



GDPR Applicability Reference Standard

DOC-IT-IS-18.1.6
Revision 2.0
NOVEMBER 1, 2025

This document contains proprietary information, which is the exclusive property of RXO, Inc. and may not be used or reproduced, in whole or in part, without the express permission of RXO, Inc.

Copyright © 2025 RXO, Inc. All rights reserved.

REVISION HISTORY

This revision history lists all changes to this document, the date of each revision, and the reason for each revision.

<i><u>Rev.</u></i>	<i><u>Rev. Date</u></i>	<i><u>Revision Description</u></i>
1.0	11/01/2022	Initial Version
2.0	11/01/2025	RXO, Inc updates, annual review

18.6.1	GDPR Applicability Reference Standard	4
18.6.1.1	Purpose	4
18.6.1.2	Scope	4
18.6.2	GDPR Cross References	4

18.6.1 GDPR Applicability Reference Standard

18.6.1.1 Purpose

18.6.1.1 A The purpose of the RXO, Inc. including its subsidiaries, divisions, and any other entities (collectively, “RXO”) GDPR Applicability Standard is to provide all RXO personnel who are required to understand the relationship between specific ISO 27002 control requirements and related GDPR privacy clauses. Typically, security and privacy are addressed separately but the criticality of GDPR privacy requirements, and the necessarily close integration of security controls, make it mandatory for relevant RXO personnel to clearly understand this linkage.

18.6.1.2 Scope

18.6.1.2 A This standard applies to all RXO security governance documents (policies, standards, procedures, or guidelines) where GDPR has been integrated. The relevant ISO 27002 control sub-domains are presented from low-to-high with the associated GDPR article references that are supported by that ISO 27002 sub-domain control section.

18.6.2 GDPR Cross References

ISO 27002 Policy Reference 5.1.1 Policies for Information Security - (GDPR Article 5, 1 (f)) In jurisdictions where GDPR data is stored, processed, or transmitted, the requirements for “Principles relating to processing of personal data” that are relevant to information security policies are defined in GDPR Article 5, Paragraph 1 (f). RXO must ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

ISO Policy Reference 6.1.1 Information Security Roles and Responsibilities - (GDPR Article 5 (f)) In all business operations, IT Processes, and jurisdictions where GDPR data is stored, processed, or transmitted, the requirements for “Principles relating to processing of personal data” that are relevant to RXO of information security are defined in GDPR Article 5, Paragraph (f). If applicable, RXO must ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental

loss, destruction, or damage, using appropriate technical or organizational measures to ensure integrity and confidentiality.

ISO Policy Reference 6.1.1 Information Security Roles and Responsibilities - (GDPR Article 37) In all business operations, IT Processes, and jurisdictions where GDPR data is stored, processed, or transmitted, the requirements for “Designation of the data protection officer” are defined in GDPR Article 37, Paragraphs 1 through 7. If applicable, the controller (RXO) and the processor (potentially RXO or a third party) shall designate a data protection officer in any case where the criteria defined in the criteria in Paragraph 1 (a) through 1 (c) applies to RXO operations.

ISO Policy Reference 6.1.1 Information Security Roles and Responsibilities - (GDPR Article 38) In all business operations, IT Processes, and jurisdictions where GDPR data is stored, processed, or transmitted, the requirements for “Position of the data protection officer” are defined in GDPR Article 38, Paragraphs 1 through 6. If applicable, the controller (RXO) and the processor (potentially RXO or a third party) must ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

ISO Policy Reference 6.1.1 Information Security Roles and Responsibilities - (GDPR Article 39) In all business operations, IT Processes, and jurisdictions where GDPR data is stored, processed, or transmitted, the requirements for “Tasks of the data protection officer” are defined in GDPR Article 39, Paragraphs 1 through 2. If applicable, RXO must ensure the data protection officer will be assigned the tasks defined in paragraph 1 (a) through 1 (e).

ISO Policy Reference 6.1.3 Contact with Authorities - (GDPR Article 31) In jurisdictions where GDPR data is stored, processed, or transmitted, the requirements for “Cooperation with the supervisory authority” are defined in GDPR Article 31. If applicable, the controller (RXO) and the processor (potentially RXO or a third party) and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

ISO 27002 Policy Reference 7.1.1 Screening (GDPR Article 10) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirement for “Processing of personal data relating to criminal convictions and offenses” are defined in GDPR Article 10. If applicable, processing of personal data relating to criminal convictions and offenses, or related security measures based on Article 6 (1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. Therefore, for EU citizens, processing of personal data relating to criminal convictions and offenses can only be performed under the control of official authority (Law enforcement). Further, RXO cannot maintain records of criminal convictions of EU Citizens. This will be likely to affect the quality and value of EU background screening.

