



ISO/IEC JTC 1/SC 27/WG 5 "Identity management and privacy technologies"

Convenorship: DIN

Convenor: Rannenberg Kai Mr Prof. Dr.



ISO/PC 317 - N205 - Text for CD Ballot ISO 31700

Document type	Related content	Document date	Expected action
General document / Other		2021-06-16	INFO



ISO/PC 317 "Consumer protection: privacy by design for consumer goods and services"

Secretariat: **BSI**

Committee Manager: **Stride Jean Ms**



Text for CD Ballot: ISO 31700: Consumer Protection: Privacy by design for consumer goods and services

Document type	Related content	Document date	Expected action
Ballot / Reference document	Project: ISO/CD 31700 Ballot: ISO/CD 31700.2 (restricted access)	2021-06-01	VOTE by 2021-07-28

**Consumer protection –
Privacy by design for consumer goods and services**

CD2 stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

14 Contents

15	Foreword	v
16	Introduction.....	vi
17	1 Scope	1
18	2 Normative references	1
19	3 Terms and definitions.....	1
20	4 General	6
21	4.1 Introduction.....	6
22	4.2 Design capabilities to enforce consumer privacy rights	7
23	4.3 Develop capability to determine consumer privacy preferences.....	8
24	4.4 Design human computer interface (HCI) for privacy	9
25	4.5 Assign relevant roles and authorities	10
26	4.6 Establish multi-disciplinary responsibilities	10
27	4.7 Develop privacy knowledge, skill and ability.....	11
28	4.8 Ensure knowledge of privacy controls.....	12
29	4.9 Documented information management.....	13
30	5 Transparent consumer communication during the product use lifecycle	14
31	5.1 Introduction.....	14
32	5.2 Clear responsibility for transparently providing understandable information to	
33	consumers.....	15
34	5.3 Accountability to Responsible persons	16
35	5.4 Responding to consumer inquiries and complaints	16
36	5.5 Communicating to diverse consumer population.....	17
37	5.6 Prepare data breach communications.....	18
38	5.7 Design post-retirement communication	18
39	6 Risk management	19
40	6.1 Introduction.....	19
41	6.2 Identify inputs to privacy risk assessment.....	19
42	6.3 Conduct a privacy risk assessment	21
43	6.4 Assess privacy capabilities of third parties.....	22
44	6.5 Assess Retirement Privacy Risks	22
45	6.6 Establish requirements for privacy controls.....	23
46	6.7 Design privacy controls for retirement.....	24
47	6.8 Monitor and update risk assessment	25
48	6.9 Include privacy risks in cybersecurity resilience design.....	26
49	7 Integrating privacy into the service consumer product's service management lifecycle	26
50	7.1 Introduction.....	26
51	7.2 Integrate privacy design in service development.....	26
52	7.3 Identify privacy controls to develop.....	27
53	7.4 Develop privacy controls	28
54	7.5 Manage the transition of privacy services.....	28
55	7.6 Manage the Operation of Privacy Services	29
56	7.7 Prepare Breach Management.....	30
57	7.8 Design privacy control testing	31
58	7.9 Operate privacy controls for the processes and aligned products through the product	
59	lifecycle.	32
60	8 Design for end of PII lifecycle	32
61	8.1 Introduction.....	32
62	8.2 Design privacy controls for end of use.....	33

63	Bibliography	35
64		

65 Foreword

66 ISO (the International Organization for Standardization) is a worldwide federation of national standards
67 bodies (ISO member bodies). The work of preparing International Standards is normally carried out
68 through ISO technical committees. Each member body interested in a subject for which a technical
69 committee has been established has the right to be represented on that committee. International
70 organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO
71 collaborates closely with the International Electrotechnical Commission (IEC) on all matters of
72 electrotechnical standardization.

73 The procedures used to develop this document and those intended for its further maintenance are
74 described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the
75 different types of ISO documents should be noted. This document was drafted in accordance with the
76 editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

77 Attention is drawn to the possibility that some of the elements of this document may be the subject of
78 patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any
79 patent rights identified during the development of the document will be in the Introduction and/or on
80 the ISO list of patent declarations received (see www.iso.org/patents).

81 Any trade name used in this document is information given for the convenience of users and does not
82 constitute an endorsement.

83 For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and
84 expressions related to conformity assessment, as well as information about ISO's adherence to the World
85 Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see
86 www.iso.org/iso/foreword.html.

87 This document was prepared by Project Committee 317 Consumer Protection – privacy by design for
88 consumer goods and services

89 Any feedback or questions on this document should be directed to the user's national standards body. A
90 complete listing of these bodies can be found at www.iso.org/members.html

91 Introduction

92 Consumers' trust in how their **personally identifiable information** (PII) is processed by organizations
 93 and the digital goods and services they produce, as well as how well their privacy needs are met, are a
 94 defining concern for the digital economy. When a consumer's PII has been compromised because of lax,
 95 outdated or non-existent privacy practices, the consequences for the consumer can be severe. In addition,
 96 there will be damage to the consumer's trust of this and other products, and potentially legal or
 97 reputational impacts on the business. Privacy by Design¹ [1, 2, 3, 4, 5, 5.1] is an approach that takes into
 98 account the privacy of consumers early on in the design of a product, before it reaches a consumer. It
 99 means that a product or service has user-oriented privacy settings by default from its design through its
 100 lifecycle, without placing undue burden on the consumer.

101 This document provides high-level requirements for **privacy by design** to assist organizations in
 102 building privacy into the design process and throughout the lifecycle of a consumer product, including
 103 data processing by the consumer. It also provides recommendations and guidance.

104 This document considers three perspectives on privacy by design as outlined below. First, each
 105 perspective is considered by itself, and then they are considered together as part of designing privacy
 106 into the lifecycle of consumer product.

107 Empowerment and transparency

108 The best outcomes from privacy by design methodologies are usually achieved when the product design
 109 effort is focused on the interests and needs of the consumers. Using a **human-centered** approach to
 110 **design** and development benefits not only the consumer but has substantial economic value for
 111 organizations. Highly usable systems and goods tend to be more successful both technically and
 112 commercially. Empowering consumers to play an active role in the management of their own data is a
 113 critical check against abuses and misuses of privacy and personal data. The ability for the consumer to
 114 understand how and in what context their PII is being processed by the product is consistent with the
 115 notion of transparency and trust.

116 There is a growing demand for provable software privacy claims, systematic methods of privacy due
 117 diligence, and greater transparency and accountability in the design and operation of software systems
 118 that process PII. The goal is to promote wider adoption, gain trust and market success, and demonstrate
 119 legal and regulatory compliance. The intent is not to stand in the way of innovative solutions, but to
 120 analyse the consumer perspective and succinctly document how privacy considerations were
 121 approached.

122 Institutionalization and responsibility

123 In today's world of shared platforms, interconnected devices, cloud applications, and personalization, it
 124 is ever more important to delineate responsibilities and perspectives of the consumer of the
 125 goods and services that process PII from other stakeholders in the ecosystems in which the goods or
 126 service operates.

127 This document focuses on the consumer perspective when thinking about privacy by design. It will assist
 128 the organization to institutionalize robust privacy norms throughout the organization and ecosystem
 129 such that the consumer's behavioural engagement with the product(s) and their expectations and

¹ The term "privacy by design" was originally used by Ann Cavoukian when she was the Information and Privacy Commissioner of Ontario, Canada. The framework consists of "7 foundational principles" that emphasize the need to be proactive in considering privacy requirements at the design phase (or earlier) throughout the entire data lifecycle. The individual should not bear the burden of striving for protection when using a service or a product but enjoy "automatically" (no need for active behaviour) the fundamental right of privacy and personal data protection. [2]

perceptions of privacy are designed early and throughout the lifecycle process. This way, decisions concerning consumer privacy needs and expectations will not only be more consistent and systematic, but also become a functional requirement alongside the interests of other stakeholders. Leadership is an essential element to embed and institutionalize privacy into design processes, through a demonstrated commitment to privacy by design.

Ecosystem and lifecycle

It has become clear that a privacy by design approach can and should be applied to the broader information ecosystems in which both technologies and organizations are embedded and must function. Privacy and consumer protection benefit from taking a holistic, integrative approach that considers as many contextual factors as possible – even (or especially) when these factors lie outside the direct control of any particular actor, organization, or component in the system.

The ways that consumer products use PII can be complex, particularly when multiple stakeholders are involved. For instance, a voice or virtual assistant could involve systems running in the home (home equipment) as well as systems running externally (organizational servers). They involve multiple lifecycles. Beyond the mere lifecycle of the consumer product (e.g. the device acting as a home assistant), other lifecycles might be involved such as, data lifecycle, organizational server lifecycles, system development lifecycle, etc. The lifecycle may involve cross-functional collaboration on activities such as quality checking and certification. The operation of a consumer goods and services can therefore involve a complex network of stakeholders. There is a need to identify the roles and responsibilities of the stakeholders in the ecosystems.

This document allows organizations to demonstrate that they respect the privacy of their consumers, not only in the design of the product, but throughout the product and data lifecycles.

This document is intended to be applicable to all products that use personal data, whether physical goods, or intangible services such as software as a service, or a mixture of both. It is intended to be scalable to the needs of all types of organizations in different countries, different sectors, regardless of organization size, sector, or maturity

Some organizations may wish to use this document to redesign internal processes to incorporate privacy by design. Although the concept of privacy by design necessitates the incorporation of privacy controls early in the product lifecycle, before its release to consumers, some organizations may find that the intention of incorporating privacy by design only forms later in the product lifecycle.

This document is neutral on the methodologies that organization may adopt to embed privacy controls, the technology that may be used to operate privacy controls, and the types of control that an organization may select to protect its consumers' privacy.

The primary audiences for this document are those staff of organizations, and their suppliers, who are responsible for the design and operation of consumer products.

The secondary audiences include:

- Senior Product and Service Management,
- Privacy Compliance and Legal Teams,
- Risk Management functions in organizations that create or operate products or components/ ingredients that process PII.

A further audience is Public Interest Stakeholders, for example:

- consumer advocates, consumer organizations, consumer associations,
- privacy and consumer protection regulators,
- privacy and consumer policy makers,

- 175 • third-party privacy accountability agents, and other organizations which supervise the consumer
- 176 product sector.

177 **Consumer protection – Privacy by design for consumer goods and** 178 **services**

179 **1 Scope**

180 This document establishes high-level requirements for privacy by design to protect privacy throughout
181 the lifecycle of a consumer product, including data processing by the consumer.

182 **2 Normative references**

183 There are no normative references in this document.

184 **3 Terms and definitions**

185 For the purposes of this document, the following terms and definitions apply.

186 ISO and IEC maintain terminological databases for use in standardization at the following addresses:

187 — ISO Online browsing platform: available at <https://www.iso.org/obp>

188 — IEC Electropedia: available at <http://www.electropedia.org/>

189 **3.1**

190 **consumer**

191 individual member of the general public purchasing or using property, products or services for private
192 purposes.

193 Note 1 to entry: For the purposes of this document, the term consumer only applies to natural persons,
194 not legal entities.

195 Note 2 to entry: The term “consumer” (including elderly, children and persons with disabilities) covers
196 both customers and potential customers. Consumer products and services can be onetime purchases or
197 long-term contracts or obligations.

198 Note 3 to entry: Property, products or services purchased or used by Consumers may be used for
199 professional purposes and not only private ones (e.g., Bring Your Own Device).

200 [SOURCE: ISO 26000:2010, 2.2, modified — Note 1 to entry has been added.]

201 [SOURCE: ISO/IEC Guide 14:2018, 3.2]

202 **3.2**

203 **personally identifiable information (PII)**

204 any information that (a) can be used to establish a link between the information and the natural person
205 to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

206 Note 1 to entry: The “natural person” in the definition is the PII principal. To determine whether a PII
207 principal is identifiable, account should be taken of all the means which can reasonably be used by the

208 privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII
209 and the natural person.

210 Note 2 to entry: This definition is included to define the term PII as used in this document. A public cloud
211 PII processor is typically not in a position to know explicitly whether information it processes falls into
212 any specified category unless this is made transparent by the cloud service customer.

213 [SOURCE: ISO/IEC 29100:2011/Amd 1:2018, 2.9, modified — Note 2 to entry has been added.]

