International Organization for Standardization
Organisation internationale de normalisation
Международная организация по стандартизации

Ch. de Blandonnet 8 | CP 401, 1214 Vernier | Geneva, Switzerland | T: +41 22 749 01 11 | central@iso.org | www.iso.org

Form 4: New Work Item Proposal

Circulation date: 2017-09-14 Closing date for voting: 2017-12-07	Reference number: Click here to enter text. (to be given by Central Secretariat)
Proposer (e.g. ISO member body or A liaison organization) ISO/COPOLCO	ISO/TC Click here to enter text./SC Click here to enter text. ☒ Proposal for a new PC
Secretariat BSI	N Click here to enter text.

A proposal for a new work item within the scope of an existing committee shall be submitted to the secretariat of that committee with a copy to the Central Secretariat and, in the case of a subcommittee, a copy to the secretariat of the parent technical committee. Proposals not within the scope of an existing committee shall be submitted to the secretariat of the ISO Technical Management Board.

The proposer of a new work item may be a member body of ISO, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Technical Management Board or one of the advisory groups, or the Secretary-General.

The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information.

IMPORTANT NOTE: Proposals without adequate justification risk rejection or referral to originator.
Guidelines for proposing and justifying a new work item are contained in Annex C of the ISO/IEC Directives, Part 1.

☒ The proposer has considered the guidance given in the Annex C during the preparation of the NWIP.

Proposal (to be completed by the proposer)

Title of the proposed deliverable.

English title:

Consumer protection: Privacy by design for consumer goods and services

French title (if available):

Click here to enter text.

(In the case of an amendment, revision or a new part of an existing document, show the reference number and current title)

Scope of the proposed deliverable.

Specification of the design process to provide consumer goods and services that meet consumers' domestic processing privacy needs as well as the personal privacy requirements of Data Protection.

In order to protect consumer privacy the functional scope includes security in order to prevent unauthorized access to data as fundamental to consumer privacy, and consumer privacy control with respect to access to a person's data and their authorized use for specific purposes.

The process is to be based on the ISO 9001 continuous quality improvement process and ISO 10377 product safety by design guidance, as well as incorporating privacy design JTC1 security and privacy good practices, in a manner suitable for consumer goods and services.

Purpose and justification of the proposal*

Purpose

Consumer Protection

To provide a standard whereby product (i.e. goods and services) designers and providers can demonstrate through consumer protection fulfilling the need to protect consumers from fraud, ransom demands, and other forms of privacy invasion and privacy breaking exploits resulting from lost and stolen personal data and high-jacking of consumer devices. Particularly of concern is the protection of children and the more vulnerable consumer.

Societal Protection improvements associated with privacy by design of consumer goods and services

In addition, given that consumer digitally connected devices have been harnessed by hackers to attack organizations, including critical infrastructure there is a vital need to prioritize a standard specific to the scoped privacy challenges of consumer goods and services design.

Incorporating the consumer perspective

There is a need for a consumer centric privacy by design standard for consumer protection in addition to organizational centric standards.

Justification

(1) Protection of consumers is a separate product discipline when designing for their network connected homes, network connected cars and presence in public places with their mobile devices and wearables.

The consumer domestic environment is very different from that of the organization. Consumers have low understanding of the technology, are often unskilled, use unmanaged devices without formal update and maintenance processes, have significant human vulnerabilities and limited capabilities that can be exploited, and use products in unexpected ways.

Consumers have specific privacy needs that design processes need to have considered and addressed. COPOLCO have identified 70 consumer privacy needs (3 security and privacy control needs and 7 needs associated with Consumer Centric Privacy Impact Assessment).

See Annex E for a report for COPOLCO and others on the proposed standard and the EU's General Data Protection Regulation. This report lists in Annex E2 the 63 primary consumer privacy needs and demonstrates that 29% of these privacy needs are for domestic privacy purposes which are not addressed by either the GDPR or the ISO/IEC Privacy Framework 29100 where personal processing by private individuals for domestic purposes is excluded in the definitions.

The report in Annex E demonstrates that the proposed standard can fulfill consumer product privacy by design regulatory requirements as well as addressing consumers' domestic privacy needs and key aspects of Cyber Security related to consumers' domestic equipment.

While many of the issues to be addressed are similar to those faced by organizations, consumer goods and services design have significantly different challenges compared to the design of corporate infrastructures, systems and applications.

Due to the many consumer factors above, the approach proposed by COPOLCO for this privacy by design standard is to emphasize technical design embedding consumer protection and control rather than human dependent risk mitigation actions.

For example: the range of goods and services in the connected smart home is rapidly expanding and much current security good practice recommends unique and high strength passwords for each device and service and yet consumers cannot cope with many different complex passwords. There are technical good practice solutions that could

be adopted which need to replace the proposed use of many different passwords, which is impractical from the consumer perspective.

(2) Societal protection improvements

As described in (1) above the more effective approach to consumer protection is through technical solutions incorporated directly into product design rather than human dependent actions. The proposed standard addresses Cyber Security protection of domestic equipment where privacy invasion threatens societal security whereby consumer goods and services may be suborned to attack others.

As an example of technical solutions:

Consumers are poor at keeping their security measures up to date, for a number of reasons such as updates interfering with the ways of using equipment that consumers are familiar with, or the complexity of the update process provided. There are a number of consumer needs and requirements that should be met in product design to address this aspect through technology design including simplified user controls with reduced human action to accept and install online delivered security software updates.

Consider the following: Is there a verified market need for the proposal? What problem does this standard solve? What value will the document bring to end-users? See Annex C of the ISO/IEC Directives part 1 for more information.

See the following guidance on justification statements on ISO Connect: https://connect.iso.org/pages/viewpage.action?pageId=27590861

Preparatory work (at a minimum an outline should be included with the proposal)

☐ A draft is attached ☒ An outline is attached ☐ An existing document to serve as initial basis

The proposer or the proposer's organization is prepared to undertake the preparatory work required:

☒ Yes ☐ No

If a draft is attached to this proposal,:

Please select from one of the following options (note that if no option is selected, the default will be the first option):

☐ Draft document will be registered as new project in the committee's work programme (stage 20.00)

☐ Draft document can be registered as a Working Draft (WD – stage 20.20)

☐ Draft document can be registered as a Committee Draft (CD – stage 30.00)

☐ Draft document can be registered as a Draft International Standard (DIS – stage 40.00)

☐ If the attached document is copyrighted or includes copyrighted content, the proposer confirms that copyright permission has been granted for ISO to use this content in compliance with clause 2.13 of the ISO/IEC Directives, Part 1 (see also the Declaration on copyright).

Is this a Management Systems Standard (MSS)?

☐ Yes ☒ No

NOTE: if Yes, the NWIP along with the Justification study (see Annex SL of the Consolidated ISO Supplement) must be sent to the MSS Task Force secretariat (tmb@iso.org) for approval before the NWIP ballot can be launched.

Indication(s) of the preferred type or types of deliverable(s) to be produced under the proposal.

