International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 32

(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1058 – Supplement on code of practice for personally identifiable information (PII) protection for telecommunications organizations

ITU-T X-series Recommendations – Supplement 32

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Supplement 32 to ITU-T X-series Recommendations

ITU-T X.1058 – Supplement on code of practice for personally identifiable information (PII) protection for telecommunications organizations

Summary

Supplement 32 to X-series Recommendations aims to complement the information provided in ITU-T X.1058 by providing additional implementation guidance for personally identifiable information (PII) protection, which are not described in ITU-T X.1058, but should further be applicable to telecommunications organizations to address PII protection.

The number of telecommunications organizations processing PII is on the rise. Accordingly, expectations for the protection of PII are also increasing.

The protection of PII is driving the need for a set of additional controls and implementation guidance for PII protection, which are applicable to telecommunications organizations. The guidance presented in this Supplement are additions to those described in ITU-T X.1058.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 32	2018-03-29	17	11.1002/1000/13593

Keywords

Controls, implementation guidance, personally identifiable information, telecommunications organizations.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 32 to ITU-T X-series Recommendations

ITU-T X.1058 – Supplement on code of practice for personally identifiable information (PII) protection for telecommunication organizations

1 Scope

This Supplement provides additional implementation guidance for Personally Identifiable Information (PII) protection, to those described in [ITU-T X.1058], which should further be applicable to telecommunications organizations when addressing PII protection.

When addressing PII protection, it is intended that telecommunications organizations should use the associated implementation guidance described in this Supplement as well as those described in [ITU-T X.1058].

This Supplement is applicable to telecommunications organizations which collect, use, and transfer PII as part of their information processing.

2 References

[ITU-T X.1058] Recommendation ITU-T X.1058 (2017) | ISO/IEC 29151:2017, *Information technology – Security techniques – Code of practice for personally identifiable information protection*.

3 Terms and Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 cloud service customer [b-ISO/IEC 19944]: Party which is in a business relationship for the purpose of using cloud services.

3.1.2 cloud service provider [b-ISO/IEC 19944]: Party which makes cloud services available.

3.1.3 control [b-ISO/IEC 27000]: Measure that is modifying risk.

NOTE 1 – Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 – Controls may not always exert the intended or assumed modifying effect.

3.1.4 de-identification process [ITU-T X.1058]: Process of removing the association between a set of identifying data and the data principal, using de-identification techniques.

3.1.5 management [b-ISO 9000]: Coordinated activities to direct and control an organization.

3.1.6 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.1.7 PII controller [b-ISO/IEC 29100]: Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes.

NOTE – A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

3.1.8 PII principal [b-ISO/IEC 29100]: Natural person to whom the personally identifiable information (PII) relates.

NOTE – Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

3.1.9 PII processor [b-ISO/IEC 29100]: Privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller.

3.1.10 policy [b-ISO/IEC 27000]: Intentions and direction of an organization, as formally expressed by its top management.

3.1.11 privacy principles [b-ISO/IEC 29100]: Set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.

3.1.12 processing of PII [b-ISO/IEC 29100]: Operation or set of operations performed upon personally identifiable information (PII).

NOTE – Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, de-identification, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

3.1.13 sensitive PII [b-ISO/IEC 29100]: Category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal.

NOTE – In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.

3.1.14 telecommunications organizations [b-ITU-T X.1051]: Business entities who provide telecommunications services in order to meet the demand of others.

3.1.15 telecommunications service customer [b-ITU-T X.1051]: Person or organization who enters into a contract with telecommunications organizations to be offered telecommunications services by them.

3.1.16 telecommunications services [b-ITU-T X.1051]: Communications using telecommunications facilities, or any other means of providing communications either between telecommunications service users or telecommunications service customers.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 PII protection policy: Overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting.

3.3 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

PII Personally Identifiable Information

4 Overview

4.1 Introduction

This Supplement is structured in a format similar to [ITU-T X.1058]. In cases where objectives and controls specified in [ITU-T X.1058] are applicable without the need for additional information, only

a reference is provided to [ITU-T X.1058]. A PII-specific set of controls and implementation guidance is described.

In cases where controls need additional implementation guidance specific to telecommunications organizations, the [ITU-T X.1058] control is repeated without modification, followed by the specific telecommunications guidance related to the control.

4.2 Objective of this Supplement

This Supplement provides implementation guidance specific to telecommunications organizations applicable to PII protection.