214 Note 3: Those using this document are encouraged to apply the term and definition that they find most
215 usable, because the language to refer to this concept varies across jurisdictions (e.g., personally
216 identifiable information, personal information, personal data).

217 3.3

218 **personal information lifecycle**

219 a natural life cycle, from creation or origination, collection, through storage, use and transfer to its
220 eventual disposal (e.g., secure destruction).

221 [Source: ISO 29151]

222 3.4

223 **privacy by design**

224 approach in which privacy is considered at the initial design stage and throughout the complete lifecycle
225 of products, processes or services including retirement and deletion of PII that involve processing
226 personally identifiable information.

227 3.5

228 **product**

229 product refers to those goods and services designed and produced primarily for, but not limited to,
230 personal use, including its components, parts, accessories, instructions and packaging which can include
231 related services or allow for services to be separately acquired and use or applied. Services is considered
232 to be the result of at least one activity, necessarily performed at the interface between the supplier and
233 customer, that is generally intangible. Products are a set of interrelated or interacting activities which
234 transforms inputs into outputs, of which four generic categories are services, software, hardware and
235 processed materials.

236 [SOURCE: ISO 9000:2005, Definitions 3.4.1 and 3.4.2]

237 [SOURCE ISO 22059:2020, 3.3]

238 3.6

239 **responsible person**

240 designated person suitably trained and qualified by knowledge and practical experience and in
241 possession of the necessary instructions to enable the assigned task to be carried out

242 ISO 24134:2006(en), 3.9

243 3.7

244 **vulnerable consumer**

245
246 consumer (3.1) who could be at greater risk of harm from products (3.5) due to their age, level of literacy,
247 physical condition or limitations, or inability to access product safety information

248 [SOURCE: ISO 10377:2013, 2.3]

249 [SOURCE: ISO 22059:2020, 3.20]

250 **3.8**

251 **vulnerable person**

252 person who is permanently or temporarily unable to represent their own interests through a mental,
253 emotional, societal or physical cause that may limit their capacity to make voluntary and informed
254 decisions

255 [SOURCE: ISO 20252:2019, 3.105]

256 **3.9**

257 **privacy risk**

258 the likelihood that individuals will experience problems resulting from PII processing, and the impact should
259 they occur.

260 Note 1 to entry: Risk is defined as the “effect of uncertainty on objectives” in ISO Guide 73 and ISO 31000.

261 Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to,
262 understanding or knowledge of, an event, its consequence, or likelihood.

263 Note 3 to entry: Privacy risk can be assessed as the likelihood and impact of individuals experiencing
264 adverse consequences resulting from PII processing.

265 **3.10**

266 **privacy risk assessment**

267

268 overall process of identifying, analysing, evaluating, consulting, communicating and planning the
269 treatment of potential privacy impacts with regard to the processing of personally identifiable
270 information, framed within an organization's broader risk management framework

271 [SOURCE: ISO/IEC 29100:2011/AMD 1:2018]

272 Note 1 to entry: This process may be documented in various ways, including with a privacy impact
273 assessment

274 **3.11**

275 **use case**

276 description of a sequence of interactions between a user and a system (e.g., IT or business process
277 component) used to help identify, clarify, and organize requirements to support a specific business goal

278 [SOURCE: ISO/TR 14872:2019, 3.9]

279 Note 1 to entry: actors can be users, engineers, systems

280 Note 2 to entry: a system of interest in this standard is a consumer product

281
282 **3.12**

283 **consumer vulnerability**

284
285 state in which an individual can be placed at risk of detriment, during his/her interaction with a service
286 provider due to the presence of personal, situational and market environment factors

287
288 [SOURCE:ISO/IEC Guide 76:2020, 3.14]

289
290 **3.13**

291 **documented information**

292
293 information required to be controlled and maintained by an **organization** and the medium on which it is
294 contained

295
296 Note 1 to entry: Documented information can be in any format and media and from any source.

297 Note 2 to entry: Documented information can refer to

- 298 • — the **management system** , including related **processes** ;
- 299 • — information created in order for the **organization** to operate (documentation);
- 300 • — evidence of results achieved (records).

301
302 ISO/IEC 27000:2018(en)

303
304 Note 3 to entry (new): Documented information is synonymous with “document” or “artefact” (or
305 “artifact”).

306
307 **3.15**

308 **privacy controls**

309
310 measures that treat privacy risks by reducing their likelihood or their consequences

311
312 Note 1 to entry: Privacy controls include organizational, physical and technical measures, e.g., policies,
313 procedures, guidelines, legal contracts, management practices or organizational structures.

314 Note 2 to entry: Control is also used as a synonym for safeguard or countermeasure.

315
316 ISO/IEC 29100:2011(en), 2.14

317
318 **3.16**

319 **requirement**

320
321 statement which translates or expresses a need and its associated **constraints** (3.18) and **conditions**
322 (3.17)

323 Note 1 to entry: Requirements exist at different levels in the system structure.

324 Note 2 to entry: A requirement is an expression of one or more particular needs in a very specific,
325 precise and unambiguous manner.

326 Note 3 to entry: A requirement always relates to a system, software or service, or other item of interest.

327 [SOURCE: ISO/IEC/IEEE 2914:2018]

328 **3.17**

329 **condition**

330 measurable qualitative or quantitative **attribute** (3.19) that is stipulated for a **requirement** (3.16) and
 331 that indicates a circumstance or event under which a requirement applies

332 **3.18**

333 **constraint**

334 externally imposed limitation on the system, its design, or implementation or on the process used to
 335 develop or modify a system

336 Note 1 to entry: A constraint is a factor that is imposed on the solution by force or compulsion and may
 337 limit or modify the design.

338 **3.19**

339 **attribute**

340 inherent property or characteristic of an entity that can be distinguished quantitatively or qualitatively
 341 by human or automated means

342 Note 1 to entry: ISO 9000 distinguishes two types of attributes: a permanent characteristic existing
 343 inherently in something; and an assigned characteristic of a product, process, or system (e.g., the price
 344 of a product, the owner of a product).

345 [SOURCE: ISO/IEC 25000:2014, 4.1, modified — The original NOTE 1 has been removed; NOTE 2 has
 346 become Note 1 to entry.]

347 **3.20**

348 **aligned product**

349 supports some aspect of a product, but is not necessarily directly related to the functionality of the
 350 product. It can run parallel and or be tangential such as product registration, processing of payment,
 351 technical support, support forum participation, and training video packages. These may be hosted and
 352 managed by the organization that designs the product or may not be.

353 **3.21**

354 **EOL product**

356 product that is at no longer useful or needed from the customer's point of view, because the product is
 357 broken, no longer functions properly or no longer satisfies the customer's requirements or an
 358 organization chooses to no longer support or continue to produce a product.

360 [SOURCE: ISO 22450:2020, 3.8]

361 **3.22**

362 **retirement**

364 withdrawal of active support by the operation and maintenance organization, partial or total replacement
 365 by a new system, or installation of an upgraded system [ISO/IEC 12207:2008 Systems and software
 366 engineering — Software life cycle processes, 4.38; ISO/IEC TS 24748-1:2016 Systems and software
 367 engineering — Life cycle management — Part 1: Guide for life cycle
 368 management, 2.43; ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle
 369 processes, 4.1.39]

370 2. permanent removal of a system or component from its operational environment

371 [SOURCE: ISO/IEC/IEEE 24765:2017, 3.3486]

372 3.23

373 human - centered design

374
375 approach to system design and development that aims to make interactive systems more usable by
376 focusing on the use of the system; applying human factors, ergonomics and usability knowledge and
377 techniques [ISO/IEC 25063:2014 Systems and software engineering — Systems and software product
378 Quality Requirements and Evaluation (SQuaRE) Common Industry Format (CIF) for usability: Context of
379 use description, 3.6]

380 Note 1 to entry: The term "human-centered design" is used rather than "user-centered design" to
381 emphasize that design impacts a number of stakeholders, not just those typically considered as users.
382 However, in practice, these terms are often used synonymously. Usable systems can provide a number of
383 benefits including improved productivity, enhanced user well-being, avoidance of stress, increased
384 accessibility, and reduced risk of harm.

385 4 General

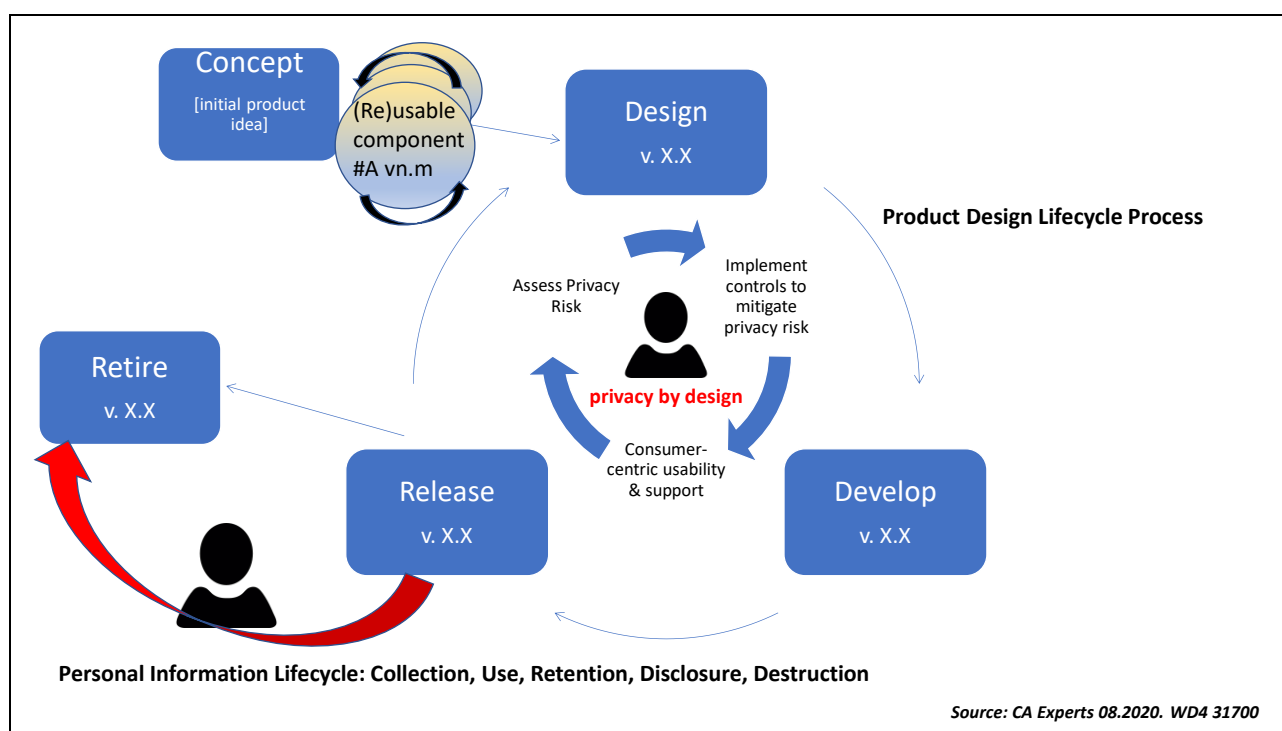
386 4.1 Introduction

387 In order to implement and adhere to privacy by design for consumer **products**, there are **requirements**
388 which shall be continuously and consistently applied. Consumer privacy rights and preferences can play
389 an important and informative role when defining privacy requirements for the consumer product.

390 PII has a natural life cycle, from creation or origination, collection, through storage, use and transfer to
391 its eventual disposal (e.g., secure destruction). The value of, and risks to, PII may vary during its life cycle,
392 but protection of PII remains important to some extent at all stages and in all contexts of its life
393 cycle. Information systems also have life cycles within which they are conceived, specified, designed,
394 developed, tested, implemented, used, maintained, and eventually retired from service and disposed of.

395 PII protection should also be taken into account at each of these stages. New system developments and
396 changes to existing systems present opportunities for organizations to update and improve security
397 controls as well as controls for the protection of PII, taking actual incidents, and current and projected
398 information security and privacy risks into account. [6]
399

400 As illustrated in Figure 1 below, the PII lifecycle and the product lifecycle are not one in the same. The
401 point at which the product is conceived as an idea is when the product's lifecycle starts. It only fully ends
402 when no instances of the device or service are still in existences, and all associated PII has been destroyed.
403 However, the processing of PII associated with the product starts when customers' PII is collected to
404 support the design and development of the product. This is the start of the PII lifecycle which only ends
405 when any PII associated with the product is no longer processed. The arc of the PII lifecycle extends from
406 the creation or collection of PII by a product to its destruction or disposal. The product lifecycle starts
407 with the inception or ideation of a product to product disposal even after support for the product has
408 ended and after the user has retired the product. Sometimes the PII lifecycle extends beyond the product
409 lifecycle. For a product to be designed with privacy in mind its designers need to understand both for
410 the product being designed and set requirements that protect the privacy and the PII of the users of the
411 product and those who interact with it throughout both lifecycles.



