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 27701:2019	[ISO 27701] 5.1 General	The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII. NOTE In practice, where "information security" is used in ISO/IEC 27001:2013, "information security and privacy" applies instead (see Annex F).	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.2.1 Understanding the organization and its context	A requirement additional to ISO/IEC 27001:2013, 4.1 is: The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor. The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include: - applicable privacy legislation; - applicable regulations; - applicable judicial decisions; - applicable organizational context, - governance, policies,and procedures; - applicable administrative decisions; - applicable contractual requirements.	User data controller vs. processor	The organization identifies and documents where the organization acts as a data processor.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.2.1 Understanding the organization and its context	A requirement additional to ISO/IEC 27001:2013, 4.1 is: The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor. The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include: - applicable privacy legislation; - applicable regulations; - applicable judicial decisions; - applicable organizational context, - governance, policies,and procedures; - applicable administrative decisions; - applicable contractual requirements.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.2.2 Understanding the needs and expectations of interested parties	A requirement additional to ISO/IEC 27001:2013, 4.2 is: The organization shall include among its interested parties (see ISO/IEC 27001:2013, 4.2), those parties having interests or responsibilities associated with the processing of PII, including the PII principals. NOTE 1 Other interested parties can include customers (see 4.4), supervisory authorities, other PII controllers, PII processors and their subcontractors. NOTE 2 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII. NOTE 3 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization be in conformity with specific standards, such as the Management System specified in this document, and/or any relevant set of specifications. These parties can call for independently audited compliance to these standards.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.2.3 Determining the scope of the information security management system	A requirement additional to ISO/IEC 27001:2013, 4.3 is: When determining the scope of the PIMS, the organization shall include the processing of PII. NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.2.4 Information security management system	A requirement additional to ISO/IEC 27001:2013, 4.4 is: The organization shall establish, implement, maintain and continually improve a PIMS in accordance with the requirements of ISO/IEC 27001:2013 Clauses 4 to 10, extended by the requirements in Clause 5.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.3.1 Leadership and commitment	The requirements stated in ISO/IEC 27001:2013, 5.1 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.3.2 Policy	The requirements stated in ISO/IEC 27001:2013, 5.2 along with the interpretation specified in 5.1 of this document, apply.	Internal Privacy Policies	The organization's Privacy Program is documented in written internal policies.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.3.3 Organizational roles, responsibilities and authorities	The requirements stated in ISO/IEC 27001:2013, 5.3 along with the interpretation specified in 5.1 of this document, apply.	Defined and Published Roles and Responsibilities	The organization's privacy roles and responsibilities are defined and published internally.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.4.1.1 General	The requirements stated in ISO/IEC 27001:2013, 6.1.1 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.4.1.2 Information security risk assessment	The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements: ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows: The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS. The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS. The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed. NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII. ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows: The organization shall assess the potential consequences for both the organization and PII principals, that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2.c) as refined above, were to materialize.	Periodic Privacy Risk Assessment	The organization conducts periodic Privacy risk assessments to identify and evaluate risks related to the handling of user data.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.4.1.2 Information security risk assessment	The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements: ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows: The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS. The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS. The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed. NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII. ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows: The organization shall assess the potential consequences for both the organization and PII principals, that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2.c) as refined above, were to materialize.	Periodic privacy risk updates	The organization reviews the risk assessment results and identify opportunities to further reduce or mitigate risk.	Privacy	Risk, Culture, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 5.4.1.2 Information security risk assessment	The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements: ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows: The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS. The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS. The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed. NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII. ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows: The organization shall assess the potential consequences for both the organization and PII principals, that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2.c) as refined above, were to materialize.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.4.1.3 Information security risk treatment	The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions: ISO/IEC 27001:2013, 6.1.3.c) is refined as follows: The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted. When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals. ISO/IEC 27001:2013, 6.1.3.d) is refined as follows: Produce a Statement of Applicability that contains: the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)]; justification for their inclusion whether the necessary controls are implemented or not; and the justification for excluding any of the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1). Not all the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to the PII principal.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.4.1.3 Information security risk treatment	The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions: ISO/IEC 27001:2013, 6.1.3.c) is refined as follows: The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted. When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals. ISO/IEC 27001:2013, 6.1.3.d) is refined as follows: Produce a Statement of Applicability that contains: the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)]; justification for their inclusion whether the necessary controls are implemented or not; and the justification for excluding any of the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1). Not all the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to the PII principal.	Periodic privacy risk updates	The organization reviews the risk assessment results and identify opportunities to further reduce or mitigate risk.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.4.1.3 Information security risk treatment	The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions: ISO/IEC 27001:2013, 6.1.3.c) is refined as follows: The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted. When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals. ISO/IEC 27001:2013, 6.1.3.d) is refined as follows: Produce a Statement of Applicability that contains: the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)]; justification for their inclusion whether the necessary controls are implemented or not; and the justification for excluding any of the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1). Not all the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to the PII principal.	Periodic Privacy Risk Assessment	The organization conducts periodic Privacy risk assessments to identify and evaluate risks related to the handling of user data.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.4.2 Information security objectives and planning to achieve them	The requirements stated in ISO/IEC 27001:2013, 6.2 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.5.1 Resources	The requirements stated in ISO/IEC 27001:2013, 7.1 along with the interpretation specified in 5.1 of this document, apply.	Defined and Published Roles and Responsibilities	The organization's privacy roles and responsibilities are defined and published internally.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.5.2 Competence	The requirements stated in ISO/IEC 27001:2013, 7.2 along with the interpretation specified in 5.1 of this document, apply.	Privacy Subject Matter Experts	A working group of privacy subject matter experts provides oversight to the organization.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.5.3 Awareness	The requirements stated in ISO/IEC 27001:2013, 7.3 along with the interpretation specified in 5.1 of this document, apply.	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 27701:2019	[ISO 27701] 5.5.3 Awareness	The requirements stated in ISO/IEC 27001:2013, 7.3 along with the interpretation specified in 5.1 of this document, apply.	Supplemental Privacy Training	The organization provides supplemental training and awareness programs to employees.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.5.3 Awareness	The requirements stated in ISO/IEC 27001:2013, 7.3 along with the interpretation specified in 5.1 of this document, apply.	Defined and Published Roles and Responsibilities	The organization's privacy roles and responsibilities are defined and published internally.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.5.4 Communication	The requirements stated in ISO/IEC 27001:2013, 7.4 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 5.5.5.1 General	The requirements stated in ISO/IEC 27001:2013, 7.5.1 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.5.5.2 Creating and updating	The requirements stated in ISO/IEC 27001:2013, 7.5.2 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.5.5.3 Control of documented information	The requirements stated in ISO/IEC 27001:2013, 7.5.3 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.6.1 Operational planning and control	The requirements stated in ISO/IEC 27001:2013, 8.1 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.6.2 Information security risk assessment	The requirements stated in ISO/IEC 27001:2013, 8.2 along with the interpretation specified in 5.1 of this document, apply.	Periodic Privacy Risk Assessment	The organization conducts periodic Privacy risk assessments to identify and evaluate risks related to the handling of user data.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.6.3 Information security risk treatment	The requirements stated in ISO/IEC 27001:2013, 8.3 along with the interpretation specified in 5.1 of this document, apply.	Periodic privacy risk updates	The organization reviews the risk assessment results and identify opportunities to further reduce or mitigate risk.