☒ International Standard ☐ Technical Specification

☐ Publicly Available Specification ☐ Technical Report

Proposed development track

☐ 18 months* ☐ 24 months ☒ 36 months ☐ 48 months

Note: Good project management is essential to meeting deadlines. A committee may be granted only one extension of up to 9 months for the total project duration (to be approved by the ISO/TMB).

***DIS ballot must be successfully completed within 13 months of the project's registration in** order to be eligible for the direct publication process

Draft project plan (as discussed with committee leadership)

Proposed date for first meeting: To be confirmed

Dates for key milestones: DIS submission To be confirmed

Publication To be confirmed

Known patented items (see ISO/IEC Directives, Part 1 for important guidance)

☐ Yes ☒ No

If "Yes", provide full information as annex

Co-ordination of work: To the best of your knowledge, has this or a similar proposal been submitted to another standards development organization?

☐ Yes ☒ No

If "Yes", please specify which one(s):

Click here to enter text.

A statement from the proposer as to how the proposed work may relate to or impact on existing work, especially existing ISO and IEC deliverables. The proposer should explain how the work differs from apparently similar work, or explain how duplication and conflict will be minimized.

See Annex A

A listing of relevant existing documents at the international, regional and national levels.

ISO 9001, *Quality management systems – Requirements*

ISO 10377, *Consumer product safety – Guidelines for suppliers*

ISO/IEC JTC1 security and privacy good practices, including ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 29134, *Information technology – Security techniques – Guidelines for privacy impact assessment*

ISO/IEC 27005,

EN 16571, *Information technology – RFID privacy impact assessment process*

Please fill out the relevant parts of the table below to identify relevant affected stakeholder categories and how they will each benefit from or be impacted by the proposed deliverable(s).

	Benefits/impacts	**Examples of organizations/companies to be contacted**
Industry and commerce – large industry	**i.** Improved consumer and regulator trust from demonstration that good privacy by design practices have been followed for consumer goods and services **ii.** Reducing cyber-attack risks from consumer devices	Click here to enter text.
Industry and commerce – SMEs	As per i. and ii. above	Click here to enter text.
Government	As per i. and ii. above	Click here to enter text.
Consumers	Better information on the data implications of products, better maintained product security, more privacy sensitive default settings and user friendly controls for managing data flows	Click here to enter text.
Labour	Click here to enter text.	Click here to enter text.
Academic and research bodies	Click here to enter text.	Click here to enter text.
Standards application businesses	Click here to enter text.	Click here to enter text.
Non-governmental organizations	As per i. and ii. above	Click here to enter text.
Other (please specify)	Click here to enter text.	Click here to enter text.

Liaisons:	Joint/parallel work:
A listing of relevant external international organizations or internal parties (other ISO and/or IEC committees) to be engaged as liaisons in the development of the deliverable(s). The standard needs cross-TC and SC expertise to contribute directly. A listing of potentially concerned TCs appears at Annex D.	Possible joint/parallel work with: ☐ IEC (please specify committee ID) Click here to enter text. ☐ CEN (please specify committee ID) Click here to enter text. ☐ Other (please specify) Click here to enter text.

A listing of relevant countries which are not already P-members of the committee.

N/A

Note: The committee secretary shall distribute this NWIP to the countries listed above to see if they wish to participate in this work

Proposed Project Leader (name and e-mail address)	Name of the Proposer (include contact information)
British Standards Institution *Project leader's name to be confirmed* c/o Sadie Homer, Consumer Interest and Policy Executive, BSI (sadie.homer@bsigroup.com)	COPOLCO c/o Dana Kissinger-Matray Secretary of ISO/COPOLCO copolco@iso.org

This proposal will be developed by:

☐ An existing Working Group (please specify which one: Click here to enter text.)

☐ A new Working Group (title: Click here to enter text.)

(Note: establishment of a new WG must be approved by committee resolution)

☐ The TC/SC directly

☒ To be determined

Supplementary information relating to the proposal

☒ This proposal relates to a new ISO document;

☐ This proposal relates to the adoption as an active project of an item currently registered as a Preliminary Work Item;

☐ This proposal relates to the re-establishment of a cancelled project as an active project.

Other:

Click here to enter text.

Maintenance agencies and registration authorities

☐ This proposal requires the service of a maintenance agency. If yes, please identify the potential candidate:

Click here to enter text.

☐ This proposal requires the service of a registration authority. If yes, please identify the potential candidate:

Click here to enter text.

NOTE: Selection and appointment of the MA or RA is subject to the procedure outlined in the ISO/IEC Directives, Annex G and Annex H, and the RA policy in the ISO Supplement, Annex SN.

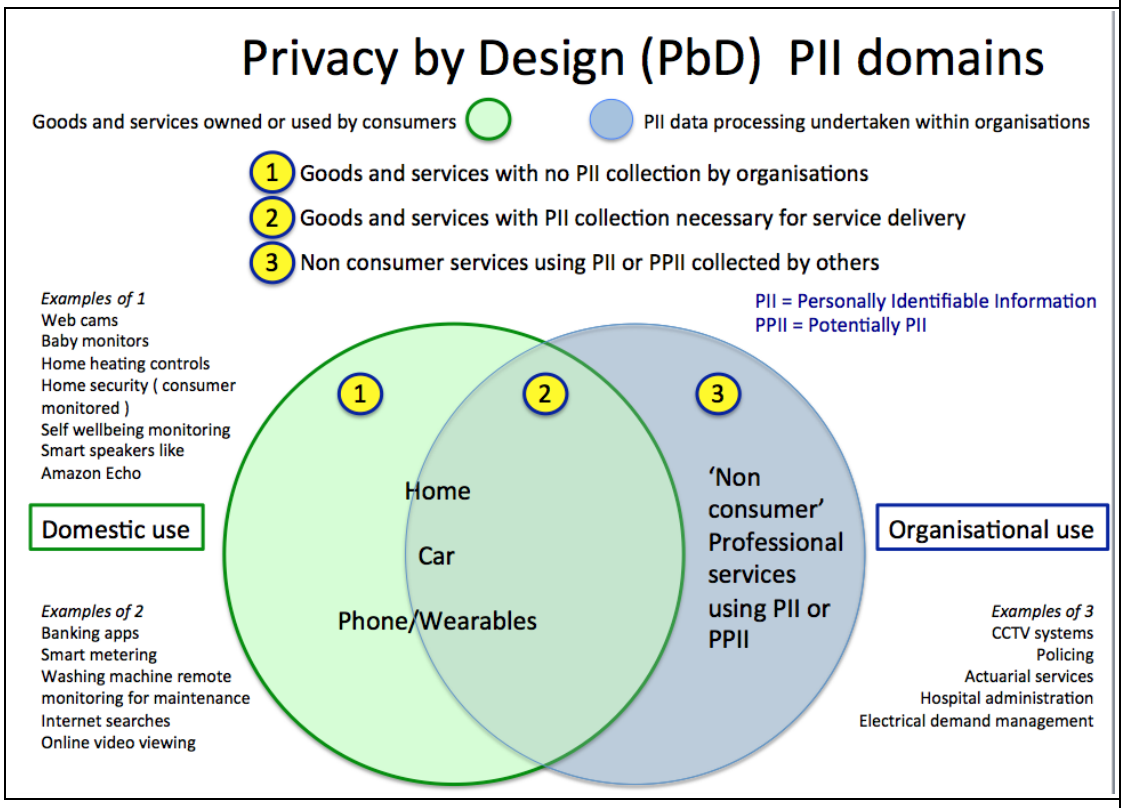
☒ Annex(es) are included with this proposal (give details)

Annex A - NWIP position with respect to current JTC 1 work and past PC 243, Consumer Product Safety

A1.1. The Personal Data Processing from the consumer perspective

Figure A1.1 Provides key background to the different domains in which goods and services process personal data (PII).