ISO 27002 Policy Reference 8.1.2 Ownership of Assets - (GDPR Article 15) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Right of access by the data subject” are defined in GDPR Article 15, Paragraphs 1 through 4. If applicable, the data subject shall have the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information defined in GDPR Article 15.

ISO 27002 Policy Reference 8.1.2 Ownership of Assets - (GDPR Article 16) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Right to rectification” are defined in GDPR Article 16. If applicable, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

ISO 27002 Policy Reference 8.1.2 Ownership of Assets - (GDPR Article 17) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the

requirements for “Right to erasure (‘right to be forgotten’)” are defined in GDPR Article 17, Paragraphs 1 through 3. If applicable, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds defined in GDPR Article 17 applies.

ISO 27002 Policy Reference 8.1.2 Ownership of Assets - (GDPR Article 18) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Right to restriction of processing” are defined in GDPR Article 18, Paragraphs 1 through 3. If applicable, the data subject shall have the right to obtain from the controller restriction of processing where one of reasons defined in GDPR Article 18 applies.

ISO 27002 Policy Reference 8.1.2 Ownership of Assets - (GDPR Article 20) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Right to data portability” are defined in GDPR Article 20, Paragraphs 1 through 4. If applicable, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the reasons defined in GDPR Article 20 apply.

ISO 27002 Policy Reference 8.2.1 Classification of Information - (GDPR Article 9) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Processing of special categories of personal data” are defined in GDPR Article 9, Paragraphs 1 through 4. If applicable, RXO is prohibited from processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (“GDPR Special Categories of Personal Data”) unless there is a legitimate business reason for collecting and maintaining the data which meets the criteria and requirements defined in

the GDPR Article 9, Paragraph 2 (a) through 2 (J) and paragraph 3. As a result of this prohibition, it is by default prohibited to grant access to these GDPR Special Categories of Personal Data. A user may only be granted access to GDPR Special Categories of Personal Data based on approved roles and the concepts of Least Privilege and need-to-know access and a requirement to access the GDPR Special Categories of Personal Data for a purpose as set out in Article 9, Paragraphs 2 and 3. In addition, regular access certification reviews (quarterly) must be conducted (especially on systems that store, transmit or process any GDPR Personal Data assets) to ensure that access provisioning processes remain effective (see 9.2.5).

ISO 27002 Policy Reference 8.2.1 Classification of Information - (GDPR Article 35) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Data protection impact assessment” are defined in GDPR Article 35, Paragraphs 1 through 11. If applicable, where a type of processing (in particular using new technologies), and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data

ISO 27002 Policy Reference 8.2.1 Classification of Information - (GDPR Article 36) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Prior consultation” are defined in GDPR Article 36, Paragraphs 1 through 5. If applicable, the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

ISO 27002 Policy Reference 8.2.3 Handling of Assets - (GDPR Article 9) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Processing of special categories of personal data” are defined in GDPR Article 9, Paragraphs 1 through 4. If applicable, RXO is prohibited from processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,

and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation ("GDPR Special Categories of Personal Data") unless there is a legitimate business reason for collecting and maintaining the data which meets the criteria and requirements defined in the GDPR Article 9, Paragraph 2 (a) through 2 (J) and paragraph 3. As a result of this prohibition, it is by default prohibited to grant access to these GDPR Special Categories of Personal Data. A user may only be granted access to GDPR Special Categories of Personal Data based on approved roles and the concepts of Least Privilege and need-to-know access and a requirement to access the GDPR Special Categories of Personal Data for a purpose as set out in Article 9, Paragraphs 2 and 3. In addition, regular access certification reviews (quarterly) must be conducted (especially on systems that store, transmit or process any GDPR Personal Data assets) to ensure that access provisioning processes remain effective (see 9.2.5).

ISO 27002 Policy Reference 8.2.3 Handling of Assets - (GDPR Article 10) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for "Processing of data relating to criminal convictions and offences" are defined in GDPR Article 10. If applicable, the processing of personal data relating to criminal convictions and offenses, or related security measures based on Article 6 (1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

ISO 27002 Policy Reference 8.2.3 Handling of Assets - (GDPR Article 13) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for "Information to be provided where personal data are collected from the data subject" are defined in GDPR Article 13, Paragraphs 1 through 4. If applicable, where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the information defined in GDPR Article 13.

ISO 27002 Policy Reference 8.2.3 Handling of Assets - (GDPR Article 14) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Information to be provided where personal data have not been obtained from the data subject” are defined in GDPR Article 14, Paragraphs 1 through 5. If applicable, where personal data have not been obtained from the data subject, the controller shall provide the data subject with the information defined in GDPR Article 14.