4.2 Design capabilities to enforce consumer privacy rights

4.2.1 Requirement CD2R001:

The organization shall ensure the **consumer** can exercise their privacy rights under legal and regulatory requirements and contractual obligations.

4.2.2 Explanation

Privacy is about recognizing that the dominion of the PII does not rest with the organization. Though the organization may retain physical control of data, the decisions about PII are governed by law or regulation, by cultural norms, by unilateral policy, by contract, by economics, or by technical controls that implement individual consent and personal preferences [CD2R002]. [7, 8, 9, 10, 11, 11.1, 12]

The organization establishes a process so the consumers can exercise their privacy rights. Privacy rights include: individual control of PII; consent change; information through privacy notice; access to PII; portability; right to be forgotten; correction). The consumers may also have the opportunity to easily configure some privacy preferences (including the activation or deactivation of functions or location tracing) in the product or service. Due to their effect or potential effect on the organization's ability to consistently provide products that meet consumer and applicable statutory and regulatory requirements, it is important to include privacy needs and expectation of consumers into the organization's process of examining those of interested parties. Consumer empowerment involves the ability to play a participatory role and to exercise effective privacy rights throughout the life cycle of their own PII that is processed by the product.

4.2.3 Guidance

CD2G001.01: The organization should determine its role as a PII controller (including as a joint PII controller) and/or a PII processor

CD2G001.02: The organization should follow a privacy information management framework Refer to Privacy Information Management Framework. Organizations developing consumer product(s) [enabled

437 by or affecting PII] should consider ISO/IEC 27701 or a similar privacy information management system
438 which provides requirements and guidelines for a PIMS [11, 13, 14].

439 CD2G001.03: Do not surreptitiously access or collect PII. An application must not secretly access and
440 collect PII about users.

441 CD2G001.04: Ensure usability and avoid excessive user prompts that will burden the user. Consider the
442 user experience.

443 CD2G001.05: Provide a short and genuinely informative privacy statement explaining in clear simple
444 terms how the consumer can get a copy of their PII or correct and update their PII. ISO/IEC 29184:2020
445 Information technology — Online privacy notices and consent [15]

446 CD2G001.06: A consumer products should access, collect and use only the minimum information required:
447 to provision, operate or maintain the application; to meet identified business purposes to meet legal
448 obligations.

449 CD2G001.07: Consumer privacy rights and preferences can play an important and informative role when
450 defining privacy requirements for the consumer product, discussed in CD2R015 inputs into privacy risk
451 assessment

452 CD2G001.08: company commitments (e.g., privacy policy or public statements) should be reviewed when
453 configuring consumer privacy settings in new or modified products to ensure no violation of company
454 commitments to users

455 **4.3 Develop capability to determine consumer privacy preferences**

456 **4.3.1 Requirement CD1R002:**

457 The organization shall determine consumer needs and expectations related to processing of their PII by
458 products designed and developed for consumers.

459 **4.3.2 Explanation**

460 Each consumer may have very different levels of insight into how distinct technologies work, for example,
461 the complexities of networks (communication networks, social networks, personal networks, etc.),
462 information communication technologies (ICTs) and other digital components with which a consumer
463 may interact. Advances in computing impact PII. A piece of information that may not appear to identify
464 a consumer, when linked with other sets of information, may actually produce results that identify
465 someone. IP addresses, MAC addresses and other types of information that was once considered machine
466 data or telemetry is now considered in many regions personal when it those pieces of information can
467 reasonably be linked to an end-user's device. The product is designed to be used by consumers. The
468 processing of their PII enables the product to function, and the organization to support the consumer
469 during the lifecycle of the product. Unless the organization has a clear view about consumers' privacy
470 preferences, it will be difficult to design the product to address these preferences in a way that both: (i)
471 protects the privacy of the consumer's PII; and (ii) enables the organization to meets its other obligations
472 (whether to the Consumer specifically or more generally under applicable laws).

473 Consumers have a range of capabilities and vulnerabilities² [16, 17, 18] that will affect how they interact
474 with the product and its privacy controls. Unless the organization understands its consumers well, it

² Refer to ISO/CD 22458 3.5 consumer vulnerability: state in which an individual can be placed at risk of detriment, during his/her interaction with a service provider due to the presence of personal, situational and market environment factors [SOURCE: ISO/IEC Guide 76:2020, 3.14] 3.12 vulnerable situation: temporary or permanent circumstance which places a consumer at risk of harm or disadvantage, if an organization does not act with appropriate levels of care

475 cannot be certain that the design of those privacy controls that require consumer action or inaction, will
476 operate as designed.

477 The use of the product by consumers will also place obligations on the organization in the form of privacy
478 rights. These obligations can be onerous for the organization, or can be designed to be effortless. Unless
479 the organization understands the consumers role in how it might fulfil these obligations, the organization
480 might waste considerable resources, while not meeting its obligations.

481 **4.3.3 Guidance**

482 CD2G002.01: If the product has privacy controls that can be operated by the consumer, the consumer
483 should be advised how to operate them, in order to prevent errors, either knowingly or unknowingly

484 CD2G002.02: The organization should understand how the consumer might operate privacy controls in
485 this way so that the product's privacy controls can remain robust notwithstanding the actions or
486 inactions of consumers.

487 CD2G002.03: The organization should see its existing and future consumers as a key resource in the
488 product lifecycle. This should and take the form of a formal approach to engaging with consumers.

489 CD2G002.04: Consumers views and preferences should be sought as part of the product design process
490 to ensure that the product's privacy controls will operate as designed, in a way that provides an
491 acceptable user experience for consumers.

492 CD2G002.05: Consumer privacy rights and preferences can play an important and informative role when
493 defining privacy requirements for the consumer product, discussed in CD2R015

494 CD2G002.06: Privacy settings and privacy management measures should take into account the
495 characteristics of the target consumers. In particular, it is important to consider minors, elderly, and
496 people with low technology literacy.

497 **4.4 Design human computer interface (HCI) for privacy**

498 **4.4.1 Requirement CD2R003:**

499 Privacy settings that can be operated by consumers shall be designed bearing in mind their wide range
500 of capabilities and disabilities, particularly sensory impairments, and adjust the assumptions around
501 privacy controls operation accordingly.

502 **4.4.2 Explanation**

503 Where a consumer might, or must, operate privacy controls over the product, these needa to be defined,
504 documented in the **use cases**, and designed to take into account user experience, human factors, and the
505 wide range of potential consumers capabilities and disabilities.

506 **4.4.3 Guidance**

507 CD2G003.01: User control and choice should be clear and evident in the design of features

508 CD2G003.02: Designing consumer preferences should adopt privacy engineering best practices.

509 CD2G003.03: Product design can convey the context for processing of PII. Product development teams
510 should avoid design practices which create consumer ambiguity on product use of PII and impedes

511 transparency. This requires careful consideration of privacy controls in all product development stages,
512 including user experience and systems design, to ensure consumers do not unwittingly share PII,
513 prevents them from managing their data use preferences or results in unexpected uses of their PII .

514 CD2G003.04: Software supply chain security best practices and measure should be implemented.

515 CD2G003.05: Hardware products should adopt product security testing measures.

516 **4.5 Assign relevant roles and authorities**

517 **4.5.1 RequirementCD2R004:**

518 The organization shall assign and maintain roles and responsibilities, including one (“Accountable or
519 **Responsible person**” or “Design authority”) for the overview of the entire product lifecycle

520 **4.5.2 Explanation**

521 Roles and authorities over a consumer product’s lifecycle, provides confidence in the effectiveness of the
522 privacy controls associated with the product.

523 **4.5.3 Guidance**

524 CD2G004.01: A single individual or group should be held accountable for the privacy status of a product.
525 This role should have oversight across disciplines, and over a product’s lifecycle, in order to control the
526 effectiveness of all the product’s privacy controls. Other roles should include: incident management
527 coordination; production manager; customer point of contact.

528 CD2G004.02: Accountability and responsibilities should be clearly defined, adequately resourced, and the
529 effectiveness of the process monitored

530 **4.6 Establish multi-disciplinary responsibilities**

531 **4.6.1 Requirement CD2R005:**

532 The organization shall designate additional Responsible Persons, from each function or organization that
533 contributes expertise to the design or operation of requirements and privacy controls, to be responsible
534 for their contribution.

535 **4.6.2 Explanation**

536 While the Responsible Person can be held accountable for the overall effectiveness of the product’s
537 privacy controls, the design and operation often require the contribution of expertise from multiple
538 functions, and from multiple organizations. Sometimes teams are formed by combining multiple
539 functional teams into one. These cross-functional teams are composed of experts from various functional
540 areas and work cooperatively towards some organizational goal. Because these members are considered
541 experts of their individual functional area, they are usually empowered to make decisions on their own
542 without needing to consult management. Cross-functional teams are believed to improve coordination of
543 interdependent activities between specialized subunits.

544 Ensuring that privacy is an integral part of the design process requires multi-disciplinary expertise.
545 Integrated design teams expose engineers to other non-technical perspectives (e.g. legal, consumer) and
546 vice versa, thereby helping to embed strong privacy norms among the technical specialists whose focus
547 is generally on security.

548 The common misperception is that information security equates to privacy. While security certainly plays
 549 a vital role in enhancing privacy, there is an important distinction to be made. From an organizational
 550 viewpoint, security is about protecting and controlling information. Encryption, identity and access
 551 management, firewalls, etc. are all about controlling the access or flow of information within the
 552 organization or between the organization and outside entities (be they vendors, customers or others).

553 Nonetheless, information privacy and IT security are both integral and must work together as a proper
 554 control mechanism. Privacy principles include information security and requirements for reasonable
 555 safeguards for PII. Privacy seeks to respect and protect PII by empowering individuals to maintain
 556 control over its collection, use and disclosure. Information security seeks to enable and protect activities
 557 and assets of both people and enterprises.

558 Unless the relevant functions contribute their expertise to the design and operation of a product's privacy
 559 controls, the controls may not be fully embedded within the product, leaving controls gaps that can lead
 560 to privacy failures.

561 **4.6.3 Guidance**

562 CD2G005.01: Senior roles within each function and organization that contribute expertise to the design
 563 or operation of privacy controls should be designated to represent and take responsibility for those
 564 contributions.

565 CD2G005.02: The roles should be sufficiently senior to ensure that the importance of privacy can be
 566 appropriately included alongside other operational priorities

567 **4.7 Develop privacy knowledge, skill and ability**

568 **4.7.1 Requirement CD2R006:**

569 The Responsible person(s) and Design Authority shall have knowledge, skill and ability in privacy by
 570 design.

571 **4.7.2 Explanation**

572 Knowledge, skills and abilities are attributes to successfully complete any task. Knowledge reflects
 573 familiarity with theory and factual information. Skills are developed proficiencies through practice
 574 (repeated). Abilities are being able to do something. Abilities and skills are practical whereas knowledge
 575 is theoretical. In addition, skills are learned but abilities are inherent. [19. 20]

576 **4.7.3 Guidance**

577 CD2G006.01: The approach to training staff in privacy by design should be tailored to the objectives of
 578 the training.

579 CD2G006.02: The impact of the training should be monitored to establish its long-term effectiveness, and
 580 the training should be reviewed and revised to keep them up to date.

581 CD2G006.03: Training should address all aspects of the PII lifecycle.

582 CD2G006.04: The need for knowledge, skills and ability in privacy by design, should also be incorporated
 583 into contracts and service level agreements with suppliers including those to whom PII is transferred.

584 CD2G006.05: Staff who operate processes for the organization to discharge its obligations to consumers,
 585 such as enabling consumers to exercise their privacy rights or preferences, should also be trained.

586 CD2G006.06: Staff contributing to the design and execution of the product need to be made aware of their
587 privacy commitments and those who provide specialist contributions trained in how to do this effectively.