Figure A1.1 – Product domains in which PII is processed



The green domain in the Venn diagram illustrates consumer domestic activities that involve the use of goods and services that are digitally connected. The blue/grey domain indicates the goods and services where personal data PII is processed by organizations and protected by Data Protection law and regulation.

Domain 1 shows the goods and services where there is no need for data collection by a 3rd party for the purposes of delivering the usefulness that the consumer is seeking. For example in this domain devices connected via domestic Wi-Fi to 'apps' on smartphones, tablets and desktops are found and may be for entertainment (e.g. music round the house). Also typically various forms of domestic 'self' monitoring that is entirely managed by the consumer for house security and personal health reasons.

Data protection law and the JTC 1 Privacy Framework ISO/IEC 29100 address these types of good and service poorly. Consumers are like data controllers when undertaking processing for domestic purposes, however ISO/IEC 29100 explicitly excludes natural persons who use data for personal purposes thereby leaving consumer domestic processing poorly addressed for the purposes of privacy by design.

Domain 2 is the overlap between the green and the blue grey areas showing those goods and services where organizations interact with consumers' data that is used in order to deliver service to the consumer.

Domain 3 shows those services where PII is processed by organizations to provide professional services to other organizations and the public, but not to provide direct service to consumers as such.

In domain 3 PII is sourced mainly by :-

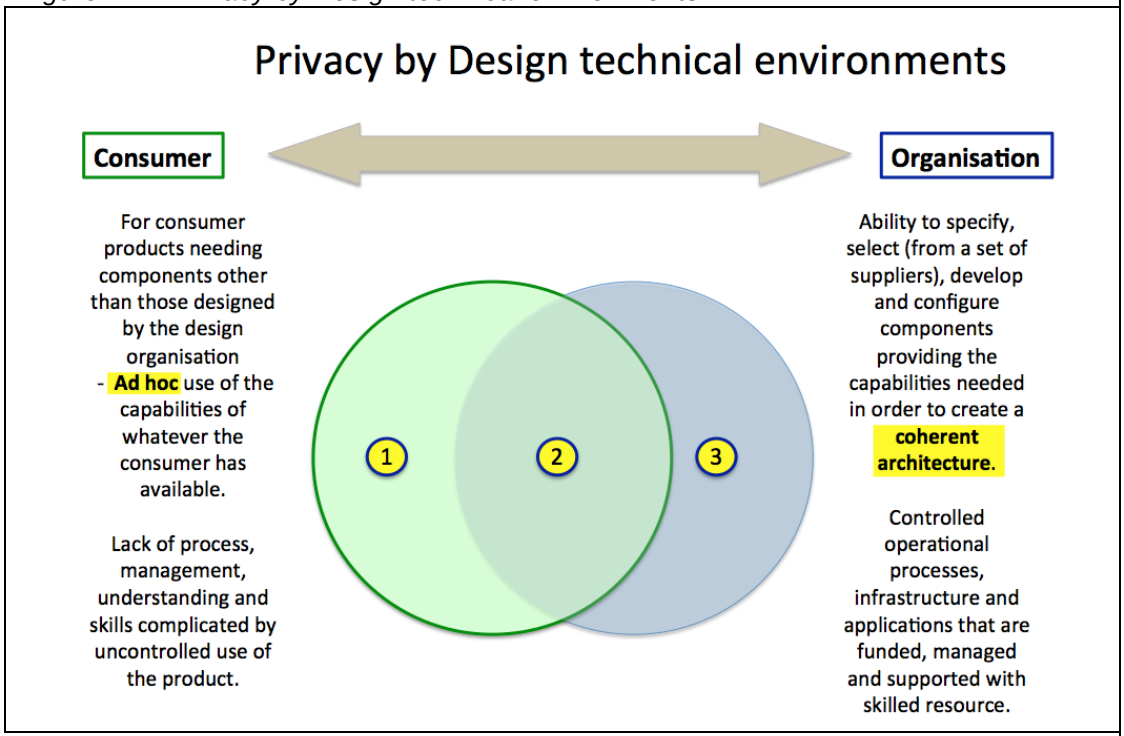
- data passed on from original PII collection that meet the original purpose for that collection

- monitoring devices and networks that can observe people such as CCTV networks, traffic control systems, security services

A1.2. The differences in technical environment between organizations and the domestic environment

The technical environments of the organization and the consumer are illustrated in Figure A1.2.

Figure A1.2 Privacy by Design technical environments



Any hardware and software residing in the uncontrolled domestic environment (the green domain - house, car or wearable) has to fit within an ad-hoc set of other consumer goods and services which will be suitable to varying degrees for use with the product provided.

Where domestic data has been collected and processed within organizations (including contracted 3rd party processors), as in domain 2, any application software running within the organization should be running on a coherent and controlled infrastructure.

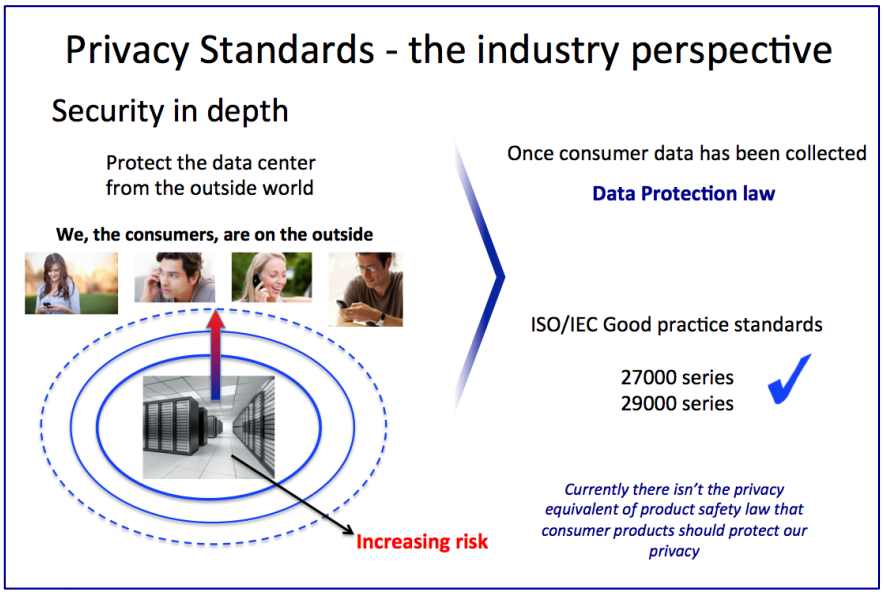
These are two very different design environments with different requirements and risks to be addressed through design.