4.3 Structure and intent of this Supplement

This Supplement follows the basic structure of [ITU-T X.1058]. If there is no additional implementation guidance or other information, this Supplement does not include the corresponding [ITU-T X.1058] clauses; guidance and other information described in the [ITU-T X.1058] clauses apply.

5 Information security policies

5.1 Management directions for information security

The objective specified in clause 5.1 of [ITU-T X.1058] applies.

5.1.1 Policies for information security

Clause 5.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should appoint a management-level individual who is in charge of PII protection.

Telecommunications organizations should augment their PII protection policy to contain a statement(s) concerning support for, and commitment to, managing compliance with applicable PII protection legislation and contractual terms agreed upon between the cloud PII processor and its clients (cloud service customers).

5.1.2 Review of the policies for information security

Clause 5.1.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

6 Organization of information security

6.1 Internal organization

The objective specified in clause 6.1 of [ITU-T X.1058] applies.

6.1.1 Information security roles and responsibilities

Clause 6.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should appoint a top management individual, who is responsible and accountable for all PII protection.

Telecommunications organizations should designate a point of contact for use by the PII principal regarding the processing of PII under the PII processing contract.

When telecommunications organizations use a cloud service provider, the telecommunications organizations should maintain a point of contact designated by the cloud service provider regarding the processing of PII under the data processing contract.

In this case, contractual agreements should allocate responsibilities among the cloud PII processors, its sub-contractors and the telecommunications organization, taking into account the type of cloud service.

6.1.2 Segregation of duties

Clause 6.1.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

6.1.3 Contact with authorities

Clause 6.1.4 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

When telecommunications organizations receive inquiries from law-enforcement agencies or investigative organizations regarding PII relating to telecommunications service users, these telecommunications organizations should confirm that the inquiries have been vetted through legitimate processes and procedures, according to national laws and regulations related to PII protection.

Telecommunications organizations should have procedures in place that specify how identified PII-leakage incidents should be reported in a timely manner.

6.2 Mobile devices and teleworking

The objective specified in clause 6.2 of [ITU-T X.1058] applies.

7 Human resource security

During the course of employment (from pre-employment screening to termination of employment and beyond), telecommunications organizations process PII of employees. This information shall be adequately protected throughout its lifecycle.

7.1 Prior to employment

The objective specified in clause 7.1 of [ITU-T X.1058] applies.

7.1.1 Screening

Clause 7.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should also further consider more detailed background checks for candidates that may be given access to PII processing systems. Screening should be carried out with regard to ethics, appropriate knowledge and skills.

7.1.2 Terms and conditions of employment

Clause 7.1.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

The legal rights and responsibilities regarding PII protection, which telecommunications organizations should take into account, are included in the laws and regulations related to PII protection.

Telecommunications organizations should ensure that employees and contractors follow all legal rights and responsibilities regarding PII protection as a term and condition of employment.

7.2 During employment

The objective specified in clause 7.2 of [ITU-T X.1058] applies.

7.2.1 Management responsibilities

Clause 7.2.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should appoint telecommunications engineers and other staff, who have the correct credentials, appropriate knowledge and skills, to be in charge of the supervision of matters related to installation, maintenance and operation of PII protection facilities for all telecommunications business. The relevant telecommunications engineers and other staff should be well aware of their assigned roles and responsibilities.

7.2.2 Information security awareness, education and training

Clause 7.2.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should have educational and training programs in place for relevant staff to be made aware of possible consequences on cloud PII processors (i.e., legal consequences, loss of business, brand or reputational damage), on staff members (i.e., disciplinary consequences) and on PII principals (i.e., physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those handling PII.

7.3 Termination and change of employment

The objective specified in clause 7.3 of [ITU-T X.1058] applies.

The following additional guidance for telecommunications organizations applies:

Employees' PII should be deleted, stored or archived based on data retention policies with notice and consent of the employee.

8 Asset management

8.1 Responsibility for assets

The objective specified in clause 8.1 of [ITU-T X.1058] applies.

8.1.1 Inventory of assets

Clause 8.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

When developing and maintaining an inventory of assets, telecommunications organizations should clearly define and document responsibilities between telecommunications facilities of the organization and those for PII protection.

The list of assets related to PII protection should be comprehensive and cover all assets related to PII protection for network facilities, services and applications.

8.2 Information classification

The objective specified in clause 8.2 of [ITU-T X.1058] applies.

8.2.1 Classification of information

Clause 8.2.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should:

– when partitioning PII, identify PII useful for each individual business process;

– logically separate PII that is useful for each business process;

– manage access rights according to individual business processes (e.g., payroll management, vacation request management, career advancement) and establish a dedicated IT environment for systems that process the most sensitive PII; and

– regularly confirm that PII is partitioned effectively and that recipients and interconnections have not been added.