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.7.1 Monitoring, measurement, analysis and evaluation	The requirements stated in ISO/IEC 27001:2013, 9.1 along with the interpretation specified in 5.1 of this document, apply.	Program Periodically Reviewed	The organization's privacy program is periodically reviewed for appropriateness.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.7.2 Internal audit	The requirements stated in ISO/IEC 27001:2013, 9.2 along with the interpretation specified in 5.1 of this document, apply.	Tracking action items from Internal Audit testing.	Action items identified from the results of internal audit control testing are assigned an owner and tracked to ensure remediation.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.7.2 Internal audit	The requirements stated in ISO/IEC 27001:2013, 9.2 along with the interpretation specified in 5.1 of this document, apply.	Independent review of privacy	Internal Audit performs a periodic assessment of privacy controls. Results are shared as necessary and are considered for ongoing improvement of the privacy program.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 5.7.3 Management review	The requirements stated in ISO/IEC 27001:2013, 9.3 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.8.1 Nonconformity and corrective action	The requirements stated in ISO/IEC 27001:2013, 10.1 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 5.8.2 Continual improvement	The requirements stated in ISO/IEC 27001:2013, 10.2 along with the interpretation specified in 5.1 of this document, apply.	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 6.2.1.1 Policies for information security	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 5.1.1 and the following additional guidance applies: Additional implementation guidance for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is: Either by the development of separate privacy policies, or by the augmentation of information security policies, the organization should produce a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and/or regulation and with the contractual terms agreed between the organization and its partners, its subcontractors and its applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them. Additional other information for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is: Any organization that processes PII, whether a PII controller or a PII processor, should consider applicable PII protection legislation and/or regulation during the development and maintenance of information security policies."	Privacy Information Management System	The organization maintains and periodically updates the Privacy Information Management System (PIMS).	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 6.2.1.1 Policies for information security	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 5.1.1 and the following additional guidance applies: Additional implementation guidance for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is: Either by the development of separate privacy policies, or by the augmentation of information security policies, the organization should produce a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and/or regulation and with the contractual terms agreed between the organization and its partners, its subcontractors and its applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them. Additional other information for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is: Any organization that processes PII, whether a PII controller or a PII processor, should consider applicable PII protection legislation and/or regulation during the development and maintenance of information security policies."	Internal Privacy Policies	The organization's Privacy Program is documented in written internal policies.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.3.1.1 Information security roles and responsibilities	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.1 and the following additional guidance applies: Additional implementation guidance for 6.1.1, Information security roles and responsibilities, of ISO/IEC 27002:2013 is: The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller, designate a point of contact for PII principals regarding the processing of their PII (see 7.3.2). The organization should appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII. The responsible person should, where appropriate: -be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks; -be involved in the management of all issues which relate to the processing of PII; -be expert in data protection legislation, regulation and practice; -act as a contact point for supervisory authorities; -inform top-level management and employees of the organization of their obligations with respect to the processing of PII; -provide advice in respect of privacy impact assessments conducted by the organization. NOTE Such a person is called a data protection officer in some jurisdictions, which define when such a position is required, along with their position and role. This position can be fulfilled by a staff member or outsourced."	Defined and Published Roles and Responsibilities	The organization's privacy roles and responsibilities are defined and published internally.	Privacy	Risk, Culture, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.3.1.1 Information security roles and responsibilities	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.1 and the following additional guidance applies: Additional implementation guidance for 6.1.1, Information security roles and responsibilities, of ISO/IEC 27002:2013 is: The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller, designate a point of contact for PII principals regarding the processing of their PII (see 7.3.2). The organization should appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII. The responsible person should, where appropriate: -be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks; -be involved in the management of all issues which relate to the processing of PII; -be expert in data protection legislation, regulation and practice; -act as a contact point for supervisory authorities; -inform top-level management and employees of the organization of their obligations with respect to the processing of PII; -provide advice in respect of privacy impact assessments conducted by the organization. NOTE Such a person is called a data protection officer in some jurisdictions, which define when such a position is required, along with their position and role. This position can be fulfilled by a staff member or outsourced."	Privacy Subject Matter Experts	A working group of privacy subject matter experts provides oversight to the organization.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.3.2.1 Mobile device policy	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.2.1 and the following additional guidance applies. The organization should ensure that the use of mobile devices does not lead to a compromise of PII. "	Mobile device policy	The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.4.2.2 Information security awareness, education and training	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.2 and the following additional guidance applies: Additional implementation guidance for 7.2.2, Information security awareness, education and training, of ISO/IEC 27002:2013 is: Measures should be put in place, including awareness of incident reporting, to ensure that relevant staff are aware of the possible consequences to the organization (e.g. legal consequences, loss of business and brand or reputational damage), to the staff member (e.g. disciplinary consequences) and to 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. NOTE Such measures can include the use of appropriate periodic training for personnel having access to PII."	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 27701:2019	[ISO 27701] 6.4.2.2 Information security awareness, education and training	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.2 and the following additional guidance applies: Additional implementation guidance for 7.2.2, Information security awareness, education and training, of ISO/IEC 27002:2013 is: Measures should be put in place, including awareness of incident reporting, to ensure that relevant staff are aware of the possible consequences to the organization (e.g. legal consequences, loss of business and brand or reputational damage), to the staff member (e.g. disciplinary consequences) and to 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. NOTE Such measures can include the use of appropriate periodic training for personnel having access to PII."	Supplemental Privacy Training	The organization provides supplemental training and awareness programs to employees.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.5.2.1 Classification of information	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.1 and the following additional guidance applies: Additional implementation guidance for 8.2.1, Classification of Information, of ISO/IEC 27002:2013 is: The organization's information classification system should explicitly consider PII as part of the scheme it implements. Considering PII within the overall classification system is integral to understanding what PII the organization processes (e.g. type, special categories), where such PII is stored and the systems through which it can flow."	Data Classification	The organization has established policies and guidelines to govern data classification, labeling and security.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.5.2.2 Labelling of information	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.2 and the following additional guidance applies. Additional implementation guidance for 8.2.2, labelling of information, of ISO/IEC 27002:2013 is: The organization should ensure that people under its control are made aware of the definition of PII and how to recognize information that is PII."	Data Classification	The organization has established policies and guidelines to govern data classification, labeling and security.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.5.3.1 Management of removable media	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.1 and the following additional guidance applies: Additional implementation guidance for 8.3.1 Management of removable media, of ISO/IEC 27002:2013 is: The organization should document any use of removable media and/or devices for the storage of PII. Wherever feasible, the organization should use removable physical media and/or devices that permit encryption when storing PII. Unencrypted media should only be used where unavoidable, and in instances where unencrypted media and/or devices are used, the organization should implement procedures and compensating controls (e.g. tamper-evident packaging) to mitigate risks to the PII. Additional other information for 8.3.1 Management of removable media, of ISO/IEC 27002:2013 is: Removable media which is taken outside the physical confines of the organization is prone to loss, damage and inappropriate access. Encrypting removable media adds a level of protection for PII which reduces security and privacy risks should the removable media be compromised."	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.5.3.1 Management of removable media	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.1 and the following additional guidance applies: Additional implementation guidance for 8.3.1 Management of removable media, of ISO/IEC 27002:2013 is: The organization should document any use of removable media and/or devices for the storage of PII. Wherever feasible, the organization should use removable physical media and/or devices that permit encryption when storing PII. Unencrypted media should only be used where unavoidable, and in instances where unencrypted media and/or devices are used, the organization should implement procedures and compensating controls (e.g. tamper-evident packaging) to mitigate risks to the PII. Additional other information for 8.3.1 Management of removable media, of ISO/IEC 27002:2013 is: Removable media which is taken outside the physical confines of the organization is prone to loss, damage and inappropriate access. Encrypting removable media adds a level of protection for PII which reduces security and privacy risks should the removable media be compromised."	