ISO 27002 Policy Reference 9.2.2 User Access Provisioning - (GDPR Article 9) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processing of special categories of personal data” are defined in GDPR Article 9, Paragraphs 1 through 4. If applicable, RXO is prohibited from processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (“GDPR Special Categories of Personal Data”) unless there is a legitimate business reason for collecting and maintaining the data which meets the criteria and requirements defined in the GDPR Article 9, Paragraph 2 (a) through 2 (J) and paragraph 3. As a result of this prohibition, it is by default prohibited to grant access to these GDPR Special Categories of Personal Data. A user may only be granted access to GDPR Special Categories of Personal Data based on approved roles and the concepts of Least Privilege and need-to-know access and a requirement to access the GDPR Special Categories of Personal Data for a purpose as set out in Article 9, Paragraphs 2 and 3. In addition, regular access certification reviews (quarterly) must be conducted (especially on systems that store, transmit or process any GDPR Personal Data assets) to ensure that access provisioning processes remain effective (see 9.2.5).

ISO 27002 Policy Reference 9.2.2 User Access Provisioning - (GDPR Article 16) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to rectification” are defined in GDPR Article 16. If applicable, the data subjects (the persons whose personal data you possess), have the right to obtain from RXO

without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subjects, have the right to have incomplete personal data completed, including by means of providing a supplementary statement. As a result of this requirement, the users that are authorized to “rectify” the GDPR Personal Data must be granted access based on approved roles, the concepts of Least Privilege, and need-to-know access.

ISO 27002 Policy Reference 9.2.2 User Access Provisioning - (GDPR Article 17) In all business operations, IT processes and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to erasure (‘right to be forgotten’)” are defined in GDPR Article 17, Paragraphs 1 through 4. If applicable, the data subjects (the persons whose personal data you possess), have the right to obtain from RXO the erasure of personal data concerning him or her without undue delay and RXO has the obligation to erase personal data without undue delay where one of the reasons apply that are defined in GDPR Article 17, Paragraphs 1 (a -f), 2, and 3 (a - e). As a result of this requirement, the users that are authorized to “erase” the GDPR Personal Data must be granted access based on approved roles, the concepts of Least Privilege, and need-to-know access.

ISO 27002 Policy Reference 10.1.1 Policy on the Use of Cryptographic Controls - (GDPR Article 5(f)) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Principles relating to processing of personal data)” are defined in GDPR Article 5, Paragraphs 1 through 2. If applicable, Article 5(f) requires that the GDPR Personal Data elements that have been designated by RXO (as requiring protection by encryption) must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing (by using strong encryption to protect the (RXO data elements classified as “Regulated”) GDPR Personal Data elements against accidental loss, destruction or damage, using appropriate technical (cryptographic protections) or organizational measures (‘integrity and confidentiality’).

ISO 27002 Policy Reference 10.1.2 Key Management - (GDPR Article 5(f)) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Principles relating to processing of personal data)” are defined in GDPR Article 5,

Paragraphs 1 through 2. If applicable, Article 5(f) requires that the GDPR Personal Data elements that have been designated by RXO (as requiring protection by encryption) must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing (by using strong encryption in combination with secure encryption key management practices to protect the (RXO data elements classified as “Regulated”) GDPR Personal Data elements against accidental loss, destruction or damage, using appropriate technical (cryptographic protections combined with secure encryption key management practices) or organizational measures (‘integrity and confidentiality’).

ISO 27002 Policy Reference 11.1.2 Physical Entry Controls - (GDPR Article 5 (f)) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Principles relating to processing of personal data” that are relevant to communication security are defined in GDPR Article 5, Paragraph (f). If applicable, RXO must ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

ISO 27002 Policy Reference 11.1.2 Physical Entry Controls - (GDPR Article 7) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Conditions for consent” are defined in GDPR Article 7, Paragraphs 1 through 4. If applicable, where processing is based on consent, the controller (RXO) must be able to demonstrate that the data subject has consented to the processing of his or her personal data.

ISO 27002 Policy Reference 11.1.2 Physical Entry Controls - (GDPR Article 13) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Information to be provided where personal data are collected from the data subject” are defined in GDPR Article 13, Paragraphs 1 through 4. If applicable, where personal data relating to a data subject are collected from the data subject, the controller (RXO) must,

at the time when personal data are obtained, provide the data subject with all of the information defined in Article 13, paragraphs 1 (a) through 1 (f).