588 CD2G006.07: Training should include sharing of good practice and should extend to those who contribute
589 from supplier organizations including those to whom PII is transferred.

590 **4.8 Ensure knowledge of privacy controls**

591 **4.8.1 Requirement CD2R007:**

592 Responsible persons and design authority shall be sufficiently knowledgeable of the controls for privacy
593 associated with the product and the organization PIM framework. [CD2R001]

594 **4.8.2 Explanation**

595 The dissemination of knowledge [19]³ of the privacy controls for the product and the organization's
596 privacy policies needs to occur prior to and during a project to allow staff to integrate this knowledge
597 with their core skills. This will allow them to identify the best means for implementing privacy controls
598 as part of the product development and ensure they align with the organization's privacy objectives.
599 Appropriate resources should be made available to staff to ensure questions can be addressed as required
600 throughout the product development stages and in the ongoing product and data lifecycles. The
601 responsible person is supported by various privacy specialists:

- 602 • Privacy Analyst /counsel: recommends compliance controls based on legal
- 603 policies/requirements and compliance risk assessments.
- 604 • Privacy Engineer/Architect: recommends and standardizes technical controls, develops tools,
- 605 supports during the implementation of controls, identifies privacy gaps in platforms, leads platform
- 606 controls
- 607 • Privacy Program Manager: maintains the overall privacy program and privacy projects across the
- 608 company
- 609 • Technical Privacy Program Manager: ensures technical controls are tracked, prioritized, progress
- 610 is made and implemented across the company. E.g. data retention across the company, data
- 611 inventory projects, data export/deletion projects.
- 612

613 **4.8.3 Guidance**

614 CD2G007.01: The organization should have privacy expertise available that can lead efforts in
615 disseminating knowledge to staff involved in the design and development of products and its data
616 lifecycle. This expertise can reside in-house or can be external to the organization.

617 CD2G007.02: Each Responsible Person that contributes expertise should be trained in privacy to ensure
618 that good practice is incorporated into the product in a structured, transparent way.

619 CD2G007.03: Each Responsible person that contributes expertise should appropriate privacy expertise
620 and understanding of the process to ensure that good privacy practices are incorporated into the product
621 in a structured way.

622 CD2G007.04: The journey of an idea towards a viable product for development that reflects privacy by
623 design should involve the contribution of multi-disciplinary expertise.

³ Cf. ISO/IEC/IEEE 15288:2015 – System life cycle processes (knowledge management process)

CD2G007.05: Compliance/Administrative Controls: E.g. privacy awareness and training, privacy impact assessments, governance and privacy program, records of processing activities, consent text, data processing agreement, binding corporate rules, 3rd party controls (agreements, DPA's)

CD2G007.06: Technical Controls: E.g. physical controls (e.g. on device), TTL (automated retention capability), encryption (in transit/at rest), de-identification/anonymization, access controls, privacy enhancing

CD2G007.07: Services. Privacy enhancing services are technical controls developed by privacy engineers that are used by other engineers. Such controls include consent toolkit/framework, data deletion service, data export service, encryption service, de-identification tools, up-to-date data inventory, user data locator (relevant for privacy rights).

CD2G007.08: The product's legal and regulatory obligations, together with the voluntary privacy policies that the organization chooses to adopt for its product constitute the source of the privacy control objectives for the product. These are the objectives that will guide designers and developers in the design of privacy controls.

4.9 Documented information management

4.9.1 Requirement CD2R008:

Organizations developing consumer product(s) shall manage **documented information** and ensure the information's integrity, relevance, availability and usability

4.9.2 Explanation

If the design and operation of a product's privacy controls are going to be embedded into the product's lifecycle, then documentation from the design stage will capture the key information that will be used by staff of the organization and its suppliers later in the lifecycle. Documented information often takes the form of a living document that is updated with details of the design of the privacy controls, information on their testing, and their operation later in the lifecycle.

The organization maintains documented information (e.g. policies, procedures, instructions to follow) and stores records for tracking the performed activities. This helps when employees carry on the activities (because they need to know the policies, procedures and instructions and to review the records of the previous tasks or of similar activities). Documented information for the privacy by design for consumer goods and services may include [21]:

- **privacy risk assessment;**
- functional and not functional requirements of the product and service;
- privacy controls to be implemented and implemented in the product and service;
- test results, acceptance decisions and authorizations for the delivery;
- instructions for the production of the product and the provision of the service;
- communication to the customers.

4.9.3 Guidance

CD2G008.01: As part of a PIMS, the organization should manage documented information including the following:

- they should be approved by relevant authorities;
- they should be readable by all intended recipients;

665 CD2G008.02: The organization's information security management system shall include, for each
666 documented information, appropriate:

- 667 - identification and description (e.g. a title, date, author, or reference number);
- 668 - format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
- 669 - review and approval for suitability and adequacy.

671 CD2G008.03: Documented information should be controlled to ensure: - it is available and suitable for
672 use, where and when it is needed; - it is adequately protected (e.g. from loss of confidentiality, improper
673 use, or loss of integrity).

674 CD2G008.04: For the control of documented information, the organization should address the following
675 activities, as applicable: - distribution, access, retrieval and use; - storage and preservation, including the
676 preservation of legibility; - control of changes (e.g. version control); and - retention and disposition.

677 CD2G008.05: Documented information of external origin, determined by the organization to be necessary
678 for the planning and operation of the information security management system, should be identified as
679 appropriate, and controlled.

680 **5 Transparent consumer communication during the product use lifecycle**

681 **5.1 Introduction**

682 Consumers of products or services that process PII expect information at the right time, that contains
683 clear, concise, accessible, meaningful, and verifiable explanations and commitments about how and why
684 a product or service will process PII and manage privacy. The objective is to facilitate confident,
685 informed decision-making by the consumer prior to purchase. Consumers of products or services that
686 process PII also want to know when incidents or errors in how their PII is processed puts them or their
687 PII at risk, or when there are changes in the purposes for which their PII will be processed.

688 Transparency and Consumer Communications support accountability. They enable Consumers and
689 others to compare actual processing details with such explanations and commitments and take action
690 (i.e. file a complaint or stop using the product or service) and challenge the responsible persons when
691 warranted. They take many forms from user-interfaces, help files, and product documentation through
692 packaging, marketing content, and customer service scripts to FAQs, notices, and policies.

693 Opportunities for transparency and consumer communications present themselves throughout the
694 Consumer facing elements of the Product's lifecycle and its ecosystem. The risk assessment should not
695 only consider the sensitive nature of the data collected by the product used by people with disabilities
696 and the diversity of users' needs (e.g., auditory, visual, or haptic), but also incorporate such
697 considerations when developing privacy disclosures, notices, and other controls within the product. [38]
698 Responsible persons include those with Consumer-facing responsibilities for creating privacy focused
699 communications, notices and documentation about the product or service. Responsible persons with
700 responsibilities for creating Consumer privacy focused communications, notices and documentation
701 about the product may be one in the same with the design authority. [Refer to R003: Multi-disciplinary
702 responsibilities]

703 5.2 Clear responsibility for transparently providing understandable information to 704 consumers

705 5.2.1 Requirement CD2R009:

706 The organization shall maintain and make available information on the product's privacy settings or
707 features to other users so that they can configure the product according to their privacy objectives.
708 Explanation

709 5.2.2 Explanation

710 Consumers need to be aware of how a product or service processes PII in order to make informed
711 decisions to use or acquire products or services that process PII. Usually, this transparency and
712 communication takes the form of manual on the product's privacy settings or features, privacy notices⁴
713 and/or product or service documentation that explain aspect of how the product or service processes PII;
714 contracts and SLAs; instructions for requiring support or sending complaints; it also takes the form of
715 user-interface labels, packaging, and marketing statements.

716 Once the product is released to consumers, the organization's ability to change its controls can be limited.
717 Unless the pre-release process of testing the operation of the product's controls is robust, products can
718 be released that fail to manage their privacy risks appropriately.

719 During the product support period, the consumer needs to be kept informed of changes to privacy risks
720 if they are to be empowered to manage those risks effectively. Unless this communication is designed to
721 be effective, consumers can find that the product exposes them to significant residual privacy risks.

722 Support can include technical fixes to software or hardware that change the privacy controls built into
723 the product during development.

724 Consumers will often need support to understand how to install, setup and operate a product and if they
725 have issues or complaints. Consumer products often involve services which are supplied by different
726 providers and this must be made clear to the customer so that they know who to contact and who is
727 responsible. Ensuring that consumers are aware of where to get support and that the support activities
728 will act to protect their privacy is necessary to maintain consumer trust and confidence in suppliers.

729 5.2.3 Guidance

730 CD2G009.01: The source information for privacy focused communications, notices, and documentation
731 should include:

- 732 • manual on the product's privacy settings or features, including the consequences of re-configuring
- 733 them from their default privacy sensitive settings;
- 734 • privacy notices and/or product or service documentation that explain aspect of how the product or
- 735 service processes PII; this will include PII processed, purposes for which the PII is processed; with
- 736 whom the data is shared (and for what purposes);
- 737 • contracts and SLAs;
- 738 • instructions for requiring support or sending complaints and how the user can exercise available
- 739 privacy rights;
- 740 • controls that will be or are used to protect the PII and the user from unfair and unauthorized access
- 741 and use of the PII;
- 742 • entity that is responsible for deciding how the PII will be processed and for incident and breach
- 743 management notification responses

⁴ Further information on contents of online privacy notices are provided by ISO/IEC 29184:2020(E) - Online privacy notices and consent

744

745 CD2G009.01: The organization should appoint appropriate roles (e.g. the design authority) for the
746 maintenance of such documentation.

747

748 CD2G009.02: The public point of contact should include the organization's identity, geographical address,
and contact information, and information on when a customer can expect to receive a response.

749

750 CD2G009.03: Where a consumer becomes deceased, their surviving friends and family may wish to
751 revoke access to, or change in some way the product and its associated arrangements. The organization
752 should plan for, design and operate controls over users' digital legacy [31], and communicate these to
consumers.

753

5.3 Accountability to Responsible persons

754

5.3.1 Requirement CD2R010:

755

756 The design authority shall ensure the Responsible persons who have Consumer facing responsibilities
are committed to including necessary privacy communications, notices, or documentation to Consumers

757

5.3.2 Explanation

758

759 This ensures that products that process PII are designed with consideration and ensures that consumers
760 of such products will have access to information on how their PII is processed in such products In some
761 cases, the Responsible persons with Consumer-facing responsibilities will be one in the same with the
entity that is responsible for designing the product (or iterations/upgrades of the product).

762

5.3.3 Guidance

763

764 CD2G010.01 These communications, notices, or documentation should be available to Consumers prior
to sale or license of the product and throughout product or service (and its data's) life cycle.

765

766 CD2G010.02 ISO/IEC 29184 provides more explanations on good practices to follow for providing
notices and readers are encouraged to consult the document. [15]

767

5.4 Responding to consumer inquiries and complaints

768

5.4.1 Requirement CD2R011:

769

770 The design authority shall make available to Consumer facing responsible persons resources as well as a
771 point of escalation to assist in accurately responding to consumer inquiries and complaints regarding the
product, or processing of PII by the product. [22, 23, 23.1, 23.2]

772

5.4.2 Explanation

773

774 As issues arise and need clarification, the design authority responsible for designing the product with
775 privacy by design has an obligation to support Responsible persons with consumer facing
responsibilities.

776

5.4.3 Guidance

777

CD2G011.01: Such resources can include:

778

779 • training and documentation for Customer and Technical Support activity instructions (including
maintaining privacy during support operations;

- FAQ on technical issues and consumer use issues related to privacy controls within the product or service;
- independent alternative mechanisms available to consumers where complaints cannot be resolved directly;
- instructions on where and how a consumer should go for assistance.

5.5 Communicating to diverse consumer population

5.5.1 Requirement CD2R012:

The organization shall ensure that communication and communication channels can be used by all intended users (including vulnerable consumers, diverse users or users with different language).

5.5.2 Explanation

Ensuring that consumers receive documentation that they can understand (see 5.x) and are aware of where to get support and that the support activities will act to their needs

As part of privacy by design, the organization that designed the product, has a responsibility to ensure consumers who purchase or use the product or service have a mechanism through which they can communicate with the re-seller or manufacturing organization .