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 27701:2019	[ISO 27701] 6.5.3.2 Disposal of media	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.2 and the following additional guidance applies. Additional implementation guidance for 8.3.2 Disposal of media, of ISO/IEC 27002:2013 is: Where removable media on which PII is stored is disposed of, secure disposal procedures should be included in the documented information and implemented to ensure that previously stored PII will not be accessible."	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 27701:2019	[ISO 27701] 6.5.3.2 Disposal of media	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.2 and the following additional guidance applies. Additional implementation guidance for 8.3.2 Disposal of media, of ISO/IEC 27002:2013 is: Where removable media on which PII is stored is disposed of, secure disposal procedures should be included in the documented information and implemented to ensure that previously stored PII will not be accessible."	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 27701:2019	[ISO 27701] 6.5.3.2 Disposal of media	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.2 and the following additional guidance applies. Additional implementation guidance for 8.3.2 Disposal of media, of ISO/IEC 27002:2013 is: Where removable media on which PII is stored is disposed of, secure disposal procedures should be included in the documented information and implemented to ensure that previously stored PII will not be accessible."	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 27701:2019	[ISO 27701] 6.5.3.3 Physical media transfer	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.3 and the following additional guidance applies: Additional implementation guidance for 8.3.3 Physical media transfer, of ISO/IEC 27002:2013 is: If physical media is 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, additional measures such as encryption should be implemented to ensure that the data can only be accessed at the point of destination and not in transit. The organization should subject physical media containing PII before leaving its premises to an authorization procedure and ensure the PII is not accessible to anyone other than authorized personnel. NOTE One possible measure to ensure PII on physical media leaving the organization's premises is not generally accessible is to encrypt the PII concerned and restrict decryption capabilities to authorized personnel."	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 27701:2019	[ISO 27701] 6.6.2.1 User registration and de-registration	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.1 and the following additional guidance applies: Additional implementation guidance for 9.2.1, User registration and de-registration, of ISO/IEC 27002:2013 is: Procedures for registration and de-registration of users who administer or operate systems and services that process PII should address the situation where user access control for those users is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure). The organization should not reissue to users de-activated or expired user IDs for systems and services that process PII. In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of user ID management. Such cases should be included in the documented information. Some jurisdictions impose specific requirements regarding the frequency of checks for unused authentication credentials related to systems that process PII. Organizations operating in these jurisdictions should take compliance with these requirements into account."	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 27701:2019	[ISO 27701] 6.6.2.1 User registration and de-registration	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.1 and the following additional guidance applies: Additional implementation guidance for 9.2.1, User registration and de-registration, of ISO/IEC 27002:2013 is: Procedures for registration and de-registration of users who administer or operate systems and services that process PII should address the situation where user access control for those users is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure). The organization should not reissue to users de-activated or expired user IDs for systems and services that process PII. In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of user ID management. Such cases should be included in the documented information. Some jurisdictions impose specific requirements regarding the frequency of checks for unused authentication credentials related to systems that process PII. Organizations operating in these jurisdictions should take compliance with these requirements into account."	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.6.2.2 User access provisioning	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.2 and the following additional guidance applies: Additional implementation guidance for 9.2.2, User access provisioning, of ISO/IEC 27002:2013 is: The organization should maintain an accurate, up-to-date record of the user profiles created for users who have been authorized access to the information system and the PII contained therein. This profile comprises the set of data about that user, including user ID, necessary to implement the identified technical controls providing authorized access. Implementing individual user access IDs enables appropriately configured systems to identify who accessed PII and what additions, deletions or changes they made. As well as protecting the organization, users are also protected as they can identify what they have processed and what they have not processed. In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of access management. Where appropriate, the organization should provide the customer the means to perform access management, such as by providing administrative rights to manage or terminate access. Such cases should be included in the documented information."	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 27701:2019	[ISO 27701] 6.6.4.2 Secure log-on procedures	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.2 and the following additional guidance applies: Additional implementation guidance for 9.4.2, Secure log-on procedures, of ISO/IEC 27002:2013 is: Where required by the customer, the organization should provide the capability for secure log-on procedures for any user accounts under the customer's control."	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 27701:2019	[ISO 27701] 6.7.1.1 Policy on the use of cryptographic controls	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.1 and the following additional guidance applies: Additional implementation guidance for 10.1.1, Policy on the use of cryptographic controls, of ISO/IEC 27002:2013 is: Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and driver's licence numbers. The organization should provide information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The organization should also provide information to the customer about any capabilities it provides that can assist the customer in applying their 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 27701:2019	[ISO 27701] 6.7.1.1 Policy on the use of cryptographic controls	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.1 and the following additional guidance applies: Additional implementation guidance for 10.1.1, Policy on the use of cryptographic controls, of ISO/IEC 27002:2013 is: Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and driver's licence numbers. The organization should provide information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The organization should also provide information to the customer about any capabilities it provides that can assist the customer in applying their own cryptographic protection."	Policy on the use of cryptographic controls	The organization maintains policies that define the requirements for the use of cryptography.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.7.1.1 Policy on the use of cryptographic controls	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.1 and the following additional guidance applies: Additional implementation guidance for 10.1.1, Policy on the use of cryptographic controls, of ISO/IEC 27002:2013 is: Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and driver's licence numbers. The organization should provide information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The organization should also provide information to the customer about any capabilities it provides that can assist the customer in applying their 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 27701:2019	[ISO 27701] 6.8.2.7 Secure disposal or re-use of equipment	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.7 and the following additional guidance applies: Additional implementation guidance for 11.2.7, Secure disposal or re-use of equipment, of ISO/IEC 27002:2013 is: The organization should ensure that, whenever storage space is re-assigned, any PII previously residing on that storage space is not accessible. On deletion of PII held in an information system, performance issues can mean that explicit erasure of that PII is impractical. This creates the risk that another user can be able to access the PII. Such risk should be avoided by specific technical measures. For secure disposal or re-use, equipment containing storage media that can possibly contain PII should be treated as though it does contain PII."	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 27701:2019	[ISO 27701] 6.8.2.9 Clear desk and clear screen policy	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.9 and the following additional guidance applies: Additional implementation guidance for 11.2.9, Clear desk and clear screen policy, of ISO/IEC 27002:2013 is: The organization should restrict the creation of hardcopy material including PII to the minimum needed to fulfil the identified processing purpose."	Securing unattended workstations	The organization has security policies that require users to lock their workstations and mobile devices when unattended.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory

Google Confidental Information