8.3 Media handling

The objective specified in clause 8.3 of [ITU-T X.1058] applies.

9 Access control

9.1 Business requirement of access control

The objective specified in clause 9.1 of [ITU-T X.1058] applies.

9.1.1 Access control policy

Clause 9.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

9.1.2 Access to networks and network services

Clause 9.1.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should implement role-based access controls, with a limited number of profiles and controlled sets of user access permissions as applicable.

Only authorized users should have access to PII processed by telecommunications services.

9.2 User access management

The objective specified in clause 9.2 of [ITU-T X.1058] applies.

9.2.3 Management of privileged access rights

Clause 9.2.4 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should have a formal authorization process for assigning personnel privileged access rights to massive PII processing operations, taking into account that high-risk PII processing may cause undetected massive breaches of PII from massive batch PII processing operations, i.e., batch query, batch modification, batch export, and batch deletion of PII.

Telecommunications organizations should assign privileged access rights to at least two or more personnel performing high-risk PII processing operations. At least two or more personnel should have different privileged rights by presenting at least two or more access rights to prevent the abuse of PII.

9.3 User responsibilities

The objective specified in clause 9.3 of [ITU-T X.1058] applies.

9.4 System and application access control

The objective specified in clause 9.4 of [ITU-T X.1058] applies.

9.4.1 Information access restriction

Clause 9.4.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Prior to allowing individuals, such as operators and administrators, to use query languages, which enable automatic retrieval of PII from databases, organizations should review the validity of the use of query languages to the PII processing systems.

When using query languages is compliant with protection requirements, organizations should provide a technical means of limiting queries to the extent agreed upon. This can mean, for example, that restrictions of access control can limit the use of queries to a few predefined sensitive fields or records.

10 Cryptography

10.1 Cryptographic controls

The objective specified in clause 10.1 of [ITU-T X.1058] applies.

10.1.1 Policy on the use of cryptographic controls

Clause 10.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should apply cryptography to protect particular types of sensitive PII, such as national identification numbers and passport numbers concerning PII principals.

10.1.2 Key management

Clause 10.1.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

When using cloud service providers, telecommunications organizations may manage cryptographic keys through their entire lifecycle, including generating, storing, retaining, retrieving, distributing, retiring and destroying keys, which are used to protect PII stored in the cloud service provider facilities.

Cryptographic keys for protecting PII should be protected by cryptographic techniques employed by the telecommunications organization. Procedures should be established for handling legal requests for access to these cryptographic keys, e.g., when requested as evidence in a court case, encrypted PII should be made available in unencrypted form.

11 Physical and environmental security

11.1 Secure areas

The objective specified in clause 11.1 of [ITU-T X.1058] applies.

11.1.1 Physical security perimeter

Clause 11.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should implement the following guidance where appropriate for physical security perimeters:

– facilities for processing PII should be equipped with adequate physical intruder detection systems; and

– physical barriers for protecting PII processing facilities should be effectively installed, with all local security policies rigorously enforced, at all times, to ensure the protection of corporate assets.

11.1.2 Physical entry controls

Clause 11.1.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should consider the following guidance:

– operation rooms for PII protection facilities should be protected by adequate strong entry controls; and

– facility visitor's PII should be protected against unauthorized access or viewing, e.g., a visitor's date and time of entry and departure records should be protected; facilities personnel should also check a visitor's belongings, at the point of entry and departure.

11.2 Equipment

The objective specified in clause 11.2 of [ITU-T X.1058] applies.

11.2.1 Equipment siting and protection

Clause 11.2.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

If PII processing systems are sited in the same data centre as telecommunications facilities, telecommunications organizations should implement appropriate measures to protect customers' PII

stored in these systems. Such systems should be physically placed at separate sites in the facility, e.g., they should be placed on a different floor or in a different room.

12 Operations security

12.1 Operational procedures and responsibilities

The objective specified in clause 12.1 of [ITU-T X.1058] applies.

12.1.1 Documented operating procedures

Clause 12.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

12.1.2 Change management

Clause 12.1.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should consider procedures and records for installation, relocation and removal of PII processing facilities.

Telecommunications organizations should implement change management processes for PII processing facilities, including both physical and logical modifications. When applicable, change management processes should be reported to and approved by the designated risk owner.