5.5.3 Guidance

CD2G012.01: Privacy settings and privacy management measures should take into account the characteristics of the target consumers. In particular, it is important to consider minors, elderly, and people with low IT-literate.

CD2G012.02: The organization should ensure by contract (if it a third-party) or internal SLA (if member of the same organization), that Consumer facing responsible persons provide consumers of the product a means of asking question, filing complaints, seeking support, or having their privacy rights addressed.

CD2G012.03: documentation should be written so that all intended consumer can understand it. This includes: documentation written for vulnerable consumers (e.g. blind people) and in the language of Countries where the product or the service is promoted.

CD2G012.04: Communications with consumers should be enabled through a diverse set of communication channels, enabling comments, questions for resolution, and complaints.

CD2G012.05: The effectiveness of these channels should be monitored, reviewed, and revised to ensure that they provide an acceptable user experience for consumers of the product.

CD2G012.06: The organization should ensure by contract (if it a third-party) or internal SLA (if member of the same entity), that Consumer facing responsible persons provide consumers of the product a means of asking question, filing complaints, seeking support, or having their privacy rights addressed.

CD2G012.07: The documentation should be written so that all intended consumer can understand it. This includes: documentation written for vulnerable consumers (e.g. blind people) and in the language of Countries where the product or the service is promoted.

CD2G012.08: Communications with consumers should be enabled through a diverse set of communication channels, enabling comments, questions for resolution, and complaints.

CD2G012.09: The effectiveness of these channels should be monitored, reviewed, and revised to ensure that they provide an acceptable user experience for consumers of the product.

820 5.6 Prepare data breach communications

821 5.6.1 Requirement CD2R013:

822 The organization, and relevant third parties, shall create, maintain, and test the resilience of its
823 communications with consumers and regulators in the event of a data breach related to the product.

824 5.6.2 Explanation

825 Communication with product consumers in the event of a data breach is critical to ensuring that they are
826 empowered to manage any residual privacy risks.⁵ In addition, regulators may also set deadlines for
827 organizations to report data breaches.

828 5.6.3 Guidance

829 CD2G013.01: The communication should be prepared in advance and form part of the preparation for
830 privacy breach management. In particular, the organization should consider, among others:

- 831 - what content should be covered in the communication (e.g., cause, type of data breached, what
- 832 actions a consumer can take, what actions taken by the organization, contact for further
- 833 information);
- 834 - what communication channel they use to communicate to affected individuals (e.g., email);
- 835 - what if the organization does not possess contact info;
- 836 - who sends the notification and when;
- 837 - in which languages notification should be prepared; and
- 838 - who signs off the communication.
- 839

840 CD2G013.02: This communication should be prepared in advance and form part of the preparations for
841 privacy breach management.

842 CD2G013.03: The organization should identify key information about the data breach that will included
843 in the communication to Consumers or regulators.

844 5.7 Design post-retirement communication

845 5.7.1 Requirement CD2R014:

846 The organization shall maintain diverse channels of communication with consumers after product
847 retirement.

848 5.7.2 Explanation

849 Following product retirement, the processing of PII by the organization is likely to continue.

850 5.7.3 Guidance

851 CD2G014.01: Consumers should be able to communicate with the organization about this through diverse
852 channels and receive assurance about the privacy of their PII.

⁵ Refer to ISO/IEC 27035 Information technology - Information security incident management developed by ISO/IEC JTC 1/SC 27/WG 4 (Security controls and services)

853 CD2G014.02: Examples of work products include:

- 854 • Communications material with consumers at retirement;
- 855 • Communications with consumers post-retirement;
- 856 • Audits of post-retirement Consumer communications

857 **6 Risk management**

858 **6.1 Introduction**

859 Like other operational risks, those related to protection of PII, benefit from a risk management approach.
 860 [24, 25] Effectively managing and mitigating privacy risks in an effort to prevent a privacy breach reflects
 861 privacy by design. The purpose of the risk management in this context is to control the privacy risks that
 862 the consumers are exposed to in relation with the consumer products in question.

863 The privacy risks associated with consumer products can result from PII being gathered from a software
 864 application or a hardware device, or from the collection of PII at the point of sale or during
 865 communication for support. Privacy risks also result from collecting consumers' PII for developing new
 866 product functionality or new products, creating marketing plans, or considering product retirement
 867 plans. Any use of consumers' PII that is associated with a consumer product, whether or not they are a
 868 direct user of the product, can incorporate privacy by design. Many different people may also interact
 869 with a given consumer device or service, so it is possible that there are secondary users or others whose
 870 PII is captured by the device or in associated services.

871 Privacy Risk Management guidance occurs globally in a number of documents and standards and may be
 872 mandated by various data protection authorities. Such guidance may:

- 873 • be integrated into an end to end privacy design process and revisited at various stages of the
- 874 product design process, such as the NISTIR 8062 [26] [29];
- 875 • be mandated by various data protection authorities, such as CNIL guidance documents [27] to
- 876 address privacy risks or described in international standards, such as ISO/IEC 29134:2017
- 877 Guidelines for privacy impact assessment [28]; ISO/IEC 27557 Organizational privacy risk
- 878 management [25]⁶
- 879 • be integrated into an overall organization's risk management processes;
- 880 • be targeted at the front end of the design process and during major changes in product design;
- 881 • be included in various technical stages of the product design, such as LINDDUN, a privacy threat
- 882 modelling approach.
- 883

884 **6.2 Identify inputs to privacy risk assessment**

885 **6.2.1 Requirement CD2R015:**

886 The organization shall identify or create documented information as inputs for the product privacy risk
 887 assessment.

⁶ ISO/IEC 27557 is under development. This standard will guide organizations on managing privacy risks (risks relating to or arising from the processing of PII) that could impact the organization and/or individuals (data subjects) as an integral part of the organization's overall risk management. It will support the requirement for risk management as specified in management systems such as ISO/IEC 27001 (ISMS) and ISO/IEC 27701 (PIMS), plus risk management standards such as ISO 31000, ISO/IEC 29134 and ISO/IEC 27005.

6.2.2 Explanation

This documented information provides the foundation of context, process, and boundaries for an informed privacy risk assessment, and support continuous risk management. Documented information includes explicit documentation of functional and non-functional privacy requirements. Examples of documented information representations include, for example, spreadsheet documentation of compliance tasks and processes, those components of consumer stories, use cases, misuse cases, interface design, DFD diagrams, sequence diagrams or activity diagrams that clearly show embedding of privacy requirements, business model diagrams that show PII flows across technology platforms, and diagrams of privacy architectures. Organizational privacy-related documentation (e.g. privacy policies, privacy training materials, documentation of go-to personnel for privacy consultations) may form part of a larger, organization-wide privacy information management approach.

Use cases (Reference Oasis PMRM privacy design process [30]) describe how the product may be used by the consumer and influence the analysis of privacy risks to consumers. Defining the central use cases allows the product designers to explore the peripheral use cases and those that represent abuse and misuse cases. Use cases can be used to identify consumer privacy needs that arise from user interactions and known technical and user vulnerabilities.

6.2.3 Guidance

CD2G015.01: There are a variety of useful inputs, from understanding the ecosystem in which the product will operate, establishing risk criteria, and selecting a risk assessment methodology to more tangible inputs like a data map, product use cases, and set of privacy requirements relevant to the product.

CD2G015.02: Ecosystem: privacy risk is influenced by the components and suppliers used to design, develop, deliver, operate, and retire the product including those to whom PII is transferred. It is important to know or predict what constitutes the product's ecosystem, in terms of suppliers and consumers, to analyse privacy risk effectively.

CD2G015.03: Risk criteria: establish the acceptance criteria against which the organization can evaluate the significance of privacy risks identified in the risk assessment in order to make decisions regarding risk acceptance or treatment.

CD2G015.04: Organizations should communicate with PII principals and other stakeholders and make sure that such criteria is acceptable to them.

CD2G015.05: A data map and records of processing activities can be a useful input because it illustrates the context and flow of PII processing, can be illustrated in different ways, and can contain varying levels of detail based on organizational needs. Data maps can include the operating environment, the owners or operators of these components, specific type of processing across the PII lifecycle, and specific elements of PII being processed across the lifecycle of the consumer product .

CD2G015.06: Privacy requirements relevant to the product can be derived initially, from a variety of sources, including legal environment (e.g., laws, regulations, contracts), organizational policies or cultural values, relevant standards, and privacy principles. The more sensitive the information or the higher the risk to rights of individuals, the greater the obligation on the organization to take measures to protect that data and to show this was considered and effected at the time of design. These requirements are updated or expanded upon based on the results of privacy risk assessments.

CD2G015.07: Use cases should address: the use of the product by multiple users, family and friends and when consumers stop using products or become inactive; normal, misuse, and malicious use of the product; consumers who might have a wide range of capabilities and disabilities, particularly sensory impairments; and person to person as well as organization to person use of the product.

932 CD2G015.08: Use cases should examine all parts of the product and its data lifecycle including post
 933 product retirement uses and misuses that may introduce risks to consumers, consumers in the second-
 934 hand market, and following the death of the consumer.

935 CD2G015.09: Assumptions about the operation of privacy controls should be adjusted accordingly. Use
 936 cases should be developed for key product lifecycle processes such as sales/product/account
 937 registration, installation and repair, end of consumer use and product retirement. Knowledge of
 938 consumer use and privacy needs may be built up over time with agile design processes where initial
 939 consumer understanding is low.

940 **6.3 Conduct a privacy risk assessment**

941 **6.3.1 Requirement CD2R016:**

942 The organization shall conduct a privacy risk assessment and make risk responses treatment, or
 943 acceptance determinations during the product lifecycle.

944 **6.3.2 Explanation**

945 Privacy risk assessments help an organization identify privacy risks engendered by the product,
 946 prioritize them, and make informed decisions about how to respond to with risk treatment or acceptance.

947 **6.3.3 Guidance**

948 CD2G016.01: Privacy risk assessments should produce a prioritized set of risks to help organizations to
 949 weigh the benefits of the PII processing against the risks and to determine the appropriate response. Risk
 950 treatment (including risk reduction) or acceptance decisions are made based on established risk criteria.
 951 Some identified risks may need to be escalated or delegated to others for decision-making outside of the
 952 accountable party due to lack of authority or resources. This process may be documented in various ways,
 953 including with a privacy impact assessment. [⁷

954 CD2G016.02: The organization should conduct a privacy risk assessment prior to the design, production,
 955 release and product retirement.

956 CD2G016.03: Retirement privacy and cybersecurity risks should be considered for the product and PII
 957 throughout the product's ecosystem.

958 CD2G016.04: The organization should consider the impact on consumers associated with stock
 959 clearances and sales practices and the impacts on the user base of ceasing design update support.

960 CD2G016.05: Lifecycle consumer support services should be briefed and enabled to continue to operate
 961 privacy controls within tolerable risk on discontinued consumer product designs while they remain in
 962 use by consumers.

963 CD2G016.06: The organization should assess the risk of retaining, for use, PII associated with the product
 964 after support has ended and after the user has retired the device

965 CD2G016.07: The output should be a prioritized set of privacy risks and risk treatment or acceptance
 966 determinations.

967 CD2G016.08: For sources of privacy risks to consider during assessment, organizations should reference
 968 internal risk registers, if used by the organization, and external sources, such as the NIST Catalog of

⁷ Reference ISO/IEC 29134:2017.

969 Problematic Data Actions and Problems NIST source: [https://www.nist.gov/itl/applied-](https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources)
 970 [cybersecurity/privacy-engineering/resources](https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources)

971 **6.4 Assess privacy capabilities of third parties**

972 **6.4.1 Requirement CD2R017:**

973 Where third parties are used to for the design or operation of the product's privacy controls, their privacy
 974 capabilities shall be assessed.

975 **6.4.2 Explanation**

976 Where third party suppliers process PII in support of the product lifecycle, their processing should be
 977 taken into account in establishing the PII lifecycle and relevant privacy controls. This may mean that the
 978 lifecycle is extended due to suppliers processing PII before the start, of after the end of the product
 979 lifecycle including those to whom PII is transferred.

980 **6.4.3 Guidance**

981 CD2G017.01: The privacy capabilities should be assessed through appropriate due dilligence, risk
 982 assessment and agreements setting out obligations, accountabilities and review of their performance,
 983 including audits and reviews.

984 CD2G017.02: The organization should liaise closely with those who contribute their expertise from
 985 suppliers to ensure that the lifecycle is accurate.