ISO 27002 Policy Reference 11.1.2 Physical Entry Controls - (GDPR Article 88) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processing in the context of employment” are defined in GDPR Article 88, Paragraphs 1 through 3. If applicable, RXO must be aware that Member States by law or by collective agreements, have the authority to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context for:

- The purposes of recruitment,
- The performance of the contract of employment, including discharge of the obligations laid down by law or by collective agreements,
- Management,
- Planning and organization of work,
- Equality and diversity in the workplace,
- Health and safety at work,
- Protection of employer's or customer's property,
- The purposes of the exercise and enjoyment, on an individual or collective basis, of the rights and benefits related to employment,
- The purposes of the termination of the employment relationship.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 7) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Conditions for consent” are defined in GDPR Article 7, Paragraphs 1 through 4. If applicable, where processing is based on consent, the controller (RXO) must be able to demonstrate that the data subject has consented to the processing of his or her personal data.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 12) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Transparent information, communication, and modalities for the exercise of the rights of the data subject” are defined in GDPR Article 12, Paragraph 1 and 8. If applicable, the controller (RXO) must take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to the processing of the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information must be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 13) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Information to be provided where personal data are collected from the data subject” are defined in GDPR Article 13, Paragraphs 1 through 4. If applicable, where personal data relating to a data subject are collected from the data subject, the controller (RXO) must, at the time when personal data are obtained, provide the data subject with all of the information defined in Article 13, paragraphs 1 (a) through 1 (f).

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 14) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Information to be provided where personal data have not been obtained from the data subject” are defined in GDPR Article 14, Paragraphs 1 through 5. If applicable, where personal data have not been obtained from the data subject, the controller (RXO) must provide the data subject with the information defined in paragraph 1 (a) through 1 (f).

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 15) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right of access by the data subject” are defined in GDPR Article 15,

Paragraphs 1 through 4. If applicable, RXO as the controller must ensure that the data subject shall have the right to obtain from the controller (RXO) confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information defined in paragraph 1 (a) through 1 (h).

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 16) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to rectification” are defined in GDPR Article 16. If applicable, the data subject shall have the right to obtain from the controller (RXO) without undue delay the rectification of inaccurate personal data concerning him or her. The process must take into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 17) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to erasure (‘right to be forgotten’)” are defined in GDPR Article 17, Paragraphs 1 through 3. If applicable, the data subject shall have the right to obtain from the controller (RXO) the erasure of personal data concerning him or her without undue delay and the controller (RXO) shall have the obligation to erase personal data without undue delay where one of the grounds defined in paragraph 1 (a) through 1 (f) applies.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 18) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to restriction of processing” are defined in GDPR Article 18, Paragraphs 1 through 3. If applicable, the data subject shall have the right to obtain from the controller (RXO) restriction of processing where one of reasons defined in paragraph 1 (a) through 1 (d) applies.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 19) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Notification obligation regarding rectification or erasure of personal data or restriction of processing” are defined in GDPR Article 19. If applicable, the controller (RXO) must communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller (RXO) shall inform the data subject about those recipients if the data subject requests it.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 20) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to data portability” are defined in GDPR Article 20, Paragraphs 1 through 4. If applicable, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller (RXO), in a structured, commonly used and machine-readable format and have the right to transmit this data to another controller without hindrance from the (originating) controller (RXO) to which the personal data have been provided, where the reasons defined in paragraph 1 (a) and 1 (b) both apply.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 21) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to object” are defined in GDPR Article 21, Paragraphs 1 through 4. If applicable, RXO must ensure the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1), including profiling based on those provisions. The controller (RXO) must no longer process the personal data unless the controller (RXO) demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 22) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Automated individual decision-making, including profiling” are

defined in GDPR Article 22, Paragraphs 1 through 4. If applicable, RXO must ensure the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 24) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Responsibility of the controller” are defined in GDPR Article 24, Paragraphs 1 through 3. If applicable, RXO must take into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The controller (RXO) must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 25) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Data protection by design and by default” are defined in GDPR Article 25, Paragraphs 1 through 3. If applicable, RXO must take into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing. The controller (RXO) shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization. Pseudonymization, and other measures which are designed to implement data-protection principles, such as data minimization, in an effective manner. RXO must integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

ISO 27002 Policy Reference 12.1.1 Documented Procedures - (GDPR Article 32) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Security of processing” are defined in GDPR Article 32, Paragraphs

1 through 4. If applicable, RXO must consider the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The controller (RXO) and the processor (potentially RXO or a third party) must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including among other things the items defined in paragraph 1 (a) through 1 (d) as appropriate.

ISO 27002 Policy Reference 12.4.2 Protection of Log Information - (GDPR Article 30) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Records of processing activities” are defined in GDPR Article 30, Paragraph 1 and 5. If applicable, RXO must as a controller and, where applicable, the RXO's representative, must maintain a record of processing activities under its responsibility. That record must contain all of the information defined in GDPR Article 10 in paragraph 1 (a) through 1 (g).