The services that use personal data in domain 3 are not directly 'consumed' by consumers but may nonetheless be of concern where agencies collect consumer data from 3rd parties or by observing individuals in order to process personal data about individuals. However this secondary use of personal data and remote observation take place in managed environments with different societal objectives and so are not included in the scope of this proposal.

Annex B – Organization-centric and consumer-centric perspectives

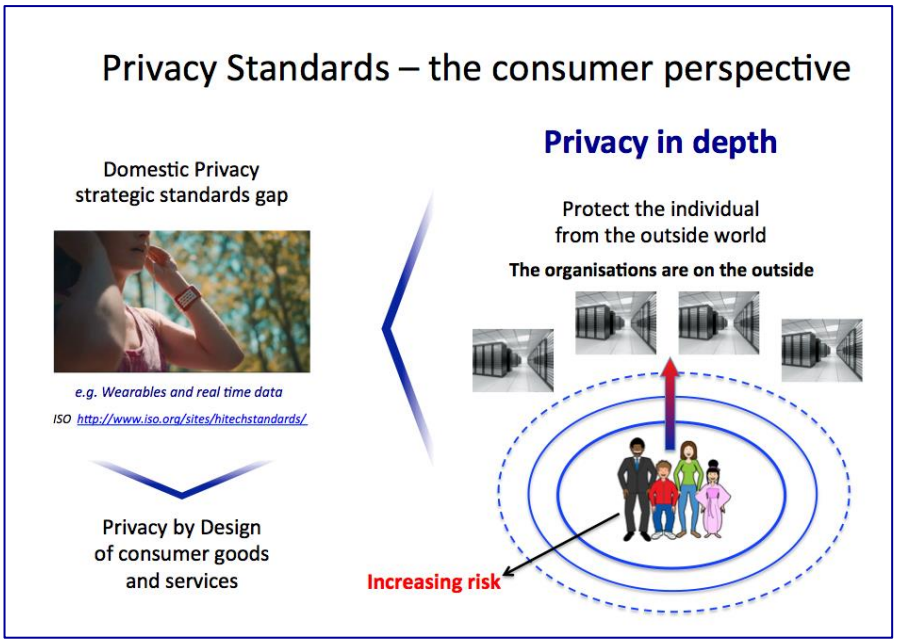
The current JTC 1 Security and Privacy standards address domain 3 and a number of aspects of domain 2 with their organization centric approach. The Industry perspective is illustrated in figure A1.3

Figure B1.1 The current Industry perspective with respect to privacy



The COPOLCO NWIP places the consumer at the centre of the design process with all organizations at the periphery. The NWIP is intended to protect the consumer when interacting with the rest of the world in a manner that delivers products that meet their domestic privacy needs, addressing consumers' use of products and technically addressing consumer capabilities and vulnerabilities that impact security and privacy control.

Figure B1.2 The Consumer centric perspective with respect to privacy



Annex C Relationship between consumer centric protection design and JTC 1 work related to consumer domestic privacy.

The common ground between the NWIP proposal that needs most care, management and cooperation are those JTC 1 standards that relate to the application software code design that runs within the controlled systems and infrastructures of organizations and the input/output communications provided by an organization for consumers to communicate digitally with the application software running in their domain.

Overall impact of consumer centric design
With personal / domestic processing excluded from current standards based on ISO/IEC 29100 the new and different ground of the COPOLCO NWIP is the privacy by design of domestic hardware, software running on domestic hardware and any domestic communications equipment used by consumers in the consumer context.

Making use of current ISO privacy and security standards
The consumer centric focus and inclusion of consumer domestic environment protection requires current security controls such as those in ISO/IEC 27001 Annex A to be reviewed and adjusted in order to be suitable for consumer goods and services privacy design. See Box 1 for 2 examples

Box 1 an initial view on 2 examples of changes needed to security controls in order to be suitable for consumer goods and services privacy design

Potential changes to security controls that could be needed for the privacy by design of consumer goods and services are shown in blue are provided for an example from ISO 27001

ISO/IEC 27001 Annex A
Example 1
A 6.2 Mobile devices

Objective: To ensure the security of ~~teleworking and~~ use of mobile devices as or for consumer products.
A.6.2.1 Mobile device policy: Control - ~~A policy and supporting~~ security measures shall be adopted to manage the privacy risks introduced by using mobile devices to access an organization's applications for both domestic and organizational processing purposes.

A.6.2.2 ~~Teleworking~~ Mobile device domestic environment processing: Control- ~~A policy and supporting~~ security measures shall be implemented to protect domestic information accessed, processed or stored in the domestic environment (homes, cars and wear-ables and portables) ~~at teleworking sites.~~

Example 2
A.8.1.1 Inventory of assets - Control – Assets associated with information and information processing facilities shall be identified including consumer product design as an asset and an inventory of these assets shall be drawn up and maintained.

A.8.1.2 Ownership of assets - Control - Assets maintained in the inventory shall be owned. Asset records shall include the ownership of equipment and product design responsibly within the organization and also design responsibility for that of 3rd party interworking assets (equipment) used by the consumer to achieve full product functionality .

The implications of interworking of products in the domestic environment
Another factor[1] in the privacy design for the consumer environment is the interworking between the product components and miscellaneous 3rd party products in the domestic environment. Both the core design work and the privacy impact assessment of the design, that is part of the overall privacy by design process, need to address the practicalities of any potential mismatch.

This means that in the privacy by design process areas where devices depend on interworking with other 3rd party products care needs to be taken to ensure that the security and privacy control capabilities of those 3rd party products are addressed and utilized effectively across all the interworking interfaces needed to deliver the product's overall functionality.

Use of the Privacy Impact Assessment guidance standard ISO/IEC 29134
Much good practice has been articulated in the JTC 1 PIA standard that can be incorporated into the privacy by design standard through requirements to undertake and document the majority of elements that apply directly to the consumer goods and services privacy by design process.

There is the potential for the new consumer goods and services privacy by design standard to enhance the 29134 PIA practices in a few places with respect to the lessons learnt from the Consumer Centric aspects of the CEN RFID PIA EN 16571. These lessons include the generic privacy risks arising from devices that can be illicitly powered up or down without the user's knowledge, and a privacy risk assessment framework based on ISO/IEC 27005 that provides consumers with a consistent numeric privacy risk score, essential for product comparison and consumer choice.

Ultimately many different product areas will need to make use of the NWIP, as indicated in Annex D that lists the 'ISO only' TC's that in time will need to make use of the standard.