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.9.3.1 Information backup	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.3.1 and the following additional guidance applies: Additional implementation guidance for 12.3.1 Information backup, of ISO/IEC 27002:2013 is: The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements. PII-specific responsibilities in this respect can depend upon the customer. The organization should ensure that the customer has been informed of the limits of the service regarding backup. Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII. Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should take compliance into account. There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified and processes put in place to resolve them (which can involve the PII principal). The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain: -the name of the person responsible for the restoration; -a description of the restored PII. Some jurisdictions prescribe the content of the logs of PII restoration efforts. Organizations should be able to to document compliance with any applicable jurisdiction specific requirements for restoration log content. The conclusions of such deliberations should be included in documented information. The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing (see 6.5.3.3, 6.12.1.2). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (6.10.2.1)."	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 27701:2019	[ISO 27701] 6.9.3.1 Information backup	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.3.1 and the following additional guidance applies: Additional implementation guidance for 12.3.1 Information backup, of ISO/IEC 27002:2013 is: The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements. PII-specific responsibilities in this respect can depend upon the customer. The organization should ensure that the customer has been informed of the limits of the service regarding backup. Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII. Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should take compliance into account. There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified and processes put in place to resolve them (which can involve the PII principal). The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain: -the name of the person responsible for the restoration; -a description of the restored PII. Some jurisdictions prescribe the content of the logs of PII restoration efforts. Organizations should be able to to document compliance with any applicable jurisdiction specific requirements for restoration log content. The conclusions of such deliberations should be included in documented information. The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing (see 6.5.3.3, 6.12.1.2). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (6.10.2.1)."	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.9.3.1 Information backup	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.3.1 and the following additional guidance applies: Additional implementation guidance for 12.3.1 Information backup, of ISO/IEC 27002:2013 is: The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements. PII-specific responsibilities in this respect can depend upon the customer. The organization should ensure that the customer has been informed of the limits of the service regarding backup. Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII. Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should take compliance into account. There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified and processes put in place to resolve them (which can involve the PII principal). The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain: -the name of the person responsible for the restoration; -a description of the restored PII. Some jurisdictions prescribe the content of the logs of PII restoration efforts. Organizations should be able to to document compliance with any applicable jurisdiction specific requirements for restoration log content. The conclusions of such deliberations should be included in documented information. The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing (see 6.5.3.3, 6.12.1.2). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (6.10.2.1)."	Data restore tests	Restore tests are periodically performed to confirm the ability to recover user data.	Availability, Integrity, Privacy	Risk, Regulatory, Contractual
ISO/IEC 27701:2019	[ISO 27701] 6.9.3.1 Information backup	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.3.1 and the following additional guidance applies: Additional implementation guidance for 12.3.1 Information backup, of ISO/IEC 27002:2013 is: The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements. PII-specific responsibilities in this respect can depend upon the customer. The organization should ensure that the customer has been informed of the limits of the service regarding backup. Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII. Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should take compliance into account. There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified and processes put in place to resolve them (which can involve the PII principal). The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain: -the name of the person responsible for the restoration; -a description of the restored PII. Some jurisdictions prescribe the content of the logs of PII restoration efforts. Organizations should be able to to document compliance with any applicable jurisdiction specific requirements for restoration log content. The conclusions of such deliberations should be included in documented information. The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing (see 6.5.3.3, 6.12.1.2). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (6.10.2.1)."	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 27701:2019	[ISO 27701] 6.9.4.1 Event logging	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.1 and the following additional guidance applies: Additional implementation guidance for 12.4.1, Event logging, of ISO/IEC 27002:2013 is: A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, event logs should record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event. Where multiple service providers are involved in providing services, there can be varied or shared roles in implementing this guidance. These roles should be clearly defined and included in the documented information, and agreement on any log access between providers should be addressed. Implementation guidance for PII processors: The organization should define criteria regarding if, when and how log information can be made available to or usable by the customer. These criteria should be made available to the customer. Where the organization permits its customers to access log records controlled by the organization, the organization should implement appropriate controls to ensure that the customer can only access records that relate to that customer's activities, cannot access any log records which relate to the activities of other customers, and cannot amend the logs in any way."	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

Google Confidental Information

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.9.4.1 Event logging	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.1 and the following additional guidance applies: Additional implementation guidance for 12.4.1, Event logging, of ISO/IEC 27002:2013 is: A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, event logs should record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event. Where multiple service providers are involved in providing services, there can be varied or shared roles in implementing this guidance. These roles should be clearly defined and included in the documented information, and agreement on any log access between providers should be addressed. Implementation guidance for PII processors: The organization should define criteria regarding if, when and how log information can be made available to or usable by the customer. These criteria should be made available to the customer. Where the organization permits its customers to access log records controlled by the organization, the organization should implement appropriate controls to ensure that the customer can only access records that relate to that customer's activities, cannot access any log records which relate to the activities of other customers, and cannot amend the logs in any way."	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 27701:2019	[ISO 27701] 6.9.4.1 Event logging	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.1 and the following additional guidance applies: Additional implementation guidance for 12.4.1, Event logging, of ISO/IEC 27002:2013 is: A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, event logs should record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event. Where multiple service providers are involved in providing services, there can be varied or shared roles in implementing this guidance. These roles should be clearly defined and included in the documented information, and agreement on any log access between providers should be addressed. Implementation guidance for PII processors: The organization should define criteria regarding if, when and how log information can be made available to or usable by the customer. These criteria should be made available to the customer. Where the organization permits its customers to access log records controlled by the organization, the organization should implement appropriate controls to ensure that the customer can only access records that relate to that customer's activities, cannot access any log records which relate to the activities of other customers, and cannot amend the logs in any way."	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 27701:2019	[ISO 27701] 6.9.4.2 Protection of log information	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.2 and the following additional guidance applies: Additional implementation guidance for 12.4.2, Protection of log information, of ISO/IEC 27002:2013 is: Log information recorded for, for example, security monitoring and operational diagnostics, could contain PII. Measures such as controlling access (see ISO/IEC 27002, 9.2.3) should be put in place to ensure that logged information is only used as intended. A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule (see 7.4.7)."	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 27701:2019	[ISO 27701] 6.9.4.2 Protection of log information	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.2 and the following additional guidance applies: Additional implementation guidance for 12.4.2, Protection of log information, of ISO/IEC 27002:2013 is: Log information recorded for, for example, security monitoring and operational diagnostics, could contain PII. Measures such as controlling access (see ISO/IEC 27002, 9.2.3) should be put in place to ensure that logged information is only used as intended. A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule (see 7.4.7)."	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 27701:2019	[ISO 27701] 6.9.4.2 Protection of log information	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.2 and the following additional guidance applies: Additional implementation guidance for 12.4.2, Protection of log information, of ISO/IEC 27002:2013 is: Log information recorded for, for example, security monitoring and operational diagnostics, could contain PII. Measures such as controlling access (see ISO/IEC 27002, 9.2.3) should be put in place to ensure that logged information is only used as intended. A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule (see 7.4.7)."	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 27701:2019	[ISO 27701] 6.10.2.1 Information transfer policies and procedures	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.1 and the following additional guidance applies: Additional implementation guidance for 13.2.1, Information transfer policies and procedures, of ISO/IEC 27002:2013 is: The organization should consider procedures for ensuring that rules related to the processing of PII are enforced throughout and outside of the system, where applicable."	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