ISO 27002 Policy Reference 13.2.1 Information Transfer Procedures - (GDPR Article 5 (f)) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Principles relating to processing of personal data” that are relevant to communication security are defined in GDPR Article 5, Paragraph (f). If applicable, RXO must ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

ISO 27002 Policy Reference 13.2.1 Information Transfer Procedures - (GDPR Article 15) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right of access by the data subject” that are relevant to communication security are defined in GDPR Article 15, Paragraphs 1 through 4. If Applicable, RXO must ensure the data subject has the right to obtain from the controller (RXO) confirmation as to whether or not personal data concerning him or her are being processed, and, where data is being processed, access to the personal data based on the criteria defined in paragraphs 1 through 4.

ISO 27002 Policy Reference 13.2.1 Information Transfer Procedures - (GDPR Article 26) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Joint controllers” that are relevant to communication security are defined in GDPR Article 26, Paragraphs 1 through 3. If applicable, where two or more controllers (potentially RXO and a Supplier) jointly determine the purposes and means of processing, they are classified within GDPR as joint controllers. If these cases exist, RXO and their joint controller must in a transparent manner determine/define their respective responsibilities for compliance within the obligations of this Regulation, in particular, supporting the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification - (GDPR Article 5 (f)) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Principles relating to processing of personal data” that are relevant to systems acquisition and development are defined in GDPR Article 5, Paragraph (f). If applicable, RXO must ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification - (GDPR Article 7) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Conditions for consent” are defined in GDPR Article 7, Paragraphs 1 through 4. If applicable, where processing is based on consent, the controller (RXO) must be able to demonstrate that the data subject has consented to the processing of his or her personal data.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 9) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processing of special categories of personal data” are defined in GDPR Article 9, Paragraphs 1 through 4. If applicable, RXO must enforce that the access to GDPR Personal Data must be specifically allocated to accounts and users based on approved roles and the concepts of Least Privilege and need-to-know.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 9) (“GDPR Special Categories of Personal Data”) unless there is a legitimate business reason for collecting and maintaining the data, which meets the criteria and requirements defined in the GDPR Article 9, 2 (a) through 2 (J) and paragraph 3. As a result of this prohibition, it is by default prohibited to grant access to these GDPR Special Categories of Personal Data. A user may only be granted access to GDPR Special Categories of Personal Data based on approved roles and the concepts of Least Privilege and need-to-know access and a requirement to access the GDPR Special Categories of Personal Data for a purpose as set out in Article 9, Paragraphs 2 and 3. In addition, regular access certification reviews (quarterly) must be conducted (especially on systems that store, transmit or process GDPR Personal Data assets) to ensure that access provisioning processes remain effective (see 9.2.5).

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 10) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processing of personal data relating to criminal convictions and offenses” are defined in GDPR Article 10. If applicable, RXO must be aware that the processing of personal data relating to criminal convictions and offenses, or related security measures based on Article 6 (1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 11) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processing which does not require identification” are defined in GDPR Article 11, Paragraph 1 and 2. If applicable, RXO must understand that if the purposes for which the controller (RXO) processes personal data do not or do no longer require the identification of a data subject by the controller, the controller (RXO) shall not be obliged to maintain, acquire or process the additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 12) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Transparent information, communication, and modalities for the exercise of the rights of the data subject” are defined in GDPR Article 12, Paragraph 1 and 8. If applicable, the controller (RXO) must take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to the processing of the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information must be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 13) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Information to be provided where personal data are collected from the data subject” are defined in GDPR Article 13, Paragraphs 1 through 4. If applicable, where personal data relating to a data subject are collected from the data subject, the controller (RXO) must, at the time when personal data are obtained, provide the data subject with all of the information defined in Article 13, paragraphs 1 (a) through 1 (f).

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 14) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Information to be provided where personal data have not been obtained from the data subject” are defined in GDPR Article 14, Paragraphs 1 through 5. If applicable, where personal data have not been obtained from the data subject, the controller (RXO) must provide the data subject with the information defined in paragraph 1 (a) through 1 (f).

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 15) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right of access by the data subject” are defined in GDPR Article 15, Paragraphs 1 through 4. If applicable, RXO as the controller must ensure that the data subject shall have the right to obtain from the controller (RXO) confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information defined in paragraph 1 (a) through 1 (h).