[1] The interworking of potentially not fully compatible designs was highlighted in the work to develop the CEN RFID Privacy Impact assessment standard EN 19571

Annex D. List of Consumer Product TC's outside JTC1 needing privacy coordination

ISO/TC 20	Aircraft and space vehicles
ISO/TC 21	Equipment for fire protection and fire fighting
ISO/TC 22	Road vehicles
ISO/TC 29	Small tools
ISO/TC 31	Tyres, rims and valves
ISO/TC 34	Food products
ISO/TC 38	Textiles
ISO/TC 42	Photography
ISO/TC 68	Financial services
ISO/TC 76	Transfusion, infusion and injection, and blood processing equipment for medical and pharma
ISO/TC 83	Sports and other recreational facilities and equipment
ISO/TC 84	Devices for administration of medicinal products and catheters
ISO/TC 86	Refrigeration and air-conditioning
ISO/TC 92	Fire safety
ISO/TC 94	Personal safety -- Protective clothing and equipment
ISO/TC 106	Dentistry
ISO/TC 122	Packaging
ISO/TC 126	Tobacco and tobacco products
ISO/TC 133	Clothing sizing systems - size designation, size measurement methods and digital fittings
ISO/TC 136	Furniture
ISO/TC 219	Floor coverings
ISO/TC 222	Personal financial planning
ISO/TC 225	Market, opinion and social research
ISO/TC 228	Tourism and related services
ISO/TC 232	Learning services outside formal education
ISO/TC 241	Road traffic safety management systems
ISO/TC 242	Energy Management
ISO/PC 245	Cross-border trade of second-hand goods
ISO/PC 252	Natural gas fuelling stations for vehicles
ISO/TC 254	Safety of amusement rides and amusement devices
ISO/TC 257	Evaluation of energy savings
ISO/TC 260	Human resource management
ISO/TC 264	Fireworks
ISO/TC 268	Sustainable development in communities
ISO/TC 269	Railway applications
ISO/PC 273	Customer contact centres
ISO/TC 274	Light and lighting
ISO/PC 283	Occupational health and safety management systems
ISO/PC 288	Educational organizations management systems - Requirements with guidance for use
ISO/TC 290	Online reputation
ISO/TC 291	Domestic gas cooking appliances
ISO/TC 292	Security and resilience

Annex D continued **– TC's outside JTC 1 that may process PII needing privacy coordination**

ISO/TC 46	Information and documentation
ISO/TC 69	Applications of statistical methods
ISO/TC 70	Internal combustion engines
ISO/TC 121	Anaesthetic and respiratory equipment
ISO/TC 130	Graphic technology
ISO/TC 146	Air quality
ISO/TC 147	Water quality
ISO/TC 154	Processes, data elements and documents in commerce, industry and administration
ISO/TC 159	Ergonomics
ISO/TC 163	Thermal performance and energy use in the built environment
ISO/TC 171	Document management applications
ISO/TC 176	Quality management and quality assurance
ISO/TC 184	Automation systems and integration
ISO/TC 194	Biological and clinical evaluation of medical devices
ISO/TC 199	Safety of machinery
ISO/TC 203	Technical energy systems
ISO/TC 212	Clinical laboratory testing and in vitro diagnostic test systems
ISO/TC 224	Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators
ISO/TC 251	Asset management
ISO/TC 262	Risk management
ISO/TC 267	Facilities management
ISO/TC 272	Forensic sciences
ISO/PC 277	Sustainable procurement
ISO/PC 278	Anti-bribery management systems
ISO/TC 279	Innovation management
ISO/PC 280	Management Consultancy
ISO/TC 282	Water re-use
ISO/PC 286	Collaborative business relationship management -- Framework
ISO/TC 289	Brand evaluation
ISO/PC 294	Guidance on unit pricing
ISO/PC 295	Audit data collection

Annex E – Preliminary report to BSI-CPIN, ANEC and ISO COPOLCO

An initial view on the proposed ISO COPOLCO Privacy by Design of Consumer Goods and Services requirements standard and the EU General Data Protection Regulation.

Pete Eisenegger 11 July 2017 Report not peer reviewed at this time.

Overview of Privacy by Design for consumer goods and services

The proposed privacy by design standard deals with the design lifetime of goods and services used by consumers

Consumer privacy = security plus privacy control

Product = both goods and services

Key steps in the privacy by design process include product privacy governance; determining product security and privacy control development requirements; testing and validation of the design including privacy impact assessment; release to market preparation such as consumer privacy documentation, product privacy labelling and putting in place market monitoring of the product for privacy issues; fixing issues and updating the product in the field online or otherwise; lastly product withdrawal.

The main steps in the proposed process applicable to the GDPR are those associated with establishing the privacy requirements for product development. These requirements are established through use case methodology which requires design teams to describe how the product is used, the types of users such as children, parents, old age pensioners, financially pressed consumers, organizations' product administrators and so on. Designers will have to consider intended uses, unintended uses, misuse and malicious use cases.

Later in the process preparing for product release steps include requirements for consumer documentation and information to be provided to regulators.

It should be noted that the detailed use case specification requires relevant GDPR details, for example, user interactions and interfaces, the types of data to be collected and returned to users, purposes of processing, data flows, use of 3rd party products such as cloud services or the consumer's home router and the geographic location of processing.

Use cases enable privacy needs and associated product requirements to be specified and the subsequent product validation steps will need to include checks that these requirements have been met and not circumvented as with VW pollution test cheats that were designed in.

Going beyond the GDPR - domestic processing and cyber security.

While the GDPR represents the regulatory base line of Data Protection by organizations in the EU, it explicitly excludes domestic processing i.e. that undertaken by individuals in their private lives involving friends and family and undertaken for personal purposes only.

Further, apart from one very high level GDPR requirement to keep data secure, consumers' detailed security needs and requirements of goods and services that they use in their homes, in their cars or as wearables are not addressed.

The key steps in the proposed process for consumer security are:

- the identification of the technology vulnerabilities that are already known, such as smartphone operating system weaknesses for those designing smartphone apps or radio links that need encryption to protect from eavesdropping of intelligible data.
- followed by the setting of product security requirements that take these known vulnerabilities into account as well as providing access controls for consumers and organizational users.
- monitoring and investigation of the products performance in the market for security and privacy control issues arising from privacy breaking exploits
- design updates resulting from market monitoring.

It should be noted that this key part of the scope of the proposed standard addresses the cyber security concerns over insecure domestic equipment like web cams, smart TV's etc.

Overall 29% of the ISO COPOLCO agreed consumer privacy needs deal with domestic processing and these feed into the proposed design process.

GDPR requirements and the proposed standard.

For the purposes of this report a Bird and Bird guide to the GDPR was used. This is a 69 page document that provides good detail on the key GDPR requirements without having to engage with the whole of the regulation that has been drafted.