ISO/IEC 27701:2019	[ISO 27701] 6.10.2.1 Information transfer policies and procedures	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.1 and the following additional guidance applies: Additional implementation guidance for 13.2.1, Information transfer policies and procedures, of ISO/IEC 27002:2013 is: The organization should consider procedures for ensuring that rules related to the processing of PII are enforced throughout and outside of the system, where applicable."	Basis for user data transfer between jurisdictions	Where the organization is a data processor, the organization informs controllers of the basis for transferring user data between jurisdictions.	Privacy	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.10.2.4 Confidentiality or non-disclosure agreements	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.4 and the following additional guidance applies: Additional implementation guidance for 13.2.4, Confidentiality or non-disclosure agreements, of ISO/IEC 27002: 2013 is: The organization should ensure that individuals operating under its control with access to PII are subject to a confidentiality obligation. The confidentiality agreement, whether part of a contract or separate, should specify the length of time the obligations should be adhered to. When the organization is a PII processor, a confidentiality agreement, in whatever form, between the organization, its employees and its agents should ensure that employees and agents comply with the policy and procedures concerning data handling and protection."	Confidentiality agreements with employees	The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.10.2.4 Confidentiality or non-disclosure agreements	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.4 and the following additional guidance applies: Additional implementation guidance for 13.2.4, Confidentiality or non-disclosure agreements, of ISO/IEC 27002: 2013 is: The organization should ensure that individuals operating under its control with access to PII are subject to a confidentiality obligation. The confidentiality agreement, whether part of a contract or separate, should specify the length of time the obligations should be adhered to. When the organization is a PII processor, a confidentiality agreement, in whatever form, between the organization, its employees and its agents should ensure that employees and agents comply with the policy and procedures concerning data handling and protection."	Code of Conduct acknowledgement	Personnel of the organization are required to acknowledge the code of conduct.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.11.1.2 Securing application services on public networks	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.2 and the following additional guidance applies: Additional implementation guidance for 14.1.2, Securing application services on public networks, of ISO/IEC 27002: 2013 is: The organization should ensure that PII that is transmitted over untrusted data transmission networks is encrypted for transmission. Untrusted networks can include the public internet and other facilities outside of the operational control of the organization. NOTE In some cases (e.g. the exchange of e-mail) the inherent characteristics of untrusted data transmission network systems can require that some header or traffic data be exposed for effective transmission."	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 27701:2019	[ISO 27701] 6.11.2.5 Secure systems engineering principles	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.5 and the following additional guidance applies: Additional implementation guidance for 14.2.5, Secure systems engineering principles, of ISO/IEC 27002:2013 is: Systems and/or components related to the processing of PII should be designed following the principles of privacy by design and privacy by default, and to anticipate and facilitate the implementation of relevant controls (as described in clauses 7 and 8, for PII controllers and PII processors, respectively), in particular such that the collection and processing of PII in those systems is limited to what is necessary for the identified purposes of the processing of PII (see 7.2). For example, an organization that processes PII should ensure that, based on the relevant jurisdiction, it disposes of PII after a specified period. The system that processes that PII should be designed in a way to facilitate this deletion requirement."	Privacy Reviews	The organization performs privacy reviews prior to product launch.	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 6.11.2.7 Outsourced development	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.7 and the following additional guidance applies. Additional implementation guidance for 14.2.7, Outsourced development, of ISO/IEC 27002:2013 is: The same principles (see 6.11.2.5) of privacy by design and privacy by default should be applied, if applicable, to outsourced information systems."	Privacy Reviews	The organization performs privacy reviews prior to product launch.	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 6.11.3.1 Protection of test data	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.3.1 and the following additional guidance applies: Additional implementation guidance for 14.3.1, Protection of test data, of ISO/IEC 27002:2013 is: PII should not be used for testing purposes; false or synthetic PII should be used. Where the use of PII for testing purposes cannot be avoided, technical and organizational measures equivalent to those used in the production environment should be implemented to minimize the risks. Where such equivalent measures are not feasible, a risk-assessment should be undertaken and used to inform the selection of appropriate mitigating controls."	Privacy Reviews	The organization performs privacy reviews prior to product launch.	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 6.11.3.1 Protection of test data	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.3.1 and the following additional guidance applies: Additional implementation guidance for 14.3.1, Protection of test data, of ISO/IEC 27002:2013 is: PII should not be used for testing purposes; false or synthetic PII should be used. Where the use of PII for testing purposes cannot be avoided, technical and organizational measures equivalent to those used in the production environment should be implemented to minimize the risks. Where such equivalent measures are not feasible, a risk-assessment should be undertaken and used to inform the selection of appropriate mitigating controls."	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 27701:2019	[ISO 27701] 6.12.1.2 Addressing security within supplier agreements	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.2 and the following additional guidance applies: Additional implementation guidance for 15.1.2, Addressing security within supplier agreements, of ISO/IEC 27002: 2013 is: The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and PII protection obligations (see 7.2.6 and 8.2.1). Supplier agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its applicable third parties (customers, suppliers, etc.) taking into account the type of PII processed. The agreements between the organization and its suppliers should provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation and/or regulation. The agreements should call for independently audited compliance, acceptable to the customer. NOTE For such audit purposes, compliance with relevant and applicable security and privacy standards such as ISO/IEC 27001 or this document can be considered. Implementation guidance for PII processors. The organization should specify in contracts with any suppliers that PII is only processed on its instructions.]"	Obligation to Protect User Data (Service Providers)	The organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.12.1.2 Addressing security within supplier agreements	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.2 and the following additional guidance applies: Additional implementation guidance for 15.1.2, Addressing security within supplier agreements, of ISO/IEC 27002: 2013 is: The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and PII protection obligations (see 7.2.6 and 8.2.1). Supplier agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its applicable third parties (customers, suppliers, etc.) taking into account the type of PII processed. The agreements between the organization and its suppliers should provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation and/or regulation. The agreements should call for independently audited compliance, acceptable to the customer. NOTE For such audit purposes, compliance with relevant and applicable security and privacy standards such as ISO/IEC 27001 or this document can be considered. Implementation guidance for PII processors. The organization should specify in contracts with any suppliers that PII is only processed on its instructions.]"	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 27701:2019	[ISO 27701] 6.13.1.1 Responsibilities and procedures	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.1 and the following additional guidance applies: Additional implementation guidance for 16.1.1, Responsibilities and procedures, of ISO/IEC 27002:2013 is: As part of the overall information security incident management process, the organization should establish responsibilities and procedures for the identification and recording of breaches of PII. Additionally, the organization should establish responsibilities and procedures related to notification to required parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation and/or regulation. Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure that they can demonstrate compliance with these regulations."	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 27701:2019	[ISO 27701] 6.13.1.1 Responsibilities and procedures	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.1 and the following additional guidance applies: Additional implementation guidance for 16.1.1, Responsibilities and procedures, of ISO/IEC 27002:2013 is: As part of the overall information security incident management process, the organization should establish responsibilities and procedures for the identification and recording of breaches of PII. Additionally, the organization should establish responsibilities and procedures related to notification to required parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation and/or regulation. Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure that they can demonstrate compliance with these regulations."	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 27701:2019	[ISO 27701] 6.13.1.1 Responsibilities and procedures	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.1 and the following additional guidance applies: Additional implementation guidance for 16.1.1, Responsibilities and procedures, of ISO/IEC 27002:2013 is: As part of the overall information security incident management process, the organization should establish responsibilities and procedures for the identification and recording of breaches of PII. Additionally, the organization should establish responsibilities and procedures related to notification to required parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation and/or regulation. Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure that they can demonstrate compliance with these regulations."	Incident reporting	The organization has an incident response program for responding to privacy incidents. Privacy incidents are monitored and tracked in accordance with internal policy.	Privacy	Regulatory, Contractual, Risk