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 16) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to rectification” are defined in GDPR Article 16. If applicable, the data subject shall have the right to obtain from the controller (RXO) without undue delay the rectification of inaccurate personal data concerning him or her. The process must take into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 17) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to erasure (‘right to be forgotten’)” are defined in GDPR Article 17, Paragraphs 1 through 3. If applicable, the data subject shall have the right to obtain from the controller (RXO) the erasure of personal data concerning him or her without

undue delay and the controller (RXO) shall have the obligation to erase personal data without undue delay where one of the grounds defined in paragraph 1 (a) through 1 (f) applies.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 18) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to restriction of processing” are defined in GDPR Article 18, Paragraphs 1 through 3. If applicable, the data subject shall have the right to obtain from the controller (RXO) restriction of processing where one of reasons defined in paragraph 1 (a) through 1 (d) applies.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 19) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Notification obligation regarding rectification or erasure of personal data or restriction of processing” are defined in GDPR Article 19. If applicable, the controller (RXO) must communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1), and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller (RXO) shall inform the data subject about those recipients if the data subject requests it.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 20) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to data portability” are defined in GDPR Article 20, Paragraphs 1 through 4. If applicable, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller (RXO), in a structured, commonly used and machine-readable format and have the right to transmit this data to another controller without hindrance from the (originating) controller (RXO) to which the personal data have been provided, where the reasons defined in paragraph 1 (a) and 1 (b) both apply.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 21) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to object” are defined in GDPR Article 21, Paragraphs 1 through 4. If applicable, RXO must ensure the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1), including profiling based on those provisions. The controller (RXO) must no longer process the personal data unless the controller (RXO) demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 22) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Automated individual decision-making, including profiling” are defined in GDPR Article 22, Paragraphs 1 through 4. If applicable, RXO must ensure the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 24) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Responsibility of the controller” are defined in GDPR Article 24, Paragraphs 1 through 3. If applicable, RXO must take into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The controller (RXO) must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 25) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Data protection by design and by default” are defined in GDPR Article 25, Paragraphs 1 through 3. If applicable, RXO must take into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing. The controller (RXO) shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization. Pseudonymization, and other measures which are designed to implement data-protection principles, such as data minimization, in an effective manner. RXO must integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

ISO 27002 Policy Reference 14.1.1 Information Security Requirements Analysis and Specification -

(GDPR Article 32) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Security of processing” are defined in GDPR Article 32, Paragraphs 1 through 4. If applicable, RXO must take into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The controller (RXO) and the processor (potentially RXO or a third party) must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including among other things the items defined in paragraph 1 (a) through 1 (d) as appropriate.

ISO 27002 Policy Reference 15.1.1 Information Security for Supplier Relationships - (GDPR Article

24) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Responsibility of the controller” are defined in GDPR Article 24, Paragraphs 1 through 3. If applicable, RXO must take into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The controller (RXO) must implement appropriate technical and

organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with this Regulation. Those measures must be reviewed and updated where necessary.

ISO 27002 Policy Reference 15.1.1 Information Security for Supplier Relationships - (GDPR Article 26) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Joint controllers” are defined in GDPR Article 26, Paragraphs 1 through 3. If applicable, where two or more controllers (potentially RXO and a Supplier) jointly determine the purposes and means of processing, they are classified within GDPR as joint controllers. If these cases exist, RXO and their joint controller must in a transparent manner, determine and /or define their respective responsibilities for compliance within the obligations of this Regulation, in particular, supporting the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

ISO 27002 Policy Reference 15.1.1 Information Security for Supplier Relationships - (GDPR Article 27) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Representatives of controllers or processors not established in the Union” are defined in GDPR Article 27, Paragraphs 1 through 5. If Article 3(2) is applicable, the controller (RXO) or the processor (RXO or a supplier) must designate in writing a representative in the Union. This article may not apply to processors that are occasional or not large scale processors as defined in GDPR Article 27.

ISO 27002 Policy Reference 15.1.1 Information Security for Supplier Relationships - (GDPR Article 28) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Processor” are defined in GDPR Article 28, Paragraphs 1 through 10. If applicable, where processing is to be carried out on behalf of a controller (RXO), the controller (RXO) must use only processors (suppliers) that can provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing

will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

ISO 27002 Policy Reference 15.1.1 Information Security for Supplier Relationships - (GDPR Article

29) In all business operations, IT Processes, and jurisdictions where GDPR Personal data is stored, processed, or transmitted, the requirements for “Processing under the authority of the controller or processor” are defined in GDPR Article 29. If applicable, the processor (RXO or a supplier) and any person acting under the authority of the controller (RXO) or of the processor (RXO or a supplier), who has access to personal data, must not process those data except on instructions from the controller (RXO), unless required to do so by Union or Member State law.