65 key GDPR factors were identified from the Bird and Bird guide, and these were examined against the current draft of the proposed standard. It appears that 100% of the GDPR requirements identified relevant to privacy by design can be addressed at a detailed product level by the proposed design process. The few remaining factors not directly relevant to the PbD process (4 out of 65) pertained to Supervisory bodies, codes of conduct, helplines etc.

A vital element is Governance and in the GDPR there are requirements to demonstrate that privacy by design has been applied and that there is accountability for compliance. These are fundamental to the proposed PbD standard which requires the assignment of key privacy responsibilities to a member of the design team.

As the proposed PbD standard is for products (that is, both goods and services), this results in a design process that addresses issues at a much more detailed level than the GDPR regulation. For example the consumer standards representative guide on domestic privacy and digitally connected devices contains sections on the domestic privacy needs and domestic requirements relevant to children including the role of responsible 3rd parties (parents and guardians), domestic privacy controls addressing 'oversharing' on social media and when content is intrusive including cyber bullying and online porn.

Preliminary conclusion

By using the proposed PbD standard and complying with its requirements those responsible for products will be able to support their Data Controllers / Data Protection Officers with the detailed product privacy design documentation and proof needed to demonstrate compliance with the GDPR.

Furthermore a significant contribution to cyber security can be made addressing the 'hack-ability' of consumer devices.

Pete Eisenegger

BSI Consumer and Public Interest Network Consumer Coordinator Digital Standards

ANEC Privacy and Internet of Things Expert

ISO COPOLCO Privacy Key Person

Supporting detail to this preliminary report:

Annex E1 – The list of 65 factors extracted from the Bird and Bird guide to the GDPR.

Annex E2 – The current ISO COPOLCO list of 63 privacy needs

Annex E3 – a 'work in progress' list of 53 key elements to the privacy by design process for consumer goods and services

Annex E1 The list of 65 factors extracted from the Bird and Bird guide to the GDPR

B-B page no	Ref no used for analysis	
5	1	Territorial scope
8	2	Consent
8	3	Transparency
8	4	Children
8	5	Personal data / sensitive data
9	6	Pseudonymisation
9	7	Personal data breach communication
9	8	Data protection by design / accountability
9	9	Enhanced rights for individuals (eg right to be forgotten)
9	10	Supervisory authorities and the EDPB
11	11	Lawfulness, fairness and transparency
11	12	Purpose limitation
11	13	Data minimisation
11	14	Accuracy
11	15	Storage limitation
11	16	Integrity and confidentiality (security, loss, damage, destruction)
11	17	Accountability (able to demonstrate compliance)

13	18	Further processing
15	19	What are legitimate interests?
15	20	Information notices must now set out legitimate interests
15	21	Specific and enhanced right to object (to legitimate interests)
15	22	Codes of Conduct
15	23	Data transfers (one off exceptional)
17	24	Consent - a wider definition (specific, informed and unambiguous)
17	25	Consent - distinguishable revocable and granular
18	26	Children and research
18	27	Language of consent (clear easily understood)
20	28	Children Parental consent
20	29	Child friendly notices
20	30	Children Misc. provisions (helplines, codes of conduct and work for supervisory authorities)
22	31	Processing of sensitive personal data
23	32	Genetic, biometric or health data
23	33	Criminal convictions and offences
25	34	What must a controller tell individuals?
25	35	When must a controller provide this information?
27	36	Right of access to data
27	37	Supplemental information (processing purposes, data types, recipients etc.)
28	38	Rectification
28	39	Portability
30	40	Right to object Processing which is for direct marketing purposes
30	41	Right to object Processing for scientific/historical research/statistical purposes
30	42	Right to object Processing based on two specific purposes:
30	43	Right to object - direct marketing
32	44	When right to be forgotten applies
32	45	Data placed in the public domain (right to be forgotten)
32	46	Notification of other recipients (right to be forgotten)
33	47	Right to restrict processing
33	48	When right to restriction is applicable
35	49	Meaning of profiling
35	50	Restrictions on automated decision-taking with significant effects
35	51	Automated decisions based on explicit consent or contractual fulfilment
35	52	Automated decision taking Authorisation by law
35	53	Automated decision taking Sensitive data
37	54	Governance Privacy by Design
37	55	Governance Privacy Impact Assessments

38 56 Governance Data Protection Officer

39 57 Governance Using service providers (data processors)

39 58 Governance Record of processing activities (type of data processed, the purposes for which it is used etc.)

41 59 Obligation for data processors to notify data controllers (data breaches)

41 60 Obligation for data controllers to notify the supervisory authority

41 61 Obligation for data controller to communicate a personal data breach to data subjects

41 62 Data Breach Documentation requirements

44 63 Codes of Conduct

48 64 Transfers of personal data

57 65 Remedies and liabilities - rights of individuals to complaint to supervisory authority

Annex E2 **–** The current ISO COPOLCO list of consumer privacy needs

General consumer domestic privacy needs

1 Network and system security

2 Consumer digital devices security

3 Keeping consumer protection up to date

4 Sourcing trustworthy apps and applications

5 Loss of digital devices

6 Consumer device security over a product lifecycle

7 Consumer security information

8 Consumer confidence in organisations' terminal equipment

9 Consumer privacy preferences and control in real time (24x7)

10 Consumer privacy control in cloud computing services via 3rd party apps

11 Consumer privacy control for the Internet of Things including smart domestic appliances and cars

12 Consumer privacy control for remote control of Things

13 Consumer privacy control when 3rd party responsible persons need to be involved (e.g. parents and carers)

14 Consumer privacy control over the social distribution of their shared data

15 Privacy controls with respect to those receiving shared personal information

16 Privacy controls when an individual is identifiable in someone else's shared data

17 Consumer privacy controls for intrusive content

18 Consumer privacy controls for intrusive (false) equipment control commands

Consumer privacy control over data collection by third parties

19 Consumer privacy preferences and control in real time (24x7)

20 Service impacts when privacy data collection preferences are changed by the consumer

21 Consumer privacy and service interactions

22 Personal data analysis that removes anonymity

23 Anonymity when personal information is collected via sensors

24 Accountability for statements and views made online:

25 Direct to individuals

26 About individuals in public virtual domains

Personal data transfer

27 General personal data transfer traceability

28 Traceability of transferred data for consumer consent

29 Traceability for consent to new processing purposes

30 Consent traceability within original data processing consents given

31 Traceability of transferred data for the purposes of personal data access and correction requests

32 Consumer query need - 'where did you get my data from?"

Personal data analysis

33 Balancing the right to privacy with the public interest

34 Governance

35 Engaging stakeholders

36 Anonymization

37 Re-identification

38 Profiling: Building up large personal profiles

39 Data fitness for purpose

40 Existing customer or client data analytics

41 Analysis of PII from open data

42 Data analytics to identify or target an individual

43 Data analytics to identify groups of people

44 Data analytics for systems

EU Data Protection (needs to be met that are essential for consumer trust)