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.13.1.5 Response to information security incidents	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.5 and the following additional guidance applies: Additional implementation guidance for 16.1.5, Response to information security incidents, of ISO/IEC 27002:2013 is: Implementation guidance for PII controllers An incident that involves PII should trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving PII that requires a response has taken place. An event does not necessarily trigger such a review. NOTE 1 An information security event does not necessarily result in actual, or the significant probability of, unauthorized access to PII or to any of the organization’s equipment or facilities storing PII. These can include, but are not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing. When a breach of PII has occurred, response procedures should include relevant notifications and records. Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals. Notifications should be clear and can be required. NOTE 2 Notification can contain details such as: — a contact point where more information can be obtained; — a description of and the likely consequences of the breach; — a description of the breach including the number of individuals concerned as well as the number of records concerned; — measures taken or planned to be taken. NOTE 3 Information on the management of security incidents can be found in the ISO/IEC 27035 series. Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as: — 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); — the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII. In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify PII principals, regulatory agencies or customers. Implementation guidance for PII processors Provisions covering the notification of a breach involving PII should form part of the contract between the organization and the customer. The contract should specify how the organization will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or PII principal or within system components for which they are responsible. The contract should also define expected and externally mandated limits for notification response times. In some jurisdictions, the PII processor should notify the PII controller of the existence of a breach without undue delay (i.e. as soon as possible), preferably, as soon as it is discovered so that the PII controller can take the appropriate actions. Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as: — 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); — the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII. In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify the customer and/or the regulatory agencies. In some jurisdictions, applicable legislation and/or regulation can require the organization to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a breach involving PII. "	Incident reporting	The organization has an incident response program for responding to privacy incidents. Privacy incidents are monitored and tracked in accordance with internal policy.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27701:2019	[ISO 27701] 6.15.1.1. Identification of applicable legislation and contractual requirements.	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.1 and the following additional guidance applies: Additional other information for 18.1.1, Identification of applicable legislation and contractual requirements, of ISO/IEC 27002:2013 is: The organization should identify any potential legal sanctions (which can result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority. In some jurisdictions, International Standards such as this document can be used to form the basis for a contract between the organization and the customer, outlining their respective security, privacy and PII protection responsibilities. The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities."	Identification of applicable legislation and contractual requirements	The approach to meeting relevant statutory, regulatory, and contractual requirements is defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.15.1.3 Protection of records	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.3 and the following additional guidance applies: Additional implementation guidance for 18.1.3, Protection of records, of ISO/IEC 27002:2013 is: Review of current and historical policies and procedures can be required (e.g. in the cases of customer dispute resolution and investigation by a supervisory authority). The organization should retain copies of its privacy policies and associated procedures for a period as specified in its retention schedule (see 7.2.8). This includes retention of previous versions of these documents when they are updated."	Retention period for privacy policies and guidelines	The organization retains historical privacy policies for a minimum duration of 5 years.	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 6.15.2.1 Independent review of information security	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.1 and the following additional guidance applies: Additional implementation guidance for 18.2.1, Independent review of information security, of ISO/IEC 27002:2013 is: Where an organization is acting as a PII processor, and where individual customer audits are impractical or can increase risks to security, the organization should make available to 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 organization’s policies and procedures. A relevant independent audit, as selected by the organization, should normally be an acceptable method for fulfilling the customer's interest in reviewing the organization’s processing operations, if it covers the needs of anticipated users and if results are provided in a sufficient transparent manner."	Independent review of privacy	Internal Audit performs a periodic assessment of privacy controls. Results are shared as necessary and are considered for ongoing improvement of the privacy program.	Privacy	Risk, Culture, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.15.2.3 Technical compliance review	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.3 and the following additional guidance applies: Additional implementation guidance for 18.2.3, Technical compliance review, of ISO/IEC 27002:2013 is: As part of technical reviews of compliance with security policies and standards, the organization should include methods of reviewing those tools and components related to processing PII. This can include: ongoing monitoring to verify that only permitted processing is taking place; and/or specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organizational requirements)."	Privacy Reviews	The organization performs privacy reviews prior to product launch.	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] 6.15.2.3 Technical compliance review	"The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.3 and the following additional guidance applies: Additional implementation guidance for 18.2.3, Technical compliance review, of ISO/IEC 27002:2013 is: As part of technical reviews of compliance with security policies and standards, the organization should include methods of reviewing those tools and components related to processing PII. This can include: ongoing monitoring to verify that only permitted processing is taking place; and/or specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organizational requirements)."	Independent review of privacy	Internal Audit performs a periodic assessment of privacy controls. Results are shared as necessary and are considered for ongoing improvement of the privacy program.	Privacy	Risk, Culture, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.2.1 Customer agreement	"Control The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization). Implementation guidance The contract between the organization and the customer should include the following wherever relevant, and depending on the customer's role (PII controller or PII processor) (this list is neither definitive nor exhaustive): - privacy by design and privacy by default (see 7.4, 8.4); - achieving security of processing; notification of breaches involving PII to a supervisory authority; - notification of breaches involving PII to customers and PII principals; - conducting Privacy Impact Assessments (PIA); and - the assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed. Some jurisdictions require that the contract include the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of PII principals."	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 27701:2019	[ISO 27701] B.8.2.1 Customer agreement	"Control The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization). Implementation guidance The contract between the organization and the customer should include the following wherever relevant, and depending on the customer's role (PII controller or PII processor) (this list is neither definitive nor exhaustive): - privacy by design and privacy by default (see 7.4, 8.4); - achieving security of processing; notification of breaches involving PII to a supervisory authority; - notification of breaches involving PII to customers and PII principals; - conducting Privacy Impact Assessments (PIA); and - the assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed. Some jurisdictions require that the contract include the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of PII principals."	Scope limitations for processing	Where the organization is a data processor, the organization limits scope of processing to what is specified in contracts with the controller.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.2.2 Organization's purposes	"Control The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expresses in the documented instructions of the customer. Implementation guidance The contract between the organization and the customer should include, but not be limited to, the objective and time frame to be achieved by the service. In order to achieve the customer's purpose, there can be technical reasons why it is appropriate for the organization to determine the method for processing PII, consistent with the general instructions of the customer but without the 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. The organization should allow the customer to verify their compliance with the purpose specification and limitation principles. This also ensures that no PII is processed by the organization or any of its subcontractors for other purposes than those expressed in the instructions of the customer."	Privacy Reviews	The organization performs privacy reviews prior to product launch.	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] B.8.2.2 Organization's purposes	"Control The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expresses in the documented instructions of the customer. Implementation guidance The contract between the organization and the customer should include, but not be limited to, the objective and time frame to be achieved by the service. In order to achieve the customer's purpose, there can be technical reasons why it is appropriate for the organization to determine the method for processing PII, consistent with the general instructions of the customer but without the 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. The organization should allow the customer to verify their compliance with the purpose specification and limitation principles. This also ensures that no PII is processed by the organization or any of its subcontractors for other purposes than those expressed in the instructions of the 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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] B.8.2.2 Organization's purposes	"Control The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expresses in the documented instructions of the customer. Implementation guidance The contract between the organization and the customer should include, but not be limited to, the objective and time frame to be achieved by the service. In order to achieve the customer's purpose, there can be technical reasons why it is appropriate for the organization to determine the method for processing PII, consistent with the general instructions of the customer but without the 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. The organization should allow the customer to verify their compliance with the purpose specification and limitation principles. This also ensures that no PII is processed by the organization or any of its subcontractors for other purposes than those expressed in the instructions of the customer."	Scope limitations for processing	Where the organization is a data processor, the organization limits scope of processing to what is specified in contracts with the controller.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.2.3 Marketing and advertising use	"Control The organization shall not use PII processed under a contract for the purposes of marketing and advertising without prior consent from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service. Implementation guidance Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing and/or advertising is planned. Organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals. NOTE This control is in addition to the more general control in 8.2.2 and does not replace or otherwise supersede it "	Scope limitations for processing	Where the organization is a data processor, the organization limits scope of processing to what is specified in contracts with the controller.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.2.3 Marketing and advertising use	"Control The organization shall not use PII processed under a contract for the purposes of marketing and advertising without prior consent from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service. Implementation guidance Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing and/or advertising is planned. Organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals. NOTE This control is in addition to the more general control in 8.2.2 and does not replace or otherwise supersede it "	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 27701:2019	[ISO 27701] B.8.2.3 Marketing and advertising use	"Control The organization shall not use PII processed under a contract for the purposes of marketing and advertising without prior consent from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service. Implementation guidance Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing and/or advertising is planned. Organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals. NOTE This control is in addition to the more general control in 8.2.2 and does not replace or otherwise supersede it "	Privacy Reviews	The organization performs privacy reviews prior to product launch.	Privacy	Risk, Culture