ISO 27002 Policy Reference 16.1.1 Incident Responsibilities and Procedures - (GDPR Article 26)

In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Joint controllers” are defined in GDPR Article 26, Paragraphs 1 through 3. If Applicable, where two or more controllers (potentially RXO and a Supplier) jointly determine the purposes and means of processing, they are classified within GDPR as joint controllers. If these cases exist, RXO and their joint controller must in a transparent manner determine their respective responsibilities for incident response programs within the obligations of this GDPR Regulation, in particular, supporting the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

ISO 27002 Policy Reference 16.1.2 Reporting Information Security Events - (GDPR Article 33)

In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Notification of a personal data breach to the supervisory authority” are defined in GDPR Article 33, Paragraphs 1 through 5. If applicable, in the case of a GDPR related personal data breach, the controller (RXO) must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the GDPR personal data breach to the

supervisory authority as defined by Article 55, unless the GDPR personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ISO 27002 Policy Reference 16.1.2 Reporting Information Security Events - (GDPR Article 34) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Communication of a personal data breach to the data subject” are defined in GDPR Article 34, Paragraphs 1 through 4. If applicable, when a GDPR related personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller (RXO) must communicate the GDPR personal data breach to the data subject without undue delay. The communication must meet the requirements set out in GDPR Article 34 (2). A communication may not be required if any of the conditions set out in Article 34 (3) are met.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual Requirements - (GDPR Article 6) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Lawfulness of processing” are defined in GDPR Article 6, Paragraphs 1 through 4. If applicable, processing of personal data shall be lawful only if and to the extent that at least one of the criteria in Paragraph 1 (a) through 1 (f) applies to RXO’s operations.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual Requirements - (GDPR Article 18) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to restriction of processing” are defined in GDPR Article 18, Paragraphs 1 through 3. If applicable, RXO must ensure the data subject has the right to obtain from the controller (RXO), restrictions of processing where one of the criteria in Paragraph 1 (a) through 1 (d) applies to RXO’s operations and processing of personal data.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 23) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Restrictions” are defined in GDPR Article 23, Paragraphs 1 through 2. If applicable, RXO as the data controller or processor may be subject to Union or Member State laws that restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5, in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22. When such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the subjects defined in Paragraph 1 (a) through 1 (J) applies to RXO’s operations and processing of personal data.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 26) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Joint controllers” are defined in GDPR Article 26, Paragraphs 1 through 3. If applicable, where two or more controllers (potentially RXO and a third party supplier) jointly determine the purposes and means of processing, they are classified within GDPR as joint controllers. If these cases exist, RXO and their joint controller must in a transparent manner determine/define their respective responsibilities for compliance within the obligations of this Regulation. In particular, it must support the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them. Unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 27) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Representatives of controllers or processors not established in the Union” are defined in GDPR Article 27, Paragraphs 1 through 5. If applicable, where Article 3(2) applies, the controller (RXO) or the processor (RXO or a

supplier) must designate in writing a representative in the Union. This article may not apply to processors that are occasional or not large-scale processors as defined in GDPR Article 27.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 28) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processor” are defined in GDPR Article 28, Paragraphs 1 through 10. If applicable, where processing is to be carried out on behalf of a controller (RXO), the controller (RXO) must use only processors (suppliers) that can provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this regulation. The measures must ensure the protection of the rights of the data subject.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 90) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Obligations of secrecy” are defined in GDPR Article 90, Paragraphs 1 through 2. If applicable, RXO must be aware that Member States have the authority to adopt specific rules to establish the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law, or rules established by national competent bodies. These rules create an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right to the protection of personal data with the obligation of secrecy. These rules shall apply only with regard to personal data, which the controller (RXO) or processor (potentially RXO or a third party) has received as a result of or has obtained in an activity covered by the obligation of secrecy.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 95) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Relationship with Directive 2002/58/EC” are defined in GDPR Article 95. If applicable, RXO must be aware that this Regulation (GDPR) shall not impose additional obligations on natural or legal persons in relation to

processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 96) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Relationship with previously concluded Agreements” are defined in GDPR Article 96. If applicable, RXO must be aware that International Agreements involving the transfer of personal data to third countries or international organizations, which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

ISO 27002 Policy Reference 18.1.1 Identification of Applicable Legislation and Contractual

Requirements - (GDPR Article 99) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Entry into force and application” are defined in GDPR Article 99. If applicable, RXO must be aware that this Regulation (GDPR) shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It regulation shall apply from 25 May 2018.

ISO 27002 Policy Reference 18.1.3 Protection of Records - (GDPR Article 7) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Conditions for consent” are defined in GDPR Article 7, Paragraphs 1 through 4. If applicable, where processing is based on consent, the controller (RXO) must be able to demonstrate that the data subject has consented to the processing of his or her personal data

ISO 27002 Policy Reference 18.1.3 Protection of Records - (GDPR Article 16) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to rectification” are defined in GDPR Article 16. If applicable,

RXO must ensure the data subject has the right to obtain from the controller (RXO) without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject must be ensured of the right to have incomplete personal data completed, including by means of providing a supplementary statement.