986 CD2G017.03: The role of suppliers and acquirers in this process is central. They can pose particular
 987 privacy risks or can provide particular privacy controls that can make a significant impact on the privacy
 988 risks posed by the product. The suppliers should provide information that will allow the organization to
 989 clarify these issues, and this sharing of information should form part of the contract and service level
 990 agreement with the supplier including those to whom PII is transferred .

991 CD2G017.04: Implement third party governance technical mechanisms and operating processes to
 992 govern data sharing and privacy risks

993 CD2G017.05: The organization should assess privacy risks introduced by the use of suppliers including
 994 those to whom PII is transferred in the product or service lifecycle.

995 CD2G017.06: The relationship with suppliers including those to whom PII is transferred should be based
 996 on a contract.

997 CD2G017.07: The organization should sign a contract if the user exercises his rights or if the service is
 998 decommissioned when providing products and services together with the third party such as with a joint
 999 controller including those to whom PII is transferred .

1000 CD2G017.08: The performance of suppliers including those to whom PII is transferred should be
 1001 periodically evaluated with appropriate means (e.g. review of reports, audits) and followed by
 1002 appropriate actions.

1003 **6.5 Assess Retirement Privacy Risks**

1004 **6.5.1 Requirement CD2R018:**

1005 The implications of decommissioning on risks to PII shall be considered in accordance with the design
 1006 clause [R0n.nn] and product development clause [R0n.nn]

1007 6.5.2 Explanation

1008 This assessment is the basis for privacy controls for Recalls, and Return, for retirement and post
1009 retirement

1010 For the design process for the retirement phase of the product lifecycle applicable to the product's
1011 consumer base including individual consumers stops using the product (including reuse passing the
1012 product on through gifts or second-hand markets, and the decease of the consumer), withdrawal of
1013 product from sale, withdrawal of product support, recycling

1014 6.5.3 Guidance

1015 CD2G018.01: The organization should treat the privacy risks of this period like any other part of the
1016 product lifecycle. The retirement privacy risk assessment should follow the requirements described in
1017 CD1R010 and CD1R011 about conducting a privacy risk assessment

1018 CD2G018.02: Inputs to the design process

- 1019 • Identification of product withdrawal criteria to be used for withdrawal of sales and support
- 1020 • Pre-withdrawal notification period
- 1021 • Consumer privacy issues to be addressed at product disposal even after support for the product has ended and
1022 after the user has retired the product.
- 1023 • Means of communicating end of life information to consumers (e.g. e mails to registered users,
1024 web site notifications, TV and radio adverts, social media, letters to consumers, information for
1025 sales outlets and support agents)
- 1026 • Ongoing market monitoring post product sales and support end of life
- 1027

1028 CD2G018.03: Outputs from the design process:

- 1029 • Consumer communications
- 1030 • Sales outlets communications
- 1031 • Support agents communications
- 1032 • Installed base vulnerabilities and exploits post product withdrawal
- 1033 • Necessary mitigation actions post product withdrawal
- 1034

1035 6.6 Establish requirements for privacy controls

1036 6.6.1 Requirement CD2R019:

1037 The organization shall establish the requirements for privacy controls to implement risk treatments
1038 resulting from privacy risk assessment

1039 6.6.2 Explanation

1040 Privacy requirements provide the foundation for designing or selecting privacy controls. Engineering
1041 activities involve the identification of requirements for privacy control to meet privacy goals, and to treat
1042 privacy risks. This requirement focuses on the latter.

1043 The controls (i.e. the means) an organization selects to achieve its privacy objectives will vary. Because
1044 of this variation in privacy controls, and potentially the actions that need to be taken by a consumer or
1045 user to protect privacy, product users and consumers generally need access to the information that
1046 explains how privacy is treated with respect to a given product. (WD4 CA-BG02)

1047 Also, while privacy controls might be designed during product design and development, they may be
 1048 reworked, re-configured, disabled or broken at later points in the lifecycle. (WD4 Introduction
 1049 CH/PD04)

1050 Privacy controls and privacy goals are included in many other management, technology, quality, safety,
 1051 and other information-related standards. Privacy goals and privacy controls that come from any source
 1052 are intended to be incorporated as part of this standard's design process. (WD4 CA-BG08)

1053 **6.6.3 Guidance**

1054 CD2G019.01: Requirements should be established based on privacy risk assessment results.
 1055 CD2G019.02: Results of the privacy risk assessment can lead to changes to the initial set of privacy
 1056 controls relevant to the product.
 1057 CD2G019.03: Requirements for privacy controls established prior to risk assessment should be updated
 1058 and/or expanded upon to create a full set.
 1059 CD2G019.04: Any aligned product or service should also satisfy the identified requirements.
 1060 CD2G019.05: The output should be an updated set of requirements for privacy controls.

1061 **6.7 Design privacy controls for retirement**

1062 **6.7.1 Requirement CD2R020:**

1063 The organization shall determine privacy criteria and design for the ceasing of product sales and support.

1064 **6.7.2 Explanation**

1065 Setting retention periods for PII makes good business sense, can help to manage risk and costs, and to
 1066 avoid regulatory action or bad publicity if things go wrong (because you kept it for too long and the data's
 1067 been compromised). PII that is retained indefinitely decreases in value over time, but it increases in cost
 1068 and risk. Identify how long a piece of PII remains necessary to the product, and securely delete it when
 1069 it's no longer required.

1070 When designing the product or service, the end of life should be considered, including cases when
 1071 consumers pass the product to other consumers through gifts or second-hand markets, and the decease
 1072 of the consumer, withdrawal of product from sale, withdrawal of product support, recycling

1073 **6.7.3 Guidance**

1074 CD2G020.01: if possible, the product should have functions, that the consumer can easily activate, for
 1075 securely erasing PII

1076 CD2G020.02: cross-functional team should determine a pre-withdrawal period for consumer notification.

1077 CD2G020.03: The cross-functional team should identify any consumer use of organizational processing
 1078 resources that needs to continue after sales or support ceases.

1079 CD2G020.04: The cross-product team should notify consumers, sales and support of privacy protecting
 1080 actions that they may need to take as a result of ceasing sales, support or organizational processing of
 1081 product data.

1082 CD2G020.05: Retention and processing of product data beyond the end of product support and consumer
 1083 product use shall only be undertaken for valid organizational purposes.

1084 CD2G020.06: Product end of life withdrawal consumer information should include:

1085 a. consumer options if they are to continue using the product

- b. any consumer alternative products
- c. consumer feedback mechanisms if product end of life actions present unanticipated difficulties for consumers

CD2G020.07: Consumer product use beyond the ceasing product support should be taken into consideration with market monitoring continued and any exploits that cause significant consumer privacy risk addressed with corrective action.

CD2G020.08: Consumer end of life use cases should include

- a. consumer ceasing use (decease of the consumer, disposal or recycling of the product)
- b. reuse passing the product on through gifts or second-hand markets,

6.8 Monitor and update risk assessment

6.8.1 Requirement CD2R021:

The organization shall monitor for changes during the product and PII lifecycle of associated PII, and update documented information, privacy risk assessment, and associated privacy control implementation.

6.8.2 Explanation

Changes to the product or organizational context may give rise to new privacy risks or necessitate adjustments to documented information, privacy risk assessment, privacy requirements, and control implementation as part of privacy risk management. The outputs should be: a) updated inputs for privacy risk assessment; b) updated privacy risks and risk response treatment or acceptance determinations; c) updated privacy control implementation

6.8.3 Guidance

CD2G021.01: Updates to artifacts, privacy risk assessment, privacy requirements, and privacy control implementation should be iterative during the product lifecycle. The organization should ensure that the privacy risks are assessed including the actual condition of customer feedback and complaints. Monitoring may involve changes to the product and associated PII processing directly, or may be external to the product, such as organizational objectives or the legal/regulatory environment. Post-release product updates may necessitate new or updated communication with consumers.

CD2G021.02: The organization should model the use of the product, including post-release and post-retirement, and assess whether when the product fails, it continues to meet privacy requirements.

CD2G021.03: The product should continue to meet established requirements, and if not, results may necessitate updates to control implementation.

CD2G021.04: The organization should ensure that update to post-release products do not degrade the operation of privacy controls. Any changes to functionality or other settings should not degrade the operation of privacy controls in a way that increases residual privacy risks, or if so, compensating controls are implemented.

CD2G021.05: The organization should also ensure that the operation of privacy controls does not degrade through an incremental release cycle. In this case, each release, and the totality of all releases for the product, should ensure that the privacy risks are managed in a way that prevents privacy controls from degrading.

1127 **6.9 Include privacy risks in cybersecurity resilience design**

1128 **6.9.1 Requirement CD1R022:**

1129 **The organization shall incorporate risks to PII when designing their resilience plan.**

1130 **6.9.2 Explanation**

1131 Organizations' operations and product supply chains can be subject to day to day disruptions, so if the
 1132 controls are to be operated continuously, preparations will need to be made to prevent, detect, recover,
 1133 and resume from disruptions that impact PII. Composability is a system design principle that deals with
 1134 the inter-relationships of components. Privacy protections may not necessarily be preserved if one
 1135 system is embedded within or connected to another system. Therefore, understanding privacy risks
 1136 within the system as well as a component of other systems is important to evaluate when designing for
 1137 privacy alongside cybersecurity resilience planning.

1138 **6.9.2 Guidance**

1139 CD2G022.01: ISO/IEC 22316 Security and resilience – Organizational resilience – Principles and
 1140 attributes

1141 **7 Integrating privacy into the service consumer product's service management** 1142 **lifecycle**

1143 **7.1 Introduction**

1144 While privacy requirements may be continuously (re)designed over the lifecycle of a consumer product,
 1145 identified privacy requirements are ultimately developed, deployed and operated as a set of concrete
 1146 privacy services which must be actively managed over the product's lifecycle to ensure they achieve the
 1147 intended privacy objectives within the product and that the services do not degrade or operate in
 1148 unintended ways. There are several international standards and practitioner frameworks for addressing
 1149 both development and engineering of privacy services (ISO 27550 and ISO 15288 [32]) and the
 1150 subsequent service transition and operation of the realized services, including ITI, aspects of COBIT and
 1151 ISO 20000.

1152 ISO 20000, for example, specifies requirements for an organization to establish, implement, maintain and
 1153 continually improve a service management system (SMS). The requirements include the planning, design,
 1154 transition, delivery and improvement of services to meet the service requirements and deliver value. In
 1155 the current context, we consider the specified privacy services which are to be developed, deployed and
 1156 operated over the consumer product's lifecycle. The success of the privacy services requires that the
 1157 organization, its suppliers and the consumers who purchase the product can operate the services in a
 1158 manner that achieve the privacy design requirements and objectives for all stakeholders.

1159 **7.2 Integrate privacy design in service development**

1160 **7.2.1 Requirement CD2R023:**

1161 The organization shall integrate the intended privacy design requirements of the consumer product into
 1162 service development

1163 7.2.2 Explanation

1164 Service development realizes the intended privacy design of the product and the associated governing
 1165 practices, processes and policies required to achieve the product's privacy goals and facilitates the
 1166 introduction of the privacy services into supported consumer use environments. The specific
 1167 development approach and the engineering of the service components will vary based on the nature of
 1168 the product and the context in which it is designed to be used.

1169 The requirements for building, deploying and operating newly designed or changed product privacy
 1170 services are typically documented within a 'service design package', here encompassing the scope of the
 1171 designed privacy requirements and reflected in the following service development components:

- 1172 • PrivacyServices Description
- 1173 • Management information systems and tools that support the services
- 1174 • Privacy service technology architectures
- 1175 • Administrative and other management processes that support the privacy services
- 1176 • Measurement methods and metrics describing the developed services, their deployment and
- 1177 performance in operation.

1179 7.2.3 Guidance

1180 CD2G023.01: The organization should maintain a single source of consistent and accurate information on
 1181 all privacy operational services that is widely available to those who are authorized to access it.

1182 CD2G023.02: The organization should ensure that all current and planned privacy services are delivered
 1183 to the agreed achievable targets. This is accomplished through a constant cycle of negotiating, agreeing,
 1184 monitoring, reporting on and reviewing privacy service targets and achievements and through the
 1185 instigation of actions to correct or improve the levels of service delivered.