ISO/IEC 27701:2019	[ISO 27701] B.8.2.3 Marketing and advertising use	"Control The organization shall not use PII processed under a contract for the purposes of marketing and advertising without prior consent from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service. Implementation guidance Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing and/or advertising is planned. Organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals. NOTE This control is in addition to the more general control in 8.2.2 and does not replace or otherwise supersede it "	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 27701:2019	[ISO 27701] B.8.2.4 Infringing instruction	"Control The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation. Implementation guidance The organization's ability to verify if the instruction infringes legislation and/or regulation can depend on the technological context, on the instruction itself, and on the contract between the organization and the customer."	External User Feedback for Privacy Concerns	The organization has established feedback processes that give external users the ability to voice privacy concerns, which are monitored.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27701:2019	[ISO 27701] B.8.2.4 Infringing instruction	"Control The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation. Implementation guidance The organization's ability to verify if the instruction infringes legislation and/or regulation can depend on the technological context, on the instruction itself, and on the contract between the organization and the customer."	Facilitating compliance with obligations	Where the organization is a data processor, the organization documents their legal, regulatory, and business obligations to controllers related to the processing of the user data within written contracts.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.2.5 - Customer obligations	"Control The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations. Implementation guidance The information needed by the customer can include whether the organization allows for and contributes to audits conducted by the customer or another auditor mandated or otherwise agreed by the customer."	Facilitating compliance with obligations	Where the organization is a data processor, the organization documents their legal, regulatory, and business obligations to controllers related to the processing of the user data within written contracts.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.2.5 - Customer obligations	"Control The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations. Implementation guidance The information needed by the customer can include whether the organization allows for and contributes to audits conducted by the customer or another auditor mandated or otherwise agreed by the customer."	Policies for access, correction and/or erasure	Where the organization is a data processor, the organization has policies regarding its obligations to customers' ability to access, correct and/or erase their user data.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.2.6 Records related to processing PII	"Control The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer. Implementation guidance Some jurisdictions can require the organization to record information such as: categories of processing carried out on behalf of each customer; transfers to third countries or international organizations; and a general description of the technical and organizational security measures."	Records of Processing	Where the organization is a data processor, the organization maintains the necessary records of processing in accordance with contractual obligations to controllers.	Privacy	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] B.8.3.1 Obligations to PII principals	"Control The organization shall provide the customer with the means to comply with its obligations related to PII principals. Implementation guidance A PII controller's obligations can be defined by legislation, by regulation and/or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion. Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a 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
ISO/IEC 27701:2019	[ISO 27701] B.8.3.1 Obligations to PII principals	"Control The organization shall provide the customer with the means to comply with its obligations related to PII principals. Implementation guidance A PII controller's obligations can be defined by legislation, by regulation and/or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion. Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a contract."	Policies for access, correction and/or erasure	Where the organization is a data processor, the organization has policies regarding its obligations to customers' ability to access, correct and/or erase their user data.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.3.1 Obligations to PII principals	"Control The organization shall provide the customer with the means to comply with its obligations related to PII principals. Implementation guidance A PII controller's obligations can be defined by legislation, by regulation and/or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion. Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a 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 27701:2019	[ISO 27701] B.8.3.1 Obligations to PII principals	"Control The organization shall provide the customer with the means to comply with its obligations related to PII principals. Implementation guidance A PII controller's obligations can be defined by legislation, by regulation and/or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion. Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a contract."	Providing copy of user data processed	The organization provides a mechanism for users to export a copy of their data in their Google Accounts to a machine-readable format, where feasible.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.3.1 Obligations to PII principals	"Control The organization shall provide the customer with the means to comply with its obligations related to PII principals. Implementation guidance A PII controller's obligations can be defined by legislation, by regulation and/or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion. Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a 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 27701:2019	[ISO 27701] B.8.4.1 Temporary files	"Control The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period. Implementation guidance The organization should perform periodic verification that unused temporary files are deleted within the identified time period. Other information 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 cannot 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."	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 27701:2019	[ISO 27701] B.8.4.2 Return, transfer or disposal of PII	"Control The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer. 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 customer, transferring it to another organization or to a PII controller (e.g. as a result of a merger), deleting or otherwise destroying it, de-identifying it or archiving it. The capability for the return, transfer and/or disposal of PII should be managed in a secure manner. The organization should provide the assurance necessary to allow the customer to ensure that PII processed under a contract is erased (by the organization and any of its subcontractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the identified purposes of the customer. The organization should develop and implement a policy in respect to the disposal of PII and should make this policy available to customer when requested. The policy should cover the retention period for PII before its disposal after termination of a contract, to protect the customer from losing PII through an accidental lapse of the contract. NOTE This control and guidance is also relevant under the retention principle (see 7.4.7). "	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 27701:2019	[ISO 27701] B.8.4.3 PII transmission controls	"Control The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination. Implementation guidance Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes (including the retention of audit data) to ensure that PII is transmitted without compromise to the correct recipients. Requirements for transmission controls can be included in the PII processor – customer contract. Where no contractual requirements related to transmission are in place, it can be appropriate to take advice from the customer prior to transmission."	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] B.8.5.1 Basis for PII transfer between jurisdictions	"Control The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract. Implementation guidance PII transfer between jurisdictions can be subject to legislation and/or regulation depending on the jurisdiction or organization to which PII is to be transferred (and from where it originates). The organization should document compliance with such requirements as the basis for transfer. The organization should inform the customer of any transfer of PII, including transfers to: - suppliers; - other parties; - other countries or international organizations. In case of changes, the organization should inform the customer in advance, according to an agreed timeframe, so that the customer has the ability to object to such changes or to terminate the contract. The agreement between the organization and the customer can have clauses where the organization can implement changes without informing the customer. In these cases, the limits of this allowance should be set (e.g. the organization can change suppliers without informing the customer, but cannot transfer PII to other countries). In case of international transfer of PII, agreements such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the countries involved and the circumstances in which such agreements apply, should be identified."	Basis for user data transfer between jurisdictions	Where the organization is a data processor, the organization informs controllers of the basis for transferring user data between jurisdictions.