet its obligations.	Terms of Service - Security Commitments	The organization's security measures, and a commitment not to degrade security are documented, and made available to customers	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.11 Contract measures	ISO Control: Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor. Public cloud PII protection implementation guidance: Information security and PII protection obligations relevant to the public cloud PII processor can arise directly from applicable law. Where this is not the case, PII protection obligations relevant to the public cloud PII processor should be covered in the contract. The controls in this document, together with the controls in ISO/IEC 27002, are intended as a reference catalogue of measures to assist in entering into an information processing contract in respect of PII. The public cloud PII processor should inform a prospective cloud service customer, before entering into a contract, about the aspects of its services material to the protection of PII. The public cloud PII processor should be transparent about its capabilities during the process of entering into a contract. However, it is ultimately the cloud service customer’s responsibility to ensure that the measures implemented by the public cloud PII processor meet its obligations.	Public cloud PII processor’s purpose	The organization only processes user data in accordance with the applicable data processing terms and does not process user data for any other purpose.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.12 Sub-contracted PII processing	ISO Control: Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor. Public cloud PII protection implementation guidance: The use of sub-contractors to store backup copies is covered by this control (see A.8.1).	Terms of Service - Subprocessing PII	The organization outlines its commitments to data protection in the event of subprocessing of user data. Commitments are made available to customers.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.11.12 Sub-contracted PII processing	ISO Control: Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor. Public cloud PII protection implementation guidance: The use of sub-contractors to store backup copies is covered by this control (see A.8.1).	Obligation to Protect Customer Data (Data Processors/Controllers)	The organization requires subprocessors to meet security & privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the “Subprocessor Data Protection Agreement (SDPA)” addendum to contractual agreements or other data processing terms.	Availability, Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27018:2019	[ISO 27018] A.11.13 Access to data on pre-used data storage space	ISO Control: The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer. Public cloud PII protection implementation guidance: On deletion by a cloud service user of data held in an information system, performance issues can mean that explicit erasure of those data is impractical. This creates the risk that another user can be able to read the data. Such risk should be avoided by specific technical measures. No specific guidance is especially appropriate for dealing with all cases in implementing this control. However, as an example, some cloud infrastructure, platforms or applications will return zeroes if a cloud service user attempts to read storage space which has not been overwritten by that user’s own data.	Separation of customer access to data	Customer access to storage is managed through the application. Unique user IDs are utilized to enforce access separation between customer accounts.	Confidentiality, Privacy	Regulatory, Contractual, Risk

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27018:2019	[ISO 27018] A.12.1 Geographical location of PII	ISO Control: The public cloud PII processor should specify and document the countries in which PII can possibly be stored. Public cloud PII protection implementation guidance: The identities of the countries where PII can possibly be stored should be made available to cloud service customers. The identities of the countries arising from the use of sub-contracted PII processing should be included. Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.	Geographic location of customer data	The organization specifies and documents the countries and/or data center locations in which customer data might possibly be stored and transferred.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27018:2019	[ISO 27018] A.12.2 Intended destination of PII	ISO Control: PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	Encryption of data-in-transit between users and the organization's production facilities	The organization uses encryption protocols to secure user data in transit between users and the organization's production facilities	Privacy	Risk, Culture, Contractual, Regulatory