1186 CD2G023.03: The organization should ensure the continuous operation of privacy services by managing
 1187 the risks that could affect those services and thereby ensure minimum continuity-related service levels.
 1188 [Ref Clause 6 Risk Management]

1189 CD2G023.04: The organization should ensure that the confidentiality, integrity, and availability of the
 1190 privacy services align with the identified privacy design requirements.

1191 CD2G023.05: The organization should ensure that all contracts and agreements with suppliers support
 1192 the privacy requirements of the product and that all suppliers meet their contractual commitments for
 1193 privacy assurance

1194 CD2G023.06: The organization should liaise closely with those who contribute their expertise from
 1195 suppliers to ensure that their participation is maintained across the product lifecycle.

1196 CD2G023.07: The role of suppliers in this process is central. Suppliers may provide individual privacy
 1197 controls that can make a significant impact on the privacy risks posed by the product. Suppliers should
 1198 provide information that will allow the organization to clarify privacy issues as they arise, and this
 1199 sharing of information should form part of the contract and service level agreement with the supplier.

1200 7.3 Identify privacy controls to develop

1201 7.3.1 Requirement CD2R024:

1202 **The organization shall identify the privacy controls prior to the development phase**

1203 **7.3.2 Explanation**

1204 Privacy controls for the product and associated PII processing include

- 1205 • Privacy controls resulting from the organization initial knowledge, such as a consent
- 1206 management, privacy preference management.
- 1207 • Privacy controls resulting from privacy risk assessment.
- 1208 • Requirements are met by implementing controls.
- 1209 • How the control is implemented is a calibration based on the risk and the desired outcome or the
- 1210 objective of implementing the control.
- 1211 • The implemented controls combine to create privacy capabilities.

1212 **7.3.3 Guidance**

1213 CD2G024.01: The organization should identify from its initial knowledge the privacy controls to meet the

1214 product's privacy requirements throughout its lifecycle and the personal information lifecycle.

1215 CD2G024.02: The organization should identify privacy controls resulting from privacy risk assessment.

1216 CD2G024.03: The output should be a set of requirements for privacy controls.

1217 **7.4 Develop privacy controls**1218 **7.4.1 Requirement CD2R025:**

1219 The organization shall design, develop, test and validate the privacy controls.

1220 **7.4.2 Explanation**

1221 Privacy controls allow the product and associated PII processing to meet privacy goals and address

1222 privacy risks.

1223 **7.4.3 Guidance**

1224 CD2G025.01: The organization should design and implement controls to meet the product's privacy

1225 requirements throughout its lifecycle and the PII lifecycle.

1226 CD2G025.02: Privacy controls should be tested to ensure that they meet the product's privacy

1227 requirements, including assessment of the viability of proposed privacy controls as part of the product

1228 options appraisal process for potential new products.

1229 CD2G025.03: Where the viability assessment results suggest that the product cannot meet privacy

1230 requirements, the product option should be abandoned.

1231 CD2G025.04: The output should be a set of privacy controls.

1232 **7.5 Manage the transition of privacy services**1233 **7.5.1 Requirement CD2R026:**

1234 New, modified or retired privacy services shall meet the designed consumer privacy needs, preferences

1235 and expectations

1236 **7.5.2 Explanation**

1237 Service transition ensures that new, modified or retired privacy services meet the expectations of the

1238 business as documented in the product strategy and design stages of the lifecycle. This stage is also

1239 responsible for the transition of the product from one lifecycle state to another (design to development;
 1240 development to operations; operations to end of life) while controlling risk and supporting organizational
 1241 knowledge for decision making.

1242 **7.5.3 Guidance**

1243 CD2G026.01: The organization should ensure that all relevant plans for privacy service transition are in
 1244 place and the associated privacy control support and coordination activities are managed to ensure
 1245 smooth and successful transitioning of new, changed or retired services.

1246 CD2G026.02: The organization should ensure that all relevant plans for service transition are in place
 1247 and the privacy support and coordination activities are taken care of and ensure smooth and successful
 1248 transitioning of new, changed or retired services.

1249 CD2G026.03: The organization should ensure that changes are systematically managed to optimize
 1250 privacy risk exposure, minimize privacy impacts, and to make implementations successful at the first
 1251 attempt and to keep all stakeholders informed promptly. The second process, change management, is
 1252 responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with
 1253 minimum disruption to IT services. . The organization should ensure that the information technology
 1254 assets required to deliver privacy services are properly controlled, and that accurate and reliable
 1255 information about those assets is available when and where it is needed. This information includes details
 1256 of how the assets have been configured and the relationships between them.

1257 CD2G026.04: The organization is responsible for planning, scheduling and controlling the build, test, and
 1258 deployment of privacy product releases to deliver any new privacy functionality required by the deployed
 1259 product while protecting the integrity of existing privacy services.

1260 CD2G026.05: The organization should ensure that existing designed, new or changed product services
 1261 match the design specification and meet the needs of the consumer. Service validation and testing is the
 1262 'quality assurance' part of the service solution. The utility and warranty of privacy services delivered in
 1263 the live production environment reflect the efficiency and effectiveness of this process. While validation
 1264 ensures meeting business requirements, testing is concerned with meeting specifications.

1265 CD2G026.06: The organization should provide a consistent and standardized means of determining the
 1266 performance of a privacy service change in the context of likely impacts on business outcomes and on
 1267 existing and proposed privacy services. This information enables change management to take
 1268 appropriate decisions in the context of privacy objectives.

1269 CD2G026.07: The organization should ensure that the systematic gathering, categorizing and storing of
 1270 data, information, and knowledge related to privacy service design, development and performance. It
 1271 enables availability of information and data in the right place at the right time for taking informed
 1272 decisions and improves efficiency by reducing the need to rediscover knowledge.

1273 **7.6 Manage the Operation of Privacy Services**

1274 **7.6.1 Requirement CD2R027:**

1275 The organization shall ensure that services affecting privacy are operated effectively and efficiently
 1276 including fulfilling user requests, resolving service failures, fixing problems, and carrying out routine
 1277 operational tasks.

1278 **7.6.2 Explanation**

1279 Service operation coordinates and carries out the activities and processes required to deliver and manage
 1280 privacy services at agreed levels to internal business users and external customers. Service operation

1281 also manages the technology that is used to deliver and support privacy services. It is at this stage that
 1282 the actual value of the service is realized by the business, customers, and users. Thus, this stage is
 1283 responsible for sustaining, maintaining and continually improving the active privacy services – in line
 1284 with the customer expectations.

1285 7.6.3 Guidance

1286 CD2G027.01: The organization should ensure the monitoring and detection of privacy-impactful events
 1287 during the consumer's operation of the product, making sense of the events and determining the
 1288 appropriate control actions and remediations. Operational privacy monitoring and control is also
 1289 fundamental to automating privacy operations management activities.

1290 CD2G027.02: The organization should be responsible for restoring normal privacy service operation as
 1291 quickly as possible and minimizing the adverse impact on business operations. In doing so, incident
 1292 management ensures that the agreed levels of privacy service quality are maintained.

1293 CD2G027.03: The organization should provide a channel for customers to request and receive standard
 1294 services for which a predefined authorization and qualification process exists. It also provides
 1295 information to customers about the availability of services and the procedure for obtaining them.

1296 CD2G027.04: The organization should manage the lifecycle of all product problems from initial
 1297 identification through further investigation, documentation and eventual removal of these problems. It
 1298 strives to minimize the adverse impact of incidents and problems on consumer privacy that may be
 1299 caused by underlying errors within the IT infrastructure and to proactively prevent recurrence of privacy
 1300 incidents related to these errors.

1301 CD2G027.05: The organization is responsible for allowing organizational users to make appropriate use
 1302 of privacy impacting IT services, data or other assets. Access management helps to protect the
 1303 confidentiality, integrity, and availability of assets by ensuring that only authorized users can access or
 1304 modify them. Access management implements the policies of information security management and is
 1305 sometimes referred to as rights management or identity management.

1306 7.7 Prepare Breach Management

1307 **Requirement CD2R028:** The organization, together with key suppliers, shall design and operate
 1308 controls to prevent and detect data incidents and breaches, correct, recover consumer information
 1309 impacted by an incident or data breach

1310 7.7.1 Explanation

1311 Data breaches seem to be almost inevitable, but the operational disruption and impact on consumers is
 1312 not. Data breach management form part of the organization's resilience arrangements, to ensure a
 1313 seamless approach to preventing, detecting, recovering from, resuming operations, and communicating
 1314 about a data breach

1315 7.7.2 Guidance

1316 CD2G028.01: Data breach management form part of the organization's resilience arrangements, to
 1317 ensure a seamless approach to preventing, detecting, recovering from, resuming operations, and
 1318 communicating about a data breach. Rehearsing data breach procedures, incident triage, escalation to
 1319 senior management, and trialling communications plans with consumers are central to these
 1320 arrangements.

1321 CD2G028.02: Refer to the ISO/IEC 27035 - Information security incident management (multipart
 1322 standard)

1323 CD2G028.03: ISO/IEC 29180:2012 Information technology — Telecommunications and information
1324 exchange between systems — Security framework for ubiquitous sensor networks and

1325 CD2G028.04: ISO/IEC 22316 Security and resilience – Organizational resilience – Principles and
1326 attributes.

1327 CD2G028.05: Identify and incorporate risks to PII when designing cybersecurity resilience design.

1328 **7.8 Design privacy control testing**

1329 **7.8.1 Requirement CD2R029:**

1330 The organization shall design tests, and set acceptance criteria, that will establish the effectiveness of the
1331 design and operation of privacy controls throughout the PII lifecycle, from conception to post-retirement

1332 **7.8.2 Explanation**

1333 Assurance about the effectiveness of privacy controls requires both the design and the operation of each
1334 privacy control to be tested (e.g. use and misuse cases and regression tests). The design of a control will
1335 be tested while the product is being developed, while the operation of the control will be tested before
1336 release, and through the support period, through to retirement, and in some cases, during the post-
1337 retirement period.

1338 **7.8.3 Guidance**

1339 CD2G029.01: All tests of the design and operation of privacy controls should be designed in advance so
1340 that they can be tested for soundness and approved at an appropriate level of management.

1341 CD2G029.02: Testing is carried out to a pre-determined plan, that should be designed alongside the
1342 privacy control.

1343 CD2G029.03: The testing should meet acceptance criteria, if the control is to be considered to be effective.

1344 CD2G029.04: Acceptance criteria should also be designed and approved in advance.

1345 CD2G029.05: Development of acceptance criteria should follow a clear methodology, for example: 1)
1346 definition of the expected result of the privacy by design process (i.e. effective protection of the assessed
1347 risks), 2) definition of the principles to be implemented to provide effective risk protection (e.g. purpose
1348 limitation, data minimisation, transparency), and 3) determination of the measures implementing the
1349 design principles (e.g. anonymisation, visual interface)

1350 CD2G029.06: A testing method should be defined to assure that each of the criteria are met effectively
1351 (e.g. differential privacy to assure data minimisation, UX design methods to assure usability of visual
1352 interface).

1353 CD2G029.07: Where testing shows that a control is not effective, its design and, or its operation should
1354 be reviewed, revised, and re-tested before it can be considered to be effective in managing privacy risks

1355 CD2G029.08: Execute privacy threat modeling based on privacy and data risk relevant test scenarios;
1356 consider augmenting existing DevSecOps threat modeling processes if possible

1357 CD2G029.09: Review privacy control test plans annually to ensure viability and relevance.

1358 CD2G029.10: tests should be repeated in case of changes that may have impacts on privacy controls

1359 **7.9 Operate privacy controls for the processes and aligned products through the** 1360 **product lifecycle.**

1361 **7.9.1 Requirement CD2R030:**

1362 The organization shall design and operate privacy controls and **aligned products** that support the
1363 product, in a manner consistent with the privacy controls for the product.

1364 Note: The specific processes used to support a product will vary based on a specific product's needs and
1365 market segment (as well as other factors). The requirements R00x and R00x in this section are exemplars
1366 for some key process that will apply to a majority of products. It is not an exclusive set

1367 **7.9.2 Explanation**

1368 The organization designs and operates privacy controls in all the supporting processes. They include
1369 sales, distribution and marketing ones. A consumer product could be designed in such a way, that when
1370 migrating data, there is no need to have an intermediate storage with the point of sale, unless the device
1371 is broken. Privacy by design could also consider avoiding the need of data collection through registration
1372 with a service, but to be working independently or interact with a service in an anonymous fashion.