12.1.3 Capacity management

Clause 12.1.4 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

12.1.4 Separation of development, testing and operational environments

Clause 12.1.5 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

When individuals require access to areas for which they normally are not authorized (e.g., operational areas), robust approval mechanisms should be implemented. Organizations should maintain a record of all such approvals.

12.2 Protection from malware

The objective specified in clause 12.2 of [ITU-T X.1058] applies.

12.3 Backup

The objective specified in clause 12.3 of [ITU-T X.1058] applies.

12.4 Logging and monitoring

The objective specified in clause 12.4 of [ITU-T X.1058] applies.

12.4.1 Event logging

Clause 12.4.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Event logs may contain PII. Telecommunications organizations should put in place measures, such as access control, to ensure that logged information is only used for its intended purposes.

12.5 Control of operational software

The objective specified in clause 12.5 of [ITU-T X.1058] applies.

12.6 Technical vulnerability management

The objective specified in clause 12.6 of [ITU-T X.1058] applies.

12.7 Information systems audit considerations

The objective specified in clause 12.7 of [ITU-T X.1058] applies.

12.7.1 Information systems audit controls

Clause 12.7.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

When conducting reviews of logging data, telecommunications organizations should provide procedures and technical means to protect customers' PII which may be contained in this logging data.

13 Communications security

13.1 Network security management

The objective specified in clause 13.1 of [ITU-T X.1058] applies.

13.2 Information transfer

The objective specified in clause 13.2 of [ITU-T X.1058] applies.

13.2.1 Information transfer policies and procedures

Clause 13.2.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Information hiding techniques should be implemented to de-identify a PII principal from their own PII or in combination with other related information.

Information hiding should:

– provide only minimum information related to business requirements; and

– hide PII, as much as possible, without affecting service operations.

Information hiding should be used in the following scenarios:

– for graphical user interfaces (GUIs) used in business operations supporting systems, scenarios where PII is required to be displayed, as well as scenarios where PII is retrieved in open environments (e.g., at open spaces and by social network channels); and

– for external interfaces, scenarios where PII is required to be transferred to external service systems, e.g., bank systems.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

The objective specified in clause 14.1 of [ITU-T X.1058] applies.

14.2 Security in development and support processes

The objective specified in clause 14.2 of [ITU-T X.1058] applies.

14.3 Test data

The objective specified in clause 14.3 of [ITU-T X.1058] applies.

15 Supplier relationships

15.1 Information security in supplier relationships

The objective specified in clause 15.1 of [ITU-T X.1058] applies.

15.1.1 Information security policy for supplier relationships

Clause 15.1.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Organizations should stipulate each party's obligations in an explicit written agreement accepted by both parties, when subcontracting is involved.

Appropriate PII protection should be included in the PII processor's contract in order to hold the processors accountable for their processing of PII.

15.1.3 Information and communication technology supply chain

Clause 15.1.4 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Supplier agreements between telecommunications organizations and its customers should include appropriate controls to ensure the non-disclosure of sensitive PII.

15.2 Supplier service delivery management

The objective specified in clause 15.2 of [ITU-T X.1058] applies.

16 Information security incident management

16.1 Management of information security incidents and improvements

The objective specified in clause 16.1 of [ITU-T X.1058] applies.

16.1.1 Learning from information security incidents

Clause 16.1.7 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should establish mechanisms and/or procedures for sharing lessons learned from past information security incidents to improve incident management including PII protection.

17 Information security aspects of business continuity management

17.1 Information security continuity

The objective specified in clause 17.1 of [ITU-T X.1058] applies.

17.2 Redundancies

The objective specified in clause 17.2 of [ITU-T X.1058] applies.

18 Compliance

18.1 Compliance with legal and contractual requirements

The objective specified in clause 18.1 of [ITU-T X.1058] applies.

18.2 Information security reviews

The objective specified in clause 18.2 of [ITU-T X.1058] applies.

Appendix I

Extended control set for PII protection

I.1 General policies for the use and protection of PII

Clause A.2 and the associated implementation guidance and other information specified in [ITU T-X.1058] apply.

I.2 Consent and choice

The objective specified in clause A.3 of [ITU-T X.1058] applies.

I.2.1 Consent

Clause A.3.1 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

It is recognized, through the words 'where feasible and appropriate', that there are certain cases where consent may be clearly implied or where it would not be necessary to provide a mechanism to obtain the consent.

I.2.2 Choice

Clause A.3.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

I.3 Purpose legitimacy and specification

The objective specified in clause A.4 of [ITU-T X.1058] applies.

I.4 Collection limitation

The objective specified in clause A.5 of [ITU-T X.1058] applies.