45 The Right to be Forgotten

46 Privacy by Default

47 Privacy by Design

Consumer privacy information provision

48 Public place privacy awareness notification and signage
49 Consumer product/service information
50 Summary of privacy impact assessment
51 Privacy risks and mitigation actions
52 Privacy control instructions
53 Privacy and security of domestic equipment maintenance instructions
54 Consumer Privacy Information Policies
55 Privacy risks and mitigation actions
56 Privacy labelling
57 Privacy complaints and queries

Data Breach

58 When personal data is lost
59 Within organisation action to prevent/reduce subsequent fraud resulting from the data loss
60 PII (personally identifiable information) loss by the organisation
61 PII loss by another organisation that could be used for fraud
62 Information for consumers about precautionary action and advice in the light of the data loss
63 Consumer action to be taken if the consumer detects fraud arising from data loss

Annex E3 – The current list of 53 key elements to the privacy by design process for consumer goods and services

Flow chart element ref. Title of flow chart element

1 Establish Product Governance
2 Decision on market volume and innovation
3 Define Product
4 Define supply chain
5 Define retail channels and distribution to consumers
6 Define Consumer and Administration use cases
7 Use case specification
8 Interworking with 3rd party products
9 Consumer requirements
10 Product technology and vulnerabilities

11 Technology security requirements
12 Product design tools, rules and support
13 Documentation of product configuration
14 Design product and produce prototype
15 Establish product testing and design validation strategy
16 Hardware functional and penetration testing
17 Software testing - static, dynamic, fuzz and hidden (cheat) processing
18 Product / system commissioning / beta testing
19 Product Privacy Impact Assessment
20 Decision 'all design criteria met?'
21 Prepare for product release
22 Production testing and system commissioning
23 Incident monitoring and response planning
24 Retail channels Privacy review and channel documentation
25 Consumer documentation
26 Regulatory information documentation
27 Release product
28 Monitor the market
29 Decision 'Have market exploits and product issues been identified?'
30 Prioritise action on privacy harm / risk
31 Identify unexpected use
32 Identify own product vulnerability exploited
33 Identify 3rd party product vulnerability exploited
34 Update use cases
35 Update product requirements
36 3rd party notification of new exploit (interworking products, application developers, regulators)
37 Update product requirements and inform 3rd party product providers
38 Determine remedial action
39 Inform consumers and regulators
40 Update product software
41 Recall product
42 Produce consumer remedial information
43 Release updated software
44 Issue product recall information
45 Monitor uptake and impact of consumer remedial information
46 Monitor uptake of software update
47 Monitor success of product recall
48 Decision 'is the remedial action effective?'
49 Decision 'have the conditions for product withdrawal been reached?'
50 Decision 'do a significant number of consumers still use the product?'
51 Put in place interim privacy support arrangements

52 Issue consumer withdrawal notification

53 Withdraw product

Note: This is a working list and other issues have yet to be considered such as the privacy implications of company takeovers where :

- the terms and conditions for existing products could change as with WhatsApp and Facebook or
- the new owner undertakes a completely new design and online update where impacts might reduce the effectiveness of the previous design such as Nokia's takeover of Withings and their Health Mate fitness tracking app.

Additional information/questions

Click here to enter text.

AN OUTLINE DESCRIPTION OF THE PROPOSED NEW STANDARD FOR PRIVACY BY DESIGN OF CONSUMER GOODS AND SERVICES

Pete Eisenegger, April 2017

---

1 Overview of the proposed standard

1.1 The need for a requirements standard

The new work item proposal aims to achieve a single standard that allows consumer goods and services providers to address all the lifecycle issues of privacy by design so that through its use and proven compliance consumers can make goods purchases and use services with greater confidence that privacy protection has been designed into the products.

A solution involving several standards to cover a number of phases of product design and update/withdrawal is seen as leading to consumer confusion should only one of several standards be taken up by providers. The digital world is faster in design change, lower cost for design update and so a more integrated process is needed round the continuous improvement cycle of ISO 9001.

Product providers will benefit from an improved trust position in the market compared to the product providers who do not use and comply with the standard.

1.2 A continuous quality improvement process

Software design and update is continuous. So the proposed standard will combine into an ISO 9001 Deeming Cycle (Plan Do Check Act) what was developed as two Safety by Design guidance standards that currently deal with initial product Safety by Design and then Product Recall.

The cycle will consist of a number of requirements pertaining to planning and preparing for product development, then the development and in-company testing phase and preparation for launch followed by product release to the market place and monitoring its performance and issues, and lastly the prioritization and product update development to address issues and improvements.

1.3 Consumer centric

The proposed standard will add to existing ISO Security and Privacy standards the elements needed to account for how we live our domestic lives to give a standard that makes compliance both legal and most importantly practical for consumers.

2 Main purpose of the standard

To provide a standard whereby product (i.e. goods and services) designers and providers can improve consumer trust by demonstrating consumer privacy protection, thereby fulfilling the need to protect consumers from fraud, ransom demands, and other forms of privacy invasion and privacy breaking exploits resulting from lost, stolen and illegally transferred personal data, as well as high-jacking of consumer devices. Particularly of concern is the protection of children and the more vulnerable consumer.

3 Scope of the proposed deliverable

Specification of the design process to provide consumer goods and services that meet consumers' domestic processing privacy needs as well as the personal privacy requirements of Data Protection.

In order to protect consumer privacy the functional scope includes security in order to prevent unauthorized access to data as fundamental to consumer privacy, and consumer privacy control with respect to access to a person's data and their authorized use for specific purposes.
The process is to be based on the ISO 9001 continuous quality improvement process and ISO 10377 product safety by design guidance as well as incorporating in a manner suitable for consumer goods and services privacy design JTC1 security and privacy good practices.

4 Consumer goods and services concept model

There is a need to provide those who use the standard with a concept model and description of the different equipment elements that are addressed in different ways by the design process standard.

The product designers are directly responsible for the design of any consumer hardware and software provided as all or part of the goods and services designed and in addition any application software that has been uniquely created as part of the product where that application software runs on organizational infrastructure, such as corporate servicer farms or Cloud services, where processing occurs outside the consumer's domestic environment.

Then there are 3rd party products that product designers decide to use in order to deliver the overall functionality and performance of their product. Examples being tablet computers on which they mount their 'apps' and routers owned by consumers, and outside the consumer environment cloud services like Amazon's 'Alexa' voice interactive services or business to business services like credit rating and age checking that may be utilized in the product design.

Such 3rd party products are treated differently in the design process as designers can only make use of existing security and privacy capabilities of 3rd party products for their own design.

This section should also provide an overview process flow chart for the 'plan do check act' activities subsequently specified in the standard.

5 Product design governance

Those making use of the standard need to ensure that the right governance arrangements are in place including at a minimum:

- Responsibilities and accountability,
- resources,
- skills and sources thereof;
- budgets,
- project management,
- product objectives,
- key privacy criteria and objectives

This section will also provide practical requirements that allow the smaller more agile product developers to apply the standard effectively when the number of consumers using the product in the market is low.