ISO 27002 Policy Reference 18.1.3 Protection of Records - (GDPR Article 20) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to data portability” are defined in GDPR Article 20, Paragraphs 1 through 4. If applicable, RXO must ensure the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller (RXO), in a structured, commonly used and machine-readable format. The data subject must have the right to transmit this data to another controller without hindrance from the controller (RXO) to which the personal data have been provided, where both of the criteria in Paragraph 1 (a) through 1 (d) applies to RXO’s operations and processing of personal data.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information - (GDPR Article 3) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Territorial scope” are defined in GDPR Article 3, Paragraphs 1 through 3. If applicable, RXO must be aware that this Regulation (GDPR) applies to the processing of personal data in the context of the activities of an establishment of a controller (RXO) or a processor (potentially RXO or a third party) in the Union, regardless of whether the processing takes place in the Union or not.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information - (GDPR Article 33) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Notification of a personal data breach to the supervisory authority” are defined in GDPR Article 33, Paragraphs 1 through 5. If applicable, In the case of a personal data breach, the controller (RXO) shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is

unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by (documented) reasons for the delay.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 34) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Communication of a personal data breach to the data subject” are defined in GDPR Article 34, Paragraphs 1 through 4. If applicable, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller (RXO), shall communicate the personal data breach to the data subject without undue delay.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 37) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Designation of the data protection officer” are defined in GDPR Article 37, Paragraphs 1 through 7. If applicable, the controller (RXO) and the processor (potentially RXO) shall designate a data protection officer in any case where the criteria defined in the criteria in Paragraph 1 (a) through 1 (c) applies to RXO operations.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 38) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Position of the data protection officer” are defined in GDPR Article 38, Paragraphs 1 through 6. If applicable, the controller (RXO) and the processor (potentially RXO) must ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 39) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Tasks of the data protection officer” are

defined in GDPR Article 39, Paragraphs 1 through 2. If applicable, RXO must ensure the data protection officer will be assigned the tasks defined in paragraph 1 (a) through 1 (e).

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 40) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Codes of conduct” are defined in GDPR Article 40, Paragraphs 1 through 11. If applicable, RXO may be expected to comply with codes of conduct that the Member States, supervisory authorities, the Board, and the Commission have encouraged to develop, which are intended to contribute to the proper application of this Regulation. The codes of conduct would take into account of the specific features of the various processing sectors and the specific needs of micro, small, and medium-sized enterprises as this may be relevant to RXO.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 45) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Transfers on the basis of an adequacy decision” are defined in GDPR Article 45, Paragraphs 1 through 9. If applicable, in the absence of a decision pursuant to Article 45 (3), the controller (RXO) or processor (potentially RXO or a third party) may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject's rights and effective legal remedies for data subjects are available.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 46) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Transfers subject to appropriate safeguards” are defined in GDPR Article 46, Paragraphs 1 through 5. If applicable, in the absence of a decision pursuant to Article 45 (3), the controller (RXO) or processor (potentially RXO or a third party) may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject's rights and effective legal remedies for data subjects are available.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 48) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Transfers or disclosures not authorized by Union law” are defined in GDPR Article 48. If applicable, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring the controller (RXO) or processor (potentially RXO or a third party) to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 49) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Derogations for specific situations” are defined in GDPR Article 49, Paragraphs 1 through 6. If applicable, in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers (by RXO) of personal data to a third country or an international organization shall take place only where one of the following conditions defined in Paragraph 1 (a) through 1 (g) applies to RXO operations.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 82) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Right to compensation and liability” are defined in GDPR Article 82, Paragraphs 1 through 6. If applicable, RXO must ensure that any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 83) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “General conditions for imposing administrative fines” are defined in GDPR Article 83, Paragraphs 1 through 9. If applicable, RXO must be aware of the criteria used for imposing administrative fines, and that each supervisory authority is capable of imposing administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 which in each individual case are intended to be effective, proportionate, and dissuasive.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 84) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Penalties” are defined in GDPR Article 84, Paragraphs 1 through 2. If applicable, RXO must be aware of the criteria used for imposing penalties and that each Member State shall establish the rules on other penalties applicable to infringements of this Regulation, in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. The penalties are intended to be effective, proportionate, and dissuasive.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 87) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processing of the national identification number” are defined in GDPR Article 87. If applicable, RXO must be aware that Member States have the authority to define the specific conditions for the processing of a national identification number or any other identifier of general application. In these cases the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

ISO 27002 Policy Reference 18.1.4 Privacy and Protection of Personally Identifiable Information -

(GDPR Article 88) In all business operations, IT Processes, and jurisdictions where GDPR Personal Data is stored, processed, or transmitted, the requirements for “Processing in the context of employment”

are defined in GDPR Article 88, Paragraphs 1 through 3. If applicable, RXO must be aware that Member States by law or by collective agreements, have the authority to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.

Certificate of Review

GDPR Applicability Reference Standard

December 18th 2025 10:31:31 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 9:47 AM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:00 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:31 AM EST