The following additional guidance for telecommunications organizations applies:

PII should either be collected from the PII principal directly, or the purpose of collection by the collector, the consent or other legal grounds, and the absence of revoking choice should be documented.

In cases where the PII is transferred to another organization, an appropriate process should be established to: update records upon mirroring content updates, and revoke the consent of PII principal requests from other organizations. Telecommunications organizations should check regularly to ensure that no additional PII is collected in relation to the PII initially identified.

I.5 Data minimization

The objective specified in clause A.6 of [ITU-T X.1058] applies.

I.6 Use, retention and disclosure limitation

The objective specified in clause A.7 of ITU-T X.1058 applies.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should:

– delete unnecessary PII immediately or as soon as is practical;

– reduce the types of PII stored (e.g., delete social security numbers if no longer needed), shorten the retention period for PII that is maintained if it is not necessary to keep it for long periods of time;
– ensure an adequate level of protection where PII is transferred or processed across borders;
– retain PII collected for monitoring purposes as long as it is necessary to fulfil the legitimate purposes identified in the notice or as required by law;
– dispose of PII collected for monitoring when it is no longer necessary to retain it;
– retain PII collected for meeting data retention requirements for only as long as is necessary to fulfil the purposes identified in the notice or as required by legal requirement;
– appropriately dispose of PII collected, for meeting data retention requirements, when it is no longer necessary to retain it; and
– use a secure deletion tool for electronic documents and a degaussing device for storage units that use magnetic technologies, in order to do the above.

I.7 Accuracy and quality

The objective specified in clause A.8 of [ITU-T X.1058] applies.

I.7.1 Data quality

Clause A.8 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

To minimize data inaccuracy, to the extent possible, PII should be entered into information systems directly by the PII principal without the need for another person to transcribe the data. However, in the event that transcription of the PII is unavoidable, organizations should consider enabling the PII principal to validate the transcribed PII. This would help in correcting errors before any consequential damage results from the processing of inaccurate PII.

I.8 Openness, transparency and notice

The objective specified in clause A.9 of [ITU-T X.1058] applies.

I.9 PII principal participation and access

The objective specified in clause A.10 of [ITU-T X.1058] applies.

I.10 Accountability

The objective specified in clause A.11 of [ITU-T X.1058] applies.

I.10.1 Governance

Clause A.11.1 and the associated implementation guidance and other information specified in ITU-T X.1058] apply.

I.10.2 Privacy risk assessment

Clause A.11.2 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

I.10.3 Privacy requirement for contractors and service providers

Clause A.11.3 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

I.10.4 Privacy monitoring and auditing

Clause A.11.4 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

I.10.5 PII protection awareness and training

Clause A.11.5 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

I.10.6 PII protection reporting

Clause A.11.6 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

I.11 Information security

Clause A.12 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should provide a means to periodically monitor and audit PII protection policies of contractors to ensure effective implementation of requirements specified in service-level agreements.

I.12 Privacy compliance

Clause A.13 and the associated implementation guidance and other information specified in [ITU-T X.1058] apply.

The following additional guidance for telecommunications organizations applies:

Telecommunications organizations should implement security controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which PII is held.

Appendix II

Privacy principles in ISO/IEC 29100

This appendix provides a list of privacy principles described in [b-ISO/IEC 29100] which has been developed from various existing privacy principles by a number of states, countries and international organizations, e.g., Organization for Economic Co-operation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC). These privacy principles should be used to guide design and development and to implement privacy policies and controls.

– consent and choice;
– purpose legitimacy and specification;
– collection limitation;
– data minimization;
– use, retention and disclosure limitation;
– accuracy and quality;
– openness, transparency and notice;
– individual participation and access;
– accountability;
– information security;
– privacy compliance.

Bibliography

[b-ITU-T X.1051] ITU-T Recommendation X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[b-ISO 9000] ISO 9000:2015, *Quality management systems – Fundamentals and vocabulary*.

[b-ISO/IEC 19944] ISO/IEC 19944:2017, *Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27018] ISO/IEC 27018:2014, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

[b-ISO/IEC 29134] ISO/IEC 29134:2017, *Information technology – Security techniques – Guidelines for privacy impact assessment*.

[b-BS 10012] British Standard 10012 (2017), *Data protection. Specification for a personal information management system*.

[b-EC] European Commission (2011), *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*.

[b-NIST SP 800-53] NIST Special Publication 800-53 Appendix J (2011), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-NIST SP 800-122] NIST Special Publication 800-122 (2010), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019