6 General requirements

The general applicability of law and regulation and standards will be specified and the requirement for product traceability for devices digitally connected to the Internet. This digital traceability requirement is not only applicable for online software updating products but also may be used to enhance product safety by enabling better consumer notification of product risks and recalls.

7 Privacy by Design documentation

There are a great many product documentation requirements bringing together guidance from both Safety by Design standards and Privacy Impact Assessment standards.

8 Definition of the product

The definition of consumer product being either a good or a service will be used.
Requirements will be included to ensure that designers detail their decisions covering:

- A description of the product
- The purposes that the product is designed to fulfil
- The intended users of the product
- An overview of the data flows generated through product use
- Identification of the 3rd party products with which interworking is required to deliver the products overall functionality

9 Definition of supply chain and retail distribution to consumer

Requirements will be established to ensure that product designers consider the security and privacy implications of supply chains and retail distribution channels including

- Supply chain security and privacy implications for any hardware or software components utilized within the product design
- Channel distribution security and privacy implications for product distribution and sale post manufacturing

10 Understanding consumers

This is a vital section of the proposed standard derived from the safety by design standard ISO 10377. It is required to ensure that designers create products that are both legal (as per section 6 above) and just as importantly that products are practical to use with respect to security and privacy protection.

The standard will require designers to undertake descriptions of consumer use scenarios as use cases, and such cases should include intended uses, and other use identified either during the initial design phrase or subsequently as a result of market monitoring of the launched product. The other use cases will include:

- unintended use cases
- misuse cases
- malicious use cases

Further to ensure better consumer understanding the standard will require the consumer types and characteristics relevant to each use case to be documented to enable unintended use to be considered as, for example, should children use a product intended for adults like online shopping.

In addition to focus designers on what is practical for consumers the digital capabilities, and limitations to those capabilities, needed for product security and privacy will be required to be identified by the designers.

Similarly the consumers' human vulnerabilities which product privacy by design should take into account will be required to be identified by the designers.

11 Detailed use cases

Designers will be required to document as a minimum for each use case

- Data flows and processing descriptions utilizing good practices where appropriate from ISO/IEC 19944 Data flows across devices and cloud services.

- Detailed user interactions
- Types of personal data processed and where in the product's modules that would be processed
- The security and privacy preference controls applicable to each use case
- The security and privacy risks to be addressed by the design

12 Consumer requirements setting

From the use cases the designers will be required to list the consumer privacy needs that the design should address. An informative annex providing the COPOLCO list of privacy needs will be provided to assist with this this requirement.

From the list of privacy needs the design process will require detailed design requirements to be set for the product development work. These detailed requirements will include the user security and privacy preference controls to be developed.

13 Establishing the security requirements for the product

Initial design should establish what consumer hardware and software is to be developed and the standard will require the identification of the security requirements for those elements of the product. This section should build on the ISO standard ISO/IEC 19678 BIOS protection as well as any other technology oriented security standards

Further the means of communication with any application software located outside the consumer environment will have been identified in use cases and the security requirements for both the communications and remote application software will be required to be identified. For the application software processed on an organization's own infrastructure ISO/IEC 27034 Application Security is expected to contribute significantly to the proposed standard.

14 Interworking with 3rd party products

The types of 3rd party products with which the product must interwork will be identified as well as specific products and their design levels where that is relevant to the products detailed design.
Then the specific security and privacy control capabilities of those 3rd party products to be used in the product design will be required to be identified by the designer.

15 Product technology vulnerabilities

To enable designers to take account of the inherent vulnerabilities to attack that are present in common technology solutions, the technologies to be used in the design, such as RFID, WiFi, optical cables, mobile phones and their operating systems, cloud services etc. will be required to be identified.

Then the known technological vulnerabilities of those technologies will be required to be identified.

16 Product design tools and support

The standard will address the design practices where these can now be helped by many forms of design tools and good practice guides. So a key part of the design process is to establish:

- sources of design rules,
- design tools
- design good practices

and ensure the standard includes requirements for assessing these support aids are of the right quality and fit for the roles they are expected to play in assisting the design process.

17 Product development testing

The standard will include process requirements for setting test requirements for hardware and software and the final product.

18 Privacy impact assessment

The standard will include privacy impact assessment requirements that build on both current ISO JTC 1 PIA standards work including ISO/IEC 29134, which is more organization centric, and the EU's EN 16571 RFID PIA standard which is more consumer device centric.

19 Product design release

This section will build on the relevant parts of the ISO Safety by Design standard ISO 10377

20 Product incident response plans and incident investigation

Key elements of this section are expected to be built on ISO/IEC 27043 Incident investigation which includes planning for when it is necessary to respond to incidents.

21 Product manufacture / system commissioning privacy reviews

In this section in addition to building on and adapting relevant sections of the Safety by Design standard ISO 10377, there are also sections of the European RFID PIA standard EN 16571 which deal with aspects of practical privacy assessment of system commissioning especially when a system is being enhanced in such a way that new equipment and software has to be added to infrastructure that is at much older design levels.

22 Retail channels privacy reviews

There are privacy implications to how retail channels are involved in getting products to consumers as originally highlighted in the European RFID PIA standard EN 16571 and this section will need to build on that as well as good practice such as that identified by OFCOM in the UK for retail sources of apps.

23 Consumer notifications, labels, signs and consen

Product information for consumers is a key element of privacy by design and ISO/IEC Guide 14 with enhancement for privacy information from, for example, ISO/IEC 29134 PIA standard and the European RFID Signage and Labelling standard EN 16570.

24 Regulatory information

At a minimum this section should contain good practice requirements for the product privacy impact assessment information to be provided to regulators

25 Active market monitoring

Requirements will be established for reporting of privacy / security incidents, investigations, complaints and concerns from professional bodies and the public.
ISO/IEC 29147 Vulnerability Disclosure and ISO/IEC 30111 Vulnerability handling should form the basis for the good practice requirements in this section.

26 Privacy harm action prioritization

This section will provide requirements for establishing clear criteria for action in rectifying product privacy problems and complaints based primarily on the degree of harm that can be experienced by an individual consumer and the number of consumers who would be affected by the issue. The setting of criteria would have to also allow for the impacts on the organization concerned such as brand damage, recompense and security breaches into commercially sensitive corporate data and likely costs of fixing a privacy problem.

27 Remedial action

A key input to the requirements in this section will be ISO 10393 Consumer Product Recall as well as digital good practices for undertaking problem fixing by product design changes, and their validation pre-release, as well as the use of consumer notifications.

Also to be included will be good practice requirements for sales and support channel actions, regulatory notifications, product recall, and product withdrawal.

28 Online software updates

This section will build on the consumer needs for ease of online software update and more detailed requirements identified in the associated ANEC/BSI-CPIN Privacy Guides adopted by COPOLCO.

29 End of life cycle privacy and associated system decommissioning

To address the privacy issues of disposing of consumer hardware and software when the consumer has finished with them requirements will be developed to deal with product disposed as consumer waste, product re-cycling and second hand markets.

Further requirements will be developed to address the issues of data protection when organizations de-commission systems.