1373 Throughout the product's lifecycle the product will process PII in a myriad of ways for processes that are
1374 necessary to the sale, marketing, distribution, support and retirement of the product. Some will be pre-
1375 existing and some will be newly designed and implemented. The important factor is that none provide
1376 less privacy protection to those who interact with the product or those whose PII is processed by the
1377 product.

1378 **7.9.3 Guidance**

1379 CD2G020.01: Marketing and Sales materials respectively should reflect the actual product functionality
1380 at any time distribution and point of sale personnel should be trained to be able to inform the consumer
1381 of and mitigate the privacy risks associated with the consumer product, e.g. when supporting product
1382 registration, installation, and activation.

1383 CD2G030.02: The promise of privacy by design is only as strong as the treatment of privacy risks
1384 throughout the product or service's ecosystem. Therefore, aligned products should meet the privacy
1385 requirements identified for the product itself.

1386 **8 Design for end of PII lifecycle**

1387 **8.1 Introduction**

1388 The lifecycle of consumer 'product support' product life' 'product use' and PII may be different. A number
1389 of events can occur at the end of each lifecycle. The organization may withdraw or retire the product
1390 from the market and phase out support, but still maintain PII that engage with the product. The user may
1391 also dispose of, transfer, sell or destroy the product. The user may be deceased. Consumers' PII may
1392 need to be processed and stored for some years after the organization has ended support of the product
1393 or the product is retired or no longer being used by the consumer. The PII lifecycle may continue beyond
1394 these events.

1395 Consumers have a key role in influencing the post-retirement life of a product, and its associated residual
1396 privacy risks. Where consumers have discretion over post-retirement uses, they must be informed about
1397 their responsibilities for managing their own and others' privacy risks in any post-retirement uses.
1398 Liability for data privacy may continue even after vendor support for the product has ended

1399 8.2 Design privacy controls for end of use

1400 8.2.1 Requirement CD2R031:

1401 The organization shall, together with relevant third parties, design privacy controls to manage risks to
1402 PII at the end of product use.

1403 8.2.2 Explanation

1404 Accountability extends to the end of the PII lifecycle; the point at which consumers' PII is no longer
1405 processed. This point may be long after the end of the product's lifecycle, so accountability should be
1406 designed for long term resilience.

1407
1408 The retirement of a product is not the end of the lifecycle of its associated PII. Consumers' PII may need
1409 to be processed for some years after the product has been retired, and the organization should treat the
1410 privacy risks of this period like any other part of the product lifecycle. Privacy controls therefore
1411 survive the product's official life, and should take into account the various post-retirement use cases
1412 considered during development. Unless the privacy risks of this period are managed appropriately, the
1413 risks to the consumer's PII can extend indefinitely.

1415 8.2.3 Guidance

1416 CD2G031.01: Privacy controls should operate as long as consumers' PII, associated with the product, is
1417 processed.

1418 CD2G031.02: the organization should ensure its accountability arrangements over these controls
1419 continue for this period.

1420 CD2G031.03: Examples of work products include:

- 1421 a) Retirement controls operation plan;
- 1422 b) Audits of retirement controls operations; and
- 1423 c) Testing reports from retirement controls operation testing.

1424
1425 CD2G031.04: When designing the product, the end of life should be considered, including cases when
1426 consumers pass the product to other consumers through gifts or second-hand markets, and the decease
1427 of the consumer, withdrawal of product from sale, withdrawal of product support, recycling

1428 CD2G031.05: Where consumers have discretion over post-retirement uses, they should be informed
1429 about their responsibilities for managing their own and others' privacy risks in any post-retirement uses.
1430 [Ref Clause 5]

1431 CD2G031.06: Once the product is given to other consumers or PII is no longer required to meet a specific
1432 legitimate business or legal requirements/obligations, it should be securely destroyed [33] or
1433 anonymised [34] ⁸

1434 CD2G031.07: The collection and retention of PII should be according to identified business needs or legal
1435 obligations and designed for implementation at a technical and business process level.

1436 CD2G031.08: The multi-product team should notify consumers, sales and support of end of product life
1437 privacy protecting actions that they may need to take as a result of ceasing sales, support or
1438 organizational processing of product data.

⁸ Refer also to the ISO/IEC 27555 (DIS stage) for further information on the deletion of personal data

- 1439 CD2G031.09: Before retirement, the product's privacy risk assessment should be revisited and updated
1440 where necessary. The retirement may take place some years after release so circumstances may have
1441 changed since the initial assessment was carried out.
- 1442 CD2G031.10: Where there are changes to the privacy risks, changes to privacy controls should be
1443 designed and tested and put into operation in the same way as during the product's development.
- 1444 CD2G031.11: Changes to proposed privacy controls should form part of the authorisation process before
1445 any product is retired.

Bibliography

- 1447 [1] International Conference on Data Protection and Privacy Commissioners (32nd October 2010)
 1448 Resolution on Privacy by Design. [https://edps.europa.eu/sites/edp/files/publication/10-10-](https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf)
 1449 [27_jerusalem_resolutionon_privacybydesign_en.pdf](https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf)
- 1450 [2] EDPS Preliminary Opinion on Privacy by Design. May 31, 2018. [https://edps.europa.eu/data-](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en)
 1451 [protection/our-work/publications/opinions/privacy-design_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en)
- 1452 [3] Privacy by Design. The 7 Foundational Principles. January 2011. [https://www.ipc.on.ca/wp-](https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf)
 1453 [content/uploads/Resources/7foundationalprinciples.pdf](https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf)
- 1454 [4] The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices
 1455 <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>
- 1456 [5] EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
 1457 ([https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en)
 1458 [25-data-protection-design_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en))
- 1459 [5.1] ISO 26000 Corporate Social Responsibilities
- 1460 [6] ISO/IEC 29151, Clause 4.6 Life cycle considerations
- 1461 [7] UNCTAD. Data Protection and Privacy Legislation Worldwide. [https://unctad.org/page/data-](https://unctad.org/page/data-protection-and-privacy-legislation-worldwide)
 1462 [protection-and-privacy-legislation-worldwide](https://unctad.org/page/data-protection-and-privacy-legislation-worldwide)
- 1463 [8] OECD Privacy Framework http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
- 1464 [9] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April
 1465 2016 on the protection of natural persons with regard to the processing of personal data and on the free
 1466 movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- 1467 [10] APEC privacy framework principles [https://www.apec.org/Publications/2017/08/APEC-Privacy-](https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015))
 1468 [Framework-\(2015\)](https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015))
- 1469 [11] ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework
 1470 <https://www.iso.org/standard/45123.html>
- 1471 [11.1] ISO 15944 - 8:2012 Information technology — Business operational view — Part 8:
 1472 Identification of privacy protection requirements as external constraints on business transactions
 1473 <https://www.iso.org/standard/51544.html>
- 1474 [12] GAPP Generally accepted privacy principles (GAPP) in privacy policy development.
 1475 [https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-](https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/business-and-organizational-privacy-policy-resources/gapp-in-privacy-policy-development)
 1476 [topics/information-management-and-technology/publications/business-and-organizational-privacy-](https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/business-and-organizational-privacy-policy-resources/gapp-in-privacy-policy-development)
 1477 [policy-resources/gapp-in-privacy-policy-development](https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/business-and-organizational-privacy-policy-resources/gapp-in-privacy-policy-development)
- 1478 [13] ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for
 1479 privacy information management — Requirements and guidelines
- 1480 [14] NIST Privacy Framework (Version 1.0)
- 1481 [15] ISO/IEC 29184:2020 Information technology — Online privacy notices and consent
- 1482 [16] ISO/CD 22458

- 1483 [17] ISO/IEC Guide 76:2020
- 1484 [18] Future of Privacy Forum. The Internet of Things and Persons with Disabilities. 2019.
1485 [https://fpf.org/2019/01/31/iot-devices-should-deal-with-privacy-impacts-for-people-with-](https://fpf.org/2019/01/31/iot-devices-should-deal-with-privacy-impacts-for-people-with-disabilities/)
1486 [disabilities/](https://fpf.org/2019/01/31/iot-devices-should-deal-with-privacy-impacts-for-people-with-disabilities/)
- 1487 [19] ISO 30401:2018 Knowledge management systems – Requirements
1488 <https://www.iso.org/obp/ui/#iso:std:iso:30401:ed-1:v1:en>
- 1489 [20] ISO 9001:2015 (ref competence and awareness)
- 1490 [21] OASIS Privacy by Design for Software Engineers [https://www.oasis-](https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se)
1491 [open.org/committees/tc_home.php?wg_abbrev=pbd-se](https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se)
- 1492 [22] ISO COPOLCO, 2016, Identification of current consumer issues in privacy and protection of
1493 personal data – Document N211/2016 Annex 1
- 1494 [23] ISO/IEC Guide 76:2008(en), Development of service standards — Recommendations for
1495 addressing consumer issues
- 1496 [23.1] ANEC Principles for Digital Devices [https://www.anec.eu/publications/other-](https://www.anec.eu/publications/other-publications/588-anec-consumer-representatives-guidance-domestic-privacy-and-the-privacy-of-digitally-connected-devices) publications/588-
1497 [anec- consumer- representatives- guidance-domestic- privacy-and-the- privacy-of-digitally- connected-](https://www.anec.eu/publications/other-publications/588-anec-consumer-representatives-guidance-domestic-privacy-and-the-privacy-of-digitally-connected-devices)
1498 [devices](https://www.anec.eu/publications/other-publications/588-anec-consumer-representatives-guidance-domestic-privacy-and-the-privacy-of-digitally-connected-devices)
- 1499 [23.2] Securing consumer trust in the Internet of Things. Principles & recommendations 2017' ANEC,
1500 BEUC, CI, ICRT
- 1501 [24] ISO 31000:2018, Risk management — Guidelines
- 1502 [25] ISO/IEC WD 27557, Organizational Privacy Risk Management
- 1503 [26] NIST privacy risk model: NISTIR 8062. "Introduction to Privacy Engineering and Risk Management
1504 in Federal Systems 2017. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf
- 1505 [27] CNIL privacy risk model: CNIL PIA manual 1- methodology: how to carry out a PIA. June 2015
1506 Edition. <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf> . CNIL is
1507 considered consistent with 29134.
- 1508 [28] ISO/IEC 29134, Guidelines for privacy impact assessment
- 1509 [29] NIST Special Publication 800-30: Guide for Conducting Risk Assessments
- 1510 [30] *Privacy Management Reference Model and Methodology (PMRM) Version 1.0*, OASIS Committee
1511 Specification 02, available at [http://docs.oasis-open.org/pmr/pmr/v1.0/cs02/PMRM-v1.0-](http://docs.oasis-open.org/pmr/pmr/v1.0/cs02/PMRM-v1.0-cs02.html)
1512 [cs02.html](http://docs.oasis-open.org/pmr/pmr/v1.0/cs02/PMRM-v1.0-cs02.html)
- 1513 [31] van der Nagel, E., Arnold, M., Nansen, B., Gibbs, M., Kohn, T., Bellamy, C., and Clark, N. 2017, Death
1514 and the Internet: Consumer issues for planning and managing digital legacies, 2nd edn, Australian
1515 Communications Consumer Action Network, Sydney
- 1516 [32] ISO 15288:2015 Systems and software engineering — System life cycle processes
- 1517 [33] ISO/IEC 27555 (DIS stage)
- 1518 [34] ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of
1519 techniques

1520

1521 [x.1] ISO COPOLCO 39th meeting – An outline description of the proposed new standard for privacy
 1522 by design of consumer goods and services, April 2017 – Annex B of Document N283

1523 [x.2] ISO 10377:2013, Consumer Product Safety - Guidelines For Suppliers

1524 [x.3] Operationalizing Privacy by Design <https://collections.ola.org/mon/26012/320221.pdf>

1525 [x.4] ISO/IEC 27001, Information technology — Security techniques — Information security
 1526 management systems — Requirements

1527 [x.5] ISO/IEC 27005, Information technology — Security techniques — Information security risk
 1528 management

1529 [x.6] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for
 1530 information security controls

1531 [x.7] NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems
 1532 and Organizations

1533 [x.8] GSMA. Mobile App Privacy by Design. <https://www.gsma.com/publicpolicy/resources/mobile-privacy-principles>
 1534