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.5.1 Basis for PII transfer between jurisdictions	"Control The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract. Implementation guidance PII transfer between jurisdictions can be subject to legislation and/or regulation depending on the jurisdiction or organization to which PII is to be transferred (and from where it originates). The organization should document compliance with such requirements as the basis for transfer. The organization should inform the customer of any transfer of PII, including transfers to: - suppliers; - other parties; - other countries or international organizations. In case of changes, the organization should inform the customer in advance, according to an agreed timeframe, so that the customer has the ability to object to such changes or to terminate the contract. The agreement between the organization and the customer can have clauses where the organization can implement changes without informing the customer. In these cases, the limits of this allowance should be set (e.g. the organization can change suppliers without informing the customer, but cannot transfer PII to other countries). In case of international transfer of PII, agreements such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the countries involved and the circumstances in which such agreements apply, should be identified."	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 27701:2019	[ISO 27701] B.8.5.2 Countries and international organizations to which PII can be transferred	"Control The organization shall specify and document the countries and international organizations to which PII can possibly be transferred. Implementation guidance The identities of the countries and international organizations to which PII might possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 8.5.1. Outside of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation."	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 27701:2019	[ISO 27701] B.8.5.2 Countries and international organizations to which PII can be transferred	"Control The organization shall specify and document the countries and international organizations to which PII can possibly be transferred. Implementation guidance The identities of the countries and international organizations to which PII might possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 8.5.1. Outside of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation."	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 27701:2019	[ISO 27701] B.8.5.2 Countries and international organizations to which PII can be transferred	"Control The organization shall specify and document the countries and international organizations to which PII can possibly be transferred. Implementation guidance The identities of the countries and international organizations to which PII might possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 8.5.1. Outside of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation."	Basis for user data transfer between jurisdictions	Where the organization is a data processor, the organization informs controllers of the basis for transferring user data between jurisdictions.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.5.3 Records of PII disclosure to third parties	"Control The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when. Implementation guidance PII can be disclosed during the course of normal operations. These disclosures should be recorded. 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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] B.8.5.4 Notification of PII disclosure requests	"Control The organization shall notify the customer of any legally binding requests for disclosure of PII. Implementation guidance The organization can receive legally binding requests for disclosure of PII (e.g. from law enforcement authorities). In these cases, the organization should notify the customer of any such request within agreed timeframes and according to an agreed procedure (which can be included in the customer contract). In some cases, the legally binding requests include the requirement for the organization not to notify anyone about the event (an example of a possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation)."	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 27701:2019	[ISO 27701] B.8.5.5 Legally binding PII disclosures	"Control The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer. Implementation guidance Details relevant to the implementation of the control can be included in the customer contract. Such requests can originate from several sources, including courts, tribunals and administrative authorities. They can arise from any jurisdiction."	Legally binding government requests	The organization reviews government agency requests for user data to determine if disclosure is required; subsequent disclosure is then limited only to that which is necessary to fulfill the request.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.5.6 Disclosure of subcontractors used to process PII	Control The organization shall disclose any use of subcontractors to process PII to the customer before use. Implementation guidance Provisions for the use of subcontractors to process PII should be included in the customer contract. Information disclosed should cover the fact that subcontracting is used and the names of relevant subcontractors. The information disclosed should also include the countries and international organizations to which subcontractors can transfer data (see 8.5.2) and the means by which subcontractors are obliged to meet or exceed the obligations of the organization (see 8.5.7). Where public disclosure of subcontractor 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 customer. The customer should be made aware that the information is available. This does not concern the list of countries where the PII can be transferred. This list should be disclosed to the customer in all cases in a way that allows them to inform the appropriate PII principals.	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 27701:2019	[ISO 27701] B.8.5.7 Engagement of a subcontractor to process PII	"Control The organization shall only engage a subcontractor to process PII according to the customer contract. Implementation guidance Where the organization subcontracts some or all of the processing of that PII to another organization, a written authorization from the customer is required prior to the PII processed by the subcontractor. This can be in the form of appropriate clauses in the customer contract, or can be a specific ""one-off"" agreement. The organization should have a written contract with any subcontractors that it uses for PII processing on its behalf, and should ensure that their contracts with subcontractors address the implementation of the appropriate controls in Annex B. The contract between the organization and any subcontractor processing PII on its behalf should require the subcontractor to implement the appropriate controls specified in Annex B, taking account of the information security risk assessment process (see 5.4.1.2) and the scope of the processing of PII performed by the PII processor (see 6.12). By default, all controls specified in Annex B should be assumed as relevant. If the organization decides to not require the subcontractor to implement a control from Annex B, it should justify its exclusion. A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and included in the documented information."	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 27701:2019	[ISO 27701] B.8.5.7 Engagement of a subcontractor to process PII	"Control The organization shall only engage a subcontractor to process PII according to the customer contract. Implementation guidance Where the organization subcontracts some or all of the processing of that PII to another organization, a written authorization from the customer is required prior to the PII processed by the subcontractor. This can be in the form of appropriate clauses in the customer contract, or can be a specific ""one-off"" agreement. The organization should have a written contract with any subcontractors that it uses for PII processing on its behalf, and should ensure that their contracts with subcontractors address the implementation of the appropriate controls in Annex B. The contract between the organization and any subcontractor processing PII on its behalf should require the subcontractor to implement the appropriate controls specified in Annex B, taking account of the information security risk assessment process (see 5.4.1.2) and the scope of the processing of PII performed by the PII processor (see 6.12). By default, all controls specified in Annex B should be assumed as relevant. If the organization decides to not require the subcontractor to implement a control from Annex B, it should justify its exclusion. A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and included in the documented information."	Facilitating compliance with obligations	Where the organization is a data processor, the organization documents their legal, regulatory, and business obligations to controllers related to the processing of the user data within written contracts.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] B.8.5.8 Change of subcontractor to process PII	"Control The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes. Implementation guidance Where the organization changes the organization with which it subcontracts some or all of the processing of that PII, then written authorization from the customer is required for the change, prior to the PII processed by the new subcontractor. This can be in the form of appropriate clauses in the customer contract, or can be a specific ""one-off"" agreement."	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27701:2019	[ISO 27701] 6.11.2.1 Secure development policy	The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.1 and the following additional guidance applies. Additional implementation guidance for 14.2.1, Secure development policy, of ISO/IEC 27002:2013 is: Policies for system development and design should include guidance for the organization’s processing of PII needs, based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organization. Clauses 7 and 8 provide control considerations for processing of PII, which can be useful in developing policies for privacy in systems design. Policies that contribute to privacy by design and privacy by default should consider the following aspects: a) guidance on PII protection and the implementation of the privacy principles (see ISO/IEC 29100) in the software development lifecycle; b) privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment and/or a privacy impact assessment (see 7.2.5); c) PII protection checkpoints within project milestones; d) required privacy and PII protection knowledge; e) by default minimize processing of PII.	Secure Development - Policies & Procedures	The organization has policies and guidelines governing the secure development lifecycle.	Confidentiality, Privacy, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27701:2019	[ISO 27701] 6.11.2.1 Secure development policy	The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.1 and the following additional guidance applies. Additional implementation guidance for 14.2.1, Secure development policy, of ISO/IEC 27002:2013 is: Policies for system development and design should include guidance for the organization’s processing of PII needs, based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organization. Clauses 7 and 8 provide control considerations for processing of PII, which can be useful in developing policies for privacy in systems design. Policies that contribute to privacy by design and privacy by default should consider the following aspects: a) guidance on PII protection and the implementation of the privacy principles (see ISO/IEC 29100) in the software development lifecycle; b) privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment and/or a privacy impact assessment (see 7.2.5); c) PII protection checkpoints within project milestones; d) required privacy and PII protection knowledge; e) by default minimize processing of PII.	Privacy Reviews	The organization performs privacy reviews prior to product launch.	Privacy	Risk, Culture